

Thinking about Security Monitoring and Event Correlation

Billy Smith 2000-11-03

Background

Over the past several years, there has been explosive growth in information technology due, in most part, to the Internet. Today, corporate networks are very complex. Much of this complexity is an indirect result of the Internet's rapid growth. The increased use of the Internet particularly by business has forced corporations to expand their information technology infrastructures significantly. As a result, information security incidents have grown at an even faster rate and are now a major concern globally.

Information security incidents can be characterized as the lack of availability, integrity, and/or confidentiality of data. Software and hardware vendors have dedicated a tremendous amount of research and development resources towards insuring information availability, integrity and confidentiality. This research has led to the development of security devices such as firewalls, intrusion detection systems, strong authentication and access control mechanisms, virtual private networks and public key infrastructure. Organizations worldwide are implementing these technologies to prevent or detect an information security incident.

Introduction

Most security devices provide logging and alerting of known and possibly unknown security events that occur on an information technology infrastructure. Despite all our technological advances and the introduction of devices like firewalls and VPNs, most companies do not monitor the information coming from these devices.

Security device logging can be extensive and difficult to interpret. Due to the detail and size of the logs, it is time consuming to manually review them. In many organizations, a dedicated staff of information technology personnel is not available to continuously monitor logs and alerts or network and system administrators use routine maintenance to review security information. This limited or non-existent monitoring of enterprise security leaves organizations blind to information attacks targeted at their corporate networks. Security logs provide details about the activity on a corporate information technology infrastructure. This activity includes valid business applications, external attacks using the Internet and internal attacks by employees. Recognizing their vulnerability, management is being forced to find a solution

quickly and is looking outside for the management of their security infrastructure. Third party management of firewalls is already commonplace, and management of intrusion detection systems is becoming more common.

But this need for outside security management has become more than just monitoring the alerts from a network-based or host-based intrusion detection system; it has become 24 x 7 security monitoring of the entire enterprise.

Security Monitoring

Today only a few companies are offering 24 x 7 enterprise-wide security monitoring services and even fewer include monitoring events from firewalls and network-based and host-based intrusion detection systems as well as the logs and alerts from routers, switches, anti-virus and content scanning applications, backup applications, PBXs and critical Unix and NT servers including but not limited to web servers, FTP servers and mail servers. In the future enterprise security monitoring will incorporate security events from physical security devices such as card readers, motion detectors and cameras, security alarms from secured doors and gates, fire alarms and climate control sensors.

Each device or application listed above can generate hundreds of lines of logs daily. A majority of the events logged are not security related so surveillance of specific security events is difficult and time consuming. For many administrators, reviewing these logs takes several hours a day and monitoring should be in real-time or near real-time so problems can receive a rapid response. For the typical system administrator, network administrator, and/or security officer, the task of reviewing logs is not a reality and monitoring events in real-time is impossible, day-to-day system maintenance demands too much time. Companies just do not have a 24 x 7 information technology staff so "off business hours" monitoring is nonexistent and internal and external hackers know this.

Some vendors do provide tools to condense their product events and logs, but even with these tools it is nearly impossible for an administrator to find time to monitor a security system, enterprise-wide. Most of these consolidation tools are vendor specific. Vendor A's tool can only be used to accept logs or events from Vendor A's products while Vendor B's tools can only be used to consolidate Vendor B's products. The reason for this is that Vendor A's products and Vendor B's products log event information differently. This situation forces administrators to have many different tools to monitor logs and event information throughout their enterprise.

Today, there are only a few companies that provide vendor independent log and event consolidation solutions, but these solutions demand an extensive amount of customization to be useful in monitoring security events enterprise-wide.

Along with lack of time and vendor independent tools, false positives are another reason why enterprise security monitoring is not easy. A false positive is when an event triggers a security alert, but the event is not security related. There has been a lot of discussion over the last year regarding intrusion detection systems and false positives. In order to have extensive "vision" on a host or network, a host-based or network-based intrusion detection system needs to be configured "loosely" so that a high number of false positives are generated. The problem with this is that many administrators do not have the time or knowledge to research the quantity of events generated by these "loosely" configured intrusion detection systems. Host-based and network-based intrusion detection systems are only two types of devices that generate false positives. Many other security devices produce them as well.

