WHITE PAPER

symantec.

Managing Security Incidents in the Enterprise

INSIDE

INSIDE

- The need for security incident management
- Understanding the value of security investments
- Characteristics of an effective incident management system
- Symantec™ Incident Manager

Contents

Executive summary

The engines of business growth in today's economy are often the information systems that control supply chains, track transactions, coordinate customer service, and so forth. When enterprises provide application access to employees on the road or in corporate offices, as well as partners, suppliers, and customers, much of the associated application data travels over the public Internet. Each application introduces some level of information security risk, and every new user group or access channel adds to that risk. Trading away security for the competitive benefits and efficiency offered by new systems is not an attractive choice. In many cases, new systems and technologies are adopted despite the increased risk and the challenges security teams have to secure them.

Most companies employ a variety of technologies to identify and thwart suspicious activity. For instance, firewalls detect suspect activity at the perimeter of a network. Antivirus packages identify malicious code entering companies' systems from various sources. Intrusion detection software scans packets on networks and monitors a variety of questionable activities on application servers and at the operating system level.

As effective as these point products are however, they do not offer the coordinated level of protection against the myriad threats to corporate information security. Many companies have full-time information security professionals who face the daunting task of trying to manage these disparate products. The data generated by these products each day can add up to gigabytes of log information across thousands of systems. Lack of coordination and the resulting isolated silos of vast amounts of data make it difficult, if not impossible, for security administrators to gain a complete picture of an enterprise's overall security situation, let alone implement timely, appropriate corrective actions to improve their security posture or respond to an attack.

Many organizations are seeking to reduce this level of risk and control the cost of doing so. Adding improved sensors will likely prove an insufficient measure to achieve this goal. Integrated incident management across multiple disparate sensing and protection technologies is the new paradigm that companies can adopt to achieve the dual goals of reducing risk and controlling cost.

This paper explains the difficulty enterprises face maximizing current security product investments and the increasing need for security incident management. It then defines the characteristics of an effective incident management system, and the implications for enterprises with no effective incident management system, as well as the benefits for those with one in place. Finally, the paper discusses Symantec™ Incident Manager, a new solution that can help enterprises maximize the value of their existing security investments.

The need for security incident management

Today's executives and security managers are under pressure to provide an open, collaborative networking environment, while protecting the company from potential legal liabilities and the financial impact of security breaches. Enterprises have responded by deploying a combination of security products and services from different vendors. These technologies, such as virus protection, firewalls, and intrusion detection, are excellent within their intended sphere, but do not provide sufficient protection from advanced, blended threats (such as Code Red and Nimda), for the following reasons:

- Because networks and applications constantly change, implementing protection with independent tools becomes unwieldy
- Protecting multiple network vulnerabilities requires analysis across the data generated by these disparate protection technologies
- The sheer volume of data generated by protection technologies is difficult, if not impossible, to manage manually
- The chronic shortage of skilled staff and budget constraints limit the number of dedicated security personnel that can analyze, and respond to, security threats

The fact is that the current layered model of security is complex, unmanageable, and insufficient to help a company maintain a strong security posture. Resource-constrained security administrators must respond to critical security incidents (such as attacks, virus outbreaks, or discoveries of vulnerable systems) with only sub-optimal and disjointed security data as guidance. Organizations do not accurately perceive their risk profile. Attacks are going undetected and business losses from security incidents are on the rise. Over the past three years, reported losses from security incidents have increased, on average, 59% each year. Of 455 companies surveyed, 80% acknowledged financial losses.[1] So, despite considerable investment in detection and prevention applications from a variety of vendors, enterprises still struggle to preserve a secure environment.

DELIVERING VALUE – AN EFFECTIVE SECURITY MANAGEMENT PARADIGM

Ensuring the effectiveness of existing security investments is top of mind throughout the enterprise. Investors, partners, customers, and the general public expect companies to comply with regulatory requirements, minimize legal liability, accept fiduciary responsibility, and meet security requirements to maintain their reputation and customer/client confidence. Chief financial officers and others responsible for security budgets are aware of the considerable monies allotted to protecting the network and information assets. In fact, IDC estimates that annual worldwide spending on security software will reach $14 billion by 2005.[2] But will these funds improve corporate security? What is required to actually improve an organization's risk profile?

With the limitations of the current approach to security so painfully evident, it is clear that a new paradigm is needed.

