TRANSFORMING TRADITIONAL SECURITY STRATEGIES INTO AN EARLY WARNING SYSTEM FOR ADVANCED THREATS

Big Data Propels SIEM into the Era of Security Analytics

September 2012

Author Commentary

> "Today the capacity of most SOCs to detect events inside organizations is not up to par with the state of the threat. We're typically finding threats not on the way into organizations or once they're already in the network, but after the exploit has occurred and the data is already out."
>
> Dean Weber, Chief Technology Officer of Cybersecurity, CSC

EXECUTIVE SUMMARY

In the past few years, a stunning range of government agencies and prominent corporations have succumbed to stealthy, tailored cyber attacks designed to exploit vulnerabilities, disrupt operations and steal valuable information. Clearly current security systems are not up to the task of thwarting these advanced threats, since many of their victims had what they considered state of the art detection and prevention systems. These systems failed to stop or sense the presence of an attack on victims' networks until the damage was done.

Given today's threat environment and the increasing openness and connectivity of digital infrastructures, security teams now realize that they must assume their IT environments are subject to periodic compromise. Gone are the days when preventive measures to secure the perimeter or trying to detect malware problems using signature-match technologies were enough. New practices based on an understanding of the phases of an attack, continuous threat monitoring, and rapid attack detection and remediation are required.

To develop the visibility, agility and speed to deal with advanced threats, traditional security strategies for monitoring, often based around security information and event management (SIEM) systems need to evolve into a central nervous system for large-scale security analytics. In particular, four fundamental capabilities are required:

1. Pervasive visibility – Achieving the ability to know everything happening within IT environments requires fusing many data sources, including network packet capture and full session reconstruction, log files from network and host devices and external information such as threat indicators or other security intelligence. Centralized log collection is no longer enough.

2. Deeper analytics – Examining risks in context and comparing behavior patterns over time across disparate data sets improves the signal-to-noise ratio in detecting advanced threats, thus speeding time to resolution.

3. Massive scalability – Platforms collecting security data must expand in scale and scope to handle the deluge of information that's increasingly needed for complete situational awareness.

4. Unified view – Consolidating security-related information in one place is crucial to investigating incidents in context and speeding decision making about prospective threats. The unified view should also enable compliance to be an outcome of a good security strategy, not a competitor to it.

Security operations centers (SOCs) need advanced analytical tools that can quickly collect and sift through security data to present the most pressing issues in context. New security analytics platforms are emerging to handle all the functions of traditional SIEM systems and far, far more – including speeding detection of advanced threats so organizations have a chance to stop covert attacks.

RSA Security Briefs provide security leaders and other executives with essential guidance on today's most pressing information, security risks and opportunities. Each Brief is created by a select response team of security and technology experts who mobilize across companies to share specialized knowledge on a critical emerging topic. Offering both big-picture insight and practical technology advice, RSA Security Briefs are vital reading for today's forward-thinking security practitioners.

Contents

Authors

Brian Girardi, Senior Director of Product Management, RSA, the Security Division of EMC

David Martin, Vice President, Chief Security Officer, EMC Corp.

Jonathan Nguyen-Duy, Director of Global Security Services, Verizon Enterprise Solutions

Mario Santana, Vice President of Secure Information Services, Terremark, a Verizon Company

Eddie Schwartz, Vice President and CISO, RSA, the Security Division of EMC

Dean Weber, Chief Technology Officer of Cybersecurity, CSC

TODAY'S SECURITY SYSTEMS FOCUS ON YESTERDAY'S PROBLEMS

Unpredictability is the golden rule that today's attackers live by. Defenders must be agile in response.

In the past, preventing threats came down to a game of cat and mouse between security vendors and attackers. A threat would be developed by an attacker and, once identified in the wild, vendors would then release signatures to their customers so that the malware was stopped at the proverbial front door. When that happened, attackers would then mutate the threat slightly to evade detection, but that didn't last long: vendors' threat analysts examined traffic, spotted instances of the new variant and blocked it accordingly. Corporate security teams would make sure they kept their patches and security signatures up to date, and aside from the occasional zero-day vulnerability, this perimeter-defense approach was largely considered effective.

