Gartner

Research

Publication Date: 24 January 2011 **ID Number: G00210104**

Understanding Vulnerability Management Life Cycle Functions

Mark Nicolett

We provide guidance on the elements of an effective vulnerability management program. Security organizations need to operationalize their security policies in order to make the IT environment more resilient against attack.

Key Findings

- Targeted attacks typically exploit multiple security weaknesses in order to achieve the ultimate goal, which is to steal data, compromise accounts or disrupt operations.
- Vulnerability management implements proactive controls that can make an IT environment more resilient against a targeted attack.
- Assessment, shielding and mitigation efforts need to be augmented by effective monitoring.

Recommendations

- Organizations need to implement assessment and mitigation processes and technologies, in combination with shielding technologies, to defend against targeted attacks, but also need to proceed under the assumption that defenses will sometimes fail.
- IT security organizations must work with IT operations to develop and implement operational processes for effective vulnerability mitigation.
- Security organizations should work with IT operations to define security configuration standards, and drive implementation of security configuration standards in desktop, network and server provisioning processes.
- Security monitoring should be used to augment assessment shielding and mitigation efforts.

TABLE OF CONTENTS

LIST OF FIGURES

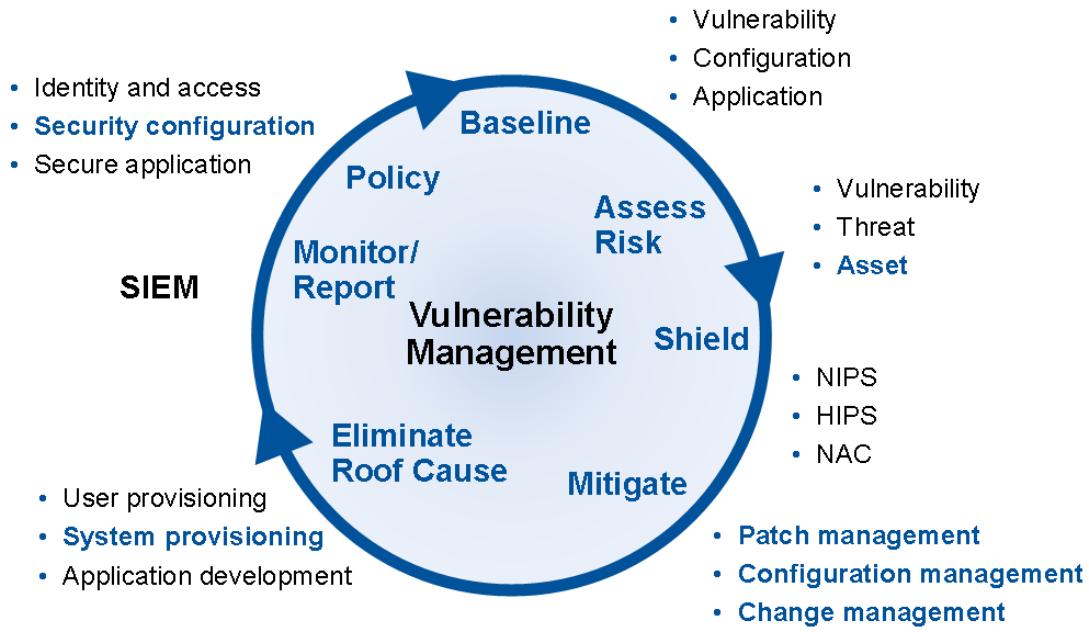
Gartner

ANALYSIS

The external threat environment has become quieter and much more dangerous. Today's attacks target specific companies, individuals and data. A typical targeted attack will exploit multiple security weaknesses to achieve the ultimate goal — usually, to steal data, compromise a specific account or disrupt operations. Organizations need to present a hard target to an attacker. This requires a combination of vulnerability management processes to find and fix security weaknesses in systems and applications, and the implementation of shielding technologies to protect systems and applications that will have long-standing vulnerabilities.

