BUILDING AN INTELLIGENCE-DRIVEN SECURITY OPERATIONS CENTER

June 2014

KEY POINTS

- Cyber attacks and intrusions are almost impossible to reliably prevent, given the openness of today's networks and the growing sophistication of advanced threats. In response, the practice of cyber security should focus on ensuring that intrusion and compromise do not result in business damage or loss.
- Organizations need to shift more security resources from preventing intrusion toward rapid threat detection and remediation.
- Improving threat detection and response requires an intelligence-driven security approach, which helps organizations use all available security-related information from both internal and external sources to detect hidden threats and even predict future ones.
- Optimizing how security technologies, personnel and processes work together is pivotal to scaling security capabilities to the mounting risks posed by advanced cyber threats—all while delivering efficiency and value back to the organization.
- Technology automation can help analysts make the most of their time by slashing the workload for closing routine, lower-level incidents. Automation frees up analysts to focus on higher-priority risks affecting the organization's most critical assets.
- Configuring security processes to automate repetitive tasks and integrate related workflows is potentially the most beneficial step that security operations centers (SOCs) can take to boost productivity, enforce policies and implement best practices for threat detection and response.
- SOCs will need to build collaborative, cross-disciplinary teams with highly specialized skill sets to combat advanced cyber threats. The security industry, however, faces a serious shortage of skills and qualified personnel. Leveraging the latest technology for time-saving automation and supplementing in-house capabilities with outsourced expertise can help organizations manage skill and resource gaps.
- Results from best-in-class security operations teams illustrate the impact of optimizing the interplay of people, processes and technologies in security operations. By aligning behind an intelligence-driven security program, leading organizations can achieve results such as reducing the average time for resolving incidents by up to 60 percent.

Contents

Perfection in security—the no-breach goal—is not only impossible but also impractical. That's because sophisticated adversaries have learned to craft their attack techniques to get around preventive security measures such as antivirus, firewalls and passwords. Adversaries also take great care to cover their tracks and stay hidden within IT environments, sometimes for weeks or even months after gaining entry. The complexity of most enterprise IT environments, combined with the prevalence of cloud and mobile services and the expanding accessibility of enterprise networks to outside parties, gives attackers many places to hide and even more points of potential intrusion.

Despite rising cyber risks and attacks, security teams face persistent budget and resource constraints in protecting the organization's prized information assets. Security spending as a percentage of IT spending has gone from 6.0% in 2008 to 5.6% in 2012, according to a Gartner report that benchmarks security expenditures and staffing.[1] In the same report, Gartner reported declines in security spending from $636 per employee in 2008 to $577 per employee in 2012. These trends indicate that security teams must learn to do more with less.

Most security spending is still invested in a multitude of perimeter-based, prevention-focused tools that advanced cyber attacks have made largely obsolete. Cyber security's most pressing goal, now and for the foreseeable future, should be to prevent business damage or loss, not to prevent intrusion and compromise.

The best way to prevent business damage is to detect and remediate cyber attacks quickly. To do this, organizations should allocate a greater share of their security investments to enhancing capabilities in threat detection and response. First, they must gain full visibility into what's happening in their IT environments. Then, they must expand their view to include outside threat intelligence. Organizations will have to learn to use new types of security data—and much more of it.

1 Gartner Inc., "IT Key Metrics Data 2013: Key Information Security Measures: Multiyear" (14 Dec. 2012), pp.

LEVELING THE THREAT LANDSCAPE WITH BIG DATA ANALYTICS

A new generation of security tools uses innovative techniques to collect and analyze massive amounts of data: data from PCs, mobile devices and servers; data from internal networks, including the composition and content of network packets; and threat intelligence about attacks on other organizations and the tools and methods used. In addition to analyzing these traditional information sources, "big data" security tools also can ingest information from non-traditional sources such as building key card scanners, personnel records and even Microsoft Outlook® calendars. Such data may be used, for instance, to assess the legitimacy of remote log-ins by employees.

The heightened visibility provided by the big data capabilities of new security analytics platforms create unprecedented opportunities to identify anomalies, uncover evidence of hidden threats or even predict specific, imminent attacks. More data creates a richer, more granular view: it presents the threat landscape in high definition, as opposed to grainy black-and-white. Security-related details can be seen in sharper focus and irregularities can be found faster. Also, because security analytics platforms integrate threat intelligence from outside sources, organizations see the threat landscape as a panorama, not just from the narrow aperture of their own internal IT environments. Enhanced visibility will lead to enhanced security capabilities, vastly expanding options for how security operations centers (SOCs) act and respond to prospective threats.

