EMPTY BATTLEMENTS - ENEMY INSIDE THE GATES

WHY IT MANAGERS NEED TO MAKE TIME FOR SIEM

Commissioned by	SecureData
Conducted by	Vanson Bourne
Published	December 2012

Part 1. Executive summary

Businesses are increasingly coming under threat of attack from both inside the organisation and outside. It is estimated that UK businesses alone lose £21bn a year to cybercrime, so what can businesses do to combat the enemy, not just at the gates, but potentially inside the castle walls?

A high level of visibility and analysis is paramount for businesses – in particular where security events, logs, network context, vulnerability and identity data have to be viewed, understood and acted upon, as part of a proactive security posture.

In order to mitigate these risks, businesses require effective Security Information and Event Management (SIEM) technology. SIEM is a working solution that provides real-time analysis of the wide range of alerts and data generated by applications and hardware, enabling a business to respond more quickly to attacks, log security data and also provide reports for compliance regulations.

SIEM solutions can be configured to control both security and non-security events, including threat detection, network behaviour, network anomalies, performance anomalies, device failure, and policy violations. Examples include tracking users logging in unusual locations, monitoring file changes or examining which admin rebooted a server and why.

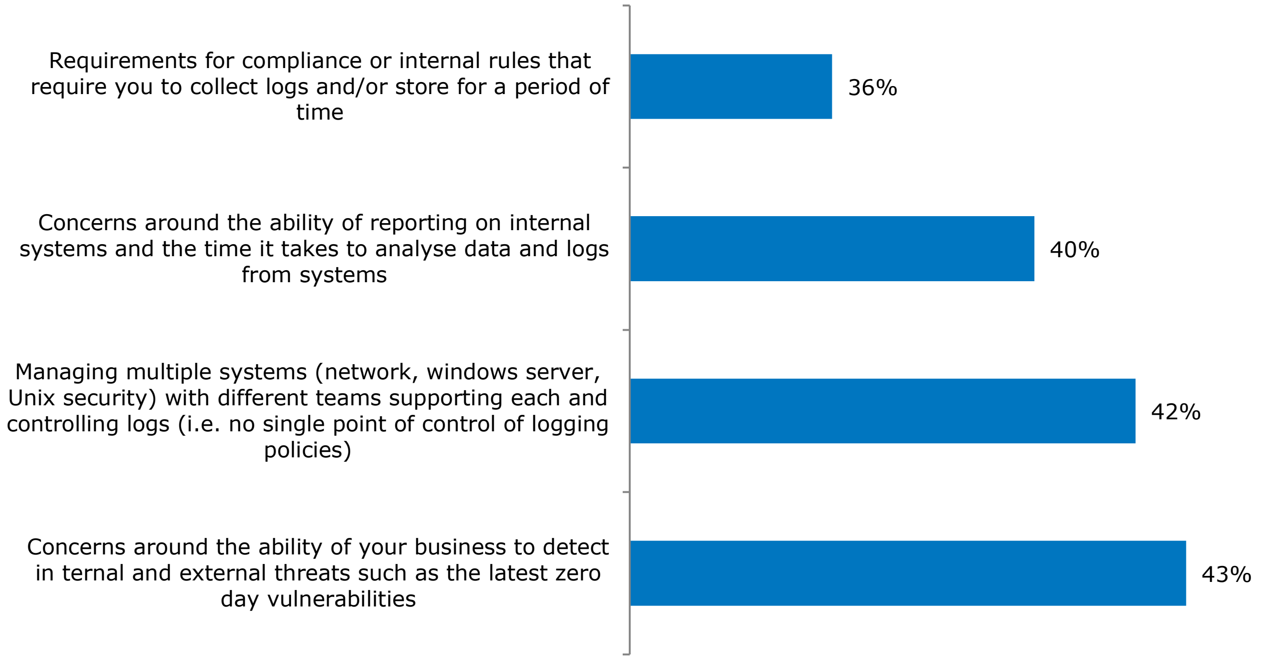
SecureData has conducted a study to review IT managers' experiences with their IT central logging systems; we believe the following are the most salient findings:

- 62% of respondents' businesses have an internal system as their IT central logging system
- The biggest challenge faced by 59% of IT managers with regards to IT logs and systems is having the time / resource availability required to regularly monitor logs for suspicious behaviour
- 43% of respondents see the ability of their business to detect internal and external threats, such as the latest zero-day vulnerabilities, as a high risk IT security challenge
- 42% of respondents believe that managing multiple systems (network, Windows server, Unix, security) with different teams supporting each and controlling logs (i.e. no single point of control policies) is a high risk IT security challenge
- 40% of respondents have serious concerns about their businesses ability to report on internal systems and the time it takes to analyse data and logs from systems

Part 2. Analysis of key findings

1. How do you rate the risk levels of the following IT security challenges to your organisation?

N.B. Each challenge outlined below was ranked from none to very high in terms of risk level. The results below show only those from respondents that rated the risk levels as high or very high.