Gartner's vulnerability management life cycle provides guidance on the operational processes and technologies that are needed to discover and remediate security weaknesses before they are exploited (see Figure 1).

Figure 1. Vulnerability Management Life Cycle



HIPS = host intrusion prevention software; NAC = network access control; NIPS = network intrusion prevention system; SIEM = security information and event management

Source: Gartner (January 2011)

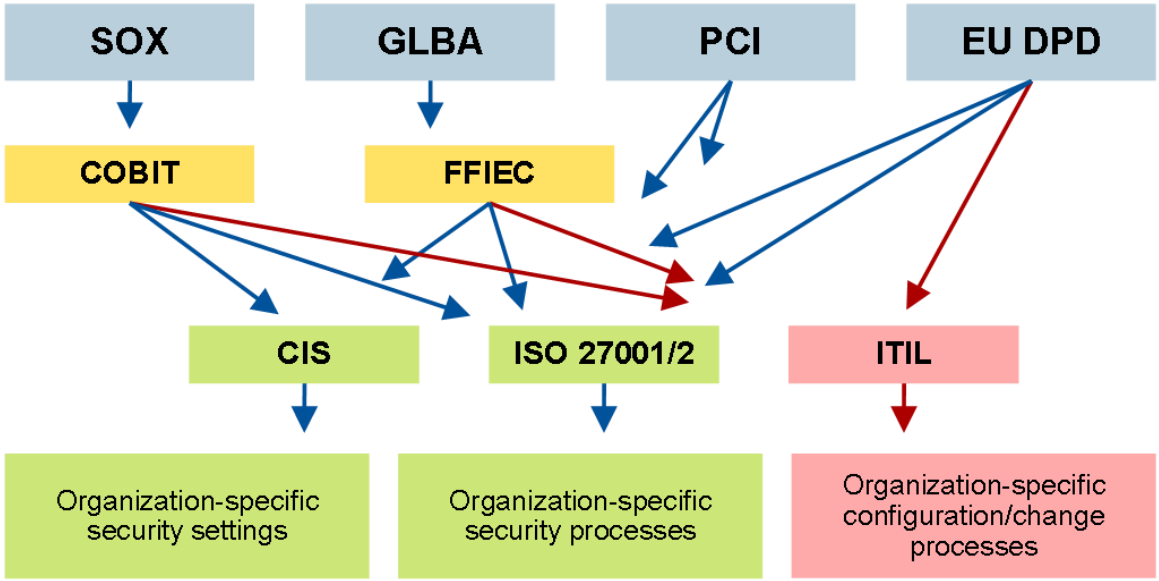
Policy

The vulnerability management life cycle begins with the definition of policies, standards and specifications that define access restrictions, and includes configuration settings that harden the IT infrastructure against external or internal threats. Security configuration policies and specifications should be based on industry-recognized best practices such as the Center for Internet Security (CIS) benchmarks, National Institute of Standards and Technology (NIST) recommendations, or federal mandates such as the Federal Desktop Core Configuration (FDCC). For most organizations, the development of security configuration policies and specifications is an iterative process that starts with industry standards and best practices as a desired state. However, most organizations need to define exceptions in order to accommodate specific applications or administrative processes within their environment. This policy development work

needs to be done with the participation of various administration and support organizations within IT operations.

Organizations should also consider a mapping of organization-specific configuration policies and operational processes to industry-recognized control frameworks and best practices (see Figure 2). Organizations that take the extra step of mapping the policies that are implemented by vulnerability management to control standards and best practices can strengthen their posture with auditors and reduce the cost of compliance reporting through automation. The mapping enables compliance reporting from configuration assessments.