Technology advancements in big data and security analytics systems are beginning to deliver "imagine if" capabilities. The bounds of what's imaginable are now being explored by security operations professionals and business leaders together.

For organizations concerned about advanced cyber threats, these "imagine if" scenarios often focus on injecting better intelligence and context into security practices. For example, if we apply new analytic approaches to historical data, what could we learn? What do the cyber attacks we've encountered tell us about our business and operational risks? If we add new log sources or external intelligence feeds to our data warehouse, what patterns could we look for that we couldn't even imagine seeing before? What types of intelligence might help us hunt down threats faster?

The Security for Business Innovation Council, a group of top security executives from Global 1000 enterprises, advises organizations to take a data-intensive approach called "intelligence-driven security" to protecting critical information and business assets.[2] Intelligence-driven security practices help organizations use all the security-related information available to them, both internally and externally, to detect hidden threats and even predict future ones. Intelligence-driven security calls for organizations to reduce their reliance on perimeter defenses and signature-based scanning tools, which only identify modes of attack that have been encountered in the past. Instead, organizations should look for suspicious activities and patterns atypical for their environment—subtle indicators much harder to detect than matching a malware signature.

Implementing intelligence-driven security will require SOCs to examine their organizations as a holistic system and to bring security tools, processes and personnel into tight alignment. Aligning people, processes and technology in and around a SOC is essential to scaling security capabilities to the mounting risks posed by advanced cyber threats—and to do it within perennial time and budget limitations.

2 For guidance on implementing intelligence-driven security programs, please read the Security for Business Innovation Council's report "Getting Ahead of Advanced Threats: Achieving Intelligence-driven Information Security" on EMC.com.

ALIGNING PEOPLE, PROCESS AND TECHNOLOGY TO SCALE SECURITY TO THREATS

The complex interplay among people, process and technology in security operations makes it challenging to adjust any one element without also adjusting the others. Harmonizing tools, skills and methodology in security operations is essential to providing defense-in-depth and to protecting the organization's critical information assets. Additionally, perfecting the people-process-technology triad can unlock operational efficiencies by automating routine tasks and streamlining workflows. The result is that security analysts will spend far less time tracking down information for an investigation or researching the status of an incident. Instead, they can focus their time on enriching intelligence sources, uncovering subtle irregularities in their IT environments that point to serious problems, or hunting down covert threats faster.

Putting the right mix of technologies in place that work well together as part of an intelligence-driven security program can be challenging. Nevertheless, the technologies now available to SOCs may be the most mature piece in the people-process-technology triad. While new tools such as security analytics platforms hold great promise, they're only as good as the people using them and the operational best practices put in place to help the larger organization work effectively and efficiently together.

From consulting with hundreds of customer organizations, RSA believes people and process are often harder to align behind an intelligence-driven security approach than the technology. That's because developing, testing and instituting new procedures for managing and responding to security incidents takes specialized expertise and time. It also takes time for security operations personnel to learn their organization's critical business processes well enough to defend them from attack.

Optimizing the interplay of people, process and technology will be different for every SOC, depending on the unique conditions and needs of their organizations. Regardless, common guidelines can apply to most SOCs striving to implement an intelligence-driven security approach.

Technology Alignment: Big Data and Automation

When aligning technology to an intelligence-driven security program, a good starting point is to take stock of the organization's existing security tools and information assets. Is the organization making the most of what it has? How effective are technical assets in serving their intended functions?

After an initial technology inventory comes an exploration of how security could be improved if new capabilities were added. Apart from acquiring new tools, new capabilities can sometimes be derived by using existing data in new ways. Capabilities expansion could also be a matter of extending the SOC's visibility into organization's networks, both internal and external. What additional instrumentation is needed to monitor remote or outsourced environments? How could technologies be adjusted or added to expand visibility or to provide valuable context for assessing an incident?

