FEATURES:

THE BIG PICTURE

Tools now can sort through “Big Data,” so security pros can connect the dots, says Preston Wood, CSO, Zions Bancorporation P20

Plugging in privacy
Ontario’s privacy commissioner is ensuring that electricity firms protect data as they roll out smart grid technology PC1

The next Cold War
Instead of military assaults, today’s adversaries hire coders to create attacks that can run for years P30
Ranked #1 in Server Security* yet again.

As businesses continue their journey to the cloud, analysts and security experts agree that risk management practices must change. Trend Micro leads the way in protecting businesses against today’s sophisticated cyber attacks by providing real-time, actionable threat intelligence and network-wide visibility and control. With our solutions you gain the certainty that your data is always secure across all environments—physical, virtual and cloud.

trendmicro.com/journey

Scan to download
IDC Analyst Connection: Server Security
for Today’s Datacenters

* IDC Worldwide Endpoints Security 2011-2015 Forecast and 2011 Vendor Shares 49-52 Trend Micro Inc. All rights reserved. "Trend Micro" and the Trident logo are trademarks or registered trademarks of Trend Micro, Inc.

4 Editorial: Evolutionary conundrums
8 Threat report The personal information of city council members in Belfast was exposed
10 Threat stats The biggest increase in zombie activity was in Vietnam
12 Update The investigation into fraudulent robocalls in Canada escalated, as the nation’s election agency said 7,000 calls had gone out to voters
13 Debate Is anti-virus necessary?
14 Two minutes on... A new way to net phish
15 Skills in demand The demand for cloud and virtualization security architects is growing rapidly.
16 From the CSO’s desk PCI: Five years older and wiser, by Mike Mitchell, American Express
17 Opinion Smart network management, by Ken Sanfratoli, Pem盛典
18 Letters From the online mailbox
19 Calendar A guide to upcoming IT security courses, shows and events
20 Last word David can be Goliath, by Michael Potters, The Glenmont Group

Regulars

Product Reviews

33 Product section This month, we look at security information and event management (SIEM) tools, an area that has been morphing for several years now.
34 Group Test: SIEM SIEM tools do a lot of things, but at the core they take data from sources and produce useful, actionable information.
48 First Look: FTK 4.0 A new iteration updates a standard to a new level of functionality by adding the optional Cerberus (malware forensic analysis) and Visualization (files and email) modules.

Features

20 The big picture Tools are available that can sort through massive amounts of “Big Data,” so security pros can connect the dots.
21 Plugging in privacy Ontario’s privacy commissioner is ensuring that electricity firms protect data as they roll out smart grid technology.
24 SC Roundtable: Government For government security professionals, focusing on priorities is key in these trying economic times.
26 The global landscape It has been difficult for law enforcement to pursue electronic crimes across international boundaries, but efforts are underway for further cooperation.
30 The new Cold War Instead of military assaults, today’s adversaries hire coders to create attacks that can run autonomously for years.

Cover photo by Bob Adler

AccessData FTK 4.0 P49

McAfee ESM P39

SC Magazine™ (ISSN No. 1096-7974) is published 12 times a year on a monthly basis by Haymarket Media Inc., 114 West 26th Street, 4th Floor, New York, NY 10001 U.S.A.; phone 646-638-6000; fax 646-638-6110. The postmaster: Send address changes to SC Magazine, P.O. Box 316, Congers, NY 10920-0316. © 2012 by Haymarket Media Inc. All rights reserved. Annual subscription rates: United States: $98; Canada and Mexico: $110; other foreign distribution: $208 (air service). Two-year subscription: United States: $175; Canada and Mexico: $195; other foreign distribution: $375 (air service). Printed in the United States. Office of publication: 225 Liberty Street, New York, NY 10281. Postmaster: Return undeliverable mail to SC Magazine, P.O. Box 316, Congers, NY 10920-0316. The information in this magazine is intended for general reference only and may not be relied upon for any specific purpose without the advice of an attorney, accountant or other professiona...
This year’s RSA Conference seemed a bit more energized than in recent years. The floor was bustling. Meetings seemed fruitful for many. Press conferences and vendor parties were happening everywhere you looked. And our own SC Awards U.S. Gala was packed.

As I await final official attendee numbers from conference organizers, it was clear that thousands of information security pros turned out (unofficial, pre-audit numbers said more than 21,000 people attended compared to 18,500 the previous year, according to one RSA Conference staffer). All the major vendors were on site, as were government officials, executive leaders, analysts, consultants and more.

To many, it seemed as if larger crowds were hitting classes and were more engaged with speakers and the information presented. As well, questions being bandied about on the show floor were more detailed—attendees really wanted to hear from vendors how their solutions worked and in what ways these offerings actually might help them.

This is an interesting observation and sort of reflects one that was voiced in an online editorial webcast we held mid-March. During that event, “Evolve and Survive,” Gene Fredriksen, CISO of Tyco International, said there were a whole host of things driving budget, resources and tweaks to security/risk management programs. Some of these include regulatory mandates, pernicious attacks, like APT, and certainly the success of many of today’s infrastructure assaults. Just as many pros believe, he warned that companies and government entities likely already have malcontents roaming their networks, which has brought into existence two groups of exes: those who have been breached and those who have no clue.

Now, what is not driving budgets is the fear, uncertainty and doubt (FUD) argument. Fredriksen said that even if some less farsighted practitioners are relying on such methods, more knowledgeable C-level cats just aren’t buying. FUD simply doesn’t fly any longer. Strategic moves made to safeguard critical data and harden systems, as opposed to sometimes haphazard tactical ones, are what is necessary for the long-run success of any business and government agency. And so, too, are traits like agility and vision.

Fredriksen said to move methodically and quickly is a necessity these days. Failing that, organizations, their leaders and, most assuredly, their CISOs/CSOs will simply transform into today’s dinosaurs. And, well, we all know what happened to those guys.

Ilenna Armstrong is VP, editorial director of SC Magazine.

“Fear, uncertainty and doubt simply doesn’t fly any longer.”
WHAT IS SCWC 24/7? SC Magazine has created a free virtual environment that is open year-round. Each month we host an event on a subject that you as an IT security professional face on a regular basis.

THIS MONTH

SC WORLD CONGRESS eSymposium
April 24
eSymposium: Cyber espionage
Those engaging in cyber espionage to steal various classified and/or proprietary documents from U.S. agencies and other organizations are riding high. The theft of this critical information shows that attackers are exploiting whatever weaknesses in systems they can to siphon corporate and government data, often going unnoticed for months. Experts share background on the types of attacks to watch out for and what you can do to thwart them.

ON DEMAND

PCI compliance Unlike other rules mandating technology usage, the PCI Data Security Standard is far more specific and not open to “user interpretation.” But, when it comes to implementing precautions, such as those outlined in PCI DSS, many companies talk because they fear the added costs. Experts provide some pointers on how they are reaching a PCI-compliant state, and staying within budget.

Mobile security To safeguard handhelds used by business execs is a constant trial – one that rarely is satisfactorily remedied. But companies must find a way to manage and protect these endpoints. We offer solutions.

FOR MORE INFO

For information on SCWC 24/7 events, contact Natasha Mulla at natasha.mulla@haymarketmedia.com. For sponsorship opportunities, contact Mike Alessie at mike.alessie@haymarketmedia.com. Or visit www.scmagazine.com/scwc247.

Rich Baich, principal, security & privacy, Deloitte & Touche
Greg Ball, global information protection and security lead partner, KPMG
Christopher Burgess, chief security officer and president, public sector, Alaris
Jaime Chanagna, managing director, CSO Board Consulting
Rufus Connell, research director - information technology, Frost & Sullivan
Dave Cuillinnane, chief information security officer, Elsevier
Mary Ann Davidson, chief security officer, Oracle
Dennis Devlin, assistant vice president of information security and compliance services, George Washington University
Gerhard Eschelbeck, chief technology officer and senior vice president, Sophos
Gene Fredriksen, senior director, corporate information security officer, Tyco International
Maurice Hampton, technical account manager, Qualys
Paul Kurtz, partner and chief operating officer, Good Harbor Consulting
Kris Lovejoy, vice president of IT risk, office of the CIO, IBM
Tim Mathew, director, information protection, KPMG
Stephan Northcutt, president, SANS Technology Institute
Randy Sanovic, former general director, Information Security, General Motors
Howard Schmidt, cyber security coordinator, White House, president and chief executive officer, Information Security Forum
Ariel Silvestre, former chief information security officer, Expedia
Justin Somaid, chief information security officer, Yahoo
Craig Spiezio, chairman, Online Trust Alliance; former director, online safety technologies, Microsoft
W. Hord Tipton, executive director, (ESCI)* former CIO, U.S. Department of the Interior
Amit Yoran, chief executive officer, NetWitness; former director, U.S. Department of Homeland Security’s National Cyber Security Division

The always-on resource for IT professionals As a complement to our annual SC Congress Conference and Expo events, SC Magazine has launched a permanent website environment that will be open to our readers around the clock all year long. Each month we host an event on the site focused around a pertinent subject that you as an IT security pro face on a regular basis. This is a completely FREE offering to keep you informed of the newest developments in the industry. Participants can earn up to eight CPE credits for an eConference & Expo, and two CPE credits for a Virtual Symposium.

Join us for our next virtual events

April 24 – Cyber espionage: Hacktivist groups have made it clear that no computer network are immune from penetration. Perhaps today’s top challenge facing senior IT personnel is to get the C-suite to sign off on implementing a 24/7 security system before the enterprise suffers a breach.

May 17 – Advanced monitoring and forensics: Hacktivist groups have made it clear that no computer network are immune from penetration. Perhaps today’s top challenge facing senior IT personnel is to get the C-suite to sign off on implementing a 24/7 security system before the enterprise suffers a breach.

For a complete schedule and to register, visit our 24/7 site: scmagazine.com/scwc247

SC WORLD CONGRESS eConference
May 24
eConference: Privacy and security
July 6
cConference: Auditing and compliance
July 24
cConference: Database security
Aug. 23
eConference: Securing the cloud
Sept 6
eSymposium: Mobile security
Sept. 18
cConference: Data security

SALES
Mike Alessie National accounts manager (646) 638-6002 mike.alessie@haymarketmedia.com

EVENTS
Anthony Curry Senior events coordinator (646) 638-6009 anthony.curry@haymarketmedia.com

SC WORLD CONGRESS
Upcoming events
May 24 eSymposium: Privacy and security
July 6 cConference: Auditing and compliance
July 24 cConference: Database security
Aug. 23 eConference: Securing the cloud
Sept. 6 eSymposium: Mobile security
Sept. 18 cConference: Data security
Oct. 9 eSymposium: Advanced persistent threats
Nov. 15 eSymposium: Vulnerability management

For more information
Netherlands top producer of zombie IP addresses
During the past month, the EMEA region (Europe, the Middle East and Africa) was the leading source of all zombie IP addresses. Of the countries making up the EMEA region, the Netherlands was the top producing country. For the other regions, the top producers were Uruguay in South America, the United States in North America and India in the Asia-Pacific region.

Source: Symantec
The biggest increases in month-over-month zombie activity occurred in Vietnam.
Hacker snitch

Following his arrest in June for a number of high-profile attacks, Hector Monsegur, a.k.a Sabu, continued to urge on his fellow hacktivists...while apparently in cahoots with the FBI to rat them out. When he was picked up by authorities, Monsegur was helping to lead LulZSec, an offshoot of Anonymous. According to the FBI, his statements helped law enforcement charge five other people with roles in hacks.

It’s absolutely outrageous,” said Maynard. “It should not be tolerated. It should be sanctioned severely.”

Maynard was called to testify to a parliamentary committee about the matter, but many Canadian media were involved in a lock-up interview with Finance Minister Jim Flaherty, who was announcing the Canadian budget.

Canada’s CBC found in an investigation this month that many voters who had received robocalls had previously been contacted by the Conservative Party and had told it that they would not be voting for it.

Some claim to have received misleading calls attempting to redirect them to incorrect voting locations, which they then tracked to Conservative Party offices.

Prime Minister Stephen Harper continues to deny Conservative Party involvement in the robocalls affair.

Malware is no imaginary problem, especially on Windows PCs. Anti-virus labs see tens and even hundreds of thousands of new samples daily, and infections are all too common. It’s better to ask, are there instances where anti-virus is not necessary? Perhaps. For instance, if your system can’t trade data or applications with other systems; it runs an operating system for which there has been no malware for a very long time, and no other vulnerabilities.

For instance, there’s no known malware for Windows XP, or Windows Server 2003, and it’s never been attacked.

Let’s make one thing clear: It’s not a question of using anti-virus software or not; it’s a question of how much should be spent on it.

As Gartner reports, consumers will spend nearly $5 billion this year on AV software. This is far too much money for something with such a poor track record, and one the bad guys evade almost at will.

It is far too much, especially when free alternatives, like Microsoft Security Essentials, give consumers the bulk of what they need and allows them to spend money on things that actually protect their data.

Computers crash, people get hacked, bad guys steal personal data...victims suffer the consequences with or without AV software.

Consumers, and businesses too, must not view AV as a primary defense. A better way for consumers to protect themselves is to take three steps that will save them money and protect their digital assets:

First, install “free” AV software. Next, invest in a good backup solution. And finally, upgrade the web browser.

THE SC MAGAZINE POLL

Does Anonymous pose a threat to the U.S. power grid?

60.44% No. Anonymous’ mission is politically motivated.

39.56% Yes, the group is becoming more capable, disruptive and destructive.

To take our latest weekly poll, visit www.scmagazine.com

THE STATS

$46m a year is the average spent on computer security by 21 energy companies surveyed by Bloomberg

69% of known cyber strikes against their systems are thwarted by the utility companies polled

Source: Bloomberg Government/Ponemon Institute, Feb. 2012

Should I be worried?

This attack vector is working throughout Europe. The bug removes the original Explorer.exe file, but doesn’t target data. Recovery is possible by restoring the original Explorer.exe file via the command line and deleting the malware executable.

How can I prevent it?

Awareness goes a long way. Plus, performing regular backups will limit the impact if data is targeted.