Today this has changed, largely due to two drivers: the rise of APTs and similar advanced threats; and the increasing openness and connectedness of digital infrastructures. The Security for Business Innovation Council defines advanced threats as cyber attacks custom-designed to breach an organization's defenses in order to steal valuable information such as intellectual property, plant false information, disrupt strategic services, damage systems or monitor operations or actions. These advanced threats are the work of hacktivists, nation states, criminal enterprises and other groups with deep funding and specialized security expertise.

Today's attackers aren't deterred by the traditional perimeter and signature-based defenses described above. They conduct reconnaissance on an organization's security systems, personnel and processes and develop techniques to exploit them. Through social engineering, escalation of privileges and other forms of probing, attackers gain access to sensitive system resources. They move patiently through an organization's network – taking days, weeks or months to accomplish their objectives – in order to avoid detection. Then, when the time is right, they execute the final stages of their attack.

Security breaches that could indicate continued growth in advanced threats appear to be on the rise. The Verizon 2012 Data Breach Investigations Report tracked 855 breach incidents in 2011, representing 174 million compromised records. That's the second-highest annual data-loss total since Verizon began tracking breaches in 2004.

What's more, many organizations today continue to lump security with (or under) compliance programs. However, the slow, structured nature and codified expectations of compliance activities often do little to protect IT environments from attack. Companies must rethink their risk management priorities to reflect today's higher chances of cyber attack. They must also re-think their security strategies to deal with the unknown or unpredictable attacks, or expect to suffer the consequences of a breach.

Progress begins with admitting the likelihood that IT environments have already been infiltrated. This change in outlook shifts the goal of security from primarily attempting to protect the perimeter to detecting threats early and minimizing damage from a prospective breach.

Once the security playing field shifts from the perimeter to the heart of the organization, security professionals can focus their efforts on gaining situational awareness to monitor and protect their organization's most important assets.

Author Commentary

"If you think about today's threats, it's no longer the good guys fighting against some mass-attack computer worm or virus, it's now the good guys against the bad guys – actual humans targeting an environment, and that's why all the classical automated defense methods fail. In a battle of creativity, humans will win out over machines."

Mario Santana, Vice President of Secure Information Services at Terremark, a Verizon Company

"What's needed is a lot of new security skills and getting people to think in different ways. Stop thinking about having to block threats, but instead figure out how to detect what has probably already happened and what to do next."

Dave Martin,
Chief Security Officer, EMC

SIEM ESTABLISHES A BASELINE FOR SECURITY MANAGEMENT

Security Information and Event Management (SIEM) systems were designed to offer a central place to gather and store security data (largely log and event information only) in order to streamline security-incident management and compliance reporting. These systems collect security alerts and logs generated by applications and systems on the network, ranging from network devices, storage and databases to firewalls, intrusion prevention systems and anti-virus software. SIEM systems help reduce the time security analysts must spend on chasing down information, allowing analysts to reallocate their time instead toward remediating incidents. Today, about one-third of enterprises have adopted security information management systems, with incident investigation and compliance as the top drivers behind the decision to adopt, according to a recent report from Forrester Research.[1]

SIEM systems today effectively perform several key security and compliance functions:

- Reporting on device activity in order to provide key insights into who, what, where, and when critical activities took place;
- Establishing "normal" baseline levels of activity for the entire IT operation, making unusual levels and types of activity easier to detect;
- Correlating event information, so that security experts don't have to wade through each of the countless security alerts that are set off daily by the many devices and applications on an organization's network;
- Following rules predefined by security experts to screen for potential threats. Rules can also be used to weed out irrelevant alerts, improving the signal-to-noise ratio and greatly reducing the number of events that must be investigated;
- Collecting log data in a central location where it can be reviewed, reported on and stored for compliance and longer-term forensic purposes;
- Providing proof of compliance for internal and external auditors through the automated generation of regular reports.