In general, as SOCs consider enhancing their capabilities, they should prioritize investments fulfilling the following technology requirements of an intelligence-driven security program:

- **Scalable analytics engines** capable of querying vast volumes of fast-changing data in real time across vectors such as geography, network partitions and databases
- **Consolidated warehouse for security data** so all sources are made available for query through one place, either as a unified repository or, more likely, as a cross-indexed series of data stores
- **Centralized management dashboard** to conduct and coordinate incident investigations and to manage incident response (e.g., blocking network traffic, quarantining systems or requiring additional verification of user identity)
- **Flexible data architecture** that allows information from many sources in many different formats to be captured, indexed, normalized, analyzed and shared
- **Automated data normalization** so analytics engines can ingest and work with highly diverse data types with minimal human intervention
- **Pattern-based monitoring techniques** that continuously examine high-value systems and information assets to identify threats based on behavior and risk models, not on static threat signatures
- **Rich correlation of incident information** so that data relevant to incident investigations automatically populate security management consoles, minimizing the amount of time analysts must spend collecting information and assessing incidents
- **Full network packet capture** enabling security analysts to reconstruct sessions in sufficient detail to make sense of what happened and what corrective actions should be taken
- **External threat intelligence services** that aggregate information from many trustworthy, relevant sources and present them in machine-readable forms that can be correlated with and analyzed alongside internal data with minimal human intervention
- **Active countermeasures and controls** such as requiring additional user authentication, blocking data transmissions or facilitating analysts' decision-making when high-risk activity is detected
- **Integrated compliance management process** that archives long-term security data through a distributed computing architecture and provides built-in compliance reports for a multitude of regulatory regimes

Process Alignment: the Greatest Productivity Driver

Designing security operations processes to automate repetitive tasks and integrate related workflows is potentially the most beneficial thing that SOCs can do to boost productivity, enforce policies and implement best practices for threat detection and response. That's because, in RSA's experience, process is typically the most immature and inefficient part of most SOCs' people-process-technology triad.

RSA recommends tight integration of processes and workflows. For example, incident management should be directly linked to incident response, and data sources should all feed into an integrated analytics and security management platform so analysts can see everything through a "single pane of glass" and derive better intelligence and context for incident investigations.

Process integration eliminates many routine steps, such as copying-and-pasting incident information, that go along with manually joining disparate security operations workflows. Integration also reduces opportunities for error, because activities for complex processes such as incident response can be programmed to follow a deterministic sequence of actions based on best practices. Finally, process integration can facilitate cooperation among different parts of the business—among audit, information security and compliance, for example—and help organizations create a unified view of conditions
and risks throughout the organization.

Process alignments are a closed-loop function. As SOCs redesign, test and implement processes, they take what they've learned to improve subsequent strategies and implementations. Because iterations breed improvement and best practices, many organizations enlist the help of outside consultants when embarking on major process changes in security operations. Inherent in the serial nature of consulting engagements is the continual refinement of best practices, and SOCs can benefit immediately from consultants' experience in designing and implementing security process improvements for other organizations.

In RSA's experience consulting to hundreds of enterprises, implementing an intelligence-driven security approach involves optimizing these processes:

- **Breach readiness assessments** to gauge the organization's current security state and increase operational maturity by designing, testing and practicing breach management and response
- **Cyber threat intelligence processes** to model threats and to develop best practices and procedures for proactively identifying threat vectors and anomalies in large volumes
  of data
- **Incident response and discovery workflows** to improve visibility into enterprise networks and to minimize the average time needed to detect a breach
- **Breach management automation** to refine processes and program procedures for a closed-loop incident handling process marked by continuous learning and improvement
- **Identity, infrastructure and information controls** focusing on privileged account management, secure communications, information rights/data classification and post-breach remediation and security

People Alignment: New Skills Needed

In a survey conducted by Enterprise Strategy Group, more than half (55%) of responding organizations said they planned to add security headcount in 2012, yet 83% said it was difficult to recruit and hire security professionals.[3] One of the ways to deal with the skills shortage in today's "do more with less" financial climate is to align process and technology to reduce analysts' routine workloads so analysts can focus on more advanced tasks. In RSA's experience, tools and process automation can slash the workload and time requirements for analysts sorting through routine, lower-level threats. In practice, RSA has seen SOCs with five analysts outperform SOCs with 25 analysts through tools and process optimization.

The techniques used in APTs and other advanced cyber attacks can be so complex that it takes cross-disciplinary teams with highly specialized security skills to detect, dissect and disable the threat. To address advanced cyber threats, SOCs will need to build collaborative teams comprising the following skills, either by cultivating the expertise in-house or by supplementing with outsourced experts:

- **Forensics knowledge**, especially in methodologies for collecting, maintaining, analyzing and reusing large repositories of data from networks and hosts/end points
- **Proficiency in coding, scripting and protocols** to help analyze vulnerabilities, debug systems and reverse malware
- **Managing threat intelligence**, especially cultivating and tracking multiple external intelligence sources and bringing relevant threat research back into the organization in a useful way
- **Breach management**, which includes coordinating the organization's response to crises and providing disclosures to outside parties
- **Penetration testing** to discover potential vulnerabilities in the IT environment resulting from poor system configuration, hardware or software flaws or operational deficiencies
- **Data analysts** who understand business risks and cyber-attack techniques in sufficient depth to develop analytical models that detect hidden threats and even predict cyber attacks

Security personnel will need to develop an investigative mindset: seeing the organization's assets and vulnerabilities as their adversaries do to anticipate attack techniques and devise countermeasures. Analysts will also have to hone hunting instincts: stalking adversaries within the IT environment, instrumenting tripwires to detect attackers' presence and setting traps such as honey pots to catch them.