Figure 2. Mapping Security and Operations Controls



CIS = Center for Internet Security; FFIEC = Federal Financial Institutions Examination Council; EU DPD = European Union Data Protection Directive; GLBA = Gramm-Leach-Bliley Act; ITIL = Information Technology Information Library; PCI DSS = Payment Card Industry Data Security Standard; SOX = Sarbanes-Oxley Act

Source: Gartner (January 2011)

Baseline/

The next step is to assess the environment for known vulnerabilities, and to assess IT components using the security configuration policies that have been defined for the environment. This is accomplished through scheduled vulnerability and configuration assessments of the environment.

Vulnerability Assessment

Network vulnerability assessment (NVA) has been the primary method employed by security organizations to baseline networks, servers and PCs. The primary strength of NVA is breadth of coverage. Thorough and accurate vulnerability assessments can be accomplished for managed systems via credentialed access. Unmanaged systems can be discovered and a basic assessment can be completed. The ability to evaluate databases and Web applications for security weaknesses is crucial, considering the rise of attacks that target these components (see Figure 3).

Figure 3. Vulnerability Assessment

	Network	Database	Application
Scope	PCs, servers, network elements and appliances.	Database properties, logs and profiles.	Web-based applications.
Capabilities	Discover missing patches, vulnerable services, weak passwords, misconfigurations.	Determine whether database is configured properly.	Discover Web application security weaknesses.
Limitations	Vulnerability assessment not oriented toward remediation. Database and application assessment is limited.	Vulnerabilities in applications that access the database (such as SQL injection).	Narrow scope and long mitigation if not applied during application development.

Source: Gartner (January 2011)

Database scanners check database configuration and properties to verify whether they comply with database security best practices, but not how a database could be exploited via vulnerabilities in applications that have access to it. Web application scanners test an application's logic for "abuse" cases that can break or exploit the application. All three scanning technologies (network, application and database) assess a different class of security weaknesses, and most firms need to implement all three. Many NVA vendors are expanding the scope of assessment to include Web applications and database management systems. Organizations should evaluate the Web application and database assessment capabilities of their incumbent NVA technology and employ point solutions in these areas if the NVA technology is inadequate. Whereas vulnerability scanning typically provides breadth via automated means, penetration testing augments this approach by providing depth over a narrow focus area coupled with insight into possible exploitation scenarios.

Security Configuration Assessment

A vulnerability management program focusing only on vulnerability assessment is weak regarding a crucial vulnerability management program objective — making the environment more secure. Although vulnerability assessment excels at discovering security weaknesses, its reporting isn't optimized for the mitigation work performed by operations areas. Chasing individual vulnerabilities often does not eliminate the root cause of the problem. A large percentage of vulnerabilities results from configuration issues (missing patches, ports that shouldn't be open or services that shouldn't be running).

Security configuration assessments (SCA) provide a policy-oriented baseline of the environment for security configuration policies that are organization-specific but derived from industry-recognized best practices. An SCA baseline is suited to vulnerability remediation, because configuration management is a core competency of network, server and PC administration areas. Policy development forces collaboration of IT security and operations to develop processes and policies that can eliminate the root cause of configuration or administration-based vulnerabilities. Policy definition and periodic audits are also important components of a regulatory compliance program. Configuration standards are a prerequisite for automated provisioning processes, and support higher levels of availability and reduced operations costs.

Many network vulnerability assessment tools provide a basic agentless security configuration assessment capability. Security configuration management and patch management point solutions also provide the function. Some operational configuration management and provisioning tools provide platform-specific assessment and mitigation functions (see "Security Configuration Management Capabilities in Security and Operations Tools").

Security organizations should work with IT operations to define security configuration standards, and should use the security configuration assessment capability within their incumbent vulnerability assessment tool (if the vulnerability assessment tool provides it) to drive implementation of security configuration standards in desktop, network and server provisioning processes.

Prioritization

Vulnerability and security configuration assessments typically generate very long remediation work lists, and this remediation work needs to be prioritized. When security organizations initially implement vulnerability assessment and security configuration baselines, they typically discover that a large number of systems contain multiple vulnerabilities and security configuration errors. There is typically more mitigation work to do than the resources available to accomplish it.