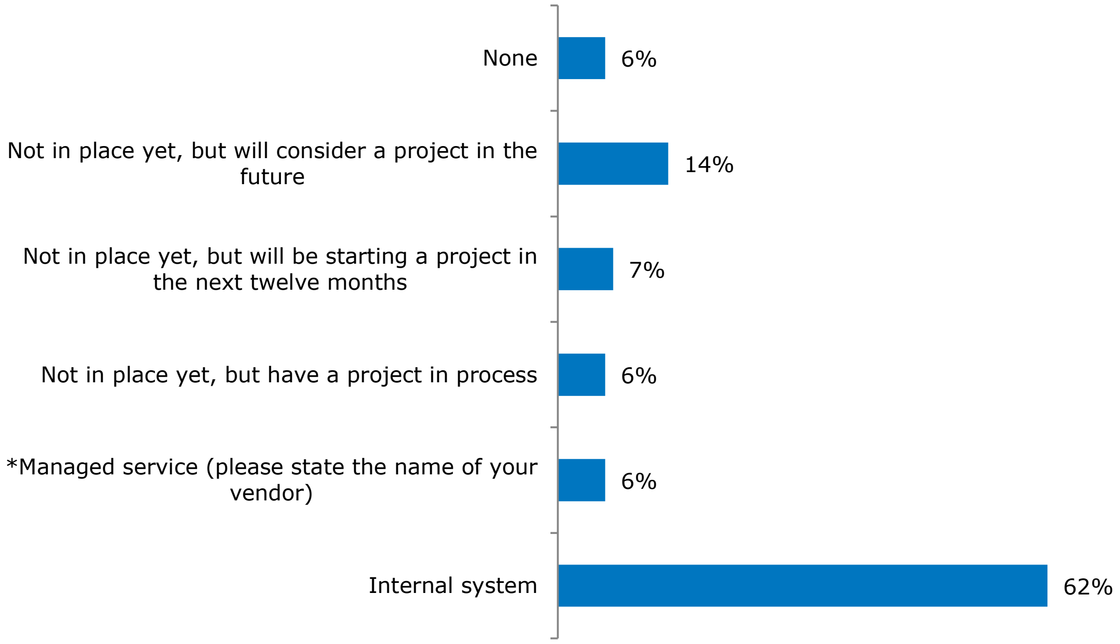
Key statistics

- 43% of respondents see the ability of their business to detect internal and external threats, such as the latest zero day vulnerabilities, as a high IT security challenge
- 42% of respondents believe that managing multiple systems (network, Windows server, Unix, security) with different teams supporting each and controlling logs (i.e. no single point of control policies) is a high risk IT security challenge
- 40% of respondents have serious concerns about their businesses ability to report on internal systems and the time it takes to analyse data and logs from systems
- 36% of respondents believe that the requirements for compliance or internal rules that require you to collect logs and/or store for a period of time, bring a high risk to their businesses IT security

Analysis

- These results show that there are some serious risks associated with a number of IT security challenges that businesses are struggling to manage with their current processes in place