In addition to building the SOC's technical and investigative capabilities, security operations teams should also cultivate communication skills within their ranks. Developing soft skills within the team can help the SOC build useful linkages to other organizations, whether it's informal information-sharing partnerships with other SOCs or fostering C-suite support for security operations programs.

3 Enterprise Strategy Group, "Security Management and Operations: Changes on the Horizon" (July 2012), pp. 19–20

INTELLIGENCE-DRIVEN SECURITY AT WORK

EMC Corporation's Global Security Organization (GSO) illustrates the impact of optimizing the interplay of people, processes and technologies in security risk management. EMC practices continuous improvement of the tools, skills and processes comprising its security operations. The company aims to achieve a holistic view of the enterprise – both physical and digital – to gain a better understanding of risk trends and threats throughout the company.

Converged Organization for Managing Risk and Security

EMC has built a converged security organization characterized by close collaboration among its Information Security, Risk Management, Customer Security Management and Corporate Protection and Investigation groups. By combining these organizations under a single umbrella, EMC is able to analyze metrics and trends to achieve a view of risk throughout the whole organization. For instance, if the Corporate Protection and Investigation team identifies repeated instances of intellectual property (IP) theft, the Information Security group can study those instances to create controls preventing future IP loss.

Converged Infrastructure for Security Monitoring and Management

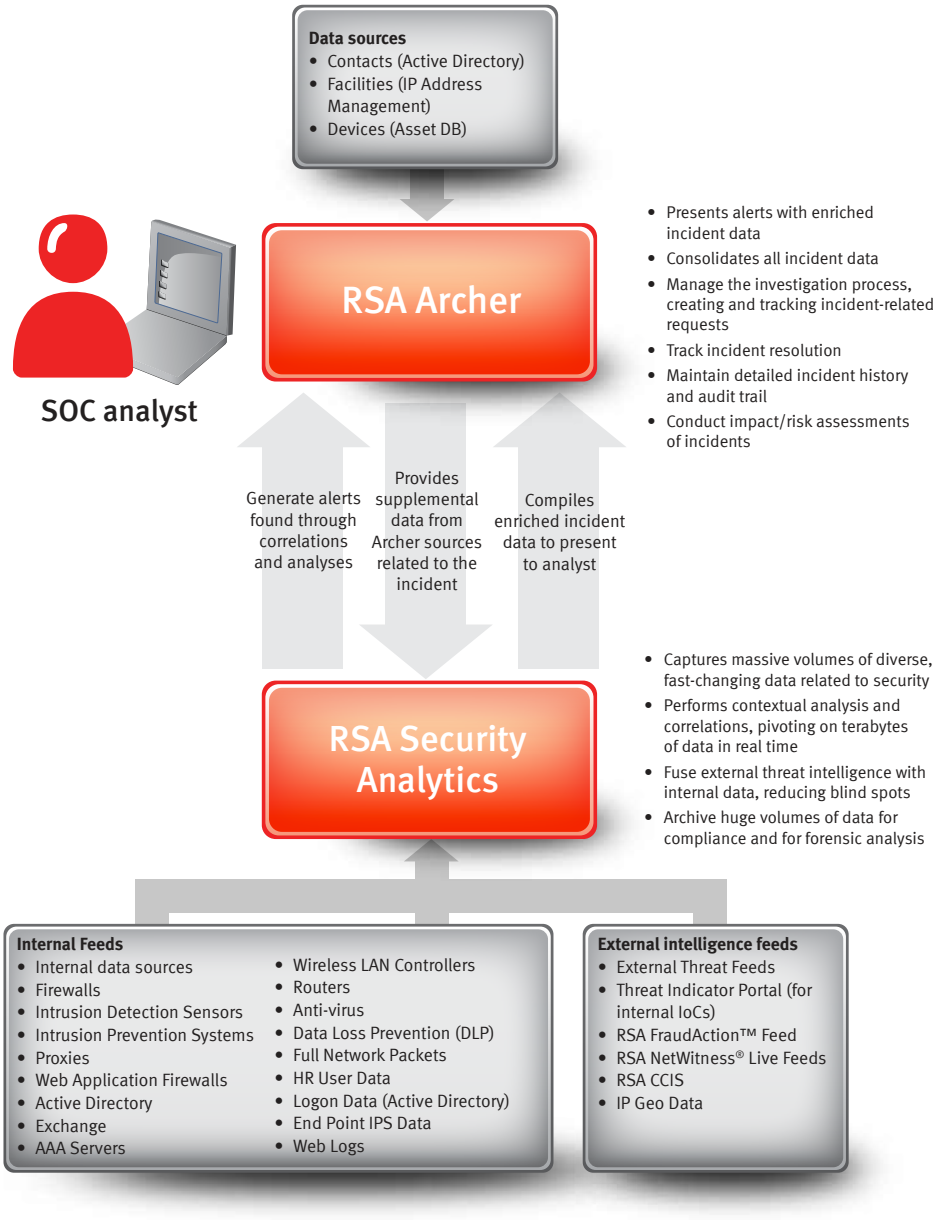
To support this converged risk and security strategy, EMC built a state of the art Critical Incident Response Center (CIRC). The EMC CIRC combines workflow and data from across the global organization and creates a central point for monitoring and enforcing the safety and integrity of the company's information assets. EMC's CIRC aggregates logs from more than 1,400 security devices and 250,000 end nodes distributed globally across 500 physical sites.

