Real time threat intelligence, PCI compliance and reporting

In the last of our three-part series on aspects of defending your enterprise systems at a time when cloud technologies are radically transforming ICT environments, Decipher Works Principal Consultant Dave Wicks explains the value of security intelligence in detecting potential threats from both inside and outside your organisation.

Internet-based threats and fraud continue to proliferate in today's complex networks and, if left undetected, can have a significant negative impact on an organisation. One of the principal challenges in securing business systems and data is the ever-changing nature of the threats. To combat this broad spectrum of potential breaches, comprehensive network security involves investment in targeted hardware and software solutions – including firewalls, virtual private networks (VPN), intrusion detection & prevention systems (IDPS) and vulnerability scanners. Many of these solutions involve continuous support from vendors and other sources maintaining up-to-the minute global databases of new and emerging threats.

Unfortunately, these solutions alone have not been able to completely protect organisations from the evolving landscape of sophisticated threats from both outside and inside the enterprise network.

So, why do organisations that have implemented a comprehensive network security infrastructure *still* find it a challenge to detect real threats in real time?

Analysing security challenges

According to recent security research[1], threats (just in terms of data breach) can be roughly divided between three sources:

- 32% of data breaches were caused by the carelessness of insiders
- Another 32% were attributed to system glitches
- 36% of breaches resulted of 'malicious' intentions from outsiders

You have little control over outsiders, given the ever-evolving methods they use, but you can mitigate the risks by subscribing to global information security services and integrating their feeds into your security infrastructure and monitoring systems.

But what value would user activity monitoring provide in overcoming insider threats? Consider the potential:

- A terminated employee taking action on your network: if terminated, how is he still on your network?
- A privileged employee accessing databases she doesn't usually access: is she performing malicious activity, was her account compromised by an attacker or did her responsibilities just change?

In this White Paper...

- Why identifying threats in real time remains a challenge
- Nearly two-thirds of threats come from inside your organisation
- Gaining visibility by integrating logs from multiple security devices
- Applying intelligence to identify real threats in real time
- Why PCI DSS matters – even if you are not required to comply
- Justifying investment in Security Intelligence Event Management (SIEM) technology

[1] **Source:** *2011 Global Cost of Data Breach,* conducted by Ponemon Institute for Symantec Corporation in early 2012 with IT, compliance and information security practitioners from 209 global organisations including 22 from Australia

- When an employee from one geography, who does not travel for business, is seen performing activity in a different geography, is this legitimate or was his account compromised?
- Is a contractor accessing a database or application that he doesn't require for his job? Can he be trusted, or do his actions require closer monitoring?

Effective security management encompasses insider threats – and this can be a challenge if you only focus technology and resources on monitoring, repelling and mitigating the minority of threats coming from outside.

Lacking insight

In many cases, IT teams are effectively flying blind, because they lack *integrated visibility* and *insight* into the security solutions they have put in place. Others lack the tools necessary to analyse aggregated data so they can accurately *identify* individuals or systems responsible for malicious behaviour or quickly analyse potential attacks in order to detect real threats.

Existing network security devices may emit a wealth of useful information, but it often remains buried in massive amounts of event and log data. Unfortunately, this information is often ignored or underutilised for many reasons, including complex data formats and overwhelming volume.

Fundamentally, the majority of targeted security systems are ineffective at providing security insight from all the data they generate. The key is in managing events and logs across the entire network and infrastructure, and then applying intelligent analysis to that data to accurately detect real threats and deliver reliable alerts that security teams can effectively action.

In a cloud environment, this also calls for event collection, regardless of the location of applications and data – and allowing for interruptions in network or internet connectivity.

Applying intelligence

So how can you unify all of your existing security systems to leverage the most efficient enterprise-wide security solution? Security intelligence involves aggregating logs and perform real-time analysis of security alerts generated by network hardware and applications.

There are a wide range of SIM/SEM (Security Information Management/ Security Event Management) and log management products available. However, even organisations which have implemented these 'overarching' surveillance systems for aggregating logs from multiple systems still face challenges, including:

- A simply unmanageable number of false positive events
- Undetected threats – especially if the network layer is unmonitored
- The ability to monitor potential breaches within application and content layers
- The delivery of forensic information to trace and prosecute offenses

Why PCI DSS matters

Any organisation processing credit card transactions with the major global providers will be well aware of the Payment Card Industry Data Security Standard (PCI DSS). However, PCI DSS provides an excellent security framework for *any* organisation, whether they need to comply with it or not.

Compliance involves building a secure network infrastructure and providing accountability, transparency and measurement to meet PCI requirements. This calls for a network-wide security monitoring solution that leverages more than logs, and actually combines important log data with vulnerability data and flow data (its network context) to deliver an accurate assessment and prioritisation of threats and potential violations.

Furthermore, standards such as PCI DSS call for more than just the collection and correlation of logs. In order to meet many of PCI's requirements, the aggregation and correlation of logs from your security and network infrastructure must be implemented in conjunction with insight into the network from passive monitoring of network communications.

So, while collection, aggregation, analysis and correlation of logs enables a multitude of threats and violations to be detected, relying on logs as your only source of surveillance data can lead to monitoring blind spots, including:

- Threats that existing security products are missing or get 'lost in the noise' of millions of events
- Lack of collaboration between network and security operations
- Layer 7 application flow data that could help detect inappropriate use of networked applications and protocols
- Timely delivery of automated analysis to either validate or refute security incidents

Getting the real picture – in real time

Security Intelligence Event Management (SIEM) technology goes beyond SIM/SEM tools by providing an accurate picture of what is *really* going in the network relative to PCI and other regulatory compliance standards.