[1] Power, "2002 CSI/FBI Computer Crime and Security Survey," "Computer Security Issues & Trends," vol. 8, no. 1, Spring 2002, p. 11.
[2] Burke, Christiansen, Kolodgy, "Worldwide Internet Security Software Market Forecast and Analysis, 2002–2006: Vendor Views," IDC, July, 2002

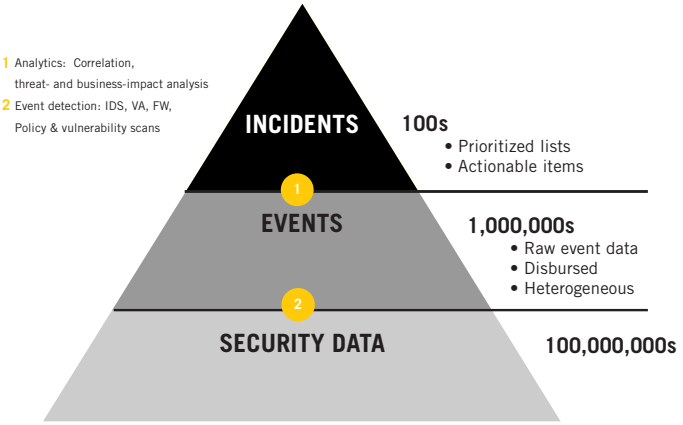
Incidents vs. events

Security products throughout the enterprise scan systems and network traffic and report on potentially suspicious activity. Each report is termed a security *event*, and many thousands of events occur each day in organizations of moderate size. An event may be anything from a malformed or over-length network packet to a failed login on a computer. Determining whether any given event indicates trouble is difficult. Malformed packets can be malicious—potentially indicating a buffer-overflow attack—or they can simply be innocent anomalies. Failed logins can signal an attempt to break into a system or they can be the result of simple typographical errors. Additional context is required to determine whether a problem exists and if so, what action is required. Lacking that additional context, companies who focus on event management suffer from poor coordination, waste time on events that are "false positives," and operate generally in a reactive and chaotic mode.

An *incident* is a set of one or more security events or conditions that requires action and closure in order to maintain an acceptable risk profile. In the haystack of events, organizations must find the "needles" that are the security incidents. Events are isolated and disconnected, but incidents add the context that enables security administrators to gain understanding and take action.

Defined in this way—as a set of events or conditions requiring response and closure—incidents comprise not only the significant threats that jeopardize business and require intervention. They include more mundane situations that occur on a daily basis and only threaten the business if *no* action is taken. Examples of these routine situations include "low and slow" port scans and some varieties of email worms. Most organizations face thousands of instances of the latter types of threats, together with the higher profile blended threats like Code Red, Nimda, and Klez.

Besides attacks, known system vulnerabilities or discovered policy violations are also incidents that require a response in order to protect the business. When related events (e.g. attacks, vulnerabilities, and policy violations) are viewed together, the true nature (or type) of the incident becomes evident. Changing from an event management to an incident management approach allows technicians to understand:



- SCOPE the number of systems affected
- IMPACT the degree to which each system is affected in terms of confidentiality, integrity and availability
- BUSINESS CRITICALITY the importance of the incident based on the business value of the impacted systems relative to other systems
- PRIORITY the urgency of the required response relative to other incidents

An incident-centric approach simplifies many of the otherwise complex and burdensome tasks of security management. Effective incident management reduces the volume of data that requires monitoring and also allows response activities to be prioritized based on a unified view of the business impact of each incident.

Incident management is proactive, controlled and consistent. In contrast, an event-centric approach ignores critical characteristics of incidents that are essential to an effective and complete response. Furthermore, relying solely on manual methods of identifying incidents is impractical and increases the likelihood of poor response decisions.

What an effective incident management system must do

An effective incident management application can help enterprises manage risk and maximize the value of current security technologies. It should do the following:

- Consolidate heterogeneous inputs
- Identify incidents
- Prioritize incidents based on business impact
- Track incidents to closure
- Integrate with major IT management systems
- Implement best practices guidelines

EVENT CONSOLIDATION

The foundation of any incident management application is the ability to collect information from sensor products throughout the enterprise. Most companies adopt a best-of-breed approach and purchase protection products from several vendors. This can increase the level of protection, but it also increases the challenge of managing multiple disparate products. A competent management system consolidates messages from the contributing sensors and stores, displays, and reports on them in a unified fashion.