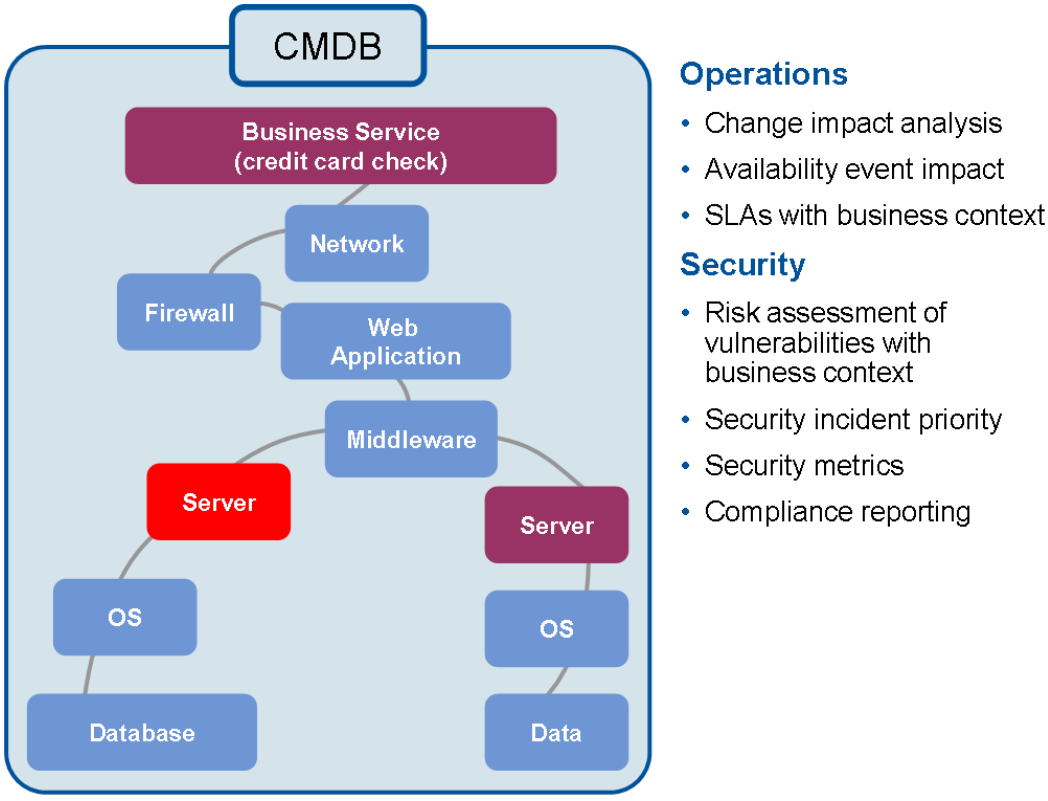
Organizations must implement a process to prioritize the mitigation of vulnerabilities discovered through vulnerability assessments and security configuration audits, and to prioritize their responses to security events. The prioritization should be based on an assessment of risk to the business. Four variables should be evaluated when prioritizing remediation and mitigation activities:

- The nature of the vulnerability and the level of access achieved if exploited
- The likelihood that the vulnerability will be exploited (based on the external threat environment, published exploit code, published exploit automation, mass or targeted attack activity)
- The ability to shield the vulnerable asset from the exploit (typically with network- or host-based security technologies)
- The business use of the application or data that is associated with the vulnerable infrastructure or application

Service Dependency Mapping

Classification of assets according to the business processes that they support is a crucial element of the risk assessment that is used to prioritize remediation activities. Assets should be classified based on the applications they support, the data that is stored and their role in delivering crucial business services. The resource mapping and configuration management initiatives within the IT operations areas can begin to provide the IT resource and business process linkage that is needed for security risk assessment (see Figure 4).

