RSA®

The Security Division of EMC

White paper

Advancing the Security Operations Function

Guidelines for Establishing a World-Class Program to Manage Risk

How can we be reasonably assured that our security controls are operating as designed in order to maintain an acceptable level of risk?

Traditional security operations programs, centered primarily on SIEM, have been long understood to be one of the most effective security investments an organization can make. However, many organizations are finding that today's high-risk environments are requiring more than just basic operations in order to effectively reduce risks. By moving to a construct that views SIEM as the foundation with critical feeds from DLP, threat intelligence and IT operations technologies, the security operations function can provide real-time insight into an organization's risk profile, allow rapid adaptations to meet changing security requirements and support cost-effective compliance. This white paper discusses a number of guidelines and considerations for implementing a more advanced approach to security operations.

October 2009

Contents

I. Introduction

One of the core questions any organization must ask itself is ‘How can we be reasonably assured that our security controls are operating as designed in order to maintain an acceptable level of risk?’ One only needs to scan daily headlines to realize that our infrastructures are under constant threat and that the level of risk we face will continue to grow. In many ways the dynamic nature of the IT infrastructure itself adds to the increasing level of risk. Consider the following factors:

– The volume of information we collect, store and manage keeps growing at an accelerated rate, and much of that information is sensitive. According to a study by IDC, the amount of digital information in existence is expected to continue doubling every 18 months.

– The regulatory environment keeps getting more complex, with new protection requirements being added all the time and many of the regulations addressing the types of information being stored and utilized by the organization. In the last decade alone, we’ve seen the introduction of numerous new regulations such as Payment Card Industry Data Security Standard, HIPAA in the US, data breach notification laws, European Union privacy laws and, most recently, new laws in the US governing the protection of Personally Identifiable Information protection, such as MA 201 CMR 17.

– The complexity of the infrastructure keeps growing; not only do we keep adding more servers, applications, databases, etc., but we also are integrating new technology layers into the environment such as virtualization, cloud computing and mobile computing.

– The number of identities we create and manage keeps growing, with each identity representing a potential point of attack.

– The number of external individuals and organizations we need to share information with keeps growing.

Each of these factors increases the number of threats we face and the attack surface of our environment, and hence serves to increase our level of risk. So how can an organization stay on top of security in this ever-increasingly complex environment?

One mechanism many organizations have implemented is a formal approach to security operations, at times in the form of a physical Security Operations Center (SOC). Either the central or distributed security operations function serves to constantly monitor and control the security and compliance environment and provide a rapid response to any detected risks or threats. Unfortunately, the perception that many managers have of security operations and SOCs is something they’ve picked up from movies – a darkened room full of large monitors on the wall full of constantly changing colorful graphs and charts, with rows of staff hunched over individual screens looking at incomprehensible information.

Having a basic SOC, often more accurately described as a SIEM deployment coupled with security operations personnel, is what many organizations consider an adequate implementation of security operations; however, this type of setup is frequently implemented without fully understanding and considering all of the factors necessary to ensure that their approach to security operations can actually meet their requirements. In addition, today’s modern risk and threat environments are straining most basic approaches to security operations, requiring an ever-increasing range of capabilities to keep up with the demand for security services.

This paper reviews a wide range of factors that should be considered by any organization evaluating the implementation of a structured security operations methodology and provides guidelines for advancing security operations functions.

Audience

This paper is targeted at security and compliance professionals in organizations that are currently or are planning on implementing a structured approach to security operations, or a SOC, or wish to advance their current approach.

> Infrastructures are under constant threat and the level of risk we face will continue to grow.

II. The Basics

Any organization that implements any form of security control is already performing some minimal amount of security operations. This can take the form of updating anti-virus definitions, installing security patches, or occasionally checking event logs on the firewall to look for possible attacks. However, these functions are not always formally defined and planned; frequently they accrete to specific members of the security or operations teams because they're the best qualified to perform them. Before an organization can implement an advanced approach to security operations, a number of basic foundations need to be in place.