Source: Donald DeBard, director of threat research, TotalDefense
A new way to net phish

S
ome 300 billion emails circulate each day, but they still can’t escape a fundamental flaw – that users who receive these messages can’t be certain who sent them. This underlying weakness has led to phishing and spam being persistent threats on the web for many years. But the age-old quest for accountability in digital communication has a new champion: Domain-Based Message Authentication, Reporting and Conformance (DMARC), a new specification whose creators hope soon will be adopted by the Internet Engineering Task Force (IETF).

DMARC has a few things working in its favor that past authentication attempts didn’t. For one, it is not a standalone protocol, but one that works in concert with popular security methods already adopted: DomainKeys Identified Mail (DKIM), a technique that associates a domain name to an email message, and Sender Policy Framework (SPF), which detects spoofing.

“DMARC standardizes how email receivers perform email authentication using the well-known SPF and DKIM mechanisms,” according to the group. “This means that senders will experience consistent authentication results for their messages at AOL, Gmail, Hotmail, Yahoo and any other email receiver implementing DMARC.”

Second, DMARC has some muscle behind it. Not only are the major email providers behind the system, but so are some of the most digitally abused brands, such as PayPal. And third, DMARC gets away from the traditional approach of blacklisting.

“DMARC gives us an ability not just to guess if that message is good or bad, but to actually know whether it came from a legitimate organization,” said Patrick Peterson, founding member of DMARC, and CEO of email security firm Agari. DMARC uses DKIM and SPF to vet, at the domain level, the trustworthiness of emails. Email providers can then, through their own policy and through user preferences, get as granular as they wish. That may mean simply monitoring unauthenticated messages all the way to outright blocking them.

The specification also allows senders to publicize their email handling practices, while receivers can offer feedback.

Critics of DMARC argue that as long as people are involved in the process, users still will fall for phishing and spam. “Humans don’t work the way technology works, they work the way humans work,” said Joseph Steinberg, CEO at Green Armor Solutions, an authentication vendor. – Marcus Colón

72% of all inbound email is spam

Source: MBG Security Labs

JOBS MARKET
Me and my job

Douglas Vitale
Information assurance and forensic expert for a major utility company

How do you describe your job to average people?
My main responsibilities are computer forensics and litigation support. On the forensic side, I assist our investigators by collecting electronic data from hard drives, servers and email to find evidence they can use in their investigation. On the litigation side, I am responsible for collecting electronically stored information (ESI) for individuals involved in lawsuits. This is done by collecting the ESI from hard drives, servers and email, and processing the data so our legal team can review and produce the relevant files.

Why did you get into IT security?
With a bachelor’s degree in criminal justice, my background is in investigations and physical security, but I’ve always had a passion for computers, so I wanted to find a way to integrate both. I went back to school for my master’s in computer science and while in school began searching for a career that I would enjoy and be able to integrate with my knowledge and experience. Once I found out about computer forensics, I knew that was the field I wanted to go into after I graduated. I was fortunate enough to find a forensic position immediately after graduation.

What was one of your biggest challenges?
One of the biggest challenges I’m constantly faced with is the new technologies that are introduced on a daily basis. As a computer investigator, I need to stay ahead and be knowledgeable of what is coming out.

What keeps you up at night?
Unlike other fields, computer forensics/litigation support is a new and evolving field. Every day, I spend an hour or more reading blogs and forums to familiarize myself with the new advancements in computer hardware and software. I also stay abreast of recent court opinions and case studies to see how the legal side of computer forensics/litigation support is progressing.

Skills in demand
As more organizations move into the cloud, the demand for virtualization security architects is growing. Vendors want to drive offerings, services firms need customer-facing solutions architects, and end-users need help with strategy and migration.

What it takes
Experience and knowledge of SaaS development, multi-tiered application environments, database, virtualization platforms, ID management and authentication, and regulatory requirements are needed.

Compensation
Base compensation ranges from $130k to $200k, plus incentives.

Tom Kellerman’s Top 10 Skills
• Anti-virus firm Trend Micro has hired Tom Kellerman as its first-ever U.S. vice president of cyber security. Kellerman, the former chief technology expert of wireless security provider AirPatrol and vice president of security awareness at Core Security, will act as an advisor to government customers. In addition, Kellerman is a member of the Commission on Cybersecurity for the 44th President, which aims to guide federal policy making. www.trendmicro.com
• Vormetric, provider of encryption and key management for enterprise systems, has appointed Tina Stewart vice president of marketing. She will oversee the company’s global marketing activities and will report directly to company CEO, Richard Gorman. Previously Stewart held marketing, branding and communication roles at Juniper Networks, Arbor Networks and Network Associations, which since has been acquired by McAfee. www.vormetric.com
• CrowdStrike, a company created to help organizations protect intellectual property and national security information, has launched. Co-founded by George Kurtz, the former CTO of McAfee, CrowdStrike will focus on determining who is behind attacks, which it believes is the most critical piece in protecting assets. Dmitri Alperovitch and Gregg Marston are the other founders. www.crowdstrike.com

Follow us on Facebook and Twitter

S
A new way to net phish

72% of all inbound email is spam

Source: MBG Security Labs

DMARC and CEO of email security firm Agari. DMARC uses DKIM and SPF to vet, at the domain level, the trustworthiness of emails. Email providers can then, through their own policy and through user preferences, get as granular as they wish. That may mean simply monitoring unauthenticated messages all the way to outright blocking them.

The specification also allows senders to publicize their email handling practices, while receivers can offer feedback.

Critics of DMARC argue that as long as people are involved in the process, users still will fall for phishing and spam. “Humans don’t work the way technology works, they work the way humans work,” said Joseph Steinberg, CEO at Green Armor Solutions, an authentication vendor. – Marcus Colón

72% of all inbound email is spam

Source: MBG Security Labs

DMARC and CEO of email security firm Agari. DMARC uses DKIM and SPF to vet, at the domain level, the trustworthiness of emails. Email providers can then, through their own policy and through user preferences, get as granular as they wish. That may mean simply monitoring unauthenticated messages all the way to outright blocking them.

The specification also allows senders to publicize their email handling practices, while receivers can offer feedback.

Critics of DMARC argue that as long as people are involved in the process, users still will fall for phishing and spam. “Humans don’t work the way technology works, they work the way humans work,” said Joseph Steinberg, CEO at Green Armor Solutions, an authentication vendor. – Marcus Colón
PCI: Five years older and wiser

Mike Mitchell
VP, global network operations, American Express

O
ver the past few years, adoption of and compliance with PCI standards has made it more challenging for criminals to steal large volumes of credit card data. Some of the improvements in the evolution of the standards, like log monitoring and other steps—a result of industry feedback and involvement in standards development—have increased the likelihood that an organization can identify anomalies indicative of breaches, and hopefully stop them before the criminals absorb with payment data.

So, where do we take it from here? Our mission at the council remains the same: protecting cardholder data must be at the center of our efforts. The PCI standards offer the best protection of payment card data across all payment channels. We must continue to increase awareness, and provide the education and resources for security and business professionals alike to secure their organizations’ data.

At the council, we are going to apply continued focus on understanding technologies that offer Payment Card Industry Data Security Standard (PCI DSS) scope reduction for merchants, including point-to-point encryption (P2PE) and tokenization. While there’s no silver bullet, we believe that through these technologies we can make it simpler, faster and more efficient for smaller merchants to adopt the PCI standards.

We will continue to engage all PCI stakeholders with new opportunities for participation, and provide a dedicated period for collecting and sharing feedback. This, in turn, will not only result in additional supplementary guidance, but also in strong revisions to the next iteration of the PCI standards, to be released in 2013. We believe that through this feedback loop we are gathering the input of the widest collection of payment and security experts around the world in an effort to reduce payment card fraud.

Since people and processes are a critical part of a successful security mix, the council is expanding the current Payment Card Industry Security Standards Council training offerings to continue to increase payment card security expertise. Additionally, we’ve incorporated awareness training so that all can better understand what PCI is about and how it applies to their role in protecting payment card data.

But we need your feedback to help us grow our knowledge base, keep up with and mitigate the latest attacks, and adopt the newest technologies safely and securely. I used to have a boss that periodically asked me a particular question, which I now turn to you to share: “What have you done for payment security lately?”

From the CSO’s desk

Shutting access to passwords

Mike Barr Photography

M
obile devices free us from being tied to an office computer when accessing personal information: web logins, passwords, PINs, account numbers, etc. Imagine a mobile device falling into the wrong hands—resulting in the draining of bank accounts co-opting of identities.

A lost or stolen phone constitutes a serious security threat because the attacker has unlimited time to gain access to its data. Therefore, important personal information should not be stored in any unsecured application. Instead, critical data should be stored in a digital wallet or password manager with strong encryption—such as 256-bit Blowfish—to keep these assets safe, secure and accessible.

Front-door attacks occur when a hacker continually attempts to guess a password. A good password manager closes this front door with a self-destruct feature that can wipe data after a number of password-entry attempts. Further, an auto-lock feature will automatically lock the application in instances where users set the device down for a moment and it disappears.

Alternatively, backdoor attacks occur when a hacker has cracked the device and can access the password manager’s database. Here too a strong password manager will help as it will encrypt personal data with a strong algorithm, and never store the password itself on the device. Assuming a strong password is used, this approach would take years for even a super computer to try every possible combination.

Finally, transmission attacks take place when data is captured during broadcast, such as during data sync activity. A solid password manager will have a sync architecture that encrypts the data with a separate, strong password before it is transmitted or stored on a cloud server.

A password manager should serve as an impenetrable lock to block front or backdoor access to your most sensitive data.

Smart network management

Mike Barr Photography

A
s IT security staff contend with the threat from cyber crime and fast-spreading malware, they consistently look for technologies to give them comprehensive network security. Implementing a network monitoring solution provides IT staff with advance warning about threats, as well as visibility into bandwidth issues that can signal security risks and point out hardware deficiencies.

Network monitoring solutions for the enterprise should be holistically integrated with the complete security suite, including various port scanners, virus monitors and encryption software that are already in place. Monitoring can identify unusual peaks in usage, which can be a sign of a threat or an indication that another part of the system is pulling too many resources and should be scanned for infection.

Without instant notification of a threat, IT admins are not able to react in enough time to limit or prevent the leakage of data or interruption of services. Enhanced visibility allows staff to better analyze and fix security gaps to prevent future problems.

The most sophisticated monitoring tool is useless if it cannot quickly alert IT staff to the existence of a security threat. Network managers need a solution that uses multiple notification technologies beyond email or SMS, including notifications to mobile devices, simple network management protocol (SNMP) traps and alarm sound files. Alerts should be segmented into logical categories, such as notices for escalations, multiple conditions, thresholds and limit warnings where usage is above/below a certain value.

Solutions that offer robust reporting will be able to provide information on requests, up and downtime percentages, the top bandwidth users and top ping times, among many other data points. By using the monitoring solution as a source of real-time reporting, IT security management can plan infrastructure updates and reduce network costs.

30 seconds on... 

» Keep on pushing
We have to keep pushing adoption of PCI DSS across the payment chain, and encourage further adoption among smaller merchants and franchise organizations, says Mitchell.

» All must get involved
When he says “we,” he means all possible parties along the payment chain—acquiring banks, technology vendors, security assessors, merchants and industry associations.

» Overcome one exports
Further, he says, efforts must be doubled so threats don’t continue to move down the chain, leaving mom-and-pop shops an easy target for an antiquated exploit.

» For further information

[Image 588x264 to 678x362]

[Image 588x645 to 679x740]
Got something to say?

Send your comments, praise or criticisms to scfeedbackUS@haymarketmedia.com. We reserve the right to edit letters.

From the online mailbag
In response Executive Editor Dan Kaplan’s January cover story, The new wave: Modern security education. I was delighted to read your article. “The new wave: Modern security education.” There is a growing gap between cyber security professionals’ availability and our national need. I’d like to share some of our observations regarding the value and future of cyber competitions to help mitigate this shortage.

Here at the Center for Infrastructure Assurance and Security, where the inaugural CCDC contest was organized in 2005, competitions are articulated as one of the three legs on which strengthening America’s cyber security depends, along with state and community exercises, and professional education and certification.

We encourage competitive programs from high school students on up because they have proven to uniquely encourage skills set vital to their professional prospects: teamwork, creative thinking and communication skills. Events like DC3 Digital Forensic Challenge, CyberPatrol, and soon, the National Cyber League, will be available to encourage thousands more. Our Panoply program, which stresses both assessment and defensive skills, is preparing an online competition: online team cyber sports allow for more students from remote or economically disadvantaged areas to participate.

So far, more than 3,500 students have participated just in CCDC events since its inception, including Alex Levinson. As your article points out, CCDC proved to be his gateway to a RIT team that competed in the CCDC last year — like many other CCDC competitors, one season was not enough for Alex.

There’s very exciting work being done here at CIAS and our University of Texas at San Antonio. Thank you, again, for the excellent article; but more, for the attention you and SC Magazine focus on security issues and the manner they are articulated.

Dwayne Williams
director, NCDC
In response to Executive Editor Dan Kaplan’s February cover story, Adjoining islands:
I just wanted to let you know that I thought you did a great job on the article. It is obvious that you knew what you were reporting. It is not that often you find someone who understands what they are writing about, and this is a complex subject. Thanks again for the opportunity.

Gordon Bruce
director, information technology, city of Honolulu
In response to our Data Breach Blog:
I follow the Data Breach Blog at your publication regularly. I find it a very concise tool for getting the point across to management. So many organizations want to put their head in the sand about security, and this blog shows them that breaches are in fact common, that companies do report breaches, even “minor” ones, and that it is not usually the end of the world when a company does report an incident.

Chris Close
IT operations manager, Western Dental Services
In response to a news item on February 21, Anonymous says power grid concerns are U.S. government spin:
Notably Jane Mayer just won a Polk Award for her exposé in the New Yorker on corruption at the NSA. These lies are par for the course for an organization that is more about depriving you of your tax money and privacy than protecting Americans. We have our own Republican Guard.