These are essential functions for any security and compliance program. In fact, some experts say if an organization can only embark on one detection-oriented security initiative, it should be to use SIEM systems to gather and correlate security–related data, which can help spot many problems.

Unfortunately, in order to deal with the high-stakes risks posed by advanced threats, conventional security approaches anchored by SIEM systems are not enough. Traditional SIEM capabilities remain necessary, but are insufficient.

Author Commentary

"Traditional SIEM capabilities are still required to alert us when a problematic pattern is detected and to present organizations with as much value from the data as possible – that can't go away. But there's much that needs to be added to SIEM to provide broader visibility and a richer context for evaluating the threat."

EDDIE SCHWARTZ, CHIEF SECURITY OFFICER, RSA, THE SECURITY DIVISION OF EMC

ADVANCED THREATS REQUIRE ADVANCED SECURITY

New security capabilities are needed to complement new mindsets and to pick up where traditional security approaches leave off.

Traditional log- and event-centric SIEM systems often provide an incomplete picture of the risks facing an organization. That's because SIEM tools only collect information from portions of the IT infrastructure, leaving critical blind spots.

No longer can an organization's security operations center (SOC) rely on device logs alone to get a reliable picture of what's happening. In order to spot anomalies, a SOC analyst may need to cross-check other types of data – the job function of the owner of a laptop connected to a critical server, for example – and have that information in a central

[1] Forrester Research, Inc., "Dissect Data to Gain Actionable Intel," August 2012

location where it can be paired with traditional security data. SOCs that see value in using diverse sources of information to detect advanced threats are now faced with a big data problem: how do they collect and analyze these data sets that traditional security solutions don't take into consideration?

Author Commentary

"Breaches aren't really smash and grab anymore. The vast majority of breach and compromise cases last year occurred over a period of months. Our experience shows it's more valuable to get a complete view of what happened over the long haul and take mitigation steps than to get a near real-time analysis of events."

Jonathan Nguyen-Duy,
director of global security services,
Verizon Business

With current SIEM systems, SOC analysts are caught in a quandary – they don't have all the data at their fingertips necessary to get a complete picture of their environment, but they can't use all the data they do have because SIEM tools can't handle it from a performance standpoint. The tools may tell them that a malware signature has been matched, but what is the business impact of that malware? How critical is the infected system? How did it get infected? What else has been infected by that malware? Has any sensitive data been moved or impacted? Traditional tools don't present security information in meaningful, actionable ways, and they lack clean interfaces and visualization capabilities that operate the way security analysts think. Because of this, organizations that use SIEM systems today are often only getting a fraction of the desired value out of these tools.

This is a critical problem. Since the SOC is an organization's last line of defense against attacks, security analysts need to have the greatest range and depth of actionable information available to them. SIEM must rise to a higher level of utility to help security analysts do their jobs more efficiently and effectively.

With so much at stake, organizations must also honestly assess their security maturity and understand the risks they face to determine if they are best served operating their SOCs internally, outsourcing to managed security service providers (MSSPs) or taking a hybrid approach.

TRANSFORMATION OF TODAY'S SIEM TOOLS INTO A COMPREHENSIVE SECURITY ANALYTICS PLATFORM

Today's SIEM systems cannot keep up with the volumes and variety of security-related information, especially as organizations add infrastructure, applications and even cloud services to their IT environments. To help organizations achieve the goal of full situational awareness, SIEM tools need "big data" analytics – the ability to work with data sets that are orders of magnitude larger, more diverse and more dynamic than the security information collected by most organizations today. Data analytics tools also need to integrate threat intelligence from external sources, which could provide rich context to help speed detection of attacks.

Author Commentary

"SIEM today doesn't provide the visibility, the breadth and depth of information to truly identify threats as they're happening. We need more complete data sources and visibility into networking data, which means the way we keep, manage, process and model data must change. We need to make it more consumable – not just more data, but better data."

