The State of SIEM **in 2014**

Huntsman®

Defence-Grade Security Platform

The State of SIEM in 2014

WHY ONLY THE SMARTEST WILL OUTWIT TODAY'S ATTACKERS

Security Information Event Management systems (SIEMs) have become an important part of information assurance and defence against cyber-attack. With their ability to aggregate and integrate system activities, a SIEM is the key to monitoring and reporting IT security risk posture across the enterprise.

However, as Gartner observed in its 2013 SIEM Magic Quadrant: 'We continue to see large companies that are re-evaluating SIEM vendors to replace SIEM technology associated with partial, marginal or failed deployments.'[1]

This will come as no surprise to many working in IT security. SIEM systems have been widely adopted by commercial and government organisations believing SIEMs provided effective protection for large networks, systems and databases. With the stakes being raised every year, in 2014 you should rethink what your SIEM needs today to outwit a smarter adversary.

In this fully-referenced Short White, we explore:

- What major users are demanding from IT security vendors in 2014;
- Why security experts are urging vendors for more intelligent, more integrated platforms;
- How you can add specialist solutions to make your SIEM work harder:
- Why real-time monitoring is crucial for early detection and greater situational awareness; and
- Why Threat Intelligence is most useful in conjunction with behaviour-based techniques.

THE RISING COST OF FAILURE

Customers of Target in the USA have launched several class actions following a data breach that compromised 40 million credit and debit card records before Christmas 2013.[2] The charge is that 'Target failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach.'[3] Banks are said to be launching suits against Target too, to help pay for the cost of cleaning up after the massive breach.[4]

Data breaches have become bigger and much more costly, both in financial and reputational terms, and that trend is expected to continue in 2014. The time taken to detect data breaches is an additional concern: a breach at Neiman Marcus in January 2013 remained undetected for 6 months.[5] This was echoed in Verizon's 2013 Data Breach Investigations Report which found that 92% of the incidents reviewed were discovered months later by third parties, including law enforcement agencies like the FBI.[6]

WHY ARE SIEM SYSTEMS FAILING?

Little has changed since late 2012 when a survey of 100 IT managers in large UK enterprises found businesses 'struggling to effectively manage their SIEM systems.' 59% of respondents said they didn't have time to regularly monitor logs for suspicious behaviour, another 40% voiced 'serious concerns about their ability to report on internal systems and the time it takes to analyse data and logs from systems.'[7] That's the reality for most organisations.

Gartner stresses that both small and larger customer segments 'place high value on deployment and operational support simplicity.' Even market-leading SIEM systems come up short on this score, Gartner points out, with some making deployment far too complex.[8]

Clearly, performance, ease of deployment and ease of use are important, so it's prudent to check them out beforehand. The best way is to run your short-listed contenders through a Proof of Concept (POC) to validate your requirements and assess their capabilities. If any refuse, the wisest move is to cross them off the list. Would you buy a car without a test drive? Certainly not, but you'd be surprised how many organisations don't insist on a POC before they buy a SIEM system.

THE SCRAMBLE FOR BETTER TECHNOLOGIES

'Existing monolithic security analytics tools are no match for advanced malware, stealthy attack techniques, and the growing army of well-organized global cyber adversaries,' writes Jon Oltsik in NetworkWorld.[9] Rather than designed for purpose, many of these are old platforms with newer functions just grafted on, so they're not flexible enough to defend your enterprise in a changing threat-scape. Some began life as log managements systems or firewalls and, like dinosaurs, are unable to adapt to the changing world of 2014.

This is why security mergers and acquisitions are on the rise: Blue Coat Systems buying Solera Networks and FireEye buying Mandiant are two recent examples. Larry Dignan at ZDNET talks about 'a merger and acquisition dance going on in the security industry right now. Small security upstarts need more sales throughput, and large tech giants need access to new technologies and approaches.'[10]

A key driver is the need for better situational awareness, supported by data-driven decision making. 'Many organizations will embrace continuous monitoring (or Continuous Diagnostics and Mitigation (CDM) as a major security initiative,' says Jon Oltsik. 'The goal? Real-time situational awareness on network activity, accompanied by data-driven decision making.'[11] In 2014, with far more advanced adversaries, effective SIEM systems must be capable of continuous monitoring, analytics and mitigation. It's that simple.