Jeff
In response to a March Opinion piece on the website, Never fully down when malware infects the weekend, by Ross Kindler, senior security researcher, Dell SecureWorks:
I have had countless systems on my kitchen table with the same problems. One trick that always seems to work: Create a new user and do all of your work from there. And last but not least, boot into the infected user and make sure the profile is clean. All in all, it’s a solid four hours of fun.

Pnarsh
The opinions expressed in these letters are not necessarily those of SC Magazine.
Tools are now available that can sort through massive amounts of “Big Data,” so security pros can better connect the dots, says Preston Wood, CSO of Zions Bancorporation. Dan Kaplan investigates.

Consumer behavior often is influenced by slick marketing tactics, like jingles that may make you want to pull your hair out. Case in point: If you’ve recently walked into a Subway to order a sandwich – and haven’t thought about five dollars and footlongs – you probably don’t own a television.

Well, the latest craze in information security doesn’t have an indelible tune to go along with it – at least not yet – but it does have a memorable, sexy-sounding name: “Big Data.” And as a result, everyone is talking about how organizations are aggregating, searching and analyzing voluminous information sets to make intelligent business decisions that may have been impossible to reach in the past.

“It’s a great phrase that has captured the imagination,” says Andrew Jaquith, chief technology officer of Perimeter E-Security, a managed security services provider based in Connecticut.

But for Preston Wood, the chief security officer at Zions Bancorporation, the parent company of some 550 bank branches in the western United States, the concept of Big Data isn’t anything new, only that there is a buzzword now to describe what Zions has been doing for more than a decade. In the late 1990s, the corporation began recognizing the enormous business value that could be generated from aggregating disparate data sets and drawing connections to glean actionable insight.

The company was an early adopter of security information and event management (SIEM) technology to make sense of its data sources. Some consider Big Data to be the next generation of SIEM.

“We had a Big Data strategy before Big Data was Big Data,” Wood, 40, recalls. “We thought, ‘How great would it be to take a lot of this unstructured data we have – that we are retaining for various reasons – and put it into a form factor to be able to analyze and mine that data to make better security decisions?’ You’d be able to start some fascinating analytics. You’d be able to ask questions of that data that you weren’t able to do in the past.”

If Zions thought it was dealing with large amounts of data that needed processing at the end of the 20th century, imagine what the number is like now. Data is growing at astonishing rates across all industries. According to IDC, the amount of information created and replicated in 2011 exceeded 1.8 zettabytes – yes, zettabytes – a nine-factor increase in just five years.

Each day, the world creates 2.5 quintillion bytes of data, according to IBM, meaning some 90 percent of the information alive today was only born within the last two years. Each sector in the U.S. economy is responsible for at least 200 terabytes of stored data, says a report from the McKinsey Global Institute.
This breathtaking amount of data being created, managed and stored – both structured and unstructured – is real, and many organizations are racing to dissect it. The vendor community also is charging full speed at the new opportunity. According to Thomson Reuters data, venture capitalists invested $3.5 billion last year into Big Data technologies. Perhaps no two verticals deal with security and Big Data more than the information-intensive industries of financial services and health care, says Sean Martin, founder of Imsmartin Consulting, who formerly held marketing roles at several security firms.

For instance, a recent panel at the O’Reilly Strata Conference examined how Big Data may help financial organizations proactively spot the next crisis. In addition, if new regulations are introduced as a result of prior events, data analysis may yield some fresh ideas of how to cope with them. When it comes to health care, meanwhile, some, such as Craig Mundie, Microsoft’s chief strategy and marketing officer, believe Big Data can help reign in soaring costs related to patient treatment. Mundie says when data is shared openly – assuming HIPAA requirements are met – providers can better identify areas that are causing higher-than-desired costs, Mundie reportedly told attendees last fall at the Technology 2011 conference. It makes sense that models like this will be explored, Martin says, considering that a Centers for Medicare and Medicaid Services report predicts that health care costs will rise from $2.6 trillion to 4.6 trillion during this decade.

Making sense of it all

To understand how Big Data came to be, it might be wise to examine the evolution of Google’s flagship product, its search engine. Some may credit the Web giant’s meteoric rise to dominance with its intuitiveness and clean interface, but what really made Google special was the superiority of its search algorithm to produce speed and relevance. Remember the early versions of AltaVista? Or Excite? They paled in comparison.

“It’s so damn fast and it’s so insightful that you take it for granted,” Jaqui’s says of Google. That had everything to do with Big Data, he says. Google developed a new way to do search by relying on non-relational databases and its home-grown MapReduce framework, which permitted the company to process queries against a massive number of distributed nodes. So instead of using conventional relational databases, Google was able to better scale and, in turn, instantaneously produce pertinent results.

“Big Data is just like the natural evolution of the fact that networks have gotten faster, bigger and servers can hold more things,” says John Kindervag, principal analyst at Forrester Research. “You just naturally want to put everything in it. If you have a big closet, by nature, you throw all your crap in the closet and sort through it when you want to. Once you have data, you can rule the world. Ask [Facebook founder] Mark Zuckerberg.”

Zions, in a way, is a microcosm of a Google or Facebook. Wood says that at the 30th largest bank in the United States, which counts nearly 11,000 people as employees and $50 billion in assets, applying a Big Data approach within his department is critical because security data is “different than the traditional data warehousing space.”

He says security assets are mostly unstructured and include things like firewalls/anti-virus logs, packet captures, web log activity across internet banking and treasury management platforms, and login behavior on internal systems. But aggregating and analyzing that type of information wouldn’t fly in Zions’ traditional database management systems. After it outgrew the SIEM technology, Wood says Zions needed to develop a more robust way to process data from its 130 different sources if it were ever going to draw any real, timely value. “Say you wanted to run a query across more than 1,500,000 pieces of content shared each month on Facebook

BIG DATA: The three Vs

Volume – Big Data comes in one size: large. Enterprises are awash with data, easily amassing terabytes and even petabytes of information.

Velocity – Oftentimes, sensitive Big Data must be used as it is streaming in to the enterprise in order to maximize its value to the business.

Variety – Big Data extends beyond structured data, including unstructured data of all varieties: text, audio, video, click streams, log files and more.

Source: IBM

That might be a better pill to swallow for low security professionals, who are well-versed in the sophistication and intentions of today’s cyber criminals, particularly well-funded nation-state adversaries who use low-and-slow techniques, known as advanced persistent threats (APT), to target coveted intellectual property, and then slowly and stealthily siphon out the booty without anyone noticing.

“If I’m a hacker of Anonymous, or part of an APT, you, I’m really excited about the Big Data concept,” Kindervag says. “This is like Christmas to me. I don’t have to steal something from each individual store. I can steal the presents under the tree.”

Implementing proper access controls is important to safeguarding Big Data, he says. But encryption may be the real saving grace because it renders data unreadable. “It’s the only thing that’s going to protect us against these nation-state attacks,” he says. “We’re never going to keep ahead of those guys.”

But Zions, which is sometimes difficult-to-manage technology, organization managers must first define their data by discovering and classifying it. In other words, they need to decipher which are their most “toxic” assets. Then, they can dissect them.

“That’s the exciting stage,” he says. “My fear is they won’t do stage one and they’ll do stage two, and people will steal stuff and they won’t know it because the data hasn’t been classified, and people don’t know how valuable it is.”

That’s not a problem at Zions, Wood says, where the security team has become the corporation’s champion of Big Data.

“We treat this environment as any environment within our organization,” he says. “Whatever security policies and controls you have. Your Big Data repository needs to be looked at in the same light. Every technology has got things that need to be considered about how you secure it. It’s like any new process or application.”
PLUGGING IN PRIVACY

Ontario’s privacy commissioner is ensuring that electricity firms protect data as they roll out smart grid technology, reports Danny Bradbury.

Canada underspent the United States by a third in upgrading its electrical systems to smart grids last year, according to analyst firms Verdantix. But, while it may be spending less overall, it is investing more in customer privacy, thanks to Ann Cavoukian, privacy commissioner for Ontario. She wants to make sure that her province leads the field on safeguarding electrical firms’ customer data.

Cavoukian has advocated her “Privacy by Design” strategy since the 1990s, which advocates that privacy be baked into products and services from the beginning, rather than adding it after the fact. Utilities must play ball too, she says, as they revitalise their power grids.

Smart grids are designed to bring intelligence to electrical distribution systems. These start in the home with smart meters. Not only do the devices monitor energy use in the household, but they can also potentially take instructions, i.e., signalling an appliance what to do. It is more frequently, but they can also potentially leak data from users that could then be used to assemble profiles on them?

“A big part of managing the distribution system appropriately has to do with knowing just where energy and demand are being created in the grid,” says Meyer. “I don’t need to know it’s Danny’s house. I just need to know the location on the grid,” he says. Some residential customers that co-generate their energy are where privacy could be breached if data is aggregated and anonymized by then. “A big part of managing the distribution system appropriately has to do with knowing just where energy and demand are being created in the grid,” says Meyer. “I don’t need to know it’s Danny’s house. I just need to know the location on the grid,” he says. Some residential customers that co-generate their energy will be exceptions to this rule.

The Privacy by Design approach seems relatively watertight and is complemented by provincial laws. But perhaps the biggest potential for privacy breaches in smart grids may not come from an over-aggressive utility, but from security flaws. Some smart meters have been shown to have basic vulnerabilities that could lead them to be compromised.

Mike Davis, a security researcher at U.S. firm IOActive, has presented extensively on smart grid security and has written self-replicating code designed to compromise smart meters.

The customer and services domains are where privacy could be breached if things are handled carelessly. However, Cavoukian’s Privacy by Design principles hardened into the service domain are undeniably well thought out, experts say. And, devices in the customer domain can only be accessed from the services domain via authenticated routes and access is recorded. The customer must authorize such access, and Hydro One built role-based security into the system so that personnel can be given access based on their responsibilities.

At the grid management level, there is little worry about privacy breaches because, with a few exceptions, data is aggregated and anonymized by then. “A big part of managing the distribution system appropriately has to do with knowing just where energy and demand are being created in the grid,” says Meyer. “I don’t need to know it’s Danny’s house. I just need to know the location on the grid,” he says. Some residential customers that co-generate their energy will be exceptions to this rule.

The Privacy by Design approach seems relatively watertight and is complemented by provincial laws. But perhaps the biggest potential for privacy breaches in smart grids may not come from an over-aggressive utility, but from security flaws. Some smart meters have been shown to have basic vulnerabilities that could lead them to be compromised.

Mike Davis, a security researcher at U.S. firm IOActive, has presented extensively on smart grid security and has written self-replicating code designed to compromise smart meters.

“There are security issues that are going on in these meters,” he says. “It’s like any other internet service. Things are vulnerable.”

Data collected from smart meters does carry potential privacy implications because it can provide insights into how energy spikes in the home. Most generically collect information approximately every 15 minutes. It could be relatively easy, then, to analyse this data and find out when someone was home or not, based on their electrical usage data.

How could that get into the wrong hands? One potential area of leakage is third-party service providers.

“Services such as Google PowerMeter; that’s where the dangers come in,” says Davis. Designed to be used in conjunction with smart meters, PowerMeter was marketed to utilities around the world as a way to provide customers with information on power use, which could be leveraged to help them make better decisions on proper consumption.

Google retired its service in October, but alternatives include Microsoft’s Hohm, PlotWatt, myEragy, PeoplePower and MyEner$ave. Could such services leak data about users that could then be used to assemble profiles on them?

“They could learn so much more about you from all other publicly available sources than from that metering information,” Davis says. As smart meters roll out across Canada, the complaints continue. For example, opponents say their bills have increased 1,000 percent since meters were installed. Thus, for Canada’s utilities, privacy may be the first of many new issues.
The faces of data thievery: We can help you defend your enterprise from them.
Arming yourself for battle

Now in its third year, SC Congress Canada has become the must-attend information security event. This is where attendees gain expert guidance and timely industry information to help your companies effectively combat today’s cyber criminals. Given huge jumps in the numbers of cyber attacks, such assistance should go a long way in helping organizations like yours to strengthen your risk management position and tighten up needed security controls.

With yet another all-star lineup of thought-leading professionals, the two-day SC Congress Canada promises to deliver practical insight about the latest methods of attack that you as security professionals can immediately put to use upon return to your offices. Luminaries speaking at the event will share the latest news on cyber crime and data theft incidents, cyber espionage and APTs, hacktivist attacks, vulnerabilities associated with business-enabling technologies, compliance mandates and more. Offered across three tracks, expert-led talks run the gamut.

The likes of Larry Clinton, president of the Internet Security Alliance, and Mary Chaput, CFO of Clearwater Compliance, will discuss in detail the economics of cyber security and how gaining C-level support of and involvement for IT security programs is critical. During yet another lead session, experts from the Royal Canadian Mounted Police, The World Bank and other leading organizations will share a more comprehensive view of what the bad guys are up to and the best practices you can enlist to thwart their efforts.

In addition to these sessions, an expo hall will be packed with leading vendors and service providers to help you make sense of the evolving threat landscape and the various security technologies that can support your efforts.

As well, we’ll announce the winners of our third SC Awards Canada, which honors the achievements of IT security pros and companies in Canada.

If you’re looking to bolster your security and risk management plans to battle today’s more sophisticated cyber criminals, implement security controls that are both resilient to attacks and support regulatory compliance efforts, and address the security risks associated with the newest technologies forming the basis of your corporate infrastructures – from mobile devices to cloud services – you don’t want to miss SC Congress Canada.

We look forward to seeing you there!

