Essential IT Monitoring: Top Five Priorities for Network Security

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for SolarWinds

October 2013

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Essential IT Monitoring: Top Five Priorities for Network Security

Table of Contents

Essential IT Monitoring: Top Five Priorities for Network Security

Essential Security

Fundamental to achieving effective enterprise IT management is enabling comprehensive visibility into all essential technology configurations, performance, and status. To enable a consolidated view, these monitoring practices must cross multiple management disciplines, and each organization will have unique sets of requirements that will define which disciplines align most appropriately with their business. Therefore, ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts recommend the adoption of management solutions that are modular and fully integrated, allowing each organization to select the most appropriate combination of administrative resources to establish a complete view of its distinctive support stack from a "single pane of glass."

EMA's series of *Essential IT Monitoring* white papers identifies key elements enterprises must target in particular management disciplines in order to rapidly identify and resolve issues and to optimize performance across IT infrastructures. Readers are advised to adopt integrated, automated monitoring solutions that bring visibility to all the identified elements in the topic areas most applicable to their IT implementation.

Top Five Priorities for Network Security

Given that there is no perfect security, and any control may fail at any time leaving assets open to some sort of harm, security professionals must keep several paradigms in mind.

Most security programs start with the goals of Confidentiality, Integrity and Availability, the famous CIA triad of information security. However, as appealing as these goals are, real-world practitioners know they are just that – goals. The day-to-day business of information security is not about lofty goals, it's about recognizing that systems, which are composed of hardware, software, storage and network components won't be perfectly secure. Security professionals are charged with delivering as close to perfect security as is achievable in the face of a continually changing threat-scape and business demands. Information security is the business of risk management and security spending is buying insurance. Since security professionals do not have infinite resources or time, they prioritize their efforts and play the odds. Given that there is no perfect security, and any control may fail at any time leaving assets open to some sort of harm, security professionals must keep several paradigms in mind.

1. Decide which risks have the highest combination of probability of occurrence and loss, and address those first.
2. Do not spend more on implementing and maintaining the control than the perceived value of the protected asset.
3. In the case of cyber-attacks or similar malicious activity, the job of the security organization is to make it take longer for a control to fail than the information will be valuable OR make it take more effort to overcome the control than the perceived value of the asset.

Networks are indispensable in today's business environment; unfortunately, attackers know this all too well and are ready to take advantage of it. Defending corporate networks today begins with strong protections that shield the systems. For security professionals, awareness and prevention are the first line of defense; however, ongoing monitoring provides the foundation for delivering an appropriate and timely response, which is key to a successful program.

The principle here is simple – given enough time and skill, all prevention-based controls are susceptible to failure. To maintain a margin of safety, security professionals must backstop prevention technologies,

like access control, with monitoring systems that report on the efficacy of the controls, the resiliency of the system and any threats and vulnerabilities that will jeopardize the systems.

Standard IT monitoring is focused on reliability, which is the *accidental* failure of one or more parts of a system causing an impact to conducting business and or harm to IT assets. Security monitoring adds another dimension to standard IT monitoring. It is focused on the intentional failure of the same components. There are two factors in security monitoring that make it a particularly advanced challenge for the practitioner – ongoing triage of new vulnerabilities and the need to correlate seemingly disparate events to identify multi-stage reconnaissance and attacks by intelligent adversaries. This means that the tools and processes must be targeted and scoped to your environment.

For any solid security program to deal with the continually changing threat-scape, it must implement a layered defense, also known as defense-in-depth, which deploys interlocking or overlapping controls to maintain the security of the environment. The best analogy is that of a brick wall. The foundation must be laid before the building. For a security program, that would be things like policy, awareness and training. Without these as a foundation, solid controls cannot be successfully implemented. Each layer of the wall is made up of multiple bricks overlapping other bricks. Staggering the bricks is the key factor in the wall's structural strength. The same is true in a security program. There are elements of each control that strengthen the others, so if one fails there is feedback of the failure, but another compensating control will continue to be enforced to maintain the overall security integrity. The mortar that holds it all together is the middleware, monitoring, reporting, processes and procedures used to make the program integrated and operational. The ultimate goal would be to have all of these controls reporting to the same data repository.

In this paper, EMA is focused on network security. EMA has found these five components are consistently at the core of network security and key to getting the job done right. Please note that the five topics are listed in no particular order; they are heavily dependent upon each other to create program success.