> *"By looking for attack patterns identified via threat intelligence in your security monitoring/ analytics function, you can shorten the window between compromise and when you detect that compromise"*
>
> **Mike Rothman, Securosis, January 2014**

THE NEED FOR THREAT INTELLIGENCE

CISOs are looking for more than products, says Oltsik. 'They want an integrated cybersecurity architecture that covers networks, endpoints, and security analytics.'[12] That's true, but it risks myopia if it prompts CISOs to put all their security eggs in one single vendor's basket and accept the limitations of a proprietary world. In fact, the trend in the security space is going the other way - towards advanced, open systems that accommodate rather than limit access to promising new technologies.

In 2014, SIEM systems need to be open, modular security risk platforms that can easily integrate with selected third-party solutions – such as Deep Packet Inspection, Data Mining, Asset Protection, Predictive Analytics and Vulnerability Scanning – to deliver far broader threat intelligence information.

The same SIEM platform must let you collect threat intelligence from open and as well as proprietary sources, and from lists of suspect new attacks and vulnerabilities. The most advanced SIEMs can combine external threat intelligence with the learned behaviour in your monitored environment, and build dynamic baselines and profiles of suspicious activities for far better threat detection and response. As Mike Rothman of Securosis put it: 'By looking for attack patterns identified via threat intelligence in your security monitoring/ analytics function, you can shorten the window between compromise and when you detect that compromise.'[13]

The crucial element here is context: the more relevant information your IT security team has to work with, the faster and more effective their actions will be. Behaviour Anomaly Detection (BAD) is a real asset here, as it can add valuable local context to this external risk information.

BIG DATA, BIG HYPE?

At times, the hype around Big Data Analytics and its role in IT security reminds us of Larry Ellison's quip that the computer industry was 'more fashion-driven than women's fashion.'[14] The demands of real-time threat detection, investigation and response are very different to intensive mining of massive amounts of data across historical time windows. Gartner analyst Anton Chuvakin's advice is: 'Do not pay for the glamour of big data if there is a low chance of benefiting from the investment.'[15]

'The noise about big data for security has grown deafening in the industry,' says Chuvakin, 'but the reality lags far, far behind. As many organisations continue to struggle with utilizing traditional security analysis tools, such as SIEM tools, with the expectation that they will magically adopt big data technologies and approaches is simply unrealistic.'

Jon Oltsik points out that '... you may need data architects, statisticians, and data scientists' to get any benefit from Big Data Analytics.[16] Specialists like these are hard to find though, and the few will be quickly snapped up by the military, intelligence agencies and big consulting firms. At this stage, Big Data security analytics is in its infancy; the revelation that intelligence agencies are collecting vast amounts of data for future investigation has little relationship to the critical capabilities demanded of today's SIEM systems.

DIVERSE DATA

Martin Borrett from IBM told Information Age: 'Security systems will greatly benefit from real-time correlation across massive structured data, such as security device alerts, operating system logs, DNS transactions and network flows, as well as unstructured data, such as emails, social media content, packet info and business transactions.'[17]

Isn't that what advanced SIEM systems should do right now – capture and process large quantities of data from diverse sources at high speed, and analyse them in real- time? Indeed, but very few can collect loads of really diverse data and actually make sense of them.

'Security analytics is more than just big data, it's also diverse data,' says Ed Bellis from Risk I/O. 'This causes serious technical architectural limitations that aren't easy to overcome with just SIEM.'[18] That's where a specialist third party application can complement the SIEM information for more informed security decision-making.

FIRST, GET THE BASICS RIGHT

With so much talk about the complexities of cyber security, it's easy to overlook the fundamentals. Gartner analysts tell us that 'the greatest area of unmet need is effective targeted attack and breach detection.'[19] They add that 'the situation can be improved with better threat intelligence, the addition of behaviour profiling and better analytics.' Gartner also advocates adding more event sources and greater use of real-time monitoring.