Brian Girardi,
Senior Director of Product Management,
RSA, the Security Division of EMC

To develop the intelligence, visibility, agility and speed to deal with advanced threats, SIEM systems must evolve into a central nervous system for large-scale security analytics. The next evolution of SIEM must deliver strong capabilities in four key areas.

Pervasive Visibility

Before organizations can stop stealthy cyber attacks, they first must be able to see them. Security analytics platforms should enable full reconstruction of activity to ensure SOC analysts have all available information to decide how best to react to potential problems. Full network packet capture, when combined with logs, events, threat intelligence and other data sources, enables a deeper view of security threats by:

- **Identifying malware** – Threats are increasingly difficult to identify because they're masked to resemble legitimate traffic traversing networks. Full network packet capture collects and reconstructs files and then automates much of the analysis required to spot telltale signs of malicious intent;

- **Tracking attackers' activities inside the environment** – Once inside an organization's network, attackers often move among systems to gather information required to mount an attack. Because endpoints are often left unmonitored, full network packet capture becomes an essential means for spotting attackers' lateral movements, all of which traverse the organization's network;

- **Presenting proof of illicit activity** – Systems capable of full network packet capture record full sessions to show an attacker's exact activities, including any exfiltration of data. Since many advanced threats go undetected until after the damage is done, security analysts need a way to assess the damage. Reconstructing the attack is often the most effective way to conduct post-attack analyses and forensic investigations.

Adding full-network packet capture and session reconstruction to the next generation of SIEM is essential for security analysts to investigate and prioritize threats. For example, today's traditional SIEM tools can say "I know your PC was talking to a malicious server," but can't tell what passed between them. Packet capture and session replay, when combined with log-based and other information, can provide deeper insight into what transpired, so security analysts can assess whether or not the activity was significant. Such detailed forensic capabilities can help SOCs move threat detection further up the "kill chain" and mitigate damage from advanced threats.

Deeper Analytics & Faster Investigations

Security analytics systems should have the sophistication to combine disparate data to detect indicators of advanced attacks. For example, security analytics systems should search for behavior patterns and risk factors, not just static rules and known signatures. Security analytics systems should also consider the relative value of enterprise assets at risk, flagging events associated with high-value assets.

By applying a risk-based approach leveraging big data, security analytics platforms can eliminate "known good" activities and improve the signal-to-noise ratio, slashing the amount of information that security analysts must review in their hunt for new threats to the enterprise. Deeper, automated analytics present items of interest to security analysts, reporting "this happens a lot" or "this rarely happens." By doing this, security analytics systems can perform triage for security analysts, highlighting events that require a closer look.

While automated, intelligent analytics are an important component of new security analytics platforms, they don't take the place of human judgment; instead they spotlight areas where human judgment, with its unique organizational and domain expertise, should be applied. In essence, security analytics systems help SOCs scale their threat detection capabilities in ways that weren't possible before, helping analysts make sense of incidents in time to make a difference in the outcome of an advanced attack.

Massive Scalability

As SIEM systems evolve into security analytics platforms, they must expand in scale and scope to handle the enormous variety and volume of security-related data from both inside and outside the organization. Looking deeper into traffic from many types of devices and from across the network multiplies the amount of data that security analytics platforms must handle. And while the fusion of up-to-the-minute threat intelligence from outside sources transforms a security console into a security intelligence center, it also compounds data scalability challenges.

To deal with today's threats, security analytics platforms must include features such as a distributed n-tier storage architecture and an analytics engine that normalizes and processes large, disparate data sets at very high speed. Data storage and analytics must scale together linearly.

Unified View of Critical Security Information

To be fully informed and view events in context, security analysts need all the security information available at any given moment. Beyond collecting data from the network, security analytics platforms should automatically integrate up-to-the-minute threat intelligence from vendors, federal agencies, industry associations, open-source intelligence and other sources. By providing all potentially relevant information at security analysts' fingertips, the platform avoids the time-consuming task of analysts collecting this information manually. Centralizing the wealth of applicable intelligence in a unified analytics platform is crucial in providing a timely view of the IT environment, putting events into context, and speeding analysts' decision-making processes. And by providing appropriate correlations and context, the security analytics platform can serve to demonstrate compliance with appropriate security regulations and practices.