Illena Armstrong
VP, editorial director,
SC Magazine Canada
May 8th agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Track 1 – Emerging threats/management</th>
<th>Track 2 – Technical</th>
<th>Track 3 – Editor’s choice</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:15 a.m.</td>
<td></td>
<td>Sessions in this track focus on the latest emerging threats faced by organizations and the best practices implemented to thwart them. This is of value to information security personnel at all levels who need to know more about what the bad guys are up to in order to protect critical data.</td>
<td></td>
<td>Given the constant change in the threat environment, every security line of business needs to be flexible. This track focuses on timely issues as seen through the eyes of Illena Armstrong, SC Magazine’s VP, editorial director. This is for all those wanting to stay on top of the latest security issues.</td>
</tr>
<tr>
<td>9:00 a.m. – 9:50 a.m.</td>
<td><strong>KEYNOTE: The economics of cyber security</strong> – Corporate executives are finally getting more involved in security in a number of organizations. But why has it taken so long and, more importantly, why is this so critical for success? How can practitioners help move this trend along?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9:55 a.m. – 10:40 a.m.</td>
<td><strong>Mobile malware</strong> – Where is the real threat? And what are some best practices to thwart mobile attacks?</td>
<td>Technical view of defense in depth: Many industry pundits consider the rash of hacktivist attacks in 2011 as a major distraction from focusing on more immediate cyber threats.</td>
<td>Who’s line is it, anyway? – When it comes to the integrity of code – the heart of application security – whose responsibility is it in the end?</td>
<td></td>
</tr>
<tr>
<td>10:40 a.m. – 10:55 a.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:55 a.m. – 11:40 a.m.</td>
<td><strong>Effectively using security intelligence to detect threats and exceed compliance mandates</strong> – Join this session to understand how to provide comprehensive network intelligence.</td>
<td>Social engineering revisited – How can your organization help mitigate this risk, and implement security awareness and training programs that actually resonate?</td>
<td>The Social Network – Social networking keeps up productivity but you need to somehow protect the enterprise.</td>
<td></td>
</tr>
<tr>
<td>11:45 a.m. – 12:30 p.m.</td>
<td><strong>The 2012 cyber security risk report</strong> – Discussed will be results from the 2012 HP Cyber Security Risks Report, as well as input garnered from the Open Source Vulnerability Database.</td>
<td>Technical look at compliance by the book – How can we practice great security so we don’t have to then jump through hoops when the auditor walks through the door?</td>
<td>Latest Threats – Pros weigh in on what they perceive to be the greatest group of threats facing organizations at the time of the Congress - noting such threats change weekly.</td>
<td></td>
</tr>
<tr>
<td>12:30 p.m. – 12:45 p.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:45 p.m. – 1:30 p.m.</td>
<td><strong>KEYNOTE: What keeps me awake at night (un-PC views on our future)</strong> – Winn Schwartau looks back on 30 years of security history, successes and failures, then tells us what really bothers him. In his customary hard-edged, honest style, he says the politically incorrect things that many of us think but rarely say. He’s going to talk about lawyers, complexification, 4G-war, the real future of mobile computing, poor defenses of networks, our inability to properly respond to cyber attacks and m profiling... just to start.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:30 p.m. – 3:15 p.m.</td>
<td></td>
<td></td>
<td></td>
<td>The international framework of cyber security – Comparative research into the policy approaches to cyber security worldwide, recently released by Ryerson University.</td>
</tr>
<tr>
<td>3:15 p.m. – 4:00 p.m.</td>
<td><strong>Privacy</strong> – How are organizations marrying privacy expectations with their business’ security practices, and how do they see customer demands in this area evolving?</td>
<td><strong>What’s a computer virus?</strong> – How does the enterprise achieve strong situational awareness and, more importantly, how do you then use that information?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:05 p.m. – 4:55 p.m.</td>
<td><strong>KEYNOTE: Cyber crime in Canada</strong> – This panel of government and law enforcement insiders will provide a deep view into the strategies that white hats are adopting to combat attacks. They will also discuss the steps and best practices you can enlist when working with law enforcement and the government to thwart today’s cyberattackers.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:55 p.m. – 6:15 p.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6:15 p.m. – 8:00 p.m.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
May 9th agenda

<table>
<thead>
<tr>
<th>Track 1 – Emerging threats/management</th>
<th>Track 2 – Technical</th>
<th>Track 3 – Editor’s choice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions in this track focus on the latest emerging threats faced by organizations and the best practices implemented to thwart them. This is of value to information security personnel at all levels who need to know more about what the bad guys are up to in order to protect critical data.</td>
<td>This track offers a deeper dive for the more technical security and IT pros at the conference. Emphasis will be on technical aspects of threats and vulnerabilities, along with relevant solutions and processes to address these. Sessions complement those offered in the two other, more executive-focused tracks.</td>
<td>Given the constant change in the threat environment, every security line of business needs to be flexible. This track focuses on timely issues as seen through the eyes of Illena Armstrong, SC Magazine’s VP, editorial director. This is for all those wanting to stay on top of the latest security issues.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:15 a.m.</td>
<td>Breakfast served in registration area</td>
</tr>
<tr>
<td>9:00 a.m. – 9:45 a.m.</td>
<td>Governance, risk and compliance: A practical implementation story – IT departments are working to better organize their risk and compliance efforts to meet growing business needs by establishing IT GRC programs.</td>
</tr>
<tr>
<td>9:50 a.m. – 10:35 a.m.</td>
<td>Sponsored keynote IBM’s Kris Lovejoy will lead a discussion on the increasing influence of CISOs in being transformational business leaders.</td>
</tr>
<tr>
<td>10:35 a.m. – 11:25 a.m.</td>
<td>The trained security professional – Security pros are constantly moving. How are these changes affecting the industry, and what steps are being taken?</td>
</tr>
<tr>
<td>11:25 a.m. – 12:10 p.m.</td>
<td>The trained security professional – Security pros are constantly moving. How are these changes affecting the industry, and what steps are being taken?</td>
</tr>
<tr>
<td>12:10 p.m. – 12:25 p.m.</td>
<td>Lunch in registration area</td>
</tr>
<tr>
<td>12:25p.m. – 1:10 p.m.</td>
<td>Sponsored lunch keynote TBA</td>
</tr>
<tr>
<td>1:15 p.m. – 2:00 p.m.</td>
<td>An APT presentation: Fighting the retro war of the future – We will examine advanced persistent threats and countermeasures available to combat these ongoing threats.</td>
</tr>
<tr>
<td>2:00 p.m. – 3:35 p.m.</td>
<td>Exhibition floor break – coffee served (Exhibition closes at 3:35 p.m.)</td>
</tr>
<tr>
<td>3:35 p.m. – 4:20 p.m.</td>
<td>Business-driven security programs: Proactively communicating value to the corner office – This presentation will outline the methods and processes used to develop an enterprise-wide security roadmap.</td>
</tr>
<tr>
<td>4:20 p.m. – 4:35 p.m.</td>
<td>Coffee break served outside breakout sessions</td>
</tr>
<tr>
<td>4:35 p.m. – 6:00 p.m.</td>
<td>Keynote: TBA</td>
</tr>
<tr>
<td>6:00 p.m.</td>
<td>Closing remarks and conference close</td>
</tr>
</tbody>
</table>
Pricing

<table>
<thead>
<tr>
<th>Conference registration options</th>
<th>Early bird rate (ends April 7)</th>
<th>Regular rate (begins April 8)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Two-day Pass</strong> (Includes access to eight breakout sessions, keynotes, expo hall, opening reception, SC Awards Canada, plus meals and breaks each day of the event)</td>
<td>$795</td>
<td>$1,115</td>
</tr>
<tr>
<td><strong>One-day Pass</strong> (One day of SC Congress Canada sessions, plus meals and breaks on the chosen day)</td>
<td>$475</td>
<td>$615</td>
</tr>
<tr>
<td><strong>Exhibits Plus</strong> (Includes access to one session of your choice, keynotes and the expo hall; does not include meals and breaks)</td>
<td>$65</td>
<td>$75</td>
</tr>
<tr>
<td><strong>SC Awards Canada Reception</strong> (Includes presentation of the 2012 SC Awards Canada winners. Food &amp; drink provided.)</td>
<td>$55</td>
<td>$55</td>
</tr>
<tr>
<td><strong>Expo Hall Only Pass</strong> (Includes access to keynotes and the expo hall; does not include meals and breaks)</td>
<td>FREE</td>
<td>FREE ($30 onsite)</td>
</tr>
</tbody>
</table>

Hotel reservations

InterContinental Toronto Centre
225 Front Street West, Toronto ON M5V 2X3

Reservations
Guest room rate: $209/CAD for single or double accommodations, plus applicable HST

Reserve your room
Call 1 (800) 235-4670 for reservations and mention SC Congress Canada 2012.

Contact

Exhibitor inquiries: Mike Alessie
mike.alessie@haymarketmedia.com

Marketing inquiries: Sherry Oommen
sherry.oommen@haymarketmedia.com

Program inquiries: Eric Green
eric.green@haymarketmedia.com

Awards inquiries: Anthony Curry
anthony.curry@haymarketmedia.com

2012 SC Awards Canada

The mission of 2012 SC Awards Canada is to honor the achievements of companies and IT security professionals striving to safeguard businesses, their customers and critical data in Canada. Nominations for the 2012 SC Awards Canada are made up of IT security products and services available for sale to Canadian companies, as well as provide both customer service and support to users in Canada. Some of the categories include: Security Company of the Year • Best Enterprise Security Solution • Best Regulatory Compliance Solution • Best Mobile/Portable Device Security • Best Managed Security Service • Best Fraud Prevention Solution • Best Security Information/Event Management (SIEM) Appliance

Mark Fabro, president & chief security scientist at Lofty Perch, receives the 2011 CSO of the Year award from Illena Armstrong, SC Magazine’s VP, editorial director.

SC Congress Canada Innovation Theatre

Stop by the Innovation Theatre to hear from some of the top companies in the IT security space as they present their latest products and services. These 30-minute presentations will be featured on both days and are open to all attendees.
SC Roundtable: Government

Rising incidents of hacktivism, cyber espionage and other online attacks have most organizations reframing their risk management plans to include more than a few tweaks.

However, many information security executives are finding that implementing desired policies and supporting technologies to forge needed enhancements is proving tricky during a time of constrained budgets and resources.

Federal government leaders especially are having difficulties as dollars dedicated to their initiatives either remain the same or continue to drop—even as the adoption of business-enabling technologies, such as cloud and mobile, spikes, according to IT security leaders attending a recent SC Magazine Government Security Roundtable in Washington, D.C.

“It is how [we] cover and continue the mission that makes the difference,” said one attendee from a large research-driven agency who asked for anonymity. “[We] can’t control everything. We just don’t have the resources.

He and others at the roundtable said getting monetary and other support needed to fully safeguard critical data, related informational flows and overall IT environments remains a huge stumbling block. Adding to this are worries about government agencies’ use of public-facing applications to exchange various bits of critical information with constituents.

Participants said it is tough enough getting needed budgets, much less convincing staff and government leaders to adhere to some additional controls despite their increasing reliance on cloud services, mobile devices and other technologies.

Finding ways to circumvent rules, or simply submitting requests to go around them, has become a frequent practice in many government agencies, some said during the gathering.

For instance, IT security pros may find themselves confronting a high-level individual in their organization who does not wish to follow policies. And, even with technologies in place that may help to enforce these, individuals will request and circumvent the rules. “He knows he’s the subject matter expert, and no one’s going to challenge him,” said the aforementioned IT security pro at the roundtable, sponsored by HP Enterprise Security.

In addition, desired redundancy in IT staff and systems is often given short shrift, he said. Having dedicated roles and backup staffers when others go on vacation or are otherwise unavailable are good practices, but higher-ups often are unwilling to fund these.

“Until we find a way to address these challenges, I don’t know how we can effectively address [associated security problems],” he said.

Whether some relief is in sight for federal cyber security practitioners is unclear and certain to remain so until after this year’s presidential election. President Obama’s budget proposal for 2013 does serve as a kick-off for negotiations with Congress. Already, however, talks are proving contentious.

Still, Obama’s wish list of spending priorities seems to favor IT pros, with $78.8 billion on overall IT operations proposed. Of that, millions are earmarked for sandbag cyber security operations and research initiatives.

Possible reinvestment of IT security funding and support couldn’t come soon enough. For the first time ever, hacking, as opposed to lost or stolen mobile devices, is the top reason for data breaches, according to the year-end “Data Breach Intelligence” report from Risk Based Security, an affiliate of the Open Security Foundation. Its findings revealed that hacking resulted in the exposure of 83 percent of the 368 million total records compromised last year.

But, trying to cover every possible entry point or be ready for every kind of attack is folly, said retired Lt. Gen. Rob Elder of the U.S. Air Force, who is now a member of the faculty at George Mason University in Virginia and was the lead speaker at the event.

“You need to take a look at this end to end,” he said. “Because there are so many different attack vectors, perhaps you should do something more like one does in the military. Typically, you don’t try to find everything.” Instead, security professionals should understand the key areas requiring protection so that the appropriate systems with the most at-risk data are defended properly.

“So, if we start thinking about [the] targets, then that could be helpful,” Elder said. “You can’t defend the ocean, so what parts can you defend?”

Whether it is a government agency working with citizens online or a bank interacting with customers who rely on it for its website processes for transactions, organizations must employ the expertise of IT security heads who fully understand the systems they can’t afford to have go offline for any length of time. This comes down to a risk management framework and what you have to fix first.

Elder, who has been involved in judging college and high school cyber security competitions that task contestants with architecting hardened systems from scratch, said such challenges reinforce for him how building security in from the start works. Often in the real world, though, systems are “cobbled together,” and require throwing good money after bad to maintain them.

“Most businesses, because they’re having to do things incrementally, can’t work

For government security professionals, focusing on priorities is key in these trying economic times, reports Illena Armstrong.
Managing use of copyrighted material across national borders is forging new partnerships, reports Greg Masters.

As Bob Dylan 2.0 might put it: 'The times, and the means of distribution, they are a-changin'.

His music and other artists' creations now are downloaded through illegal peer-to-peer (P2P) networks, various social media and other sites by individuals who want to avoid paying the entertainment companies representing them.

On Jan. 19, MegaUpload, a P2P file-sharing site, became the victim of its own success when New Zealand police, following a request from the FBI, shut down its operations with a raid on its headquarters in a rented $30 million mansion near Auckland.

Certainly the parameters of "acceptable use" have altered considerably since Napster in its early days, this site, established in 2005, had put up a pretense of legitimacy by agreeing to remove files when infringement complaints came in. This gesture proved insufficient, however. Its dissemination of pirated films, television shows, music and other digital content clearly skirted copyright laws.