Within the CIRC, a team of highly skilled analysts continuously monitor EMC's global IT and security environments, responding to threats and vulnerabilities such as malware and data leakage to physical security incidents such as threats of violence and equipment theft. With this single integrated view of the global enterprise, security analysts can provide advice and guidance to EMC management – providing a critical feedback loop for continuously improving the company's security posture.

The EMC CIRC is built predominantly on technologies and best practices developed by RSA. While many technology tools are used within the CIRC, at the heart are the RSA Archer® GRC platform and the RSA® Security Analytics solution. These two systems integrate data from many other tools, providing CIRC personnel with a single big data repository and a central management console for security analytics. (See Figure 1.)

The integration of RSA Archer GRC platform with RSA Security Analytics streamlines many security operations workflows, helping the EMC CIRC accelerate investigations and reduce the time needed to close incidents.

Figure 1: Unified Platform for Data Analytics and Security Management



Automating the Use of Intelligence and Incident Data

Hundreds of alerts are generated each day for review by the EMC CIRC. Before an alert is presented to security analysts for investigation, RSA Archer technology and RSA Security Analytics automatically collect and correlate a rich variety of data related to the incident. Several processes and technologies have been engineered to integrate contextual data and intelligence into threat detection and response processes.

EMC's CIRC has developed a threat indicator management system to assimilate advanced-threat intelligence artifacts derived from public and private intelligence sources, intelligence sharing partnerships, and the CIRC's own Advanced Analysis and Cyber Threat Intelligence functions. The indicators of compromise (IOCs) in this system run the spectrum from known hostile domains and IP addresses to communication characteristics such as strings and elements of hostile email messages, including email headers.

IOCs are classified by severity and automatically integrated into the RSA Security Analytics platform as a capture feed, generating specific metadata tags. For example, a known advanced-threat domain tagged in the threat management system will generate a "Severity 1" metadata tag (the highest priority rating) for any activity to that domain found by RSA Security Analytics. Alerts for these metadata tags are designed to channel through the RSA Archer security management console to facilitate a near real-time response by the CIRC.

But before the alert is even presented to security analysts, additional data elements that can provide valuable context about the threat are retrieved from the CIRC's centralized security database. This provides the analyst with all available artifacts related to the incident and to the source and destination endpoints. The example in

