No Blind Spots in Perimeter Security with Security Event Information Management
Table of Contents

The Growing Need for a Consolidated or “Context Aware” View into Enterprise Security ........................................... 3

2011 Emerging Threats ................................................................................................................................................. 3

Multi-Vulnerability Attack Campaigns .......................................................................................................................... 4

The Need for Complementary Security Technologies .................................................................................................. 4

What Can a SEIM Do For You? .................................................................................................................................. 5

Defining the Requirements of a SEIM ............................................................................................................................. 5

APSolute Vision: Assuring There are No Blind Spots in Perimeter Security ................................................................. 6

Best-of-breed Reporting and Forensics Engine ................................................................................................................. 7

Complete Alignment with Enterprise Compliance Requirements and Regulations ............................................................ 7

Tight Integration with Enterprise Data Center NMS ........................................................................................................... 7

Full Alert Lifecycle Management ................................................................................................................................... 7

Conclusion.............................................................................................................................................................................. 8
Security Event Information Management (SEIM) can provide the security leap-frog in a world of point solutions – to ensure there are no blind spots in your network security architecture.

The Growing Need for a Consolidated or “Context Aware” View into Enterprise Security

Even with dedicated security personnel, it’s tough to monitor the millions of messages and log records generated by various security edge devices such as intrusion detection systems, firewalls, anti-DoS and application firewalls. Even more difficult is identifying patterns occurring over time and across separate devices, but an SEIM system can build a centralized architecture that makes such tasks more feasible and allows for speedy compliance reports, audits and is absolutely required when prosecution of a perpetrator is needed.

The concept of SEIM is not new – it has been delivered through dedicated platforms for over ten years. Plenty of vendors offer internal management products which combine a core correlation engine, user interface, and log collection capabilities. As for the dedicated marketplace, these systems deliver the unique ability to monitor disparate security events generated by VPN software, firewalls, antivirus software, databases, Web servers, IDS, and other pieces of the security puzzle. But most systems aren’t cheap, with prices starting around $50,000 and running well into the six-figure range for complex environments.

SEIM grew up because of a fundamental problem with security architecture today – nearly all solutions are designed and deployed as point solutions. That is, they are not designed to speak with other security systems, correlate alerts or provide for a ‘big picture’ within the entire enterprise. The SEIM system was designed to be the single ‘console’ in which an operator would get both total situational and context-awareness.

2011 Emerging Threats

By all indications 2011 will be known as a historic year in information security as threats added a whole new category of motive to attack profiles. This new “Hacktivism” category will go down in the record books as one of the most active periods of cyber attacks in the history of information security. Moreover, given the current efficacy of these ideological-based multi-vulnerability attacks such as WikiLeaks revenge attacks (December 2010) and Sony DDoS & MySQL attacks (May / June 2011), etc, we believe this will only serve to encourage even more actors to enter the picture and spawn a vicious cycle of future malicious activity.

No one can say for certain how all of this will play out, however given the increased frequency, directed attacks, and effectiveness of the techniques, we can safely assume the following:

- **Cyber attacks go mainstream for activists and for financially motivated criminal organizations.** Attackers’ motivation has evolved and from publicity and vandalism they are looking for financial gain or protest without going out of their homes.
- **Reassessing the risk – your organization is likely a target.** For example eCommerce sites, which were the prime target for financially motivated attackers, have now also become targets for hacktivism.
- **Cyber weapon of mass Disruption deploy multi-vulnerability DoS & DDoS attacks.** This turns traditional network security measures useless, as they typically can detect and defend only some of the attack vectors.
- **The need for complementing security technologies.** Mitigating multi-vulnerability and multi-vector attacks requires more than one security technology in place, adding behavioral analysis technologies on top traditional signature detection and rate based protection.
Architecting the perimeter for attack mitigation. Deployment of complementing network security technology requires rethinking of perimeter security.

Counterattacks are needed! Defense mitigation strategies are also evolving and now include active counterattack strategies.

Multi-Vulnerability Attack Campaigns

The resultant impacts of the 2011 “Hacktivist” attacks were significant. The attacks were hard to defend against as they were aiming at multi-vulnerability points in the network including network infrastructure equipment, TCP/IP stacks and servers’ application. These multi-vulnerability attacks included high volume DDoS attacks as well as “Low & Slow” attacks – all of which were generated simultaneously against multiple weakness points in the networks. They also combined application based attacks such as SQL injection and server reconnaissance and enumeration flurries.

The following is a list of the attacks we have witnessed throughout 2011:

- Jan – Feb: Operation Payback (Wikileaks’s Revenge)
- Feb: H.B. Gary Attacks
- Mar: Wordpress.com / Operation Payback II
- April: CIA & FBI InfraGard Attacks, NPR, Foxnews
- April – June: Operation Sony
- July: Paypal
- August: Bay Area Regional Transit (BART) / Hong Kong Stock Exchange

The above attacks represent very effective attack campaigns and each of them is serving to be both simple in execution and complex in defense.