Define Goals

To begin, an organization needs to review, understand and document the reasons for implementing structured security operations and, if applicable, a SOC. Too frequently, the implementation is limited to creating a SOC and is justified with generic statements such as 'We need to improve security' or 'We need to reduce risk' without any detail backing up such decisions. Consider the implementation of almost any other type of IT component – new applications, virtualization, new networks. In most organizations, the IT staff and CIO must develop detailed justifications for spending money and resources on acquiring, implementing and managing any new processes or solutions. These justifications frequently include detailed analysis of factors such as Total Cost of Ownership (TCO) and Return on Investment (ROI). This same approach should be taken for Security Operations and SOCs, with some of the potential factors to be considered including:

- If the stated goal is to improve security, how does the organization measure security? Improvement implies a measurable process, which many organizations do not currently implement in the context of security.
- If the stated goal is to reduce risk, once again, how is risk measured? Does the organization have a formal approach to measuring and managing risk? How will the performance of the Security Operations team be measured in this context?
- Will Security Operations be subject to formal Service Level Agreements (SLAs) that are frequently required for other critical IT operations?

As with any IT analysis, the business needs of the organization must be the drivers for considering the implementation of a formal Security Operations methodology and a SOC, and these needs should be well quantified and documented before proceeding.

Define Roles and Responsibilities

The next area that should be addressed is the formal definition of the roles and responsibilities of the Security Operations team. Since the security operations function can potentially interact with and impact all other IT components in the infrastructure, what it should and should not do, as well as what it can and cannot do, should be clearly defined. Agreement must also be reached with all of the impacted parties (e.g. IT operations, business units, management, legal, human resources, etc.). Some standard roles for a Security Operations team include:

- Monitor the infrastructure
- Maintain security controls
- Process and resolve incidents
- Perform vulnerability and penetration testing
- Maintain and report security metrics
- Proactive remediation
- Drive security awareness across the organization

While these types of roles are fairly straightforward and well understood, there are a number of additional factors regarding the roles and responsibilities of the team that need to be addressed as part of the planning process. These factors include:

- **Security versus compliance** – In most organizations, regulatory compliance is one of the primary drivers for implementing security controls, and thus drives many of the Security Operations team's goals. In that context, will the team be responsible for ensuring compliance, or does another group have that responsibility? In either instance, the Security Operations and Compliance teams should be integrated to ensure smooth compliance and security operations.
- **Authority versus responsibility** – This is frequently one of the biggest areas of contention for Security Operations personnel. They are held responsible for the security of the organization, but they do not have the authority to take appropriate action when security may be compromised. Consider a scenario where the Security Operations team detects that a mission-critical database

is under attack – does the team have the authority (and ability) to take that database offline to prevent or minimize the impact, or do they need to submit a request to another group? In the second scenario, the additional time required to submit a request and have the database taken offline may significantly increase the level of exposure caused by the attack. Therefore, such processes must be formally documented and defined in a manner that drives the most efficient resolution.

– **Integration with other operations teams** – Many organizations have implemented other types of operations teams, such as network and systems. How will the Security Operations team interact with these teams, and who will be responsible for what? Close interaction among various operations teams is critical for effective security. Consider a scenario where the Network Operations team detects an upsurge in the amount of outgoing network traffic; they may spend some period of time investigating the source of the traffic and fail to recognize that it is a piece of malware that has entered the environment undetected. If security and network operations were integrated, the Security Operations personnel may be able to recognize the traffic pattern as a potential attack and quickly take appropriate action to contain it. If they had to wait until the Network Operations team informed them the damage may be considerably higher.

Monitoring

Monitoring the IT environment to identify potential security incidents is one of the primary functions of Security Operations; this involves collecting, reviewing, analyzing and managing information that may be of interest from a security perspective from components within the infrastructure, usually via event logs. However, one of the most difficult aspects of planning an effective monitoring solution is the definition of exactly what needs to be monitored and, more importantly, the meaning of the information that is collected. Basic security operations focuses on collecting and analyzing event logs from standard security tools such as VPNs, firewalls, IDS/IPS, and anti-virus tools. This is frequently automated through a Security Information and Event Management (SIEM) tool.

> Close interaction among various operations teams is critical for effective security.