Traditional SIEM's strengths	SIEM's limitations	Security analytics expands SIEM's strengths and addresses limitations
Automates collection, archiving and reporting of log and event data from many different sources, from network devices and servers to firewalls and anti-virus software	The data architecture of traditional SIEM systems weren't built to handle the huge variety and volumes of security information now available and that are needed to attain sufficient enterprise visibility	Provides a distributed data architecture to collect security data at "big data" scale (hundreds of terabytes and beyond). Such platforms also normalize and analyze these massively large, disparate data sets at very high speed
Creates a unified repository for security-related data, giving SOC analysts centralized access to data needed for investigations	Even though SIEM systems collect logs and events from a wide variety of systems, its visibility is confined to the data contained in collected logs, which often cover only a small fraction of potentially relevant activity	Captures network traffic, with some advanced security analytics platforms even offering full network-packet capture and session reconstruction to detect and investigate how attackers infiltrated the IT environment and what they did once inside. Also, advanced security analytics platforms automatically ingest threat intelligence from external sources, providing valuable views of the threat environment outside the enterprise
Unifies log data to help create a comprehensive repository for key security-oriented data	While SIEM systems are rich in data, they're often poor in usability. Most are weak in their ability to support analysts in time-sensitive incident investigations	Delivers the high performance needed for ad hoc investigations, as well as provide a user interface built to complement how security analysts conduct investigations
Provides out-of-the-box control reports, which can be important contributors to proving compliance with government and industry regulations	Proving compliance, while necessary, does not control security risks or enhance the security position of the organization	Provides proof of compliance as an outcome of a security-focused program
Provides a basic alerting on known sequences through correlation rules	Detection relies on having attack signatures or knowing methods of attack in advance. With advanced threats there are often no existing signatures and exact attacker behavior is hard to predict in advance	Creates a unified platform for collecting security data from across the environment. Detection is not based on signatures or static correlation rules but on dynamic comparisons to normal baseline behaviors and to suspicious activities that may be indicative of attackers. This speeds identification of active threats for which there's no signature and reduces the number of incidents analysts must investigate

CONCLUSION

Successful security leaders know they must operate under the assumption that their IT environments have been infiltrated. The challenge lies in finding where the greatest dangers are hidden.

Traditional security tools are adept at following rules set by security personnel ("look for this, not that"). By contrast, security analytics platforms find anomalies of which analysts weren't even aware. Human involvement will always be required, but security analytics systems expand the field of vision while narrowing the field of threats to drive fast and accurate decision-making.

Security analytics systems give organizations the situational awareness and decision-support capabilities required to keep advanced threats from doing harm and to confer significant business benefits besides just protection. By integrating these capabilities into one unified security solution, the total cost of ownership decreases while the usefulness of the platform goes up. By investing in security analytics rather than a traditional SIEM solutions, organizations "future proof" their platforms for the escalating threat environment, while gaining a highly scalable information repository that can serve many disparate functions and business units. By automating tasks and lending context, security analytics platforms make SOC analysts more productive. And by focusing efforts on defending an organization's most valuable assets, security becomes more strategic to the organization.

ABOUT THE AUTHORS

Brian Girardi
Senior Director of Product Management,
RSA, the Security Division of EMC

Brian Girardi oversees development of advanced security analytics and management solutions within RSA, the Security Division of EMC. He joined the company when EMC acquired NetWitness in 2011.

As a founding employee in NetWitness, Mr. Girardi was responsible for many of the analytical concepts and methods that make up the NetWitness technology platform today. At NetWitness, he was responsible for strategic product positioning and marketing, technology strategy, defining product functionality and driving product launches.