Monitoring an entire security enterprise takes an experienced 24 x 7 staff of security analysts who have responsibility for continuously analyzing events and filtering out the false positives. For an enterprise security manager a large number of false positives are difficult to manage because they do not have a dedicated security staff, so people are diverted from their regular work to respond to false attacks. But, false positive analysis is critical to protecting an organization's information assets. Is there another way? Maybe.

Event Correlation

The next advance in enterprise security monitoring will be to capture the knowledge and analytical capabilities of human security experts for the development of an intelligent system that performs event correlation from the logs and alerts of multiple security technologies.

For example Company A has a screening router outside of their firewall that protects their corporate network and a security event monitoring system with reliable artificial intelligence. The monitoring system would start detecting logs where the access control lists or packet screens on the screening router were denying communications from a certain IP address. Because the intelligent system is intelligent it begins detailed monitoring of the firewall logs and logs of any publicly accessible servers for any communications destined for or originating from the IP address. If the intelligent system determined that there was malicious communication, the system would have the capability to modify the router access control lists or the firewall

configuration to deny any communication destined for or originating from the IP address. In this example, the access control lists deny logs from the router triggering the intelligent system to "look for" suspicious activity from a certain IP address. Using event correlation the reaction mechanism has more time to monitor and react to an attacker. If the system did not correlate events, the system would only detect an event that had already occurred based on a known attack signature or the system might even read a malicious attack as "normal" traffic.

What if the intelligent system began detecting multiple failed logins to an NT server by the president of the company? It would be useful for this technology to determine where these failed logins were originating from and "look for" suspicious activity from this IP and/or user for some designated timeframe. If this system determined that the failed logins originated from a user other than the president of the company, it could begin to closely monitor for a period of time all actions by this user and the company president (the user could be impersonating the president). This monitoring could include card readers, PBXs or voice mail access, security alarms from secured doors and gates and access to other servers. If the monitoring system were not correlating events the user impersonating the company president would probably bypass all access control and security monitoring devices because the user's actions appear as "normal" activity.

Today there is one major obstacle to intelligent event correlation enterprise-wide. There is no standard for logging security related information or alerts. Every vendor uses their own logging or alerting methodology on security related events. In many cases there are inconsistent formats among products from the same vendor. These issues make enterprise security monitoring difficult and event correlation almost impossible with artificial intelligence. The industry will need to impose a standard method or protocol for logging and alerting security related events before an intelligent system can be developed and successfully implemented enterprise-wide.

Conclusion

The usefulness of developing an intelligent monitoring system that performs event correlation for internal and external security events is obvious. Today security technology needs human intervention and action. 9 to 5 security monitoring by an already busy IT staff is not enough for organizations to maintain maximum information security and integrity. They need a dedicated team of security analysts continuously looking at their enterprise-wide security infrastructure. This team needs to spend the time to research false positives so they can build a database of

events for comparison and correlation. And of course there needs to be a security analyst monitoring the enterprise 24 x 7, ready to respond to malicious attacks and anomalies according to predetermined policies and procedures. For most organizations 24 x 7 monitoring is too expensive, but as information integrity is compromised and downtime increases the effect on the bottom line becomes real. The most effective alternative to internal monitoring is to outsource an organization's security management and monitoring to a company that has the experience and expertise to share responsibility, 24 x 7, for an organization's information assets. Until we have artificial intelligence available, we can rely on human intelligence to keep our information secure.

Billy Smith is the Surveillance and Countermeasures Research and Development Team Leader at LURHQ Corporation in Myrtle Beach, SC. Smith recently completed the development and testing of Managed SherlockESM, a 24 x 7 enterprise-wide, event correlation and security monitoring service that includes real-time reaction and response. He regularly is contracted by businesses to provide forensic analysis and incident response. Smith has a Bachelor of Science degree in Applied Mathematics from The Citadel.

Relevant Links

[Subscribe to the FOCUS-IDS Mailing List](#)

SecurityFocus.com

[Managed SherlockESM](#)

LURHQ Corporation

[Privacy Statement](#)

Copyright 2006, SecurityFocus