1. ***Identity and access management*** – Provide structure and reporting for authentication services for personnel and systems throughout the enterprise.
2. ***Vulnerability management*** – Identify and address vulnerabilities across all enterprise systems and applications.
3. ***Change monitoring*** – Identify unauthorized changes to your network infrastructure and who performed them.
4. ***Correlated centralized event management*** – Maintain continuous monitoring for anomalous, unusual, noncompliant, and malicious activities with a centralized portal for collecting and displaying all recorded events with out-of-the-box and user customizable intelligence and reporting.
5. ***Incident response*** – The regularly updated and tested conglomeration of documented manual and automated response processes and procedures available to the security personnel.

Priority 1: Identity and Access Management (IAM)

Understanding the proper context for IAM starts with understanding how identity is established in a system. Something or someone that requests authorization to access a system is called a user. These can be people or other systems. To get access, the external entity needs a token, such as a user or account id, to identify itself to the target system and an authenticator, such as a password, to validate that the request is coming from the owner of the credential. Once on the target system, the user id is considered a principal. The principal makes requests in the system on behalf of the user. The requests are known as subjects. Subjects interact with the object/resources on the system to achieve the users' objectives. Subjects may also make additional calls to generate other subjects for this same purpose.

Identity management prepares the user ID for use in the system. These types of systems perform account registration, provisioning, propagation, profile updates, password reset, group/role membership, separation of duties, and deprovisioning. The majority of these tasks require tracking by many audit regulations to confirm compliance so visibility into identity provisioning is a key requirement for most network security engineers.

Access management systems are concerned with receiving identity and authentication credentials and enforcing authorization decisions based upon the credentials presented. The access management systems report on the identity (who) using the system and what they are doing. Access management systems make for excellent security checkpoints. By design, they should not be able to be bypassed. Moreover, all the decisions that access management systems make, whether access granted or access denied, are by definition interesting security events.

Since a user can be a system as well as a person, knowing exactly who or what an id represents is imperative. When new personnel arrive, they have to have an ID to access the network and its associated resources. Administrators and security personnel agree that leaving the default accounts in operating systems and applications enabled is an unwarranted risk. We need to follow the same paradigm with systems that attach to our networks. In many environments, DHCP is enabled so that any new computing device that attaches to the network, wired or wireless, is given an IP address to begin operation. This is giving those systems a guest account on the network. We need to track activities of systems as well as people. Managing user identities and access within the enterprise ecosystem is crucial.

Organizations of all sizes suffer from user "access creep." As users change positions (roles) within the business, administrators often just bolt on their new access privileges without regard for the old. Generally when this is done, it is a function of admin work overload. Characteristics of new systems introduced to the environment must be considered to determine proper authorization and access. Being able to identify inappropriate "user" activities is impossible without proper IAM (Identity and Access Management). A solid IAM provides the capacity to report user behavior and network usage on a granular level including protocol, port, application and system access.

Access logging is not strictly a passive exercise. Access logs allow the security team to respond to security and availability events either manually or in some cases with automated response. Actions here may include modification of access privileges, whitelisting or blacklisting usage of sites, servers, or protocols, or blocking users based on policy or usage patterns.

Priority 2: Vulnerability Management

The goal of vulnerability management is simple – find the weak spots before the attackers do. Security personnel are responsible for finding all of the vulnerabilities (attack vectors) in their environment to maintain security. Attackers only have to find one vulnerability to exploit. In its most basic

implementation, a vulnerability management program is centered on regularly scanning environments looking for unpatched systems and then deploying patches as they are released by vendors. A mature program includes activities such as reviewing firewall, router and switch rules for excessively permissive, inaccurate or outdated rules before the threats can find them. The latter activities are applicable to vulnerability management because if the attackers can't get to it, they can't exploit it. These activities are generally performed in organizations where compliance to some regulation or standard is required but not done regularly in organizations where there is no compliance driver. The findings should be reported and communicated to a central management system for triage and remediation.

The goal of vulnerability management sounds simple, but achieving the goal in a complex enterprise environment can become complicated.

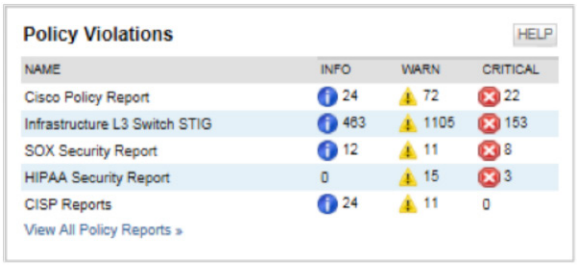
The goal of vulnerability management sounds simple, but achieving the goal in a complex enterprise environment can become complicated. Scanning systems is generally the easy part of the equation. Several challenges follow:

- Filtering out false positives before passing vulnerabilities on to administrators.
- Determining remediation priority based upon the environment.
  - A vulnerability ranked as critical on a limited access system does not generally need attention as quickly as a vulnerability ranked as high on a public facing system.
- Coordinating a deployment window on the key systems.
  - Most systems are not an issue; however, getting permission to patch a legacy system running a critical application or a high volume transaction system can be very difficult.