In other words, in 2014 an effective SIEM must have the ability to:

- Detect targeted attacks and breaches before serious damage is done;
- Deploy dynamic behaviour profiling for real-time detection;
- Perform continuous monitoring of more and diverse sources; and
- Merge appropriate threat intelligence for improved analytics and response.

SOME REAL INTELLIGENCE, PLEASE

You might have read about security analysts sifting through mountains of data, looking for indicators of compromise. To your organisation and others in big business and the public service, this might seem more like a scene from a Hollywood movie; most barely have enough staff to man the lookouts, let alone comb the surrounding fields for footprints.

The reality is that data volumes and threats are growing while IT budgets are not. In 2014, IT security teams are expected to contain the business risks posed by cloud computing, mobile computing, BYOD, IT consumerisation, 'Shadow IT' (IT solutions built or used by business units without IT approval) and more. To do that, they need systems with real intelligence that can automate more of the mundane tasks, prioritise threats and protect against an ever increasing attack surface.

A different kind of intelligence is needed by company directors and C-level managers wanting to fulfil their information governance and compliance obligations. In 2014, SIEM systems have to provide easy-to-understand risk reports customised for business not technical users, such as the CEO, CFO, CIO (CSIO) and Board Risk Committees.

MORE TOOLS IN THE KIT

The best SIEM systems make your IT security staff more productive, and give them the time, visibility and information they need to make sound decisions about managing security risks.

The most advanced SIEM systems also ship with sets of tools and facilities that make the job easier, such as:

- Automated continuous compliance and security management reporting;
- Report templates for analysts, operation managers, auditors and business users;
- 'Out-of-the-box' analysis rules which can be simply customised or added to;
- Real-time event correlation for quickly joining the dots between seemingly unrelated events;
- A master console for real-time presentation of security incidents and events; and
- Wizard-driven installation, and software that learns on the job.

Some vendors provide some of these, while others charge extra for them – often at an additional capital cost or as Professional Service fees for 'care and feeding' which are much harder to calculate.

> *" ...the situation can be improved with better threat intelligence, the addition of behaviour profiling and better analytics."*
>
> **Gartner SIEM Magic Quadrant 2013**

FEWER SKILLED RESOURCES

Lately, the advice from the security experts has been 'assume you've been breached'. They advocate probing more deeply into your logs and every packet that's crossed your network, to find the footprints of the intruder. Then, as soon as you find them, you're supposed to send in the SWAT team.

This may be possible for global banks, aerospace companies and governments, but most organisations don't have the time, the specialist skills or the luxury of this painstaking analysis. It's not just lack of resources; there's also 'an acute shortage of cyber security professionals who are adequately skilled for today's threat landscape.'[20] The big enterprises and consulting firms are hiring as many professionals as they can, and 'SMEs will struggle to compete for the best talent, putting the future of their businesses at risk,' says Christian Toon from Iron Mountain.

What organizations need are SIEM systems that deliver more value for less effort, smarter systems that let your staff focus on the vital few instead of being swamped by the trivial many; SIEM systems that put an end to wasting precious time on routine housekeeping chores; SIEM systems that automatically update their behavioural and threat intelligence databases by learning on the job.

DON'T SETTLE FOR SECOND BEST

Gartner says: 'the greatest area of unmet need is effective targeted attack and breach detection.'[21] This is backed up by a recent report from Forrester Research, which found that 63% of the security decision makers surveyed cited improved threat detection monitoring as a high priority.[22]

Gartner's latest Critical Capabilities for SIEM report[23] provides a useful summary of essentials you should insist on when selecting a SIEM system today, among them:

- Real-time monitoring with event correlation, predefined correlation rules and the ability to easily customize these;
- A security event console for real-time presentation of security incidents and events;
- Behaviour profiling that builds profiles of normal activity for various event categories
- network flows, user activity, server access and more – alerts on deviations from normal;
- User activity and database access monitoring, file integrity monitoring;
- Threat intelligence – sources should include security research teams/ security vendors/ MSSPs;
- Deployment and support simplicity through a combination of embedded SIEM use- case knowledge, and design that minimizes deployment and support tasks.