Since products from different vendors use varied message formats to express similar events or conditions, a common message vocabulary—into which all messages are translated—must be used. This translation, commonly called *normalization*, is a critical part of the consolidation operation.

INCIDENT IDENTIFICATION

Complete and accurate identification of an incident is necessary before resolution can occur. Comprehensive incident management applications provide tools to help operators identify important characteristics of an incident so that appropriate activities can be executed to achieve closure. Although the process of incident response involves human expertise, significant portions of the process can be automated so that security staff can focus on activities that best leverage their skills.

Correlation—associating two or more factors into a unit—is an effective technique for identifying incidents. Two types of correlation are essential when identifying information security incidents: 1) event-to-event correlation, and 2) event-to-vulnerability correlation. The first type of correlation determines the scope of the incident, and the second type indicates whether the incident will impact the business (events that do not exploit a vulnerability in the system generally do not affect business operations.) By associating events to form incidents, correlation helps operators to completely and accurately identify important characteristics of the incident, thereby laying the foundation for successful resolution.

PRIORITIZATION AND BUSINESS IMPACT ANALYSIS

Individual incidents can vary widely in terms of scope and criticality. The challenge for security teams is to strategically allocate resources (often simultaneously) based on the potential business impact of the various incidents they must resolve. Comprehensive incident management applications can help.

To determine prioritization, the incident management system needs to know the value of systems and information that can potentially be impacted by security incidents. This may entail someone within the organization assigning a *monetary* value to each computer and file on the network or assigning a *relative* value to each system and the information on it.

System value can be rated in three different ways:

1) Confidentiality of the information
2) Integrity of the applications and information
3) Availability of the system

Each of these system values is an independent valuation of a system to the business. For example, a public Web server may possess low confidentiality requirements (since all the information is public), but high availability and integrity requirements. In contrast, an Enterprise Resource Planning (ERP) system may score high in all three areas.

An effective incident management application accounts for these separate measurements and prioritizes incidents based on the potential loss to the business. The application also calculates the priorities that it assigns in relation to other incidents that are currently being tracked.

TRACKING INCIDENTS

Complete and accurate identification of an incident is necessary before effective resolution can occur. Comprehensive incident management applications provide tools to help operators identify important characteristics of an incident so that appropriate activities can be executed to achieve closure. The SANS institute has articulated a thorough framework for incident handling that lends consistency to an often muddled process. Between identification and closure, according to SANS, the following types of activities should occur:

- CONTAINMENT Limiting the scope and magnitude of the incident
- ERADICATION Eliminating the source of the problem or avenue of entry
- RECOVERY Returning affected systems to their fully operational state
- FOLLOW-UP Documenting the impact of the incident and implement measures to avoid recurrence[3]

Many organizations continue to suffer the effects of attacks long after they occur because security personnel do not consistently track incidents to closure through these phases.

Organizations can realize measurable benefits by implementing an incident management system that tracks and reports on incident handling activities in the context of each of the phases that SANS has identified. Many security-savvy organizations execute Service Level Agreements (SLAs) that define a required response within a specified timeframe for each of these phases. An incident management application that models SLAs and issues alerts as deadlines approach can help organizations meet their response targets and ensure business continuity.

[3] The SANS Institute, "Computer Security Incident Handling Step by Step," Version 1.5, May 1998.

ENTERPRISE-WIDE INTEGRATION

Incident management applications do not exist in a vacuum. While they primarily serve the information security team, this team depends on the larger IT organization to implement secure computing. Hence, comprehensive incident management applications should integrate with applications such as network management system frameworks and helpdesk systems to extend the scope of security management.

BEST PRACTICES GUIDANCE

The shortage of experienced information security staff poses one of the greatest challenges to security teams—a situation that is likely to continue for the foreseeable future. In addition, many organizations are consolidating all network monitoring operations, including security monitoring, into a centralized Network Operations Center (NOC). To ensure optimal operations, information security teams need to enhance the expertise of the network technicians assigned to these monitoring duties. Incident management applications can help by providing access to expert information and best-practice guidance within an organization's operational policies.

What if no incident management system is in place?