Vulnerability management falls under the purview of many audit requirements, so reporting and dashboards for vulnerability lifecycle are critical. Ongoing, end-to-end vulnerability management is a highly distributed process, but the management is best handled and reported on from a centralized console.

Security is very often a reactive job. Security teams try to respond faster and better. Vulnerability management is one area where security teams can be proactive not just reactive. Vulnerability scans, triage and remediation can be done on a regular, ongoing basis, and together these activities give the security team a chance to get ahead of the threats.

Priority 3: Change Monitoring



The core functions of change management such as review, approval and scheduling are more readily addressed in a systems management white paper of this series called, *Essential IT Monitoring: Ten Priorities for Systems Management*. However, the critical aspects applicable to security revolve around identifying the fact that a change was made. Was the change authorized? Did it violate existing security policies including compliance requirements? Did it reduce the overall organizational security posture? Additionally, it is important to know who made the change and when, so accountability can be assigned with a timestamp to determine if it aligned with other invasive or possibly hostile activities. Most attacks involve some sort of privilege escalation in order to accomplish the end goal of systems compromise. The sequence of change can often tell the security analyst or investigator the intent of the instigator. Identifying which configuration files or account permissions change is fundamental to a forensic investigation and remediation plan.

Priority 4: Correlated, Centralized Security Information Event Management (SIEM)

Maintaining visibility to activities within your scope of control or management area is crucial. Every application on every system in an environment has the capability to send operating and audit log data concerning its users, interactions and health. That is just the beginning. When other control systems such as firewalls, intrusion sensors, mobile security, data management, etc. are added in, the burgeoning data swell creates two problems for the security practitioner:

1. Even in most SMB environments, the sheer volume of information coming in is tremendous and humanly unmanageable. More so with large enterprises.
2. Organizing and interpreting events to gain a clear picture of what has and is happening in the environment is difficult to impossible without advanced event filtering and correlation abilities in the single view.

Handling these two issues requires the ability to manage the data in one place and model its context. That requires technology to pull all of the collected data into a single engine to ingest, process and manage it over time. Having numerous point solutions to deliver the various logs is better than nothing, but lacks the ability to gain a full context view providing real event correlation. Getting all events managed through a single user interface is a key operations requirement.

Having numerous point solutions to deliver the various logs is better than nothing, but lacks the ability to gain a full context view providing real event correlation. Getting all events managed through a single user interface is a key operations requirement.

Along with getting everything into the "single pane of glass," the ability to filter events is crucial for the personnel involved. Having everything in one place only helps if events can be filtered out based upon priority, event context or job function. In the most basic context, job function, security admins don't focus on application performance, network admins don't focus on storage alerts and application admins don't focus web content filtering. However, during a major or chronic event, any or all of those groups may want to pull into context any of the other organization's alerts to understand how those alerts are affecting the situation. An example of that is when the application personnel get a call that their application is slow and, not seeing anything in the application logs, incorporate the network performance events to see if it is being affected by a network event.

At its roots, threat management is about identifying the threats relevant to the environment before they can be exercised against a vulnerability, thereby reducing the window of opportunity it has to act on assets. A common example is that of a lake being held back by a dam. Below the dam is a town. The lake represents a threat. It is not a problem so long as it has no vulnerability to exploit. If the dam develops a crack, that is a vulnerability. If it is not addressed in a timely manner, the lake will begin to exploit that vulnerability

until it is repaired or fails. If it fails, the town, representing one or more assets, will be damaged. Correlated SIEM takes into account the fact that many threats and their associated attacks are not identified by a single event but through multiple events. To realize there is an issue, the collection system must evaluate numerous events and tie them together to identify the more complex attack vectors. To do this, the system has to have an intelligence engine behind it that has signature-based analytics and/or anomaly- and pattern-based analytics. The difference between a signature and a pattern is a signature is a defined sequence of network packet data in a protocol stream that is matched using some form of Boolean logic with regular expressions. A pattern is made up of multiple events created at multiple layers of the OSI model, generally 3–7, that are identified by an analytics engine rather than a packet sniffer. The patterns are more difficult to identify since they can be strung together from multiple sources and data types.