Facebook and YouTube began their own country's laws as they pertain to electronic crimes, "says Art Bowker, a senior security adviser at Sophos Canada, says many law enforcement agencies have been forging for cross-national law enforcement efforts to enable charges to be laid internationally," he says.

But, this is a process that law enforcement agencies have to first agree that certain enforceable laws are broken, and then work together to coordinate the actual arrests within their respective jurisdictions.

While a police agency from one country can't enter another to arrest someone, many nations have treaties in place in which suspects will be locally arrested and held for extradition, says Bowker. That is what is occurring in New Zealand now with the MegaUpload case. This kind of law enforcement action just doesn't happen by magic, Bowker adds.

Authorities around the globe recognize that contacts need to be developed and maintained and, when the need arises, they reach out to their foreign counterparts.

Concurrently, the recent arrests of LulzSec and Anonymous members clearly has led to revelations that the FBI investigation association (HTCIA), which provides education and collaboration to its global members. And, other obstacles persist, Bowker says. Companies may still wish not to report incidents, for instance. As well, a number of countries don't have developed laws in place for dealing with cyber criminals, and some lack the investigatory resources and capability to go after the thieves, he explains.

Who has provenance?

Today, the principal challenges for any cross-national law enforcement efforts involve both jurisdictional rights and international laws, says Marcus Chung, CEO of Global Cyber Risk, a Washington, D.C.-based consultancy that helps global businesses manage risks.

As for cross-border cooperation, countries are making strides. Chester Wisniewski, a senior security adviser at Sophos Canada, says many law enforcement agencies regularly collaborate on international cyber crime cases. He points to cases in Russia, Egypt, Estonia and other countries.

"To some degree, criminal law is being passed in a coordinated fashion to enable charges to be laid internationally," he says.

But, this is a process that law enforcement agencies have been forging for years. "The advanced countries have specialized computer investigation units, who are familiar not only with computer forensics and investigation, but their own country's laws as they pertinently to computer crimes," says Art Bowker, a member of the High Technology Crime Investigation Association (HTCIA), which provides education and collaboration to its global members. And, other obstacles persist, Bowker says. Companies may still wish not to report incidents, for instance. As well, a number of countries don't have developed laws in place for dealing with cyber criminals, and some lack the investigatory resources and capability to go after the thieves, he explains.

Who has provenance?

Today, the principal challenges for any cross-national law enforcement efforts involve both jurisdictional rights and international laws, says Marcus Chung, CEO of Global Cyber Risk, a Washington, D.C.-based consultancy that helps global businesses manage risks.

As for cross-border cooperation, countries are making strides. Chester Wisniewski, a senior security adviser at Sophos Canada, says many law enforcement agencies regularly collaborate on international cyber crime cases. He points to cases in Russia, Egypt, Estonia and other countries.

"To some degree, criminal law is being passed in a coordinated fashion to enable charges to be laid internationally," he says.

But, this is a process that law enforcement agencies have been forging for years. "The advanced countries have specialized computer investigation units, who are familiar not only with computer forensics and investigation, but their own country's laws as they pertinently to computer crimes," says Art Bowker, a member of the High Technology Crime Investigation Association (HTCIA), which provides education and collaboration to its global members. And, other obstacles persist, Bowker says. Companies may still wish not to report incidents, for instance. As well, a number of countries don't have developed laws in place for dealing with cyber criminals, and some lack the investigatory resources and capability to go after the thieves, he explains.

Who has provenance?

Today, the principal challenges for any cross-national law enforcement efforts involve both jurisdictional rights and international laws, says Marcus Chung, CEO of Global Cyber Risk, a Washington, D.C.-based consultancy that helps global businesses manage risks.

As for cross-border cooperation, countries are making strides. Chester Wisniewski, a senior security adviser at Sophos Canada, says many law enforcement agencies regularly collaborate on international cyber crime cases. He points to cases in Russia, Egypt, Estonia and other countries.

"To some degree, criminal law is being passed in a coordinated fashion to enable charges to be laid internationally," he says.

But, this is a process that law enforcement agencies have been forging for years. "The advanced countries have specialized computer investigation units, who are familiar not only with computer forensics and investigation, but their own country's laws as they pertinently to computer crimes," says Art Bowker, a member of the High Technology Crime Investigation Association (HTCIA), which provides education and collaboration to its global members. And, other obstacles persist, Bowker says. Companies may still wish not to report incidents, for instance. As well, a number of countries don't have developed laws in place for dealing with cyber criminals, and some lack the investigatory resources and capability to go after the thieves, he explains.

Who has provenance?

Today, the principal challenges for any cross-national law enforcement efforts involve both jurisdictional rights and international laws, says Marcus Chung, CEO of Global Cyber Risk, a Washington, D.C.-based consultancy that helps global businesses manage risks.

As for cross-border cooperation, countries are making strides. Chester Wisniewski, a senior security adviser at Sophos Canada, says many law enforcement agencies regularly collaborate on international cyber crime cases. He points to cases in Russia, Egypt, Estonia and other countries.

"To some degree, criminal law is being passed in a coordinated fashion to enable charges to be laid internationally," he says.

But, this is a process that law enforcement agencies have been forging for years. "The advanced countries have specialized computer investigation units, who are familiar not only with computer forensics and investigation, but their own country's laws as they pertinently to computer crimes," says Art Bowker, a member of the High Technology Crime Investigation Association (HTCIA), which provides education and collaboration to its global members. And, other obstacles persist, Bowker says. Companies may still wish not to report incidents, for instance. As well, a number of countries don't have developed laws in place for dealing with cyber criminals, and some lack the investigatory resources and capability to go after the thieves, he explains.

Who has provenance?

Today, the principal challenges for any cross-national law enforcement efforts involve both jurisdictional rights and international laws, says Marcus Chung, CEO of Global Cyber Risk, a Washington, D.C.-based consultancy that helps global businesses manage risks.

As for cross-border cooperation, countries are making strides. Chester Wisniewski, a senior security adviser at Sophos Canada, says many law enforcement agencies regularly collaborate on international cyber crime cases. He points to cases in Russia, Egypt, Estonia and other countries.

"To some degree, criminal law is being passed in a coordinated fashion to enable charges to be laid internationally," he says.

But, this is a process that law enforcement agencies have been forging for years. "The advanced countries have specialized computer investigation units, who are familiar not only with computer forensics and investigation, but their own country's laws as they pertinently to computer crimes," says Art Bowker, a member of the High Technology Crime Investigation Association (HTCIA), which provides education and collaboration to its global members. And, other obstacles persist, Bowker says. Companies may still wish not to report incidents, for instance. As well, a number of countries don't have developed laws in place for dealing with cyber criminals, and some lack the investigatory resources and capability to go after the thieves, he explains.
was actively notifying governments and companies to potential vulnerabilities it was uncovering during its investigation, he says, recalling one report that 300 public and private entities in the United States and around the globe were notified. In the United States, Infracall—an offshoot of the FBI to work in partnership with the private sector—serves such a purpose. There is also the Secret Service Electronic Crime Task forces performing similar functions.

“Law enforcement and the private sector both within and outside of the United States are seeing the value in networking to protect themselves from cyber threats,” Bowker says.

Malwarebytes’ Chung agrees, pointing out that the recent efforts of the U.S. Department of Justice (DoJ), FBI, Hong Kong authorities, and law enforcement in the Netherlands, Germany, Canada, U.K, and New Zealand highlight what is widely perceived as a successful anti-piracy operation that seized more than $50 million in assets and yielded several high-profile arrests against the principals of MegaUpload. The authorities, he says, had to coordinate multiple arrests, freeze financial assets and issue search warrants across eight countries.

If a crime against an American organization occurs overseas, the FBI will escalate it to its liaison who works with the foreign government’s federal police, adds Winnieks. The bar is set high for this to occur, but collaborating MegaUpload founder Kim Schmitz (aka Dotcom) and extradition, which can also include approaches and coordination with government agencies, says Westby. “You can bet that if the recent Anonymous hack (which was not successful as they appeared, that case will become one key argument for why information needs to be shared,” Bowker says.

Mitigation and control

In the MegaUpload case, Dotcom was freed on bail, but had conditions put in place that prohibit him from connecting to the Internet, Bowker says. “This is an area more and more community corrections officers are going to have to get up to speed on, learning how to enforce conditions that restrict and/or monitor cyber offenders’ computer and internet use.”

Mitigating and controlling the activities of cyber criminals across borders is part of the ongoing challenge to coordinate international efforts among various law enforcement agencies, both foreign and domestic, says Chung. There are privacy laws and due process that differ at both the regional and international levels. Due to this level of complexity, at a minimum there are typically local “search warrants,” financial information (to facilitate the freezing of assets) and evidence of criminal behavior that is shared among the agencies.

Westby adds that sharing often is facilitated informally through relationships and contacts because the formal process can be cumbersome. Regulations begun under the Homeland Security Act of 2002 allow the Department of Homeland Security to share critical infrastructure data with foreign governments, she says.

The role of ISACs

One important resource is Information Sharing and Analysis Centers (ISACs). They can play a valuable role in facilitating data exchange within their industry sectors and coordination with government agencies, says Westby. “Many ISAC members are multinational companies, so this sharing also has a spill-over effect to international locations,” Westby says. “They can also help facilitate cooperation among providers.”

One must keep in mind, however, that ISACs are not designed for or intended to pursue cyber criminals, she says. ISACs are primarily useful in sharing information among their members, including approaches and coordination on cyber crime.

Chung says ISACs are likely to take an increasingly prominent role in coordinating inter-agency efforts and assisting in both the hunting and evidence-gathering stages of prosecuting cyber criminals.

“If you share information about threats, you can develop patterns, which can lead to common players,” says Bowker. “The more you communicate, the more you are able to identify the bad actors. You can’t arrest them until you identify them.”

Westby adds that sharing information that allows members to protect themselves while at the same time can lead to arrests and prosecutions. That is why he advocates law enforcement cooperation and remain active in these groups.

Other information-sharing bodies exist as well. Westby says that IMPACT, the International Multilateral Partnership Against Cyber Threats, is helping to build a 24/7 point-of-contact database and helping countries coordinate. It now has more than 130 nations signed up and is now the official operating arm of the U.N.’s International Telecommunication Union (ITU) Global Cybersecurity Agenda, she says.

For its part, the United States has failed in its efforts to build a framework to help build international cooperation and harmonize cyber crime laws, Westby says, which has contributed to the soaring nature of cyber crime here and abroad. Winnieks agrees, adding that “if we want to stop the death of a million cuts that we are all suffering online, we need to ramp up the resources and cooperation and we need to do it quickly. Criminals overseas are acting with impunity, knowing that only the biggest offenders who attract the wrong sort of attention from their governments will ever face prosecution. Law enforcement budgets need to adjust to this new reality, and we need a whole lot more talented internet security experts to be trained to meet the needs of a new era in computer crime.”

In a final analysis, most agree that in a world increasingly tied together by global markets, it only makes sense that everyone comes together to protect each other’s cyber assets.
Cyber espionage

History books tell us that the Cold War ended roughly 1991 after the dissolution of the Soviet Union. But, today’s security practitioners say the Cold War has simply morphed from a threat of armed conflict among major world powers into a battle of computer-savvy “troops” fighting from the comfort of offices.

Instead of countries spending billions of dollars to create new weapons, supply massive armies and spend millions of dollars to create new weapons, today’s adversaries hire code-writers to create attacks that can run autonomously for years with little or no human intervention. By repurposing code to spawn new attacks, the cost of cyber warfare can be a fraction of the cost of a conventional war.

While China and Russia generally are considered by industry experts to be the leaders in state-sponsored cyber attacks against the United States, they are not the only countries to have sophisticated espionage infrastructures in place, says Richard Bejtlich, chief security officer at Alexandria, Va.-based Mandiant. Other nations with sophisticated capabilities include North Korea, Iran, France, Israel and, of course, the United States.

Instead of military assaults, today’s adversaries hire coders to create attacks that can run autonomously for years, says Stephen Lawton.

North Korea, Bejtlich says, uses technology against its neighbor, South Korea, and to make political statements against the West, generally resulting in attacks against the United States, he says. Iran primarily uses its cyber weapons to suppress internal dissidents.

In the past, he says, U.S. politicians spoke in general terms about cyber attacks, choosing not to name those believed to be responsible. That all changed late last year when the Office of the National Counter Intelligence Executive released a report, “Foreign Spies Stealing U.S. Economic Secrets in Cyber space,” which specifically identified China and Russia as key perpetrators. However, the report also said U.S. allies are actively involved.

“Certain allies and other countries that enjoy broad access to U.S. government agencies and the private sector conduct economic espionage to acquire sensitive U.S. information and technologies,” the report states.

“Some of these states have advanced cyber capabilities.”

It cited four factors that will shape the cyber environment over the next three to five years. These are:

• April 2012 • www.scmagazine.com

A technological shift, including the use of smartphones, laptops and other internet-connected devices; an economic shift that changes the way corporations, government agencies and other organizations share storage, computing, networking and application resources; a cultural shift in the U.S. workforce, where younger employees mix personal and professional activities; and a geopolitical shift as globalization of the economy is trained at an early age as cyber warriors. These academies provide the students with respectability and good pay. In China, for example, the Communist Party codified cyber warfare in 2010, and President Hu Jintao deemed cyber war a priority. Author and retired U.S. Marine Corps Lt. Col. William Hagastad says in an upcoming book that China bases its policies on the Art of War, Sun Tzu’s doctrine written around 500 B.C., one of whose tenets is: Keep your friends close, but keep your enemies closer. Chinese officials, however, regularly deny they are involved in any cyber spying efforts.

In the United States, the military is also shifting its war strategy to further prioritize cyber efforts. The soldiers who pilot military drones over Pakistan and Afghanistan actually sit in control rooms at Creech Air Force Base in Nevada. This, Carstensen says, is not unlike cyber attackers who might work out of a hotel to conduct assaults.