Operations and Incident Handling

Security Operations is frequently tasked with monitoring the environment and detecting security and compliance incidents. These incidents can range from something as simple as out-of-date anti-virus definitions to something as complex as an orchestrated attempt by an insider to steal sensitive information. What needs to be clearly defined is exactly who is responsible for resolving these incidents and how. Basic security operations need to define the scope, authority and processes used by Security Operations for handling incidents. In some instances, organizations implement a separate critical incident response team (CIRT) which is responsible for investigating and resolving incidents beyond basic operations tasks.

IT Infrastructure Requirements

Given that one of the primary roles of Security Operations is to monitor and manage the security of the information and IT infrastructure, it follows that infrastructure components and tools must be capable of providing the information and controls the Security Operations team needs to accomplish its goals. In order to accomplish this, Security Operations personnel should actively participate in the IT technology acquisition and implementation process, including:

– Definition of standards for any new technology acquisitions and their ability to be monitored

    Event log generation

    Event documentation

    Granularity of event logging

    Exporting or sharing of event logs to a central collection tool

– Definition of standard event log configuration baselines for deploying any new components

– Testing of monitoring as part of the system acceptance process

Security Operations personnel should also analyze how event logs from new components may impact the performance of the SOC and its infrastructure. Each new data source will require additional disk space to store the logs as well as additional resources to analyze the information they represent.

Policy

Ultimately, the role of the Security Operations team is to enforce security and compliance with policy and to control risk. An organization's statement of what it considers acceptable is the security policy and should be used as a starting point for what the Security Operations team should monitor. The security policy should offer guidance on specific types of sensitive information including who is allowed access it, where it can be stored, and how it can be used.

Staffing

Staffing is one of the most critical and often one of the most difficult aspects of designing and implementing a structured approach to Security Operations. Experienced security professionals can be difficult and expensive to hire and maintain, yet they are absolutely critical to a successful Security Operations program. Organizations should generally begin with existing security staff to determine their appropriateness for Security Operations work.

Once an experienced core team is established, less experienced personnel can be utilized for basic monitoring duties. Having a strong suite of automated tools and well-defined processes and procedures can dramatically simplify the process of staffing a Security Operations team, as such tools can significantly reduce the burden on the Security Operations personnel by eliminating the need to manually review and analyze large amounts of event data.

> A strong suite of automated tools and well-defined processes and procedures can dramatically simplify the process of staffing a Security Operations team.

The exact skills required to operate a successful Security Operations team will vary by organization, but include:

- Extensive background in a broad range of security technologies, especially those utilized by the organization
- Strong analysis skills
- Strong communications and interpersonal skills
- Experience with the IT technologies utilized by the organization
- CISSP or other advanced security certification

Operating hours will also impact staffing requirements. A Security Operations team that needs to be operational 24x7 will need to ensure enough personnel are available to cover situations such as vacation and sick days.

Processes & Procedures

As with any other group in an organization, Security Operations personnel perform certain tasks on a regular basis. These workflows might include event analysis, incident notification, investigation (if not handled by a separate incident response team), and reporting. The various activities performed by the Security Operations team should be documented, and a standard set of processes and procedures should be created and maintained. Each procedure should include items such as:

- Incident alert and notification
- Tools to be used
- Documentation
- Personnel to be notified (along with up-to-date contact information)
- Mechanisms for notification
- Investigative procedures
- Test procedures (e.g. penetration testing, vulnerability testing, DR testing, etc.)
- Disaster recovery procedures
- Review process
- Reporting process

All processes and procedures should be tested and reviewed on a regular basis to ensure their effectiveness and applicability.

Security Operations Infrastructure

The infrastructure that supports the Security Operations team is an important consideration when designing the program. Given the critical and sensitive nature of the functions that Security Operations teams and SOCs perform, ensuring the supporting infrastructure is highly available, functional and secure should be a top priority during the design process. The following sections describe specific areas that should be considered.

Network

The network used by the Security Operations team to collect data and run its tools is of vital importance to its operation and should be as secure against attack as possible. To this end, it is generally advisable to implement a separate physical network to support all of the Security Operations team's systems to minimize the potential for attacks. Note that while a virtualized network (VLAN) approach may be considered, there have been instances of vulnerabilities in some vendor's technology that would allow an attacker to bypass the VLAN's segmentation, rendering it ineffective[1.] The Security Operations team's network connection(s) to the rest of the infrastructure should also have its own dedicated firewall.