The real issue is the difficulty with being able to identify the low and slow or other complex multistep attacks and put the various pieces together in a timely manner, preferably before the attacker gets a foothold in your environment or achieves his or her other objective(s). New sophisticated attacks such as Advanced Persistent Threats (APT), Advanced Targeted Attacks (ATA), and never before emerging threats (zero day), are designed to bypass common signature checking tools like IDS/IDP, antivirus, etc. These sophisticated attacks leave less of a trace for an automated tool to pick up. The end result here is that it becomes a forensic game. To identify something that is occurring or has happened, visibility tools are used to collect and correlate sequences of activities that can lead or have led to a security breach. Tools must employ capabilities that can identify anomalous, unusual, noncompliant, and malicious activities with intelligence to keep up with evolving threats.

Alerting from the SIEM system may be generated on a single event or multiple events correlated into a single message. Generating an appropriate and timely message is critical to success. If the system doesn't generate any messages, the threat has succeeded in executing the attack. If the system generated too many messages, the nuggets of information the analyst needs may be hidden or otherwise masked and again the threat has succeeded in executing the attack. Threat response can be done in one of two ways – blocking or non-blocking. In a blocking approach, upon identifying anomalous activity the system drops the connection or otherwise denies the request. The more common non-blocking approach is when the threat management system reports the event, along with any useful context to the SIEM system but does nothing to contain with the activity.

Priority 5: Incident Response

Priorities 1–4 are about tools and process, but tools and processes for daily implementation and management are not enough when there is an incident. If the operations team is not prepared for how to respond when security events arise, it can be devastating to the enterprise. Just as faults in daily operations can cost money, so can the inability to respond quickly after a security incident, particularly breaches.

When an incident occurs, the security team needs tools that provide the best visibility into how the event is unfolding. Real-time alerting, with notification within milliseconds to seconds, of an identified event is key. The longer the system takes to notify, the longer the head start the attacker has, giving that attacker a greater chance of success.

For those organizations that are not normally under all-out attack, an incident response plan is a necessary tool to assist the response personnel in an orderly response. Such a plan would discuss who takes control of the investigation and recovery process, who provides internal management and external

customer communications, and answers the key question as to which is more important – recovery or forensics. Depending upon the level of virtualization in the environment, these can be two very conflicting requirements. It often means wiping a system and restoring from the last known good backup which restores the revenue stream but erases all of the forensics data on the system that is required for understanding the root of the problem and facilitating prosecution or restitution. If the focus is on forensics the priority will be on the investigation and will delay restoration. With virtualization, snapshots can be taken to collect state data, losing only some of the live forensics data, and restoration can occur more quickly.

However, effectively using the plan takes practice and coordination. There are several options for testing and training. "Live fire" exercises that extend from penetration testing and similar exercises are very helpful but can be disruptive. Planned scenario drills are a good second as they are more controlled but still provide valuable feedback on the state of documentation for recovery. In any case, documenting the processes and procedures and conducting these exercises *before* an actual event occurs is invaluable preparation. The heat of battle is no time for doing a proof of concept.

Automated response technologies supplement manual incident response processes by immediately responding to threats identified by a SIEM system while, at the same time, alerting IT security personnel.

Automated response technologies supplement manual incident response processes by immediately responding to threats identified by a SIEM system while, at the same time, alerting IT security personnel and triggering human intervention. Responses might include blocking an IP address, detaching a USB device, killing a process, logging a user off, removing a user from groups, and/or shutting down a machine. Automated response is particularly important in organizations without 24/7 IT security staffing.

Incident response processes benefit from iterative learning, ongoing process improvement and automated response implementation. Threats evolve and defenders should too. This includes periodically updating techniques for event identification, escalation and remediation, and the scope of automated response. The goal for incident response programs is to accumulate knowledge and hone in on the right tool for the right job.

EMA Perspective

Information security is one of the most challenging IT disciplines. It affects or is affected by application, systems, network, and change management, as well as every other discipline in IT. It also requires a range of different tactics to be successful – dealing with evolving threats, new vulnerabilities, identity and access management, and monitoring change. Security is generally perceived as a system-level property that practitioners must try to deliver one project at a time. While in reality, it is an environmental-level property that should be broken down into composite parts like the construction of the brick wall. For many organizations, it is difficult to keep the big picture strategy of what that final wall will look like while they are in the middle of assembling all of the pieces over the course of years.

Many organizations begin building this environment with tools like those available from SolarWinds, a provider of IT management technologies including security. In recent years, SolarWinds has significantly expanded its portfolio through product development and acquisition. With that drive, it has created a broad portfolio of products that not only addresses the top five network security priorities, but also provides many of the other components needed by security professionals to build their defense-in-depth "brick wall" and address many other IT management needs.