Mr. Girardi has spent more than 13 years working in information security, providing innovative solutions and services to federal law enforcement, the U.S. intelligence community and commercial enterprises. He is a published author and patented inventor in the field of information security. Mr. Girardi holds a B.S. in Mechanical Engineering and an M.S. in Electrical Engineering from Virginia Tech.

David Martin
Vice President,
Chief Security Officer,
EMC Corp.

David Martin manages EMC's industry-leading Global Security Organization focused on protecting the company's multi-billion dollar assets and revenue. As EMC's most senior security executive, he is responsible for establishing EMC's brand of trust with its customers and for providing business protection operations worldwide.

Mr. Martin is a Certified Information Systems Security Professional and brings a range of experience to EMC in information security and management developed through more than a decade of professional business protection experience from various roles in internal audit, security services development and consulting.

Prior to joining EMC, Mr. Martin built and led security consulting organizations, focusing on critical infrastructure, technology, banking and healthcare verticals, where he developed and delivered enterprise security programs, incident response, investigations, policy and assessment practices.

Mr. Martin holds a BEng in manufacturing systems engineering and provides frequent testimony to the U.S. Congress and government agencies as an expert witness on corporate enterprise protection issues.

Jonathan Nguyen-Duy
Director of Global Security Services,
Verizon Business

Jonathan Nguyen-Duy leads managed security services product management at Verizon Business. He is responsible for developing security solutions that address a wide range of threats and compliance requirements. In the past three years, his team has developed anti-DDoS, reputational intelligence correlation and a new generation of cloud-based security services. During this time, Verizon grew to be recognized as security industry leader and the world's largest provider of managed security services.

Prior to his current role, Mr. Nguyen-Duy was responsible for the development of Verizon's business continuity practice, physical security solutions, managed storage and hosting services. Before joining Verizon, he served as the Regional Director of Operations for Central America with the U.S. Foreign Service. Mr. Nguyen-Duy has over 15 years of experience in information security and risk management – helping enterprises and government agencies address issues involving armed conflict, civil strife, labor strikes, natural disasters, terrorist attacks, power outages, pandemic disease, industrial espionage and a wide range of cyber security threats.

A recognized expert in security and continuity-of-operations, he is a regular speaker at industry events and serves on several security task forces. Mr. Nguyen-Duy holds an MBA in IT Marketing and International Business, as well as a BA in International Economics from the George Washington University.

Mario Santana
Vice President of Secure Information Services, Terremark, a Verizon Company

Mario Santana joined the Secure Information Services (SIS) group at Terremark Worldwide in January of 2006. There, he leads the analytics team within SIS, and consults with Terremark clients on topics of security, technology and risk management. Following Terremark's merger with Verizon in 2011, Mr. Santana worked to build and integrate a new high-performance security organization, redesigned strategies, streamlined operational processes and retained elite personnel.

Formerly, Mr. Santana founded an identity management technology company, consulted for SteelCloud, Inc., and worked in IT for over 25 years. Mr. Santana has worked with numerous Fortune 1000 organizations worldwide, including financial, health care and educational institutions, airport security and airlines, retail conglomerates, and technology and legal firms. He has led projects and engagements around such security and risk management concerns as corporate governance; forensics and electronic discovery; incident response; intellectual property fraud; insider incidents; and the assessment of networks, systems and applications. His specialties include threat awareness, assessment and mitigation, network instrumentation, security administration and compliance.

Eddie Schwartz
Vice President and CISO, RSA, the Security Division of EMC

Eddie Schwartz is Chief Information Security Officer (CISO) for RSA and has 25 years of experience in the information security field.

Previously, he was a co-founder and the chief security officer of NetWitness (acquired by EMC), CTO of ManTech, EVP and General Manager of Global Integrity (acquired by INS), SVP of Operations of Guardent (acquired by VeriSign), CISO of Nationwide Insurance, a Senior Computer Scientist at CSC, and a Foreign Service Officer with the U.S. Department of State. Mr. Schwartz has advised a number of early stage security companies, and served on the Executive Committee for the Banking Information Technology Secretariat (BITS).