An SIEM platform aggregates and analyses the event data produced by devices, systems and applications. Its primary source is log data, but the technology can also process other forms of data to obtain network context about users, IT assets, data, applications, threats and vulnerabilities.

It collects this event data in near real time in a way that enables immediate analysis via:

- Receipt of a syslog data stream from the monitored event source
- Agents installed directly on the monitored device or at an aggregation point, such as a syslog server
- Invocation of the monitored system's command line interface
- APIs provided by the monitored event source
- External collectors provided by the SIEM tool
- Netflow traffic

Being able to complement host/application/database logs, security event data and vulnerability information with network context allows for an additional layer of analysis and correlation – significantly improving accuracy and prioritisation of detected incidents. Logs from a large variety of security and network devices can be compared and correlated with what is occurring on the network for validation purposes.

For organisations running applications in the cloud, an effective SIEM platform will enable the replication of an enterprise security monitoring and threat management infrastructure across multiple operating environments.

SIEM can also be enhanced through automatic updates on the current threat environment from a variety of sources, including open-source lists, the threat

SIEM Deployment Scenarios

Amongst our clients, different motivations create business cases for investment in a Security Intelligence Event Management (SIEM) platform. Whatever the initial justification, we aim to deploy those capabilities rapidly – after which the implementation can be extended to meet other business imperatives.

Compliance is one of the major reasons for implementing log management and is especially useful in addressing a number of key controls required by PCI DSS, as well as delivering reporting under the regime. In this case, deployment is tactical, focused on specific compliance reporting requirements, and a subset of relevant servers. Log management is weighted heavily, because it provides the basic 'check box' that a superficial audit would require. User and resource access reporting is important because SIEM technology is commonly deployed as a compensating control for weaknesses in user or resource access management – and an effective SIEM solution reduces compliance costs. Implementation time frame is typically short, so simplicity and ease of deployment are valued over advanced functions and the capability to customise heavily.

Improved **threat management** and **incident response capabilities** make a solid case for SIEM deployment. In this scenario, higher weighting is given to real time event management and correlation, threat intelligence, anomaly detection and support for security event analysis.

In a **hybrid scenario**, for example, where the IT security team has secured funding to close compliance gaps, but also wants to improve threat management/incident response, the SIEM technology platform selected must support rapid deployment of compliance reporting, and provide for subsequent implementation of security event management capabilities.

and reputation content developed and maintained by security research teams within security vendors, and data developed by managed security and other service providers. This threat intelligence data can be integrated in the form of watch lists, correlation rules and queries in ways that increase the success rate of early breach detection.

An SIEM platform will thus provide a high level overview of your environment, along with the ability to quickly identify and understand where risks and vulnerability exist. In this way it helps identify potential threats occurring both within your network and beyond – including detecting inside 'whistleblower' threats to information security such as WikiLeaks-related breaches over recent years.

How will your business benefit?

Benefits from deploying an SIEM platform depend on each organisation's specific needs and priorities, but can include:

- **Reduced risk** through the ability to detect and manage potential threats in real time
- **Significantly reduced IT resources** involved in monitoring and analysing application and network logs from multiple security systems – freeing skilled personnel for more proactive tasks
- **Increased information security** through the ability to monitor server and database resource access as well as the activities of privileged users
- **Reduced cost and time** in completing PCI audits from automated PCI DSS reporting that meets the requirements of your financial services providers
- **Customised reporting** on compliance with other information security standards, corporate policies, industry standards or legislative requirements
- **Peace of mind** from reducing the risk of human error through the application of advanced automation and intelligence

How to get started

Decipher Works can help you select an appropriate security intelligence platform – then deploy it to meet your immediate requirements in the shortest possible time. We can also help you get the most from your investment, by extending deployment to deliver additional business benefits.

Naturally, strong user identity and access systems are a prerequisite for a security intelligence platform and are the subjects of the previous papers in this series:

> *How to let the good guys in and keep the bad guys out?*

> *Who's having an identity crisis?*

Dave Wicks is a partner in Decipher Works and Practice Lead, with over 13 years' experience, he specialises in Identity and Access Management and related security solutions and has been involved in significant Australian implementations for Allianz, Macquarie Bank, Qantas, AMP and the Queensland Treasury Corporation. Holding a Bachelor of Information Technology from Griffith University with awards for academic excellence, he has also undertaken studies in Master of Business and Technology at the University of NSW.

About Decipher Works

Decipher Works is a Cybersecurity Specialist in Identity, Access, Governance & Federation. Working with some of Australia & New Zealand's largest organisations within the financial, telecommunication, transportation and utilities sectors. Decipher Works secures critical resources within organisations and facilitates users access to the most important productivity tools whilst enforcing strong security.

Decipher Works draws on its strong industry experience to design, deliver and manage customised IT solutions aligned to our clients' business goals. We provide best of breed solutions leveraging leading market technologies.

Phone 1300 724 880
Email services@decipherworks.com.au
Web www.decipherworks.com.au

okta Technology Partner | DELL PartnerDirect | SailPoint | Advanced Business Partner IBM