However, the level of expertise of foreign cyber attackers varies widely from so-called script kiddies, who download exploit software that is widely available on the internet, to experienced computer engineers who have either religious or political reasons for staging actions. Some of these attacks are advanced persistent threats (APTs) that are designed to enter a computer system and perhaps sit dormant for a period of time. The intrusions are designed not to be noticed.

This tactic varies significantly from those of hacktivists, who attack websites with the expressed purpose of drawing attention to the site being breached. Some groups, such as Anonymous and LulzSec, have claimed credit for damage to sites they have compromised.

Unlike hacktivists, cyber spies are so concerned about flying under the radar that once they successfully enter a target system, they actually install security patches to ensure that other attackers are unable to access the system using the same vulnerability, says Daniel Teal, founder and chief technology officer of Austin, Texas-based CoreTrace and a former officer at the Air Force Information Warfare Center (AFIWC). By installing fixes, he says, the attacker will have the compromised systems all to themselves and will not have to worry about a sloppy rival alerting the IT manager that there has been a breach.

Admins might actually see their network performance improve while the attacker ensures that others are unable to infect the environment, Teal says. Because the attacker does not want to draw attention, they simply can leave a back door open so that the malware payload is not accidentally identified by the target network.

Toney Jennings, CEO of CoreTrace, adds that companies might have the equivalent of a “cyber atomic bomb” in the server that “is not doing anything bad today.” That bomb could be set off by an intruder at a later date, well after the initial breach took place. Addition-
Mandiant’s Bejtlich says that despite the 100 percent effectiveness against intruders, the need for IT security, the full resources of a sophisticated technology and staff. Even still, he says, computers, and no shortage of defensive technologies and staff. HP determined that the manufacturer was sending data off the network simply by sending random data bits without being easily accomplished. He contacted the system manufacturer, Hewlett-Packard, and discovered that the keyboard he purchased for his daughter’s computer. Such devices could be plants with the parking lot or those handed to them not to insert thumb drives they find in the company’s primary computer systems, outside attacks.

The whole idea behind SIEM has been evolved, with copyspace for several years now. Personally, I find SIEM to be one of the most important devices on the network. It takes that position because a really good SIEM will do two things for you. First, it will allow alerting on complicated events that might otherwise escape notice. Second, it allows detailed analysis into root causes of security events that are forensic perspective. From the alerting perspective, because the SIEM is taking its input from a variety of sources, it gets different perspectives on the data flowing through the network. An especially important aspect is the ability to correlate net flows with events. This provides a sort of vectoring ability that can help the analyst figure out where devices in the enterprise have been affected by an event. From the analytic viewpoint, a major analytical challenge is dealing with very large amounts of data. Information security should focus on the data, so even if there are devices involved – which, of course, there are – understanding how the data flows through these devices is the key to understanding how to analyze the event. The SIEM facilitates that understanding because it correlates the large amount of information on the network to pare it down to a manageable size.

Be sure that you define your needs thoroughly. There are a few of these products that excell in log management, for example, so if that is what you need, take a look at them. One of the great advantages of a maturing product group is that there should be available exactly the product for your application. This month’s offerings are no exception.

—Peter Stephenson, technology editor

**Product Section**

**GFI**

Easy-to-use SIEM that can function sans agents P43

**NetIQ**

Tool with the most mature features P44

**SolarWinds**

A SIEM that is full of options P45

**How we test and score the products**

Our testing team includes SC Magazine Labs staff, as well as external experts who are respected industry-wide. In our Group Tests, we look at several products around a common theme based on a pre-determined set of SC Labs standards (Performance, Ease of use, Features, Documentation, Support, and Value for money). There are roughly 50 individual criteria in the general test process. These criteria were developed by the lab in cooperation with the Center for Regional and National Security at Eastern Michigan University. We developed the second set of standards specifically for the group under test and use the Common Criteria (ISO 1548) as a basis for the test plan. Group Test reviews focus on operational characteristics and are considered at evaluation assurance level (EAL) 1 (functionally tested) or, in some cases, EAL 2 (structurally tested) in Common Criteria– speak. Our final conclusions and ratings are subject to the judgment and interpretation of the tester and are validated by the technology editor. All reviews are vetted for consistency, correctness and completeness by the technology editor prior to being submitted for publication. Prices quoted are in American dollars.

**What the stars mean**

Our star ratings, which may include fractions, indicate how well the product has performed against our test criteria.

- Four stars – Outstanding. An “A” on the product’s report card.
- Three stars – Carries out basic functions very well. A “B” on the product’s report card.
- Two stars – Carries out all basic functions to a satisfactory level. A “C” on the product’s report card.
- One star – Fails to complete certain basic functions. A “D” on the product’s report card.

**What the recognition means**

Best Buy goes to products the SC Lab rates as outstanding. Recommended means the product has shone in a specific area.

Lab Approved is awarded to extraordinary standouts that fit into the SC Lab environment, and which will be used subsequently in our test bench for the coming year.

---

This article originally appeared as an SC Magazine ebook. For more information about ebooks from SC Magazine, contact Ilenna Armstrong, vice president, editorial director, at ilenna.armstrong@haymarketmedia.com.
Security information and event management (SIEM) tools do a lot of things, but at the core they take data from sources and get useful, actionable information from it, says Peter Stephenson.

McAfee Enterprise Security Manager (ESM) is one of the most interesting groups that we examine. It is particularly interesting because over the years the definition of what we mean by a SIEM has evolved. It came out of two separate product categories: security information management (SIM) and security event management (SEM). At the beginning of the genre there was a distinction made between event and information management. Today, they are combined and have been for some time. While some refer to SIEM as security incident and event management, most professionals today agree that SIEM is security information and event management. The term was coined by Gartner back in 2005 and it has stuck with us.

This is totally appropriate since information is necessary to interpret events. Certainly it’s the events that trigger alerts, but it’s the information that gets the analysis done. So, what should we be looking for in a capable SIEM? Given that this is an evolving category – even though it’s pretty mature at the moment? SIEMs do a lot of things, but at the core of why we need one of these beasts is that they take lots of data from lots of sources and provide useful, actionable information from it.

Let’s dig into that a bit. Useful security-related data in a large enterprise comes from a lot of sources. Firewalls generate logs. Intrusion detection systems (IDS) or intrusion prevention systems (IPS) generate logs and alerts. Routers and switches generate net flow data. Computers generate system logs. All of these assets need to be aggregated and correlated in order to be of any use. For a large enterprise, that could mean quite a bit of data. So what does a SIEM give us that helps us analyze and alert?

First, the SIEM must aggregate the incoming data. That means that it must know how to read the different file types that generate data for it. There are a variety of ways that SIEM developers do this, but the bottom line is: If the SIEM at which you are looking cannot decode most types of security data, it is not of much use to you. The other piece of aggregation is the ability to collect all of the data without dropping packets. Next, the SIEM needs to be able to correlate data that it has collected. This means distilling it into common events and flows. The analysis cannot begin until the correlation is complete. SIEMs alert as well as analyze, so there must be a good way of determining alerts. Limiting or eliminating false positives, alerting based on weighting, and criticality and correlation with vulnerabilities are all important aspects of the alerting functions of a capable SIEM.

Also, the tools need a good way of displaying the results of their analysis. That usually means a good graphical dashboard, but there also is the need to drill down to original data, particularly the original source. This leads into the need today for compliance reporting. Finally, SIEMs can process a lot of input. So you need to consider how you are going to archive the massive amount of facts that the sources feeding the SIEM generate daily. There are a couple of sides to this particular requirement. On one hand, you can archive metadata and that will let you perform credible analysis over time to get historical perspectives on threats and vulnerabilities. However, that usually does not let you drill down to the source data. That means that you will not be able to reconstruct sessions, including the data payloads of the source packets.

So, what distinguishes one SIEM from another? The SIEM that you select needs to have the features that you need in your environment. It usually needs to be scalable, and that might mean being able to function in a widely distributed network. SIEMs that do that often have a master device that communi- cates with subordinate devices. Don’t focus too much on cost. Rather, concentrate on value. For a large-scale SIEM, you might pay a bit more, but you may need its capabilities.

Frank Oldhorst and Mike Stephenson contributed to this Group Test.
**AlienVault Professional Threat Management S3000**

Part of the fun of doing these product reviews is that we get to see new products as they emerge into the marketplace. AlienVault’s Professional Threat Management S3000 is no exception. This product is a component to the AlienVault Unified Security Management platform, which started out as an open source project and has now grown into a solid security event management tool. The platform contains more than 30 open-source security tools built in and ready to go out of the box. Some of these tools include intrusion detection system (IDS), host-based intrusion detection system (HIDS), Forefront Identity Manager (FIM), wireless intrusion detection systems (WIDS), netflow, asset inventory and vulnerability assessment. Working together, these tools can provide overall security management from posture assessment through finding ways to remediate and improve overall network security throughout the environment.

We found this product to be quite easy to install. The installation has to be done on a bare metal server or virtual machine. To install the product, the installation DVD is inserted into the server, and once booted, the Linux-based installation wizard is launched. The installation can be fully automated, or the user can pick a more customized installation method if needed. We chose to go with the default automated install. The installation of the software took only about 15 minutes, and the server was up and running. All configuration is done using a web GUI. We found this to be easy to navigate and intuitive to use overall, but we did have to navigate around a bit to get comfortable with how the system was organized.

This tool is pretty empty after installation by default, and there is a lot of configuration that has to be done to get everything up and running. We found configuration to be fairly simple with the help of the documentation. One thing we instantly noticed was the amount of customization that we could do with the dashboards.

Documentation was comprised of installation and user guides, plus several other pieces of supplemental material. We found all documentation to be easy to follow, with clear instructions, screen shots and configurations.

AlienVault offers a few support options. Customers can purchase a support pack, which includes a limited number of tickets or support hours. Alternatively, they can purchase assistance as part of an annual contract. This offers both eight-hours-a-day/five-days-a-week and 24/7 options, which include phone and email-based technical support, contacts and access to a portal. All customers can access a small portion of the portal which includes product documentation and other useful resources, at no cost.

At a price of $32,000 before hardware and support, this product does come with a hefty price tag. We find AlienVault Professional Threat Management to be an average value for the money. While it does sport some nice features, we find the overall cost of ownership to be a little bit high, especially considering that a 24/7 support contract can cost up to $50,000 annually.

**LogLogic MX**

When we first saw LogLogic a few years ago, it was a strong log management appliance that could do some nifty stuff, but overall was focused on log management. Well, times have certainly changed, and this appliance has grown immensely in functionality over the years. Its latest iteration offers some exciting new features, including a full compliance manager, but more on that later. The LogLogic MX can collect data and logs from network devices, such as routers and firewalls, as well as many other sources, including intrusion detection system (IDS)/intrusion prevention system (IPS), Windows, Unix and load balancers. After logs are gathered, the MX solution indexes, compresses and stores the data for use in forensic analysis and compliance assessments.

Installing the appliance itself takes just a few minutes. Once up and running in the network, all configuration is done via a web-based management console. The tool also comes with the Compliance Suite and Compliance Manager as separate installs. The Compliance Manager can be easily installed on a Windows Server and it provides all the necessary components, including the web-based management interface. After the installations are complete, all that needs to be done is to add the appliance to the Compliance Manager and add sources to the appliance.

After our initial configuration was complete, we began navigating around the management interface and found it to be quite comfortable to move around in. The majority of the interface has not changed much, and we felt right at home managing the appliance. The combination of the MX appliance and the Compliance Suite make managing compliance easy as well. This product comes preloaded with many compliance-based reports and customizable dashboards. Also included are ready-to-go alerts based on several standards, including PCI DSS, HIPAA, SOX, COBIT, NERC, FISMA, ISO, FTTL, and the HITRAC Act.

Documentation came as several PDF guides, including installation and administrator guides for the appliance and quick-start and user guides for the Compliance Manager, along with several supplemental pieces of documentation, including log source configuration guides for a variety of log sources. We found all these to be complete and easy to navigate.

LogLogic offers two levels of support—both available at an annual cost. Customers can purchase gold support, which includes phone and email technical help during business hours, or platinum support, which is 24/7.

Starting at around $35,000, this product may seem quite expensive, but we find it to be a good value for the money. Included in the price is not only the appliance and software, but also the Compliance Manager and Management Suite, which add a lot of compliance auditing/management features and functionality. Ongoing support is also quite affordable, with business-hour support coming in at around $7,000 per year and 24/7 assistance only around $12,000 per year.
**LogRhythm**

Back again this year is one of the most powerful SIEMs that we have seen, and it is more powerful than ever with the new version 6. To start, the LogRhythm appliance combines log management, SIEM, file integrity monitoring and host activity monitoring into a single integrated platform. From there, all these functions use the advanced intelligence engine to provide full correlation and pattern recognition to stay on top of security threats throughout the enterprise.

From beginning to end this appliance is easy to deploy and configure. The first thing that needs to be done is to get the appliance up and running. The tool is pretty much ready to go out of the box, but does need some initial configuration. At first boot the appliance will run through a short Windows setup wizard where networking and other settings can be configured. After the appliance is up and running, all management is done via a powerful management console application. Overall, we found the management console to be easy to navigate, as well as intuitive to use. We also liked that the interface can be highly customized to meet the needs of the user and is not a one-size-fits-all layout.

The management interface has a plethora of features and functions. Some of these include fully customizable dashboards – along with predefined dashboards that offer specific information at a glance, many graphs and charts that can be drilled down into all the way to the raw log data if needed, and quick navigation controls for easy movement throughout the interface. Aside from all of the management capability, this product also features many strong compliance functions, including a brand new SmartResponse system. Security administrators can use this to deploy instant and automated remediation of common alerts. The final strength of this product is a solid rule engine. While administrators can use this to deploy instant and automated remediation of common alerts, the appliance is able to gather and analyze logs with or without the use of agents, using the rule builder interface. Finally, in terms of performance and flexibility, this appliance is able to gather and analyze logs with or without the use of agents, using the rule builder interface. Finally, the appliance has the ability to collect data and logs. The LogRhythm appliance is able to gather and analyze logs with or without the use of agents, depending on the type of log and needs of the environment.

The LogRhythm documentation set is included in the management console and can be easily accessed if needed. It features installation, configuration, and administrator guides. We found all documentation to be well-organized and easy to follow, with many screenshots and step-by-step configurations.