2. What type of IT central logging system does your organisation have?



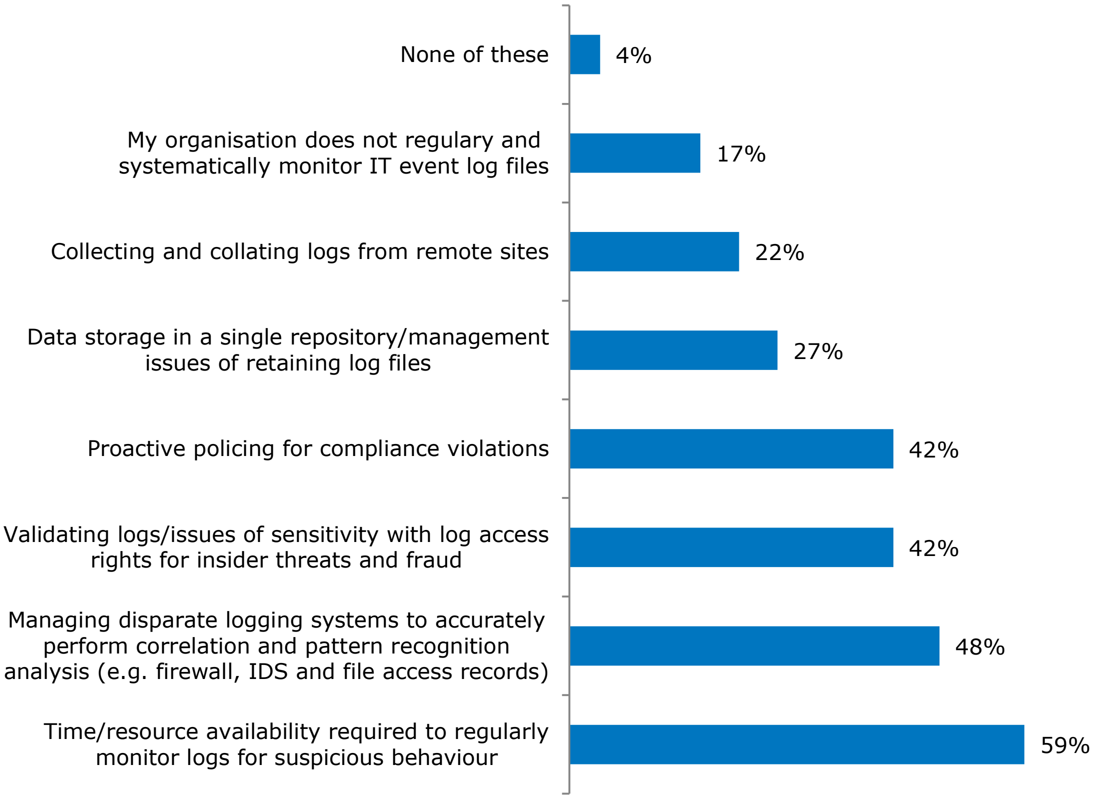
Key statistics

- 62% of respondents' businesses have an internal system as their IT central logging system
- Only 6% of respondents employ managed services for their IT central logging system
- 27% of respondents do not have an IT central logging system but have a project in process (6%), will be starting a project in the next twelve months (7%), or will be considering a project in the future (14%)

Analysis

- The results reveal that a large proportion of IT managers are still trying to run their central logging systems in-house, with only a minor percentage outsourcing to an external managed service provider. SecureData believes many IT managers questioned confuse having a series of log files with a true SIEM solution

3. What challenges, if any, do you face with your management of IT logs and systems?



Key statistics

- The biggest challenge (59%) faced by IT managers with regards to IT logs and systems is having the time / resource availability required to regularly monitor logs for suspicious behaviour
- The second biggest challenge in this area faced by 48% of IT managers is managing the disparate logging systems to accurately perform correlation and pattern recognition analysis (e.g. firewall, IDS and file access records)
- 42% of respondents said that validating logs / issues or sensitivity with log access rights for insider threats and proactive policing for compliance violations were both challenges they faced with the management of IT logs and systems

Analysis

- The results show that there are a large number of challenges faced by the management of IT logs and systems – most notably IT managers are struggling to find the necessary time and resources to regularly monitor logs for suspicious behaviour
- All of the biggest problems revolve around uncertainty and therefore increase the risk to the business - the accuracy of pattern correlation; proactive policing and validation of logs/issues for example, all require real-time management and analysis

Part 3. Summary

The results show that a large number of IT managers control their central IT logging system in-house, yet they admit what a huge challenge it is to find the time and resources to manage these systems, and all that they encompass, adequately and effectively. With near-on half of IT managers feeling that their inability to detect internal and external threats is putting their businesses at huge risk, this illustrates that now is the time for them to act.

Businesses need a system that supports both day-to-day system management and resilience with advanced cyber threat defence, detection and response to protect their networks from a rapidly evolving threat landscape. They need real-time detection of anomalies and alerting, advanced correlation and pattern recognition for forensic analysis and rapid analysis of the cause of any threats.

This research highlights that outsourcing SIEM to an independent third party might be the only viable option to ensure it gets the attention it requires, and to minimise risk of log tampering and other insider threats.

Part 4. Appendix

SecureData commissioned a Vanson Bourne Omnibus survey of 100 IT managers in large UK enterprises (more than 1,000 employees) across the financial services, manufacturing, retail, distribution/transport and commercial sectors. The following questions were asked:

- How do you rate the risk levels of the following IT security challenges to your organisation?
- What type of IT central logging system does your organisation have?
- What challenges, if any, do you face with your management of IT logs and systems?

For more information please contact us on:

D: +44 (0) 1622 723456 | E: marketing@secdata.com

December 2012
SecureData, SecureData House, Hermitage Court, Hermitage Lane, Maidstone, Kent, ME16 9NT
SecureData, Unit1, Horizon Business Park, 1 Brooklands Road, Weybridge, Surrey, KT13 0TJ

T: +44 (0)1622 723400 | F: +44 (0)1622 728580 | E: info@secdata.com | www.secdata.com | Follow us on Twitter: @securedataeu