Figure 2: Automated Enrichment of Event Data

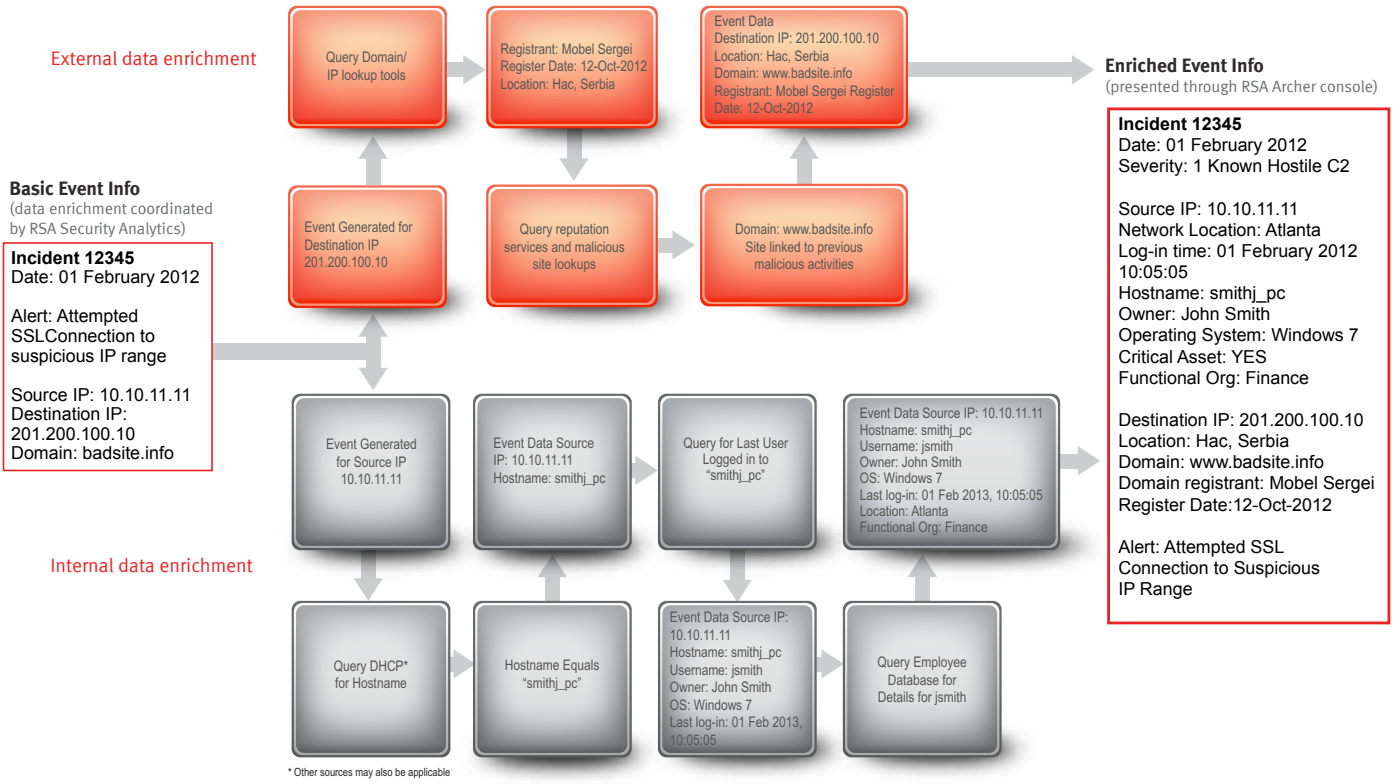


Figure 2 illustrates how this data enrichment process and integrated approach to alerting provides EMC CIRC with the details necessary to rapidly analyze and respond to critical incidents.

The EMC CIRC's data enrichment and intelligence integration capabilities help analysts focus their efforts on rapidly responding to threats, reducing exposure time to attacks and eliminating the manual collection of additional data elements correlated to incidents.

Automating Big Data Collection

Traditional SIEM and monitoring applications are limited in their ad hoc query and advanced analysis capabilities by architecture and performance concerns. EMC's CIRC addresses this challenge by streaming a mirror of all log events to a big data repository that collects approximately 1 billion records per day across 25 device types—more than 900 GB of data per day. Data in this centralized storehouse can be queried by analysts to correlate activities to threats. For example, the EMC CIRC uses its big data capabilities for basic behavioral analysis, such as detection of potential beaconing patterns within web proxy and firewall event logs. Also, as EMC's CIRC receives new security intelligence, historical activity potentially related to newly discovered threats can be analyzed to determine what damage, if any, was done. The processing power of EMC's big data platform has reduced the time to collect and make sense of security information
related to a threat from several hours to minutes, shrinking exposure time significantly.