**McAfee Enterprise Security Manager (ESM)**

In the ever-changing marketplace of today’s network security products, it is not uncommon to see a company acquire another company with the idea of taking a good product and making it better. We have seen firsthand that sometimes this works and sometimes it doesn’t. However, in the case of McAfee, it has found a real winner with this product. The Enterprise Security Manager from McAfee is a new iteration of our old friend, the NitroView from NitroSecurity. When we see acquisitions such as these, it always makes us nervous because we fear that a good product can easily go bad. So far, this is not the case with this one. So what does the Enterprise Security Manager, or ESM, have to offer? A lot if you ask us.

This product features a powerful correlation engine that is driven by an ultralight proprietary backend database. The ESM is able to gather, store and analyze logs and data from a large amount of sources and then correlate events based on rules, possible risk or historical trends.

An appliance that has this much power must be difficult to configure, right? Not at all. The initial setup process takes just a few minutes and can be done directly on the LCD screen on front of the appliance. This is where all the network configuration is done, and after the appliance is connected to the network all further management is done via a web GUI. We found this interface to be one of our favorite parts of the appliance. The management interface is loaded with visuals and dashboards that include many charts and graphs that can be drilled down into all the way to raw log data. Dashboards also can be customized to meet the analysis needs of the user by simply adding or removing the various dashboard modules.

This product can take logs from just about anything with an IP address, but what makes it stand out is its Database Activity Monitor and Application Data Monitor. Using these two features, security administrators can easily collect data from database and application logs for deep forensic analysis. The ESM also comes preloaded with more than 200 different predefined compliance report templates, along with a reporting function that enables the creation of custom reports quickly and easily.

Documentation included an installation and a full user guide. We found these materials to be complete and well-organized.

McAfee offers customers 24/7 phone- and email-based technical assistance as part of an annual agreement. Customers also can access a web-based portal via the website, which includes a knowledge base, downloads, support case management and other resources.

At a price just shy of $39,000, this product may seem quite expensive at first. However, we find that its combination of features, paired with the solid correlation engine and backend database, make it an excellent value for the money. The tool can provide security event management and analysis along with forensic capability that is easy to deploy for almost any size environment.
Trustwave SIEM

The Trustwave SIEM appliance is designed to collect, normalize, analyze and store events and logs from a wide array of network devices and security products. Administrators can then use all of the collected data to do forensic analysis of security events along with compliance management and reporting. The most interesting function of this product is its deployment flexibility. The Trustwave SIEM can be deployed as a standalone appliance that is managed by the organization or it can be deployed as a managed appliance that is monitored by Trustwave to keep everything up to date and functioning properly. If an organization deploys a managed appliance, it also has the option to have Trustwave provide analysis of mission-critical data.

Not much has changed with installation and management of the appliance since we saw it last year. The initial setup is quite straightforward. It is guided by a setup wizard, which can be accessed via a web browser that goes to the IP address of the appliance. At the completion of the initial setup, all further configuration is done using the web-based management interface. Overall, we found this to be intuitive to navigate, but we still had to spend some time navigating around and getting familiar with how to configure log sources and get the appliance collecting logs. We would like the process of adding and managing devices to be a little more intuitive.

We found this appliance to offer a lot in terms of analysis capability. The product comes preloaded with preconfigured collectors for many types of devices, including routers, switches, Windows-based event logs, and some generic log sources. Custom log sources also can be added if needed and, at no charge to the customer, Trustwave will help add support for any commercially available device.

Along with the preconfigured collectors, this appliance features many predefined compliance and policy templates that make overall analysis of events quite simple. Trustwave is also constantly pushing new updates to the appliance, which include updated log parsing definitions, new and updated reports, new charts and correlated alert definitions. This ensures that log and compliance analysis is always up to the latest standards and alerts are always kept up to date.

The Trustwave SIEM comes with a good amount of documentation. We found all of it to be well-organized and easy to follow.

Trustwave offers support to customers through an annual agreement. Customers can purchase 12/7 or 24/7 support, which includes access to phone and email-based technical support. Also available to customers is an online assistance portal, which includes a knowledge base, FAQ section and many other helpful resources.

At a price of $19,000, we find the Trustwave SIEM to be a reasonable value for the money. The appliance offers a lot in the way of features and analysis capability, as well as ease of management, particularly after the initial configuration is complete.

CorreLog Correlation Server v5.1.0

The CorreLog Server is a web-based solution that leverages browser technology to present an easy-to-use, multi-platform interface that stresses point-and-click simplicity for the harried network administrator. Designed from the outset as a product that supports regulatory compliance objectives, as well as security posturing, CorreLog Server is chock full of features and reporting capabilities.

The product can be installed under two distinct scenarios, where it operates as either as a “Small Business Server” or as an “Enterprise Server.” The “Small Business Server” configuration was chosen for testing because it features the capabilities of the Enterprise Server, but without the high-end hardware and processing requirements associated with the Enterprise Server implementation.

That said, the Small Business Server configuration proves to work fine under virtualized environment, using a virtual PC as a host. The product runs on a variety of Windows operating systems, including Vista, XP and Windows 7, as well as various editions of Windows Server. That helps to make the product very flexible to deploy and eliminates the need for proprietary hardware and high-end server components.

CorreLog Server relies on an included version of Apache Server for access via a browser, and browser security is handled via an included copy of Apache SSL Server. Installation was straightforward, requiring only basic networking knowledge, and used a wizard to install and configure the product. There are a few manual steps. However, the PDF-based quick-start guide makes it almost point-and-click easy.

Once installed, the main management console is accessed using Internet Explorer v7 (or equivalent). On initial logon, the administrator will need to set up accounts and passwords. Once again, that proves to be easy, allowing administrators to get the system ready for full deployment rather quickly.

CorreLog Server uses a client/server model to gather information.

Installing the client application is by no means complex, but it can take some time on a larger distributed network. One caveat is that the client should be installed on every system that interacts with the network internally and falls under the purview of compliance, security or performance.

Integration and setup aside, the real meat and potato of CorreLog Server is the information it can provide to a network manager – which is key when it comes to a security information and event management product. Here, CorreLog Server offers several reporting capabilities and, interestingly, integration into Microsoft Excel, which gives analysts some flexibility when analyzing specific events.

In short, CorreLog server offers a lot of bang for the buck and proves easy to install and use. Excellent documentation and very good support highlight some of the advantages offered by the product, while reporting flexibility paired with Excel integration make it a valuable ally for the harried compliance officer.
Prism Microsystems
EventTracker v7.2

Nowhere does a product name better describe its capabilities than with EventTracker from Prism Microsystems. From the outset, EventTracker appeared as a more than capable system, the potential for which came to fruition with its GFI EventsManager 2012. Although it may sound like something a wedding planner may use, EventsManager 2012 is aimed directly at the SIEM market segment.

The product is designed to do exactly as the name implies—manage events—and in the case of SIEM, those events can originate from any number of network-attached devices in the typical enterprise, whether they are servers, PCs, firewall appliances, and so forth.

GFI EventsManager takes a KISS (keep it simple & short)-approach to gathering data, while not sacrificing any robustness of the data collected. The product's log and event management capabilities prove to be more than adequate and incorporate an impressive array of filters, classifications and triggers.

A notable capability is the product's ability to work without using any Windows agents. Rather, GFI has built the ability to read native Windows events from Windows systems without the need to install a software client on the subject system.

Installation proved straightforward—as with most products today, the installation is wizard-driven. However, the product is designed to run on a Windows Server-class system, but also can be run on Windows XP in a pinch. Nevertheless, there are some prerequisites that must be met, such as having.NET installed on the system acting as a server. Luckily, GFI does an excellent job of documenting those requirements, and provides a straightforward getting-started document that helps to smooth out any installation speed bumps.

EventsManager sports an excellent interface that proves to be both intuitive and loaded with actionable information. The GUI gathers up related information and displays it in a fashion that makes it easy to see correlations between events and devices, as well as using color coding to highlight the priority of alerts. However, that clean interface design proves to be a necessity simply because EventsManager does not have a threat correlation engine. In the big scheme of things that proves to be much less important than one would think, because GFI makes it easy for an administrator to correlate threats.

EventsManager offers a robust reporting engine that allows administrators to define a multitude of reports with custom parameters, which helps to ease auditing chores and streamlines the event discovery process. Perhaps, one of the product's biggest strengths lies in its ability to associate and define critical events and then choose to automatically alert administrators about critical events or even launch scripts to auto-remediate specific problems.

All things considered, GFI EventsManager proves to be very apt at what it is designed for, managing events driven by the SIEM methodology. Strong reporting tools and an interactive GUI round out the product, making it one to consider for most any SIEM project.
NetIQ Sentinel v7

S
entinel from NetIQ is one of those security products that is supposed to make administrators feel assured about network events that can indicate trouble. Using the SIEM methodologies, NetIQ’s Sentinel v7 looks deep into Syslogs, simple network management protocol (SNMP) incidents and other event-driven reporting mechanisms to sum up the security health of a network.

Probably one of the newest releases of a SIEM product covered here, v7 of Sentinel was announced on February 28 at the RSA Conference. That means Sentinel should have the latest and most mature features of the lot and should impress most anyone that is looking for the latest in SIEM products.

However, just because something is the newest doesn’t always make it the best. That said, Sentinel 7 does a bang-up job of taming the SIEM beast. NetIQ went for a common thread with Sentinel v7 – ease of use. Indeed, great strides were taken to make the product one of the easiest-to-use SIEM solutions on the market.

One of the first elements of confusion that NetIQ chose to tackle was licensing. The company takes the unique approach of licensing the product based on events per second. In other words, low traffic networks, even those that sport a lot of different components, may be able to get by with a license that just supports 500 monitored events per second. High-value, busy networks may need to go with a license that supports 50,000 events per second. It all comes down to traffic and not physical components.

Other elements that suggest simplicity include plug-and-play deployment, as well as auto-configuration wizards. Sentinel is delivered as a virtual appliance, which can run on virtualized hardware, making it easy to scale the product by just throwing more resources at it. What’s more, the virtual appliance approach makes it easier to backup or transfer Sentinel. It even seems to fit better into a failover or quick-disaster recovery scenario, as well.

The offering comes pre-equipped with packaged intelligence to detect many threats out of the box without time-consuming rule-writing and configuration. Built-in anomaly detection automatically establishes baselines of normal activity and detects changes that can represent emerging threats. New or custom rules can be created easily by business users through an intuitive and easy-to-navigate GUI.

The product is able to gather events from a multitude of sources and quickly analyze those events to present alerts to administrators in a fashion that is both easy to understand and actionable.

Also, Sentinel gathers as much information as physically possible when following an event. Information such as the who, what, when and where is readily preserved for future analysis, making the product suitable for dealing with both insider and outsider threats.

Extensive reporting capabilities are driven by NetIQ Sentinel’s ability to capture rich data, instead of just the ordinary, or basic events, allowing administrators to look at “what-dids,” as well as “what-happened” in an intelligent fashion.

SolarWinds Log & Event Manager v5.3

S
olarWinds is one of the smaller players in the SIEM market, but as a vendor specializing in system management and reporting tools, the company uses its smarts as the intelligence to effectively create a SIEM product.

Nevertheless, SolarWinds has focused on value as the keystone of the company’s SIEM product, which goes by the moniker Log & Event Manager (LEM for short) and is now in v5.3. LEM has a bargain-basement price of $4,495 and is shipped as a virtual appliance. Although the product lacks some features found in other SIEM products, such as Netflow analysis, it remains surprisingly robust. As a virtual appliance, installation proves to be rather simple – it is just a matter of importing the virtual appliance files onto a virtual server and then configuring the virtual server with the appropriate networking and storage configuration. Simply put, installation requires little more than knowledge of how a virtual appliance is added to the network infrastructure.

LEM works with hundreds of different network devices and can import Syslog data, as well as work directly with the log capabilities of dozens of security appliances, firewalls, intrusion detection systems and so on. LEM can gather data from servers, desktops and other pieces of network equipment as well.

Initial configuration proves straightforward, as the company includes hundreds of pre-defined rules and reports that make it easy to get started. The browser-based GUI offers excellent, actionable information in a clean and easy-to-use interface. Setup wizards and best practice tips round out the configuration tasks, allowing most anyone to quickly get the system up and running.

One of the key features of LEM is its ability to visualize events. The product offers a plethora of charts, graphs and more that make it easy for an administrator to observe what is going on across the network. Many of those visualizations support real-time feeds as well. The product includes more than 300 built-in templates for report generation, making it a little easier to satisfy requirements for PCI DSS, Gramm-Leach-Bliley Act (GLBA), Sarbanes–Oxley Act (SOX), NERC CIP, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) reporting.

The product also includes the ability to monitor for specific events and then execute scripts to take action. Administrators also can define notifications based on specific occurrences. Other features include compliance reporting and the ability export out data for further analysis.

A correlation engine rounds out the product’s capabilities, which can process events in real time and in memory, using nonlinear and multidimensional techniques. The tool comes with nearly 700 built-in event correlation rules, potentially saving an administrator hours of work from defining rules.

Like many of the better SIEM products available on the market, LEM not only identifies and reports on anomalous behavior, it is also able to automatically take action to prevent that behavior from increasing and potentially compromising systems further, which means that LEM is able to prevent attacks in real time.
Tenable Network Security Log Correlation Engine v3.6

Log Correlation Engine (LCE) from Tenable has been around for several years and has constantly been improved, enhanced and updated as needed to meet the ever-evolving needs of SIEM. The latest iteration of LCE can be considered something that is part of a bigger picture. Tenable refers to this as a unified security monitoring (USM) approach. Through this option, the company combines security management with log analysis and vulnerability scanning. That said, LCE is still a fine product when used independently of those other capabilities. However, it is nice to now that there is a bigger, integrated picture involved if one is looking to pursue a USM paradigm.