Radware believes that there is a clear need to complement existing network security technologies such as firewalls and network IPS in order to protect businesses against existing and future attacks.

The Need for Complementary Security Technologies

As was widely reported during Wikileaks’s Operation Payback, MasterCard and VISA both suffered debilitating outages from this attack. It was also reported they had intrusion prevention tools and firewalls in place which alone were not adequate. However, there were a few organizations which fared remarkably better. Lessons can be drawn from the contrasting technologies.

We have learned that to successfully mitigate these types of attacks, the deployment of multiple security tools is essential. The following technologies have proven invaluable in repealing these types of attacks and need to be resident in the perimeter of any business network:

- Anti-DoS and DDoS attack tools (at the network and application layers)
- Network behavioral analysis (NBA) tools with real-time signature writing capabilities
- Intrusion prevention systems (IPS)
- Application-level active defense mechanisms – such as challenge & response
- Active emergency counter-attack strategies
- Situational Awareness provided by Security Event Information Management

Most of the severely affected organizations appeared to have had inadequate DoS and DDoS protection. It is recognized that many organizations are not using DoS protection at all. The second key technology ingredient required is behavior analysis which is geared toward DoS and can quickly mitigate illegitimate traffic.
**What Can a SEIM Do For You?**

Network and IT infrastructure may have changed significantly since your original deployment of Firewalls, IDS, and other security products. Users may have relocated physically or migrated to new methods of accessing their applications and data. Products don’t stand still; features and capabilities are added with each release. It may be possible to retire some of your security systems and consolidate networks because their functionality has now been added to other products or the topology no longer makes operational sense.

An organization can run into the challenge that most of these events are parsed differently. Essentially what may occur is that the data just has different formats, so it’s like trying to compare an apple and an orange. A security information event management system is not just going to collect all the data, but it’s then going to normalize it so that an analysis engine can go in and basically be looking at two apples to make its correlations and comparisons.

This normalization process is key to SEIM’s success because you’re not forced to revamp your security architecture simply so it plays nicely with your new, expensive event manager. Security event management vendors understand and appreciate companies’ vastly varying security needs and in turn build products that support hundreds of security devices from different manufacturers. SEIM systems are highly configurable to mesh with security architectures of varied sizes and ingredients and contain rules and templates that let administrators easily bring the systems up to speed.

The nice aspect of a SEIM is that only part-time monitoring of SEIM software is required, and the IT skill level inherent in most small to midsized enterprises is sufficient enough that specialized personnel aren’t required to run the systems. Most systems include easy-to-use wizards that automatically discover components on the network and give administrators the option to audit and monitor them, and included security tests can instantly analyze the strengths and weaknesses of networks by performing simulated attacks and offering suggestions to patch potential holes.

The benefits of SEIM reach far beyond the simple management of logs, as these systems can easily boost efficiency and uptime. Thanks to intuitive interfaces that drill down to pertinent information, administrators no longer need to spend countless hours weeding through herds of harmless events to identify the few that actually pose significant risk. When major threats such as worms do strike, an SEIM system can immediately alert security personnel, so they can take appropriate action before servers are shut down cold.

**Defining the Requirements of a SEIM**

SEIM has become the central nervous system for perimeter security professionals in the twenty first century. If implemented and designed properly, these systems will define the detection, analysis (correlation), and reactions / mitigations to all attacks going forward.

SEIM’s technical and operational requirements have been heady over the years and the expectations have been incredibly lofty. Over time, the common security requirements for SEIM have been distilled into three primary features which are as follows: preventive, detective, and corrective, and, of course, the system must provide robust auditing and reporting (forensics). Radware sees the SEIM collection of tools breaking down into seven “minimum” and an additional eight “attractive” requirements as follows:

**Minimum SEIM Requirements**

1. **Risk management dashboard** – users of SEIM tools should have the ability to provide for unique and meaningful ‘dashboards’ or visual tools which can allow them to track performance of risks against known or agreed to risk models. This is a key element to any SEIM tool.
2. **Threat management** – detect threats that would otherwise be missed by product or operational silos - this may also be called non-linear event correlation
3. **Log management** – respond to the right threats at the right time through effective analysis of log files
4. **Rule-builder capability** – automated rules are the ingredients of SEIM operations and most security tools which provide for automated responses (e.g. IPS’, anti-DDoS, Anti-Virus, etc). The ability to manually configure and customize these rules are essential in enterprise and managed service environments going forward.
5. **Compliance** – implement a compliance and reporting safety net with comprehensive event storage and reporting
6. **Add alerts**, escalation and trouble ticketing
7. **Forensics / raw packet** analysis capability

**Additional Attractive Requirements**

1. Application activity analysis
2. Network anomaly detection – or network behavior analysis (L2 – L7)
3. Desired configuration management
4. Anti-malware
5. IT efficiency – extract IT value that is latent but lost by maximizing existing network and security investments
6. Unmanaged mobile device behavior analysis
7. Database activity analysis
8. Data flagging capability - user ‘flagged’ data (private or confidential information) is marshaled for analysis, oversight, and protection

Radware believes each one of these attributes would need to be represented in a comprehensive solution.