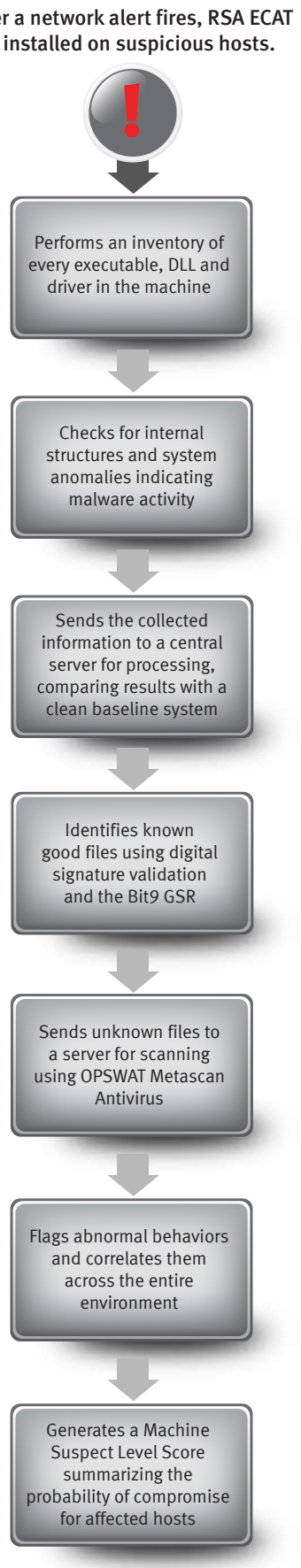
Automating Host-based Analytics

Traditional antivirus and host-based IDS/IPS products primarily rely on signatures to identify malware. Yet, signature-based techniques have been overwhelmed by the growth of malware and entirely bypassed by targeted attacks such as APTs and other advanced threats. While traditional malware scanning technologies will continue to have a routine role as a layer of defense in depth, they alone are simply not equal to combating today's more sophisticated threats.

Integrating behavior-based intelligence into host analysis and remediation helps fill the gaps left by signature-based tools such as AV and IDS/IPS. EMC's CIRC has deployed the RSA® Enterprise Compromise Assessment Tool (ECAT) to help monitor and protect endpoints that network monitoring or other intelligence resources have identified as potentially compromised.

RSA ECAT's approach to malware detection is highly distinctive. Malware often modifies internal operating system structures to hide its activity. By validating important internal kernel and application structures, RSA ECAT identifies anomalies that are typically generated by malware such as hooking, kernel object modification, file/process/registry/communication hiding, etc.

Figure 3: RSA ECAT Automates Detection of Host-based Threats



As deployed within EMC's CIRC, ECAT provides the threat detection capabilities seen in Figure 3, RSA ECAT at Work.

After compromised hosts and processes have been confirmed, EMC's analysts can define the scope of the threat with a single action and from behind a single pane of glass, as RSA ECAT identifies all other hosts harboring the same malicious file or process. Security analysts can quickly use the ECAT Machine Suspect Level score to evaluate the probability of compromise: a high score indicates problems, while a low score indicates a host is probably clean. While a low score does not guarantee a clean machine, the scoring system nevertheless helps prioritize investigative workflows, resulting in faster containment and remediation for larger-scale, more serious threats.

RSA ECAT has enabled EMC's CIRC to significantly reduce host analysis time and to contain much of the workload for malware analysis and validation to the earlier triage stage of EMC's threat detection process, which is handled by EMC's more junior security analysts. EMC estimates RSA ECAT saves its CIRC approximately 30 analyst hours per high-priority incident.

EMC Outcomes in Aligning Behind Intelligence-Driven Security

By aligning people, process and technology behind an intelligence-driven security program, the EMC CIRC estimates it has slashed the average time for closing incidents by up to 60 percent.

Technology and process integration accounts for much of the efficiency gain. It eliminates many time-consuming tasks for manually gathering incident-related information and has even automated aspects of threat detection, as seen in EMC's use of RSA Security Analytics and RSA ECAT.

The automation created by technology and process integration has helped scale up the CIRC's threat detection and response capabilities, freeing up analysts to devote more of their time to higher-priority incidents. Analysts can examine all data available on prospective threats through the centralized RSA Archer security management console, accelerating analysis and decision-making.

The integration of security technologies and workflows, combined with EMC's convergence of various risk- and security-related functions under a single organizational umbrella, has helped EMC mount a faster, more efficient and complete response to attacks. This, in turn, has greatly reduced EMC's exposure time to threats and empowers EMC—with its 60,000 employees—to operate with greater confidence in the digital world.

RSA thanks Mike Gagne, Chris Harrington, Jim Lugabihl, Jeff Hale, Jason Rader, Garrett Schubert and Peter Tran for contributing their time and expertise to the development of this technical brief.