For CIOs and CISOs focused on the ROI of their SIEM investment, the last point about deployment and operational simplicity is important. These are hard costs and, while organisations need sharper tools to protect their sensitive data and IP, the sharpest tools are no use if they're too heavy and too hard to use. A SIEM solution can be a large investment with a long term legacy, so the prudent advice remains: know your requirements and take a test drive before you commit yourself to the bright red imported model at the front of the lot.

REFERENCES

1 Gartner SIEM Magic Quadrant 2013

2 Target Sued for Credit Card Hack, TIME, December 20, 2013

3 vTarget Sued Over Data Breach As Customer Backlash Causes PR Nightmare, Fierce Retail, December 20, 2013

4 Banks could sue over Target breach, December 23, 2013

5 Breach at Neiman Marcus Went Undetected From July to December, Business Day, January 16, 2014

6 Verizon 2013 Data Breach Investigations Report, April 2013

7 Constraints lead to failure to effectively manage SIEM systems, SC Magazine UK, December 11, 2012

8 Gartner Magic Quadrant for SIEM 2013

9 Strong opportunities and some challenges for big data security analytics in 2014, NetworkWorld, Dec 13, 2013

10 Network security spending to surge in 2014, ZDNET, January 9, 2014

11 Enterprise CISO Challenges In 2014, NetworkWorld, January 10, 2014

12 Enterprise CISO Challenges In 2014, NetworkWorld January 10, 2014

13 Leveraging Threat Intelligence in Security Monitoring: Benefiting from the Misfortune of Others, Securosis Blog, Jan 26, 2014

14 Larry Ellison Is Sick Of 'Cloud Computing' Hype, CRN, September 26, 2008

15 Security Information and Event Management Futures and Big Data, Gartner Blog, January 21, 2014

16 Enterprise CISO Challenges In 2014, NetworkWorld, January 10, 2014

17 The 2014 cyber security roadmap, Information Age, January 9, 2014

18 Moving Beyond SIEM For Strong Security Analytics, darkREADING, December 16, 2013

19 Gartner Magic Quadrant for SIEM, March 2013

20 The 2014 cyber security roadmap, InformationAge, January 9, 2014

21 Gartner Magic Quadrant for SIEM, March 2013

22 Network security spending to surge in 2014, ZDNet, January 9, 2014

23 2013 Gartner Critical Capabilities For SIEM, May 2013

Author: Peter Woollacott

Co-Founder and CEO, Tier-3

Peter Woollacott is the co founder and CEO of Tier 3 Pty Ltd, the software company that holds the patent for Behavioural Anomaly Detection and developed Huntsman® Intelligent Security.

He has 25 years' experience in operational and risk management with companies like Lend Lease, CBA, AXA, EDS, PWC and Bain International. Peter holds Masters Degrees in Applied Finance and in Business Administration, and lectures in executive post graduate education at Macquarie and Sydney Universities.

Peter may be contacted at
pwoollacott@huntsmansecurity.com

Please visit the Huntsman Resources page at
www.huntsmansecurity.com/resources
for White Papers, Compliance Guides, Solution Briefs and more resources by this author.

Huntsman | Tier-3 Pty Ltd

Asia Pacific

t: +61 2 9419 3200
e: info@huntsmansecurity.com

Level 2, 11 Help Street
Chatswood NSW 2067

EMEA

t: +44 845 222 2010
e: ukinfo@huntsmansecurity.com

100 Pall Mall, St James
London SW1Y 5NQ

North Asia

t: +81 3 5809 3188
e: info@huntsmansecurity.com

TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

Americas

toll free: 1-415-655-6807
e: usinfo@huntsmansecurity.com

Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com   linkedin.com/company/tier-3-pty-ltd   twitter.com/Tier3huntsman