Enterprises seek to increase their competitiveness via technology, yet this reliance on technology means more security risks. These security risks translate into an unacceptable risk profile for the organization and, without an effective incident management system in place, the company experiences costs on many levels, such as the following:

Operational costs include monitoring, sensor management, training, reporting and auditing. Without an effective incident management system, it is inefficient for staff to monitor and review event logs from disparate products; a significant amount of time is spent investigating false positives. In addition, training and turnover are constant challenges for the teams that monitor security and handle front-line response duties. Staffing these positions is difficult and expensive due to the chronic scarcity of experienced security personnel. Accordingly, organizations that rely on manual incident identification and handling typically face more risk and incur higher costs.

Recovery costs include response and system recovery. Organizations are spending increasing amounts to recover from security problems that affect their computing infrastructure. It can cost more to respond to and recover from incidents that are not discovered and dealt with rapidly, as these incidents often affect various systems before they can be contained. In addition, restoration of impacted systems results in downtime and disrupts business processes that rely on those systems. Accordingly, organizations that rely on manual incident identification and handling typically face more risk and incur higher costs.

Ineffectively handled incidents can result in business impairment, such as halted operations, legal liability, reduced competitiveness, and damaged brand equity. Downtime due to a security incident results in lost productivity and revenues—when business operations are halted, employees, partners, and customers do not have access to critical systems and information. Should a security incident compromise an organization's compliance with privacy and security regulations, the company may incur additional expenses to comply with regulatory or court orders. Many of today's security attacks are focused on the theft of proprietary company information. The loss of such assets can pose serious consequences, including damaged brand equity and the inability to effectively compete in the marketplace.

Without an effective incident management system in place, security administrators will continue to struggle to gain a comprehensive view of the company's overall security posture, maintain an acceptable risk profile, and control the cost of doing so.

Symantec™ Incident Manager

Symantec Incident Manager, a real-time incident management application, helps enterprises maximize the value of their security technologies, and identify and respond rapidly to security breaches.

DATA CONSOLIDATION ACROSS DISPARATE SOURCES

Symantec Incident Manager consolidates messages from key third-party products and displays them in a unified central console. Symantec Incident Manager is built in compliance with the Symantec Enterprise Security Architecture (SESA™) which allows multiple protection products from disparate vendors to be "plugged-in" and report events in a common format to a centralized DataStore. This clean event stream is the foundation of the system's other real-time incident handling capabilities. It eliminates the time-consuming effort required to manage security using multiple management consoles from point products, enabling the rapid transformation of security data into actionable, prioritized intelligence.

ATTACK ANALYTICS

Symantec Incident Manager embeds attack analytic technology that eases the process of correctly and completely identifying the boundaries and characteristics of each incident. Network technicians can use the system in the NOC to perform monitoring functions that were once handled by dedicated security staff, as the solution simplifies and automates the identification process. Security personnel are then free to focus on more strategic initiatives.

DYNAMIC PRIORITIZATION

A risk analysis engine determines the business impact of each incident based on the relative confidentiality, integrity, and availability ratings of each asset in the system. The risk analysis engine accounts for actions taken to resolve an incident and dynamically balances the priority of each incident compared to all open incidents. The result is incident prioritization that simplifies the problem of responding to multiple incidents, allowing security staff to focus resources on solving the most critical problems first.

INTEGRATED MANAGEMENT

Symantec™ Incident Manager integrates with the leading antivirus, intrusion detection, and firewall solutions from both Symantec and third-party vendors. This integration of disparate security systems allows issues to be prioritized and tracked to closure so that the security staff can operate from a single actionable list. In addition, its alerting and escalation functions can interoperate with helpdesks and network management systems, thereby extending visibility into events and incidents.

DYNAMIC GUIDANCE

Symantec Incident Manager provides expert guidance tailored to the specific characteristics of each incident. Guidance is provided within the widely acknowledged SANS/CERT incident response framework[4] and powered by security intelligence from Symantec. The system utilizes a comprehensive database of attack signatures, vulnerability information, safeguards and response guidance, regularly updated by Symantec Security Response, the world's leading Internet security research and support organization.

MEASUREMENT AND REPORTING

Comprehensive reporting captures every action taken to identify and resolve an incident. This enables the system to generate reports that illustrate the type and severity of threats, as well as the effectiveness of the organization's response. It also maintains a comprehensive log of resolution activities that analysts can annotate to record the rationale and authorization for each decision. This resource can be leveraged to meet audit requirements and improve response procedures.