A Security Operations network should also have its own external network connections, preferably more than one from different service providers. This minimizes the possibility that an incident, such as a Denial of Service (DoS) attack on the organization, will impact the team. As with the connection to the internal infrastructure, these connections should be strongly firewalled.

Note that both of these recommendations apply to situations where the Security Operations team resides in its own physically separate location (e.g. a SOC) as well as when the team operates in a more physically dispersed configuration. While implementing a separate physical network for a dispersed team would be a more complex undertaking, doing so would provide the ability to implement a hardened isolated environment, which in turn can be critical to minimizing the vulnerability of the Security Operations infrastructure.

Simplifying Security Operations

An organization's information attack surface for a given type of information is the sum of all the possible threats and vulnerabilities that exist for that type of information. This may include a database that contains the information, a storage array that stores the database, network shares extracted information is stored on, an email system that sends the information, laptop computers with the data, backup tapes of the database, and more. By developing an understanding of the attack surface for each type of sensitive information, an organization can gain a thorough understanding of all of the components that must be monitored by Security Operations to ensure security for that type of information. However, when an organization performs a detailed information attack surface analysis, they frequently discover that the information is spread over hundreds or even thousands of locations around the infrastructure, accessed in dozens of different ways, and moved around using a wide range of mechanisms. In this scenario, translating an understanding of the attack surface into a monitoring plan for Security Operations can become an extremely difficult and expensive proposition.

One way to simplify the task and improve security is to take steps to reduce the information attack surface. How this can be done depends on the exact nature of the attack surface, but may include areas such as:

- Storage and network share consolidation
- Backup consolidation
- Content management systems
- Tokenization of sensitive data
- Data loss prevention tools
- Information rights management tools

Once the footprint for sensitive data is reduced to the smallest possible size, it becomes easier for the Security Operations team to monitor that sensitive data.

For more details on understanding and reducing your information attack surface, please request a copy of the white paper entitled 'Understanding and Addressing Your Information Attack Surface' from RSA.com.

[1] Cisco Security Response:
http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml

Availability

Once implemented, a Security Operations infrastructure generally becomes the centerpiece of an organization's security and compliance efforts. As a result, it represents a significant investment on the part of the organization. If any of the components in the infrastructure become unavailable, the security of the organization can be potentially compromised until it is brought back to a fully operational state. To minimize any potential window of exposure, the Security Operations infrastructure should be designed with the highest possible level of availability. This should include utilization of capabilities such as clustering for the servers running the Security Operations tools, local and remote replication of the databases and automatic fail-over of tools in the event of a failure. High availability requirements should be a key consideration when evaluating tools for Security Operations.

The Security Operations infrastructure should also be designed to be highly available in the event of a disaster. Organizations are usually more vulnerable during a disaster, with the emphasis being placed on getting everything operational, frequently at the expense of security and compliance. The infrastructure should be considered mission-critical, and no other components should be brought online after a disaster until after the backup Security Operations infrastructure is fully operational[2].

III. Advancing Security Operations

Once an organization has addressed the basic foundations required for implementing a structured approach to security operations, the next logical step is to examine how it can be taken to a higher level and leveraged as an integral part of a formal approach to reducing risk. Security tools and technologies have dramatically advanced in terms of functionality and capability in recent years, providing a Security Operations team with the ability to manage, monitor and control larger and more complex infrastructures more effectively with fewer resources. This in turn allows the Security Operations team to play a much more significant role in managing and reducing risk to the organization.

The following sections define a number of approaches and capabilities that can be implemented in support of an organization's security operations to dramatically expand its ability to address a modern risk environment.

Focus

Before an organization can begin to effectively plan and implement advanced security operations there are a number of considerations regarding the focus of the Security Operations team that need to be rethought. By understanding and addressing these areas, the capabilities and effectiveness of the Security Operations team can be greatly increased.