Interpretational capability is paramount and it is desirable that each of these functionalities is currently resident in one system and not add-ons. Interoperability is the key to allow for active monitoring of system security posture and to provide robust assessment or other routine IT operations. The interoperability attributes that we find needed are as follows:

- The ability to aggregate, normalize, and correlate data from all of the ten disparate sources listed above
- Provide automated information gathering and risk assessment
- Map regulatory requirements to policies and support auditing and reporting
- Provide a unified framework that can be modified to fit an enterprise’s needs
- The ability to do conduct some real-time analysis
- The ability to quickly ascertain severity of an attack and correlate to critical data, servers or network devices.

The tool also needs to accept data from a wide range of devices.

**APSolute Vision: Assuring There are No Blind Spots in Perimeter Security**

Fighting known and emerging network threats, such as multi vulnerability attack campaigns, Radware provides an integrated solution approach called Attack Mitigation System (AMS), that combines an advanced layer of protection tools designed for online businesses, data centers and service providers. Radware AMS protections layer consists of a set of security modules including: Denial-of-service (DoS) protection, Network Behavioral Analysis (NBA), Intrusion Prevention System (IPS), Reputation Engine and Web Application Firewall (WAF) - to fully safeguard networks, servers and applications against known and emerging network security threats.
Radware AMS includes an integrated Security risk management - built-in Security Event Information Management (SEIM) collecting and analyzing events from all modules to provide enterprise-view situational awareness – APSolute Vision. APSolute Vision™ is the management and monitoring tool for the Radware family of application delivery and security solutions. It permits the setup, configuration and management of all APSolute products from one central unified console. It accompanies Radware’s security solution with an enterprise-wide view of security event information management (SEIM) and compliance platform.

**Best-of-breed Reporting and Forensics Engine**
APSolute Vision provides an enterprise-wide view of security and attack statuses from a single console. Data from multiple devices can be collected and evaluated in a consolidated view of dashboards and reports.

In addition, it provides extensive yet simple drill-down capabilities that allow users to easily mine information in order to expedite incident identification and provide root cause analysis.

**Complete Alignment with Enterprise Compliance Requirements and Regulations**
APSolute Vision provides complete alignment with the enterprise’s compliance, regulations and business processes, providing compliance and audit professionals with a complete picture of compliance across the enterprise.

It ensures the appropriate separation of duties, collection of information, configuration, and operation auditing mandated by business processes, regulations and information security standards (PCI-DSS, SOX, HIPAA, etc).

**Tight Integration with Enterprise Data Center NMS**
APSolute Vision is designed to tightly integrate with the enterprise data center’s network operation centers (NOC) and the network management systems (NMS) used by the NOC operators.

Providing NOC operators with a single site-wide monitoring and alerting view of all managed devices and applications, APSolute Vision automatically sends notifications (syslog, email, etc) to the NOC’s NMS application.

**Full Alert Lifecycle Management**
APSolute Vision provides IT managers with a rich set of tools to manage all the alerts (availability, performance, security, and more) within their infrastructure. Alerts are managed from the moment they surface (identification stage), through ticket opening, analysis, resolution, and verification until the problem is resolved and summarized.
Conclusion

Security Event Information Management (SEIM) is no longer an optional implementation decision. In a world of point security solutions that need to mitigate emerging network and application security threats, it becomes a must. Security managers are required to achieve full view of their network and application performance – and this can be achieved through a new information layer that provides enterprise-wide security awareness.

Specifically, a SEIM is the only solution that can combat multi vulnerability attack campaigns that seek to infiltrate through point security solutions, exploiting blind spots that are not covered by standard, out-of-the-box security profiles. Maintaining a thorough and effective corporate security policy across multiple point solutions requires an intelligent overlay that can provide the security leap-frog in a world of emerging threats – to ensure there are no blind spots in your information security architecture.

SEIMs will be future secret between effective security tools and ineffective point-solutions. Moreover, SEIMs which are integrated out-of-the-box with the detector tools from which they’ll be reporting and directing mitigation defenses from are a leading edge infrastructure and indicative to proactive infrastructure built for today’s and tomorrow’s threats!