The SolarWinds solutions can appear at first glance as an amalgam of point solutions. They can be used individually to achieve results quickly. This makes them appealing to SMBs that need to find something to plug a specific "hole in the dam." For larger enterprises, the ability of these individual solutions to work together should not be underestimated. SolarWinds provides a highly modular suite of products that can stand alone or integrate into the "single pane of glass" methodology placing event management and reporting in one place. With the competition for budget dollars faced by security organizations, cost is a key factor in the decision process. Though ROI and ROSI are not part of the top five network security priorities, they are part of the top five business priorities. SolarWinds licensing plans are very cost effective and many of SolarWinds' products have a fully-functional free trial download available, which is great if you are in a bind and need to try before you buy.

In reviewing the five network security management areas, EMA finds a number of products SolarWinds provides fit in nicely. For identity and access management, SolarWinds provides a useful user and device management application called User Device Tracker that can locate and track devices that require your special attention for whatever reason by whitelist, hostnames, IP and MAC addresses and identify the users on the network associated with each. It also shows the node or access point, port or SSID, and VLAN through which a tracked object is connected.

For vulnerability management, SolarWinds Patch Manager provides patching automation and delivery services for both Microsoft and third-party applications from a single point of control. Additionally, Patch Manager delivers centralized visibility into the patch status of systems and includes an extensive collection of easy-to-use, built-in reports for patch compliance reporting, along with the added ability to schedule reports and create custom reports. With these reports, users can get key information, such as missing or failed patches, security-related group policy settings and how they are configured enterprise-wide, or the update status of anti-virus definitions.

Switching context a little and moving to the broader view of environmental, rather than just system, vulnerabilities, SolarWinds offers two solutions that address other vulnerability and threat vectors. One is their USB Defender technology, which is a component of the company's SIEM product, SolarWinds Log & Event Manager. USB Defender delivers the ability to log, monitor and control the introduction of USB devices in your environment. If a device is inserted into a machine, USB Defender can be configured to automatically eject it, even when the machine is offline. It can also provide audit reporting on USB device usage/introduction within the environment. The other useful tool is SolarWinds NetFlow Traffic Analyzer. In most cases, the network operations teams use this tool to see which users, stations or protocols are the bandwidth hogs and analyze when high and low usage times are as a part of capacity planning. It can also be used to identify rogue machines operating outside normal time windows or communicating excessively; it can identify chatty applications and the ports they are using, which may indicate poor application performance or worse, like malware infections scanning the network or communicating for command and control or relaying company data to the outside on allowed protocols.

SolarWinds has a complimentary set of solutions to aid in Change Monitoring. Its Network Guardian Bundle composed of SolarWinds Firewall Security Manager and SolarWinds Network Configuration Manager provides capabilities for establishing change policies, then detecting changes to security and network devices and flagging changes that fall outside of established policies. It provides "what-if" change modeling for multiple firewall platforms as well as delivering a variety of security and compliance reports.

The core of the SolarWinds IT Security solution is SolarWinds Log & Event Manager. This SIEM solution ingests data from a wide range of data streams then provides real-time, in-memory event correlation for immediate threat detection. It can analyze millions of events and deliver customizable

automated responses for the identified events. It also provides advanced search capabilities and visual data exploration tools to facilitate forensic investigation, as well as pre-packaged templates for regulatory compliance reporting. Additionally, SolarWinds Log & Event Manager includes hundreds of built-in, filters, rules, searches, and reports that are already categorized for ease of use.

Just as it is important to identify the security problems, you must be agile in your ability to respond. As we mentioned earlier, in some cases you may want SolarWinds Log & Event Manager to provide an automated response. But in many cases, the event requires further investigation from an analyst to deliver an appropriate response. For these scenarios, Alert Central, a free product from SolarWinds, consolidates, manages, and escalates alerts from not just SolarWinds' solutions, but a multitude of other vendors' products. It can be configured via routing rules to use individuals or Active Directory (AD) groups to engage help/support desk personnel for triage or analysts or tier 3 personnel for a more in-depth review and response.

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide from Fortune 500 enterprises to small businesses. SolarWinds' approach is consistent across all market segments – focusing exclusively on IT Pros and striving to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with simplicity through products that are easy to find, buy, use and maintain while providing the power to address any IT management problem on any scale. Additional information on SolarWinds can be found at http://www.solarwinds.com/.

Additional Reading…

For information on optimal monitoring practices in other management disciplines, please see EMA's other White Papers in the *Essential IT Monitoring* series:

Essential IT Monitoring: Five Priorities for Cross-Domain IT Management

Essential IT Monitoring: Ten Priorities for Systems Management

Essential IT Monitoring: Seven Priorities for Network Management

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter or Facebook.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

2775.093013