Prevention vs. Detection/Correction

Traditional security operations programs have focused on a fairly narrow set of inputs and controls integrated with a security information and event management (SIEM) platform, usually with the goal of detecting security threats and correcting them quickly. This is illustrated by the tools that these teams have had available to perform their functions – VPNs, firewalls, anti-virus, etc. While there are some capabilities for prevention in these tools, most of it has been directed to addressing external threats. When advancing security operations, the focus needs to shift from primarily detecting and correcting all forms of threats to preventing them from occurring in the first place. In order to accomplish this, Security Operations needs to develop a new set of capabilities, supported by modern security tools, and its focus needs to change to understanding and minimizing risk.

Authority

With an increased range of responsibility comes the requirement for expanded authority when dealing with threats. In the past, Security Operations personnel frequently had to submit requests to other operations teams such as Network Operations or Database Operations to take any required actions such as taking down a server under attack, stopping an employee from leaving with a laptop full of sensitive data, or updating security patches on a critical server. Increased operational responsibility requires increased authority in order to be able to quickly and effectively deal with threats as they are detected. For example, processes should be established that define how security operations may take steps to remediate threats associated with IT infrastructure components out of the team's immediate purview. This, by virtue of current authority and responsibility roles, requires the Security Operations team to work very closely with IT operations.

[2] For more details on the relationship between security and disaster recovery, please request a copy of the RSA white paper titled 'Security Considerations for Disaster Recovery' from your local RSA representative.

> Compliance is one area where an advanced security operations capability can assist an organization in meeting its requirements.

Compliance

Compliance is one area where an advanced security operations capability can assist an organization in meeting its requirements. Security has frequently been implemented as a result of industry and government regulatory requirements, with the Security Operations team being driven by external factors. By allowing them to participate in the broader compliance process, significant improvements in the way an organization manages compliance can be realized while at the same time economies of scale resulting from a Security Operations framework can actually reduce the cost of compliance.

Scope

At its most basic implementation, Security Operations focuses on security, while all other aspects of the IT infrastructure are the responsibility of other IT teams. However, advancing security operations requires that the Security Operations team be responsible for a much broader range of infrastructure and information security, in turn requiring that the team take a much more active role in areas such as new system planning, IT solutions design, and infrastructure component acquisition. Since the team will be held accountable for security across the infrastructure they must be able to influence the design and implementation of IT systems to ensure they can be effectively monitored and controlled.

Advanced Monitoring

As previously discussed, monitoring is one of the core functions that should be performed by a Security Operations team. Traditionally monitoring has been limited to collecting and correlating logs from a few specialized security tools, such as VPNs, firewalls, IDSs, etc. However, this approach can leave large gaps in the team's understanding of the environment and exactly what is occurring. Given that security operations is basically a stimulus/response activity, a lack of the ability to collect a comprehensive range of information on the entire infrastructure will inevitably lead to a failure to identify and address some risk-generating activity. Advancing the monitoring function requires the collection, analysis and correlation of information from across all infrastructure components as well as from tools that provide insight into the organization's sensitive data.

Event Information Management

The ability to enable events across the infrastructure, generate context-sensitive events and the ability to monitor sensitive information are critical to advancing a security operations function. However, without the ability to easily and effectively collect, manage, analyze and correlate these sources of information, they provide very little value in terms of security operations. The cornerstone of an advanced security operations function is commonly referred to as Security Information and Event Management (SIEM), and it supports the collection and analysis of event logs. However, while traditional SIEM tools have focused on supporting a fairly narrow area of the infrastructure (primarily security tools and controls), implementing an advanced security operations function requires a tool with more integrated and far-reaching capabilities. These include:

- **Support for a wide range of event sources** – The ability to monitor the IT infrastructure, generate context-sensitive events and monitor a wide range of event information is critical; the SIEM tool selected by the Security Operations team should be capable of collecting, analyzing and correlating events across a wide range of event sources.
- **Automated event log lifecycle management** – With an expanded range of events sources, the rate of growth of event log data will be considerably higher than with traditional event sources. The tool must be capable of automatically archiving and deleting older event logs based on policies defined for each event source type or group.
- **Contextual alert generation** – In order to prevent the Security Operations team from having to manually review and investigate every event, the tool should be capable of generating alerts based on context, such as the number of events in a given time period exceeding a pre-defined threshold. The tool should also be able to provide events based on a holistic view of the infrastructure, such as the overall rate of failed login activity.