As the name implies, LCE is all about processing system logs and putting some sense to them in the form of intelligence and correlation. Its primary function is to collect, normalize and analyze logs from devices throughout the network. This, in turn, allows it to identify threats and vulnerabilities in real time. LCE accomplishes that by analysis and data correlation from firewalls, intrusion detection and prevention systems, and data disruption prevention solutions, as well as from raw network traffic, application logs and user activity. The product also features an added bonus: the capability to perform traffic inspection, monitoring and analysis via NetFlow data, which many SIEM products cannot do.

Tenable has a focus on performance and claims that LCE can normalize and analyze one billion events in as little as 10 seconds, which speeds remediation efforts. Much of LCE’s capabilities come from an anomaly detection engine that works hand in hand with event correlation to create statistical profiles, which trigger alerts when unusual behavior and never-before-seen events occur.

Simply put, LCE is one of the most sophisticated SIEM solutions on the market. However, that sophistication comes at a price – one that consists of a dedicated Linux (Redhat or CentOS) server and a significant investment in licensing fees. Still, those costs are offset by the high performance offered and the advanced capabilities included in the product.

LCE proves to be one of the more complex products to install and provision, requiring some Linux knowledge and a significant familiarity with networking devices and communications. Nevertheless, that setup complexity is offset by the product’s easy-to-use GUI, which breaks events and devices up into manageable chunks so as to correlate directly with managed assets.

LCE shows real promise when integrated with Tenable’s other products and wrapped under the company’s top-of-the-line SecurityCenter product. Even alone, though, LCE offers some pretty amazing capabilities, such as 3D visualizations, real-time log analysis and intrusion correlation.

It is clear that LCE is designed for larger, more complex, highly active networks where SIEM is just one part of a larger posture. Yet, the product doesn’t require a scientist to understand what is going on. Sure, a medicum of network and security knowledge is required to effectively use LCE, but one can leave the doctorate at the university when looking to leverage LCE’s abilities.

Tripwire Log Center v6.5

Tripwire, a company better known for change management solutions, provides the perfect foundation for SIEM. After all, change management is related to tracking what’s going on via logs, agents and other technologies, just like SIEM solutions do. That is not to say that Tripwire is new to the SIEM market, just that the company’s Log Center product, which is in v6.5, has a great foundation to work from.

Log Center was created by Tripwire to deal with the intricacies of SIEM, which can differ from change management in several ways. First of all, there is more of an urgency surrounding SIEM. In other words, administrators need to know what is happening now as opposed to later during an audit. Log Center accomplishes that real-time data gathering by looking at log activity, such as Syslog updates, simple network management protocol (SNMP) events and so on, to monitor events that fall out of norms or baselines.

Like other products in the SIEM realm, Log Center is part of a larger product line that unifies compliance and security management. Still, the product can be used for the standalone process of SIEM, which many businesses not bound by compliance regulation only look to do.

Log Center goes a few steps further than the typical SIEM. For example, the product offers a capability called system state intelligence, which is context-aware information that combines the security state of a system with customer-specific notions of priority and risk. That may sound complex, but in practice it proves to be a valuable option, which improves security response. Log Center is able to do that, and much else, by relying on more than just native OS auditing, by looking deeper into Syslog, SNMP, Windows Management Instrumentation (WMI) and other events. The tool then takes that raw data and performs real-time analysis to create baselines, as well as detect anomalies. By comparing the raw data against baselines and applying intelligence via defined rules, the Tripwire product can quickly identify breaches or other security threats and alert the appropriate administrator via email or other mechanisms. That creates the opportunity for a faster response to suspicious events, before they turn into full-blown security breaches.

The solution uses an intuitive GUI for management and reporting. However, this interface does not hide the product’s sophistication and always seems to imply that one should be doing more with the product. It is that information overload that can prove both beneficial and detrimental at the same time. However, if Log Center is integrated into Tripwire’s unified security products, the GUI makes a lot more sense and provides drilled-down, resolution-enforcing capabilities that many administrators are looking for with a unified security product.

Installation of the solution is relatively straightforward and wizards are there to help. There are some steep prerequisites though, including the need for an SQL engine of some type and a 64-bit version of Windows Server. However, those requirements do lay out the foundation for installing the rest of the company’s suite of products without having to restart from scratch.

As regular readers know, one of my occasional pet peeves regards the lack of innovation in our field, especially in digital forensics. In this field we tend to see more of the same tired old tools with a few new capabilities or a new point solution to specific forensic problems. But as for a sea change in the core computer or network forensics tools? Not so much.

All of that ended when AccessData introduced FTK 4.0 with Cerberus and Visualization. I almost never say this about a forensic tool, but this one blew me away. The things that you can do with this are so varied and so powerful that I predict it will become the benchmark for computer forensic tools for some time to come.

Cerberus allows one to do a deep analysis of every executable in an image for the presence of malware elements. That wants a bit of explaining. Just because an executable has some malware elements doesn’t mean that it is malware, so the expert knowledge of the examiner comes into play. This tool is not as useful if one doesn’t have at least a modicum of knowledge about malware mechanics. If one does, though, a deep dive into executables is possible, performing both static and dynamic analyses.

Cerberus – named after the three-headed dog of mythology that guards the gates of Hades – dissects every executable in an image and then shows all of the internals, such as memory usage, system calls and more. It scores these so that at a glance one can get an idea of which files need a bit more attention. Then one can drill into the code and Cerberus does all of the reversing and analysis for the user. It really is quite amazing, and it is very powerful if one knows how to take full advantage of it.

But the feature I found most useful was email visualization. Most visualizers break at around 25,000 items. I have a case that has been bedeviling me for some time. There are more than 26,000 emails, so I thought, “What the heck...I’ll just load them up and see where this takes me.” It took quite a while to load – that is a lot of data – but once in, I was able to see things that I had not immediately can put to use back in the core computer or network forensics tools? Not so much.

For example, the social display shows with whom a particular individual has communicated. It gives a strong social network display – a circle with the origin in the center and the recipients toward the perimeter of the circle, closer or further depending on frequency of emails.

All of the difficult mathematical analysis and weightings have been done for the user who is left with only the need to look at the pretty pictures and draw conclusions. Lest that sound as if I am trivializing this impressive tool set, the pictures are pretty, and that is part of FTK’s power. It helps the examiner get to the heart of the matter faster so that the real head work – the deep thinking and analysis that only an experienced examiner can perform – can start sooner, resulting in clearer more cases faster and with a higher percentage of wins. Even though this one seems a bit pricey, for a busy FTK shop – or a shop contemplating moving to FTK – it is worth every penny. I really liked this one and I will be using it in the SC Lab. – Peter Stephenson, technology editor

April

**APRIL**

**» SANS Northern Virginia 2012**

April 15-20

Do you need to become a more effective leader when implementing security improvements for your organization? Are you looking for more in-depth knowledge of the theory and implementation of computer security, virtualization or securing your private cloud? Then, this is the show for you.

Venue: New York

Contact: www.sans.org/

**info/92299**

**SANS AppSec 2012**

April 24-May 2

The theme for this year’s conference is “Application Security at Scale.” With billions of records in the cloud, millions of smart mobile devices, and millions of developers writing new code, what cutting edge techniques are attackers using?

Venue: Las Vegas

Contact: www.sans.org/

info/90589

**» 2012 ASIS NYC Security Expo**

April 25-26

The 22nd NYC Security Conference and Expo is expanding. This year, there is a two-day format, offering more education, additional face time with exhibitors and extended networking. This event attracts attendees from both the public and private sectors who are looking for the latest security solutions, as well as benefiting from the wealth of information provided by security industry leaders. New this year: The ASIS Global Terrorism Conference and the CSO Roundtable Conference are co-locating with the NYC Security Expo.

Venue: New York

Contact: www.asisonline.org

**MAY**

**» SC Congress Canada**

May 8-9

Following up on the success of two previous events, the third annual SC Congress Canada conference and expo, a unique experience for the information security industry, offers up practical solutions to help both public and private sector chief information security officers thwart cyber attackers, safeguard critical corporate and customer assets, come into compliance with countless mandates and, ultimately, contribute to the overall profitability of their organizations. Information security leaders will be on hand to share insider experiences and vast knowledge so attendees will leave the event armed with plenty of actionable information they immediately can put to use back in the office. Speakers to include Rick Yuen, Direct Energy; Craig Gibson, European Union Project MA$IF; Faiza Kacem, National Bank of Canada; Larry Clinton, Internet Security Alliance; Winn Schwartau, M.A.D. Partners; and many others.

Venue: Toronto

Contact: scocongresscanada.com

**JUNE**

**» Compliance Week 2012**

June 4-6

Compliance Week’s annual conference is a peer-to-peer event that spotlights corporate financial, legal, risk, audit and compliance leaders. It has featured the chief compliance officers of Google, Yahoo, HP, GE, Starbucks, Pfizer, PepsiCo, Raytheon, Lockheed Martin, Coca-Cola, Sprint, McDonald’s, Intel, Boeing, Ferrari, Mac, Aftria, Ford, BP, Office Depot, Wal-Mart, and other leading public companies. SC Magazine readers get $400 off. Use code CW12SNDI to sign up.

Venue: Washington, D.C.

Contact: conference.compliance-week.com

**» SANS Forensics and Incident Response Summit 2012**

June 23-27

The fifth annual event will focus on high quality and relevant content, as well as panel discussions in the fields of digital forensics and incident response.

Venue: Austin, Texas

Contact: www.sans.org/

info/98799

**JULY**

**» SANSFIRE 2012**

July 7-15

SANS courses will cover penetration testing and hacker exploits, security, management, wireless, forensics, secure coding and much more.

Venue: Washington, D.C.

Contact: www.sans.org/

info/97901

**AUGUST**

**» WM World 2012**

Aug. 28-30

VMWorld, hosted by VMware, is a virtualization and cloud infrastructure event designed for IT pros seeking to accelerate success in their enterprises while aligning their requirements to enable cloud implementations.

Venue: Las Vegas

Contact: vmworld.com

**SEPTEMBER**

**» SANS Melbourne 2012**

Sept. 3-8

Following requests to bring its technical tracks to Melbourne, SANS is pleased to bring three of its top courses.

Venue: Melbourne, Australia

Contact: SANS.org

Contact: www.sans.org/

info/90539

**ADVERTISER INDEX**

<table>
<thead>
<tr>
<th>Company</th>
<th>Page</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bellevue University</td>
<td>5</td>
<td><a href="http://www.bellvue.edu">www.bellvue.edu</a></td>
</tr>
<tr>
<td>Compliance Week 2012 Conference</td>
<td>19</td>
<td>complianceweek2012.com</td>
</tr>
<tr>
<td>ESET Back Cover</td>
<td>6</td>
<td><a href="http://www.eset.com">www.eset.com</a></td>
</tr>
<tr>
<td>SANS Virtual Conference</td>
<td>7</td>
<td><a href="http://www.sans.org">www.sans.org</a></td>
</tr>
<tr>
<td>SANS Congress Inside Back Cover</td>
<td>8</td>
<td><a href="http://www.sans.org">www.sans.org</a></td>
</tr>
<tr>
<td>Trend Micro Front Cover</td>
<td>9</td>
<td><a href="http://www.trendmicro.com">www.trendmicro.com</a></td>
</tr>
</tbody>
</table>

**FIRST LOOK**

Something new under the sun
David can be Goliath

Be patient and give staffers a real chance to show their stuff, says recruiter Michael Potters.

Unless you are a die-hard Giants or Knicks fan, you did not have a clue who Victor Cruz or Jeremy Lin were until recent events put them in the headlines. Two years ago, Cruz, a great speedster receiver who grew up in the old mill city of Paterson, N.J., went to school at the University of Massachusetts in a season – at 1,536 – and was a big factor in making quarterback Eli Manning look so good in this year’s Super Bowl win over the New England Patriots.

Next we come to Jeremy Lin. Once again, in 2010 Lin goes unwanted at the NFL draft and bounces around the league. The Knicks claimed him off waivers to sit on the bench and essentially be a backup’s backup. He moved to New York and ended up sleeping on his brother’s couch in Manhattan since he undoubtedly thought, “No way am I buying a condo in the city if I am going to be cut.” It’s likely you’ve since heard of his remarkable run and the excitement, and wins, he’s brought to a formerly mediocre team. A few weeks ago no one had any idea who this person was.

And now for the lessons learned. If you are a looking to hire an IT security professional to run your network or protect your data: Look outside the box. Not all the successful recruits come from the best schools or the top companies: 32 NFL teams and 30 NBA teams passed on these guys, despite all of their high-paid research.

Be patient, give people a real chance to show their stuff: The NBA’s Warriors and Rockets are shooting themselves now for having Lin and letting him get away. When you realize you may have a gem, let them loose to succeed. Don’t become an impediment to their growth. Further, make sure your team embraces their success, and all raise their games accordingly.

It’s also a good idea to not be cheap. Just because you lucked out and hired a particularly bright and energetic person at a steal, pay them what they should be paid – or you will lose them as easily as you found them.

Meanwhile, if you are a candidate looking to break into this demanding field, don’t ever believe that you can’t compete with the big players from the better colleges or companies. You can. Fifty percent of the top people in the IT security industry fit into this category. As well, if given the chance by a client, don’t blow it. Work hard, perfect your craft, and when the door opens a crack, kick your way through and do the job better than you ever imagined.

However, don’t be greedy. If the only way into the firm is to take a lower-than-desired fee, do it. You can prove yourself once you are in there and then potentially, at least, make all the money you deserve. And, don’t be selfish. Look to make your team better around you. They will appreciate it and pay you back by making you look better – which will, of course, earn you more money and a stable career.

Final message to hiring authorities: Two years ago, the general manager of the Giants had no idea who Victor Cruz was. A few weeks ago, the general manager of the Knicks had little clue who Jeremy Lin was. They both look like geniuses now and are likely going to be rewarded for the serendipitous nature of these events. Think outside the box.

Michael Potters is CEO and managing partner of Glenmont Group, a Montclair, N.J.-based recruitment firm.
Thank you!

SC Magazine readers choose ESET No.1
Best Anti-Malware Management

And the best keeps getting better—IT experts everywhere agree.

© 1999-2012 ESET. All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET. All other names and brands are registered trademarks of their respective companies.