APPENDIX: INTELLIGENCE-DRIVEN SECURITY SOLUTIONS FROM RSA

RSA® Advanced Cyber Defense Practice provides a holistic range of solutions to help clients protect their organizational mission, drive operational efficiencies and evolve with a dynamic threat environment. Targeted attacks often focus on the theft of critical assets and data and utilize techniques that bypass traditional defenses. RSA helps organizations enhance their existing security capabilities and implement countermeasures designed to prevent cyber adversaries from achieving their objectives. Services offered by RSA include gap analysis, maturity modeling, cyber threat intelligence, infrastructure hardening and security operations development and automation. RSA's NextGen SOC solution is designed to help organizations converge their technical and operational capabilities into a unified security program that aligns with risk management priorities and business objectives. RSA emphasizes the preventive measures required to protect the organization while also providing incident response and remediation services to reduce breach exposure time and to mitigate attacks.

RSA Archer® GRC Suite is a market-leading solution for managing enterprise governance, risk and compliance (GRC). It provides a flexible, collaborative platform to manage enterprise risks, automate business processes, demonstrate compliance and gain visibility into exposures and gaps across the organization. The RSA Archer GRC platform is designed to draw data from a wide variety of systems to serve as a central repository for risk-, compliance- and security-related information. The RSA Archer Threat Management solution is an early-warning system for tracking threats. The RSA Archer Incident Management solution helps organizations escalate problems, track the progress of investigations and coordinate problem resolution. The platform's ability to integrate information on security alerts and threats, to gather and present metrics about the effectiveness of security controls and processes and to analyze contextual information about the security and business environment helps create actionable, real-time intelligence across the enterprise.

RSA® Cybercrime Intelligence (CCI) is a service providing information about corporate assets compromised by malware, including corporate machines, network resources, access credentials, business data and email correspondence. CCI monitors underground cybercrime to uncover compromised corporate data that have leaked into the wild. The service reports to clients any data related to their organizations recovered directly from malware log files, including employee credentials, email accounts, IP addresses of infected machines and compromised domains. Going beyond malware, CCI scans open source intelligence (OSINT), reporting information back to clients on employee credentials, corporate email addresses and d0xing data that have been traced in the wild and compromised by hackers or fraudsters. CCI also reports details on email content, IP addresses and compromised credit card numbers belonging to the corporation or its employees that are being shared and/or sold by cybercriminals in closed, deep-web communities. In addition, CCI offers organizations insight into malware-infected online resources via daily blacklist feeds. These feeds expose IP addresses and resources either presently hosting or likely to host malicious content, allowing information security staff to take preemptive measures to mitigate risks.

RSA® Education Services provide training courses on information security geared to IT staff, software developers, security professionals and an organization's general employees. Courses combine theory, technology and scenario-based exercises to engage participants in active learning. The current curriculum covers topics such as malware analysis and cyber threat intelligence. RSA Education Services also offers a workshop on addressing advanced threats such as APTs. Courses are designed to deliver the maximum amount of information in the shortest period to minimize staff downtime.

RSA® Enterprise Compromise Assessment Tool (ECAT) is an enterprise threat detection and response solution designed to monitor and protect IT environments from undesirable software and the most elusive malware—including deeply hidden rootkits, advanced persistent threats (APTs) and unidentified viruses. RSA ECAT automates the detection of anomalies within computer applications and memory without relying on virus signatures. Instead of analyzing malware samples to create signatures, RSA ECAT establishes a baseline of anomalies from "known good" applications, filtering out background noise to uncover malicious activity in compromised machines. The RSA ECAT console presents a centralized view of activities occurring within a computer's memory, which can be used to quickly identify malware, regardless of whether a signature exists or if the malware has been seen before. Once a single malicious anomaly is identified, RSA ECAT can scan across thousands of machines to identify other endpoints that have been compromised or are at risk.

RSA® Security Analytics is designed to provide security organizations with the situational awareness needed to deal with their most pressing security issues. By analyzing network traffic and log event data, the RSA Security Analytics system helps organizations gain a comprehensive view of their IT environment, enabling security analysts to detect threats quickly, investigate and prioritize them, make remediation decisions, take action and automatically generate reports. The RSA Security Analytics solution's distributed data architecture collects, analyzes, and archives massive volumes of data – often hundreds of terabytes and beyond – at very high speed using multiple modes of analysis. The RSA Security Analytics platform also ingests threat intelligence about the latest tools, techniques and procedures in use by the attacker community to alert organizations to potential threats that are active in their enterprise.

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 solve 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, continuous network monitoring, and fraud protection with industry leading GRC 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

179827-H11533.1-ASOC_BRF_0214