Mr. Schwartz has a B.I.S. in Information Security Management and an M.S. in Information Technology Management from the George Mason University School of Management.

Dean Weber
Chief Technology Officer of Cybersecurity, CSC

Dean Weber is a director and Chief Technology Officer for CyberSecurity at CSC, where he provides vision and guidance for solution development and support for strategic cyber security initiatives.

With more than 30 years of experience in information and physical security, Mr. Weber joined CSC after serving as Chief Technology Officer at Applied Identity, which recently was sold to Citrix. Earlier, he was Chief Security Architect at Teros, a leading manufacturer of application security gateways, also acquired by Citrix. He was responsible for developing and implementing solution deployments, including assessment and intelligence gathering at TruSecure/ICSA Labs (now Verizon Business Security Solutions). Mr. Weber helped found a large Midwestern reseller-integrator specializing in secure architectural design and deployment for both public- and private-sector clients, and he served for many years as its technical vice president. Additionally, he spent several years in the U.S. Navy working in physical and electronic security.

Mr. Weber is a frequent speaker at information security events such as InfoWorld, ITEC, InfoSec Europe, InfraGard, Secret Service Security Roundtable, ISSA and various focus engagements.

SECURITY SOLUTIONS

The products and services described below align with the guidance described in this RSA Security Brief. This is not a comprehensive list of applicable solutions; rather, it is a starting point for security and risk management practitioners interested in learning about some of the solution and service options available to them.

CSC's Managed Security Services

CSC's Managed Security Services are delivered through integrated security operations centers across the globe and provide a compelling alternative to self management of security functions. CSC's Managed Security Services enable organizations to most effectively meet their security obligations in an environment of constrained budgets, limited skilled resources, tightening regulatory mandates and an escalating threat landscape. A holistic set of offerings provide tailored cyber protection, ranging from core monitoring and management to the most sophisticated analytics and state of the art cyber security protection through advanced threat detection, global threat intelligence, situational awareness and governance risk and compliance capabilities. CSC today is one of only a few vendor-independent managed security services providers for mid-market and large enterprises, integrating the best available tools from a broad spectrum of leading vendors with CSC's intellectual property.

RSA® Security Analytics

The RSA® Security Analytics solution is designed to provide organizations with the situational awareness needed to deal with their most pressing security issues. By offering enterprise-wide visibility into network traffic and log event data, the RSA Security Analytics system can help organizations gain a comprehensive view of their IT environment, enabling security analysts to prioritize threats quickly, investigate them, make remediation decisions and take action. The RSA Security Analytics solution's distributed data architecture is engineered to collect and analyze massive volumes of information – hundreds of terabytes and beyond – at very high speed using multiple modes of analysis. The solution is also capable of integrating external threat intelligence about the latest tools, techniques and procedures in use by the attacker community and of helping organizations track and manage responses to security issues identified through the solution. The RSA Security Analytics platform is planned for commercial release in late 2012.

Verizon's Managed Security Services

Verizon is a global IT, security, and communications partner to business and government with one of the world's most connected public IP networks. Verizon offers the most comprehensive set of managed security services, backed by more than 1,200 experts in 30 countries. Verizon employs its proprietary State and Event Analysis Machine (SEAM) correlation and classification technology to filter out millions of benign security events and escalates only incidents that are more likely to pose a threat. This technology, combined with a vast amount of threat and vulnerability intelligence generated by Verizon's expansive global network, allows the company to address a wide range of cyber threats and compliance requirements. That's why Verizon is considered a security leader by analyst firms such as Gartner, Forrester, Frost & Sullivan and others. It's also why thousands of enterprises and government agencies rely on Verizon to help secure business data and the infrastructure that delivers it, as well as address security standards and regulations.

ABOUT RSA

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance management solutions for business acceleration. RSA helps the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, encryption & key management, SIEM, Data Loss Prevention and Fraud Protection with industry leading eGRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

www.rsa.com