- **Alert weighting** – The tool should be able to adjust the level of an alert based on its potential impact on the environment. For example, the tool should be able to take input from vulnerability assessment tools and generate a lower-level alert if a given detected attack will not succeed due to timely patch application by the IT staff; conversely, if the know vulnerability data indicates that an attack will most likely succeed, the tool should be capable of automatically taking more aggressive action to minimize the organization's exposure (e.g. shutting down a database under attack).
- **Analysis support** – The tool should provide a mechanism that supports advanced searching of the database to support detailed analysis and forensics by various criteria such as sources, dates, and users.
- **High availability** – Organizations are generally at their most vulnerable when a disaster strikes and management and workers are focusing primarily on getting the business running again. It is during these times that the ability to collect, monitor and correlate event information is most critical, as the potential risk to the organization is highest. A SIEM tool should provide the capability to fail-over and be restarted during a disaster to ensure a continuous chain of monitoring and risk awareness.

A SIEM solution is at the core of a enhancing the Security Operations function – it must be able to support the advanced capabilities required today while being expandable to accommodate future requirements.

Infrastructure Components

In order to provide effective insight into the risks occurring in the infrastructure, the Security Operations team must first have insight into what is happening across the entire infrastructure. This includes all IT components – servers, operating systems, networks, storage, virtualization technology, etc. This in turn mandates that the Security Operations team understands what exists in the infrastructure in order to effectively monitor it, and that they have a tool set that can collect, analyze and correlate event logs from all of these disparate data sources.

Some of the components that should be monitored include:

- Servers and operating systems
- Endpoints
- Mobile devices
- Networks
- Applications
- Databases
- Storage systems
- Security controls
- User accounts/Administrative accounts
- Network shares
- Content management systems
- Web sites
- Virtualization layers

Gaining this understanding can be a daunting and complex task even in a small infrastructure. New servers are constantly added, new applications are installed and new storage is being added. Developing a comprehensive understanding of the infrastructure components requires the use of automated discovery tools. These tools can be used to scan the environment and identify and document all of the infrastructure components that exist and detect new ones when they are added. Security Operations can then review the list of all components in conjunction with the IT and business unit personnel to identify which components are critical and create and implement a monitoring plan for those components. This plan should include the components that need to be monitored, the specific events that are of most concern, and the actions that should be taken for each type of critical event.

> When disaster strikes, the ability to collect, monitor and correlate event information is most critical, as the potential risk to the organization is highest

Having access to an up-to-date configuration management database can greatly assist the Security Operations team in creating a monitoring plan.

Real-time notification of changes to the IT infrastructure should also be available to the Security Operations team. For example, if a new application shows up on the network, the Security Operations team should be automatically notified so they can analyze it to ensure it is an approved application and not a new form of malware. Note that this task can be significantly simplified by providing the Security Operations team with access to an organization's change management system – detected changes can be compared to those that have been submitted to ensure that the changes have been reviewed and approved.

Consider a scenario where a sensitive database is stored on an intelligent storage array on a Fiber Channel SAN. The database is mounted on a server running the database application, with extensive security controls around access to the server and application. However, it may be possible to utilize capabilities on the storage array itself to make a copy of the database (commonly referred to as snapshots or clones), then mount that copy on test server also connected to the SAN. The database can then be accessed from the test server, bypassing all of the controls on the primary server. If the Security Operations team wasn't monitoring the SAN storage array, they would not detect that a copy of the sensitive data had been created.

One mechanism that can simplify the Security Operations task of qualifying what infrastructure components exist as well as their interrelationships is a configuration management database (CMDB). CMDBs are frequently utilized by IT operations teams to provide a centralized source of information regarding the infrastructure and frequently collect and federate information from numerous sources. Having access to an up-to-date CMDB can greatly assist the Security Operations team in creating a monitoring plan; continuing access allows the team to maintain an on-going understanding of the infrastructure and any changes that occur. Optimally, the Security Operations team should incorporate automatic notification of any changes to the CMDB into their monitoring plan.