Figure 4. Service Dependency Mapping



CMDB = configuration management database; SLAs = service-level agreements; OS = operating system

Source: Gartner (January 2011)

IT operations areas need service dependency maps for change impact analysis, to evaluate the business impact of an outage, and to implement and manage SLAs with business context. IT operations owns and maintains the asset groupings and asset repositories needed to support service dependency mappings.

This information is typically stored in an enterprise directory, asset management system or a CMDB.

IT security organizations need the same information in order to include business context in the risk assessment of vulnerabilities, to prioritize security incidents, to publish security metrics with business context and to publish compliance reports that are focused on the assets that are in scope for specific regulations.

IT security organizations should engage IT operations areas to determine the sources for IT service dependency maps and should configure security assessment functions to dynamically access or import this data for risk analysis, security monitoring and compliance reporting functions. The security organization should also participate in CMDB projects as a stakeholder and supporter.

Risk Assessment

Larger issues should be expressed in the language of risk (e.g., see ISO 27005), specifically expressing impact in terms of business impact. The business case for any remedial action should incorporate considerations relating to the reduction of risk and compliance with policy. This incorporates the basis of the action to be agreed on between the relevant line of business and the security team

"Fixing" the issue may involve acceptance of the risk, shifting of the risk to another party or reducing the risk by applying remedial action, which could be anything from a configuration change to implementing a new infrastructure (e.g., data loss prevention, firewalls, host intrusion prevention software). Elimination of the root cause of security weaknesses may require changes to user administration and system provisioning processes. Many processes and often several teams may come into play (e.g., configuration management, change management, patch management). Monitoring and incident management processes are also required to maintain the environment.

Shielding and Remediation

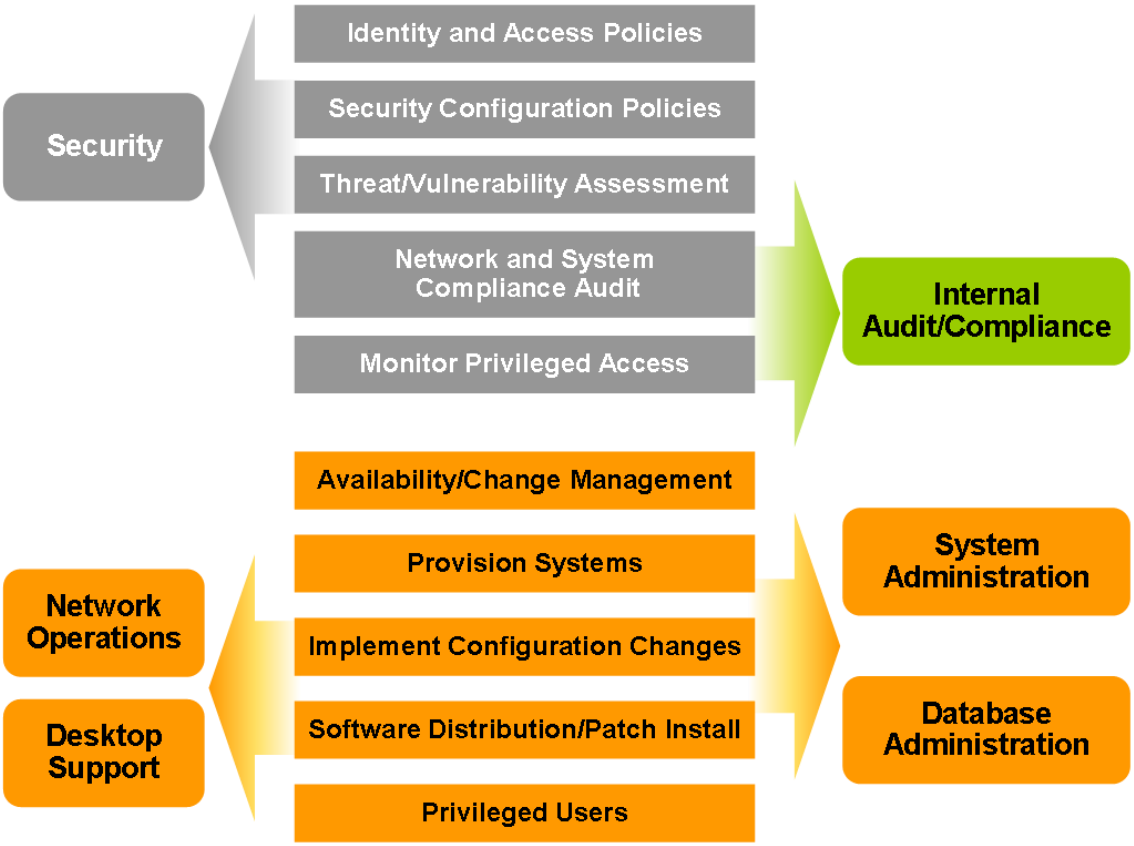
Security is improved only when mitigation activity is initiated as a result of the baseline and monitoring functions. Remediation is facilitated through cross-organizational processes and workflow. Although the vulnerability management process is security-focused, the majority of mitigation activities are carried out by IT operations areas, such as network operations, desktop support, server administration and database administration. Mitigation processes are supported through workflow and incident management.