Benefits of Symantec Incident Manager

By prioritizing incidents, providing best practices response guidance, and tracking incidents to closure, Symantec Incident Manager increases the effectiveness of response activities and reduces the cost of managing risks.

REDUCE COSTS

Effective incident management, aided by Symantec Incident Manager, can reduce the cost of incident response to the organization in the four key areas of monitoring, response and recovery, false positives, and training.

- MONITORING COSTS With Symantec Incident Manager, information security monitoring activities can be consolidated from multiple different silos into the NOC (or SOC, where appropriate). The central console provides technicians a unified view of security incidents. The correlation and attack analytics reduce the amount of data that must be manually reviewed, so staff can focus on actionable incidents. The result is that fewer people are required to monitor security and better coverage of the reported information is achieved.
- COSTS OF FALSE POSITIVES Symantec Incident Manager enables security personnel to differentiate between real threats and false positives. Security staff are better able to allocate their time and focus on activities which add real value.

[4] The SANS Institute, "Computer Security Incident Handling Step by Step," Version 1.5, May 1998.

- RESPONSE AND RECOVERY COSTS Symantec™ Incident Manager's dynamic guidance, prioritization, and security intelligence enable front-line monitoring staff to handle most incidents before they grow out-of-control. Accurate, real-time incident identification enables organizations to respond in time to contain an incident, rather than after the damage is done. Hence, the total response cost is controlled because problems are solved before they spread.
- TRAINING COSTS The regularly updated security intelligence and dynamic guidance included in Symantec Incident Manager reduce the need for classroom training. Staff learns on-the-job and keeps up-to-date on the latest threats, vulnerabilities and safeguards.

IMPROVE SECURITY RESOURCE ALLOCATION AND EFFICIENCIES

In addition to significantly reducing the cost of security in the enterprise, Symantec Incident Manager improves enterprise resource allocation and security processes. By helping enterprises clearly and rapidly identify and prioritize incidents, this solution enables enterprises to balance resources based on the benefit to the business at any given time. Symantec's security expertise means that security teams can leverage other IT personnel to augment security efforts, and are freed up to focus on revenue-enhancing initiatives.

FACILITATE EFFECTIVE SECURITY AND HELP ORGANIZATIONS ACHIEVE AN ACCEPTABLE RISK PROFILE

Symantec Incident Manager facilitates the execution of effective risk management and enables total risk levels to be lowered economically. The ability to respond more quickly and effectively to discovered vulnerabilities and active attacks reduces the probability that the business will be damaged, while also reducing the severity of any damage that may occur. By making better use of the information that each point product provides, the solution increases the value of each of these point products, and hence the value of the entire security infrastructure. In this way, Symantec Incident Manager can reduce security risks while actually improving the return on investment that enterprises realize on their existing security infrastructure.

Summary

Enterprises build their competitive differentiation on the business assets that reside in a complex information infrastructure. The more reliant a company becomes on that infrastructure, the greater the risk it faces, especially with the growing incidence of network attacks of all types. While companies have responded to today's sophisticated network threats with a variety of security products, security efforts are hampered by the lack of coordination amongst these products and the data they generate. Enterprises are thus challenged to minimize their risk and realize a measurable return on their current security investments. Yet in today's economic climate, companies need to fully leverage and maximize the value of their technology investments.

Organizations that make better use of the information generated by isolated protection products can achieve an integrated approach to security and incident management, thus lowering costs and improving their overall risk profile. Symantec Incident Manager can help by aggregating security data across the enterprise and providing a framework and tools for timely and effective incident identification and resolution. By providing a comprehensive view of a company's overall risk exposure, organizations can effectively manage their security posture and realize a better return on their security investments.

SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOLUTIONS TO INDIVIDUALS AND ENTERPRISES. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY MANAGEMENT, INTRUSION DETECTION, INTERNET CONTENT AND EMAIL FILTERING, REMOTE MANAGEMENT TECHNOLOGIES, AND SECURITY SERVICES TO ENTERPRISES AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS LEADS THE MARKET IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM.

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408.517.8000
800.721.3934

www.symantec.com

For Product information in the U.S., call toll-free 800.745.6054.

Symantec has worldwide operations in 38 countries. For specific country offices and contact numbers please visit our Web site.