Infrastructure Context

While collecting, analyzing and correlating information for individual components across the infrastructure is necessary for implementing advanced security operations, requiring the team to understand the context of each type of event can be an almost impossible requirement. In even a small infrastructure, the team can have a difficult time determining if any discrete event results in a security or compliance risk. For example, is creating a new user account on a sensitive server a risk or not? If the Security Operations team has to manually investigate each of these incidents, they will quickly be overwhelmed.

To support the Security Operations team in this analysis, a suite of tools that can automatically monitor and analyze changes to infrastructure components and provide context-aware alerts is required. These types of tools are frequently utilized by the IT Operations to manage and monitor various components such as servers, networks, storage and endpoints, and provide capabilities such as standard configuration deployments, patch management, change management and comparison with standard baselines., Many of these same tools also provide the capability to compare changes to a defined baseline determine if a given change results in a component becoming non-compliant with the organization's requirements; if such a situation is detected the tool can generate an alert. These alerts can then be received by the SIEM tool and investigated, eliminating the need for the team to constantly monitor every discrete event from all critical components. The underlying detailed events can be viewed and analyzed when a higher-level alert has been generated to determine the chain of events and what corrective action needs to be taken.

Sensitive Information

Another area that should be considered as part of an advanced Security Operations monitoring function is the monitoring of sensitive information itself and what is happening to it. While holistically monitoring the underlying infrastructure is critical, this alone will not necessarily provide any insight into the sensitive information being stored, moved and accessed by that infrastructure and the users it supports. For example, a file server system can generate an event when a new file is stored by a user, but it is generally incapable of determining if the file contains sensitive data and is being stored in violation of policy.

To gain insight into what information should be monitored an organization should undertake a discovery and documentation process to identify the following:

- What types of sensitive information exist in the infrastructure
- Risks associated with each type of information (e.g. fines, data breach, etc.)
- Where the sensitive information is stored
- How sensitive information is accessed and by whom
- How sensitive information is moved
- What IT components ‘touch’ sensitive information

Identifying the types of sensitive information in the infrastructure can usually be accomplished by interviews with the various business units to determine what types of information they collect, store and create. Additionally, the risks associated with each type of information can usually be defined by the owners of the information, or through interviews with an organization’s Legal and Compliance teams. However, effective monitoring of the sensitive information requires a detailed understanding of where and how the information is stored, accessed, and used. As with the general infrastructure, obtaining this level of detail for an infrastructure of any size usually requires the use of automated discovery tools. These types of tools are generally referred to as Data Loss Prevention (DLP) tools, and some provide the ability to discover and report on the various types of sensitive information in the environment as well as how the information is being moved and used. There are three broad functional areas that should be supported by any DLP tool set in order to support an advanced security operations capability:

- **Data at rest** – The first capability of a DLP tool set should be to discover sensitive information stored in the infrastructure by locating, opening and scanning content stored in any supported type of ‘container’ (e.g. network shares, SharePoint® sites, databases, etc.). The reports produced by this type of scan should be used to develop a plan for what IT infrastructure components that ‘touch’ the sensitive data should be monitored by Security Operations. The tool should be run on a regular basis to allow detection of potential risk situations where new data has been stored in the infrastructure and be capable of automatically enforcing policies set by the organization (e.g. deletion or encryption of improperly stored content, etc.) while at the same time reporting on the violations.
- **Data in motion** – The second capability of a DLP tool set should be to monitor content moving out of the infrastructure through any supported communications mechanism (e.g. mail, FTP, HTTP, etc.), identify sensitive content, and take appropriate actions when policy violations are detected. This component should also be capable of reporting on detected violations so that Security Operations can monitor and detect trends.

What types of sensitive information exist in the infrastructure?

What risks are associated with each?

Where is it stored?

Who accesses it?

How is it moved?

What IT components touch it?

- **Data in use** – The third capability of a DLP tool set should be to monitor the use and movement of sensitive information off of endpoints. This includes areas such as copying to USB drives or optical disks and printing. As with the other two functional areas, the tool should be capable of monitoring and reporting any attempted violations.

There are also a number of common capabilities that should be supported across all functional areas of the DLP tool set that can simplify its use by Security Operations including:

- The ability to control all functional behavior via a policy-based manager
- The ability to rank reported events based on thresholds (e.g. a single violation is logged at a low-level; multiple violations within a given time period result in a higher-level alert being generated)
- Out-of-the-box integration with the Security Operations team's event log collection and management capability
- Policy-driven management

External Data Sources

No modern IT infrastructure exists in a vacuum – they are connected to the Internet, users bring in and take out portable media such as optical disks and USB drives, and outside users such as consultants are granted temporary access. However, one of the more common limitations of traditional approaches to security operations is that they tend to be almost exclusively inwardly focused. The result of this organizational myopia is that the Security Operations team is frequently ill-prepared to handle external threats.

In order to effectively provide an advanced security operations capability, the Security Operations team must collect and evaluate information sources from both inside and outside the organization. Ongoing collection and review of this external information can provide a much broader view of the organization's security within the actual context in which it must operate – e.g. connected to the outside world. So what are some of the sources of external data that a Security Operations team can leverage to develop and maintain this context-aware understanding? The following list describes several well-known sources that should be considered:

> No modern IT infrastructure exists in a vacuum – they are all connected to the Internet.

- **SANS Internet Storm Center** (http://isc.sans.org/) – Provides real-time information on Internet security activity, including known virus outbreaks.
- **Common Vulnerabilities and Exposures** (CVE) Database (http://cve.mitre.org/) – A dictionary of publicly known information on security vulnerabilities and exposures that covers a wide range of vendor products.
- **Vendor vulnerability management system** – Some vendors provide a system to track, report and monitor vulnerabilities for their products.

While these types of information are critical to advanced security operations, they are not in themselves sufficient to provide a complete understanding and awareness of all of the outside factors that impact an organization's risk profile. To maintain a complete understanding requires that the team obtain organization-specific intelligence regarding potential threats and risks. Since few organizations can afford to develop the capability to monitor hacker web sites in real-time to discover potential threats and risks of concern, organizations should consider subscribing to a threat intelligence service. These subscription-based services monitor a wide range of potential sources on the Internet to provide automatic notification when the organization may be targeted by a threat. Potential threats may include compromised credentials being sold in hacker forums, new malware tools, or organization-specific sensitive information being sold. This information allows an organization to take proactive steps to minimize or eliminate any potential risk.

Content Management Systems

One of the functions of a Security Operations team (and its associated Incident Response Team) is to investigate threats and risks when they are uncovered. A big part of this investigative process is the collection of large amounts of information such as event logs snapshots, directory listings, digital surveillance video, and forensic data. This information needs to be controlled, managed and shared by the team and may include requirements for evidentiary protection (if the threat or risk involves potential legal action). While managing this information by storing it in shared subdirectories may have sufficed for more limited security operations, advanced management capabilities are usually required when the team expands its scope and roles.

Modern content management systems (CMS) are ideal for addressing this requirement. They provide capabilities such as check-in/check-out, revision control, structured process and workflow support and support for a broad range of content types. Many of these systems also provide support for formal rules of evidence, ensuring that the content can be used effectively if legal action is required.

IV. Summary

Planning, organizing, designing and implementing an advanced structured approach to Security Operations can be an involved and complex task. While most organizations recognize the need for formal Security Operations and can implement a basic approach, ensuring it can effectively meet the needs of the organization in today's modern risk environment on an on-going basis requires careful analysis of a large number of factors and considerations, combined with modern tools that provide an appropriate level of insight and control across the infrastructure. A poor implementation can result in a false sense of security and actually increase the level of exposure. When implemented and managed correctly, an advanced Security Operations function can provide a dramatic reduction in the level of risk to which an organization is exposed.

References

For more details on the RSA and EMC solutions that enable an organization to implement an advanced Security Operations capability, please refer to our web sites at http://www.rsa.com and http://www.emc.com. More information regarding RSA and EMC solutions for security operations centers and other technology areas may be found at http://www.rsa.com??.

About the Author

John McDonald is a Security Evangelist for RSA, and is responsible for working with customers to deliver the EMC and RSA message and strategy. He has over 25 years experience in the security industry, and has been actively involved with security at EMC since he joined the company over 7 years ago. Before EMC he worked with several consulting companies performing security audits and security infrastructure design for numerous customers, including several Fortune 500 ones. John is a CISSP.

About RSA

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring 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.

SECOP WP 1009

RSA®
The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com