Remediation Workflow and Segregation of Duties

Organizational structure and separation of duties dictate that security teams should be responsible for policy development and assessment of the environment, but should not be responsible for resolving the vulnerable or noncompliant conditions. Information sharing between security and operations teams is crucial to properly using baseline and monitoring information to drive remediation activities.

Vulnerability management products should provide native support for incident and case management that is oriented to the needs of the IT security organization. These products should also provide interfaces to enterprise workflow systems so that mitigation tasks can be assigned to the appropriate groups within IT operations and application support (see Figure 5).

Figure 5. Security and Operations: Integrated Processes With Segregation of Duties



Source: Gartner (January 2011)

Vulnerability and security configuration assessment technologies collect and store sensitive information on the vulnerability and security state of the IT infrastructure and applications. This road map of vulnerable systems can easily be used to gain unauthorized access or disrupt services if in the hands of a malicious interloper. Security organizations should share vulnerability data with the operations areas that are responsible for mitigation, but only to the degree that supports mitigation. Develop reports that are organized for mitigation activity. Implement strong role-based access control and ensure that the concept of least privilege is used so that no single role, user or group can view more data than is required for them to perform their duties. This entire area needs to be re-evaluated in light of the changes brought by virtualization.

Root Cause Elimination

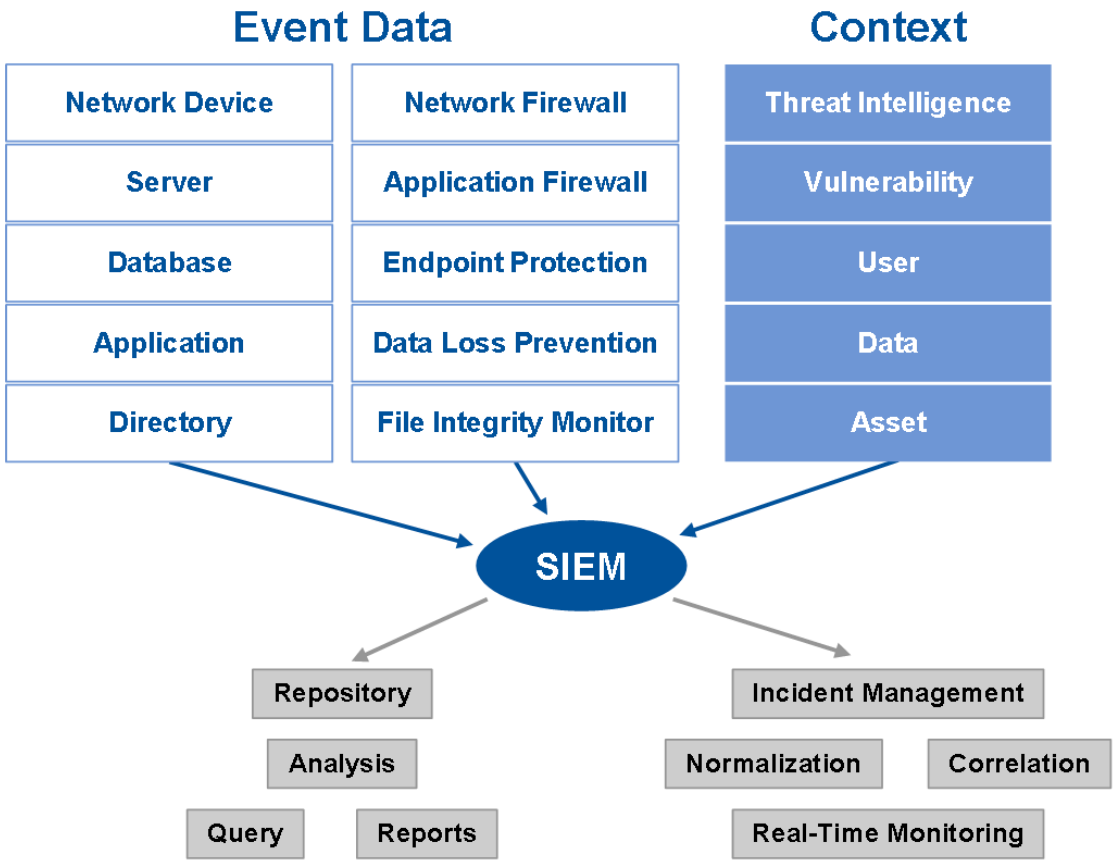
It is important to analyze security and vulnerability assessments in order to determine the root cause. In many cases, the root cause of a set of vulnerabilities lies within the provisioning, administration and maintenance processes of IT operations or within their development or the procurement processes of applications. Elimination of the root cause of security weaknesses may require changes to user administration and system provisioning processes. IT security

organizations need to drive project work to resolve these issues. Many processes and often several teams may come into play (e.g., configuration management, change management and patch management).

Monitoring

While a vulnerability management program can make an IT environment less susceptible to an attack, assessment and mitigation cannot completely protect the environment. It is not possible to immediately patch every system or eliminate every application weakness. Even if this were possible, our users would still do things that allowed malicious code on systems. In addition, zero-day attacks can occur without warning. Since perfect defenses are not practical or achievable, organizations need to augment vulnerability management and shielding with more-effective monitoring. Targeted attacks take time to execute, and the longer a breach goes unnoticed, the greater the damage. Better monitoring is needed to detect targeted attacks in the early stages, before the final goals of the attack are achieved. Use security information and event management (SIEM) technologies or services to monitor, correlate and analyze activity across a wide range of systems and applications for conditions that might be early indicators of a security breach (see Figure 6).

Figure 6. Security Information and Event Management



Source: Gartner (January 2011)

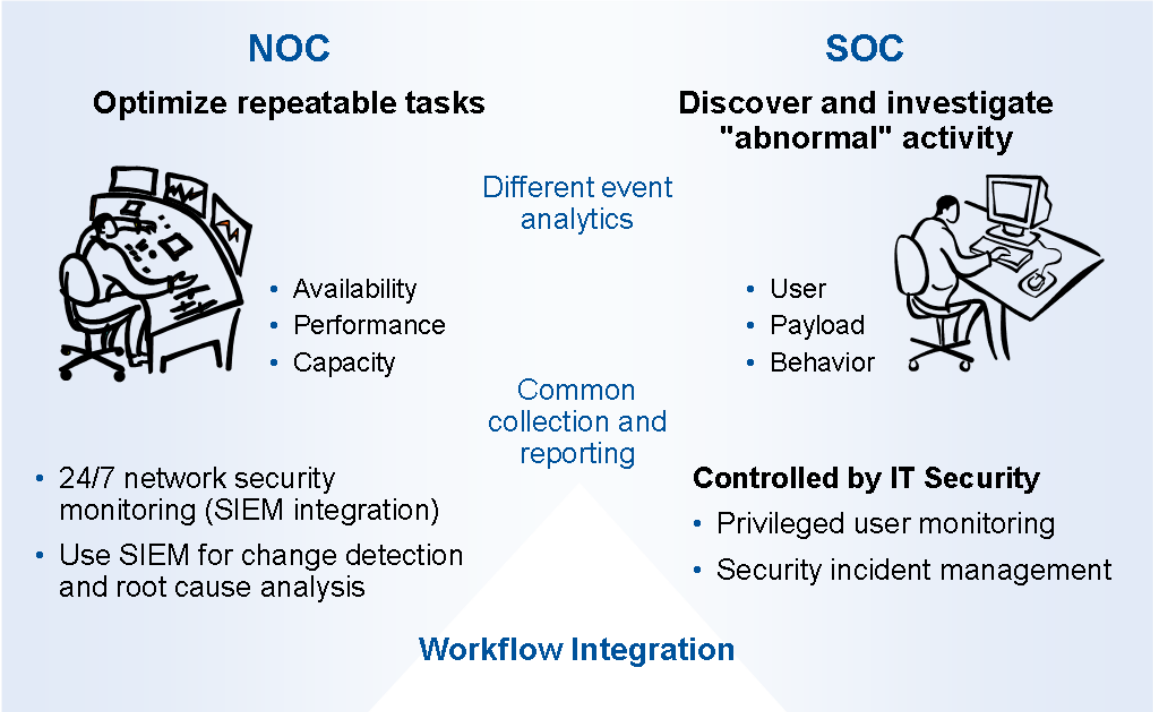
SIEM technology and services provide broad-scope monitoring of events from network and security devices, servers, database management systems, directories, identity and access

management infrastructures, and applications. SIEM provides security information management functions: Event data is normalized, indexed, compressed and stored, and reporting and search capabilities are supported. SIEM technology also provides security event management functions — real-time monitoring, event correlation and incident management. Security organizations should use SIEM to monitor and analyze activity across a wide range of systems and applications for conditions that can be defined through filters and correlation rules, and conditions that can be discovered through anomaly detection.

Security Monitoring: Integration Opportunities and Limitations With IT Operations

Event monitoring is needed by both security and operations, and both areas need to monitor applications and IT infrastructure. There are overlaps in technologies, requirements and processes, but significant differences will impede full convergence indefinitely (see Figure 7).

Figure 7. Security and Operations Monitoring Integration Opportunities and Boundaries



NOC = network operations center; SOC = security operations center

Source: Gartner (January 2011)

Both the security and operations organizations need to collect, store and analyze event information from the same sources (network, security, server, PC, application and data components). There is an opportunity to implement a shared infrastructure to collect, normalize and store events. Another area of convergence is the use of operations event consoles to externalize critical events uncovered by security event management functions. This allows IT operations staff to provide 24/7 monitoring, with security specialists providing on-call Level 2 support. Workflow integration is also required.

The obvious place where security and operations event monitoring differ is in what each seeks in the events. Security requirements focus on user behavior and access patterns, as well as

configuration changes that indicate an actual or a suspected violation of data confidentiality or integrity. Operations requirements typically focus on the availability and performance of application, infrastructure and software components. Still, there's room for convergence on many levels. The analysis engines are different, potentially coming from diverse vendors.

There are also some boundaries in the areas of monitoring and incident response. Some monitoring and incident management tasks are too sensitive for IT operations involvement and so there is a need for strong role-based access controls on security monitoring and incident management functions.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner