



Security intelligence: solving the puzzle for actionable insight

...reducing the time to detect
and respond to advanced cyber threats

author • Fran Howarth



Executive summary

THE EXTENT OF SECURITY incidents and breaches seen today is so high and so widespread that no organisation should be complacent. Rather, organisations should work on the principle that it is probable that they have already been breached. Traditionally, many security technologies have focussed on preventing threats from penetrating their networks, but, faced with increasingly sophisticated, well-resourced, and businesslike attackers with the ability to target specific individuals and organisations with tailor-made exploits and to evade such defences, such tools are no longer sufficient. Prevention alone is not enough.



The ability to defend against the advanced cyber threats and breaches that are a fact in today's complex threat landscape requires a combination of three capabilities—prevention, detection and response. Detection is the new imperative, but security incidents and breaches are taking ever longer to discover. Only by being able to quickly detect threats can the ensuing damage be effectively contained. Remediating events is another area where many organisations fall short, relying on manual efforts owing to reluctance to take actions that might introduce further threats, in part because they lack full visibility over what is happening on their network.

A new breed of security intelligence platforms give the visibility that is required into all network threats and incidents and provide the context that is needed to gauge what events are impacting the network and their potential impact. From the information that such platforms provide, organisations are able to gain actionable insight that can lead to better informed decision-making. Actionable insight can be defined as the ability to analyse large quantities of data to infer behavioural patterns for people and things to enable the automation of business processes that leverage that insight, replacing what were, historically, manual activities. In a security context, it requires the ability to collect and analyse massive volumes of event data from throughout the network and all devices, users, and applications that connect to it in real time so that appropriate action can be taken.

Fast facts

- Log collection and management—including the collection of massive volumes of logs from throughout the network, their normalisation and centralised aggregation, secure long-term retention, efficient search and reporting capabilities.
- Advanced analytics—capabilities include log correlation, classification and analysis using statistical and behavioural analysis techniques based on machine-learning capabilities regarding expected normal behaviour. The analysis should provide context regarding all events so that the real impact can be gauged and remediation prioritised.
- Continuous monitoring—of all activity across the network and all hosts, users, endpoint and applications that connect to it in real time.
- Automated remediation—to respond automatically to alerts in real time, whilst including an optional manual approval process for remediation actions that warrant review prior to initiating the response.
- Forensics—the ability to delve into massive volumes of historical data and rapidly pivot through the information to discern pertinent patterns to accelerate investigations and to find the root cause of incidents
- Centralised management—a central repository should be provided for all management and administrative tasks and should provide one central point for managing and enforcing policies. This will also provide the audit and reporting capabilities required to improve overall security posture and meet regulatory mandates.



Security intelligence platforms have their roots in security information and event management and log management systems, but have expanded beyond traditional capabilities to include a host of complementary capabilities that extend the power of such systems for efficient real time detection of events and incidents, and automated response so that remedial actions can be swiftly applied. They are essential tools for any organisation that are looking to optimise operational and security risk management across their organisation and are key for defending against advanced threats and for achieving compliance objectives.

This document is intended for any organisation that is looking to improve its overall security posture and risk management capabilities throughout the enterprise in a cost-effective manner. It provides statistical evidence regarding the challenges that organisations are facing and demonstrates how security intelligence platforms can answer those challenges by providing actionable insight into the true state of affairs so that remedial action can be taken to ensure the organisation's network is secure. Such platforms allow organisations not only to take immediate action to counter threats, but also to discern patterns from events that have occurred through forensic analysis.

The bottom line

Without being able to see the full picture regarding how security events and incidents are impacting all parts of the network, organisations are stymied in their efforts to not only detect events, but to respond to them in an appropriate manner based on real intelligence regarding their relative importance. This leaves an organisation wide open for damaging security incidents and breaches because they have no way of knowing what vulnerabilities and exploits exist using manual or only partially automated solutions alone. Tying together nuggets of information from disparate systems and security controls is a challenge too far for many organisations unless they have the right security controls in place.

Security intelligence platforms provide those security controls by tying together information from throughout the network, allowing vast swathes of security-related information to be correlated and analysed to provide actionable insight into how the organisation is affected and what is the best remedial action to take. Such platforms have now come of age, providing full automation for effective decision-making and integrating a number of complementary controls that increase their value considerably. Any organisation that embraces the use of such platforms will find they have a considerable competitive advantage over those that do not, who will remain floundering around in the dark.

Prevention alone is not enough

ANY SECURITY INCIDENT can take its toll, causing an organisation to divert resources to correct the problem and get everything running again. But if that incident results in a breach where data is potentially exposed or actually disclosed to an unauthorised party—especially if it is personally identifiable information related to persons such as employees or customers—the stakes are much higher. Figure 1 shows the most damaging consequences of data breaches caused by malicious actions.

In recent [research](#), the Ponemon Institute found that 68% of organisations experienced a security breach or incident in the past two years, yet it cautions that many security professionals find it hard to keep track of the threat landscape and are not even sure whether or not they have been the victim of an attack.

[Statistics](#) produced by PwC estimate that the problem is even greater, showing that 81% of large organisations have had a security breach in the past year. Security breaches are everyday news, but the report cautions that what we see is just the tip of the iceberg since it found that 70% of organisations keep their most serious security breaches under wraps.

However, the same report found that, whilst the average number of security breaches suffered by each organisation is actually falling, the cost of each data breach has doubled over the past year, rising to an average of £600,000 to £1.15 million for the worst security breach encountered.

Much of this is because attacks are becoming more menacing, using ever-more insidious techniques and increasingly targeted at specific organisations or even individuals within them. Traditional technologies such as anti-virus are no longer effective against such attacks that use malware strains not previously seen, often written specifically for one attack and never seen again. According to FireEye, 70% of malware is seen [just once](#) and 82% disappears within one hour. ▶

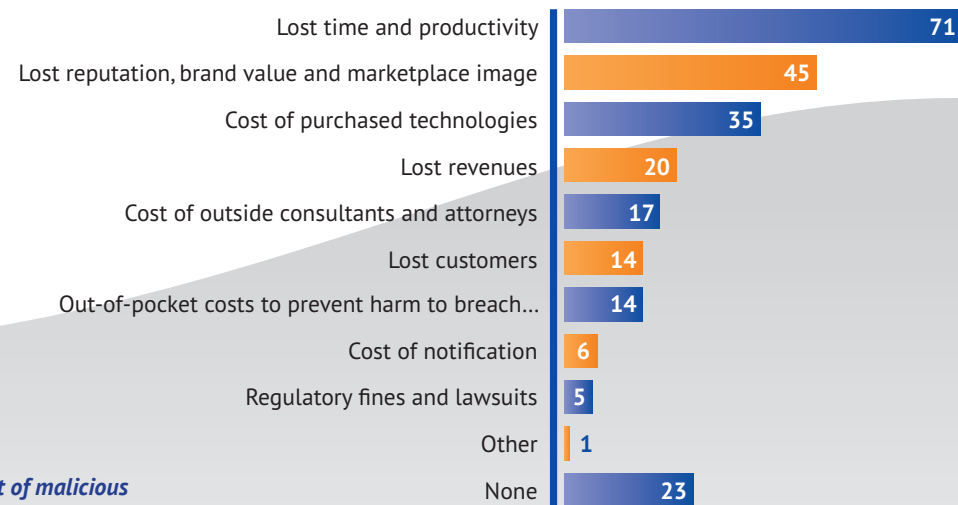
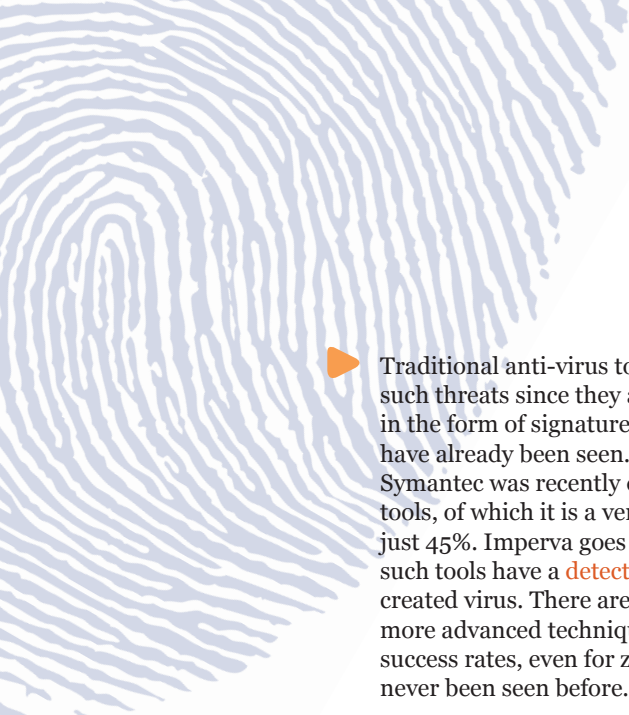


Fig 1.
Impact of malicious data breaches



▶ Traditional anti-virus tools are incapable of detecting such threats since they are based on countermeasures in the form of signatures for malware strains that have already been seen. A senior executive at Symantec was recently derided for claiming that such tools, of which it is a vendor, have a **success rate** of just 45%. Imperva goes even further and states that such tools have a **detection rate** of just 5% for a newly created virus. There are newer technologies that use more advanced techniques and have much higher success rates, even for zero-day threats that have never been seen before.

However, using malware is not the only way of gaining a foothold on a network. Increasingly, specific individuals are being targeted through social engineering exploits, albeit in many cases in combination with malicious exploits. The DBIR 2013 report stated that 76% of network intrusions exploit weak or stolen user credentials. Among the

methods used are phishing techniques aimed either at tricking a user into supplying credentials, brute force password guessing, or the use of application-level attacks such as SQL injection to retrieve credentials or to bypass the authentication system. Once attackers manage to infiltrate a network, they often look to get their hands on credentials with higher levels of privilege and entitlements attached to them to move through the network in search of high value information. The use of stolen credentials played a key part in the recent breach suffered by eBay (see text box).

But no prevention technology—even modern-day technologies for guarding against zero-day threats—is a panacea, especially since there are so many threat vectors to guard against in the form of mobile devices, cloud-based applications, social media, USB sticks and more, with their number growing every day, and users are far from infallible. As the numbers show, the vast majority of organisations are being breached and everyone should consider themselves a target—no matter how small the firm is, as a small business can be used as a conduit into larger organisations, as was shown in the recent Target breach involving an HVAC contractor.

As the new mantra goes: **“It is not if, it is when”** an organisation will be breached. Prevention alone is not enough.

The data breach at eBay in 2014

In the late February/early March timeframe of 2014, attackers were able to breach eBay by purloining login credentials for a small number of employees of the firm. From there, they were able to steal information that included customer names, encrypted passwords, email and physical addresses, phone numbers and birthdates. In all, 145 million customers could potentially have been impacted by the attack. Because the credentials belonged to actual employees, the attackers were able to stay under the radar and take what they wanted.

Had eBay been using machine-based behavioural analytics tools, it could have detected anomalies in user behaviour so that compromised credentials could have been identified, and affected user accounts could have been reset before the damage was done.

However, the attack went unnoticed until early May, at which point eBay called in specialists, including law enforcement, to use forensic techniques to investigate what happened. This, plus the fact that it took another three weeks to inform customers of the breach, led to its share price dropping, its auction takings falling and its reputation being tarnished. It is also facing investigations from three US states and the Information Commissioner's Office of the UK

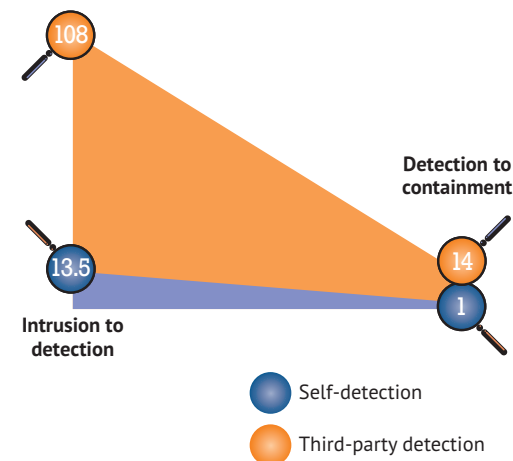
Detection is the new imperative

SINCE IT IS ALMOST A GIVEN that every organisation will, at some point, be breached, an organisation's ability to respond in a timely and efficient manner is critical to containing the incident, and can make the difference between a security incident causing only minor damage and a situation that results in a major incident. However, many organisations currently lack the ability to detect breaches in a timely manner, with more than a third of breaches taking months or even years to discover, as shown in Figure 3. According to Mandiant, the median time taken for organisations to detect that threat groups are present on their network is 229 days—just a few days shy of eight months.

Further evidence of the inability of organisations to detect breaches themselves is provided by a variety of data sources that show that many breaches are discovered by external sources rather than by the organisation itself. Many sources state that the majority of breaches are discovered by third parties—including the DBIR 2014, which states that this is 85%, and Mandiant, which estimates that this is 67%.

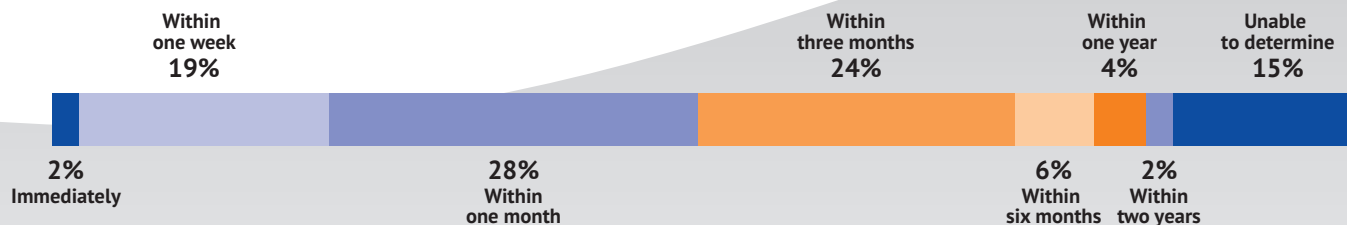
As Figure 4 shows, organisations that are able to detect breaches themselves not only do so faster, but are in a much better position to resolve the problem than when it is discovered by an external source.

Fig 4. Length of time from detection to containment in days



Source: Trustwave

Fig 3. How long malicious breaches take to discover



Source: Ponemon Institute

▶ Among the reasons why breaches are so hard and take so long to discover is that attackers are using increasingly evasive techniques and aim to move laterally through, and stay hidden for long periods of time, on networks in order to collect swathes of sensitive information over time. This means that there may be few obvious indicators of a breach unless the attacker surfaces, often trying to exfiltrate data to command and control servers under their charge, or data is discovered elsewhere than is expected. The longer detection takes, the more costly an attack can be in terms of stolen data and the more difficult it can be to resolve, since the attacker is so firmly entrenched.

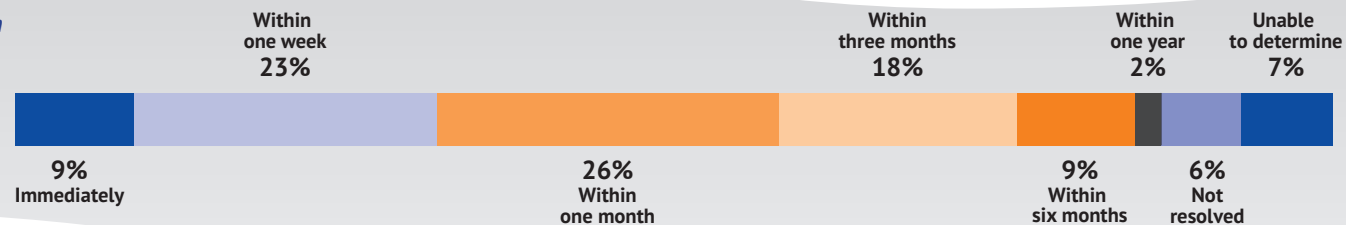
As **Figure 5** shows, organisations not only face challenges in detecting breaches, but also in resolving breaches—often because the attackers have embedded themselves so deeply in the network. Detection is the new imperative.

Where remediation falls short

Once a breach has been detected, organisations need to determine what remedial action to take. For many organisations, this requires much manual work in order to pore through logs and event reports to review the situation in order to determine where action needs to be taken and what events should be prioritised. Lack of automation stifles this labour-intensive process.

Many, however, are reluctant to fully automate remediation processes for fear that a critical application or system is shut down by mistake, causing disruption to the business, or that a person's access is removed and they are unable to perform critical tasks. In many cases, this is because they lack the visibility across the network to gauge the consequences of their actions. According to the Ponemon Institute, 59% of organisations do not have adequate intelligence regarding the state of their network or are unsure about attempted attacks and their impact. Without this information, it can take months to work through the entire process of event investigation, service restoration and verification—even after an incident has been discovered.

Fig 5.
Time taken to resolve a breach



Source: Ponemon Institute

How security analytics and intelligence help

IN ORDER TO EFFECTIVELY detect and respond to security incidents, technology is available in the form of security intelligence platforms that provide greater visibility across all events occurring on the network and enable organisations to more efficiently and effectively detect and respond to unwanted or anomalous events. Such platforms give organisations the ability to correlate and analyse information to provide actionable insight into the relative severity of events and incidents so that they can be prioritised and suitable remedial decisions can be made, driving effective response. Security intelligence platforms provide organisations with the ability to see exactly which devices, users and applications are impacted by security events so that response can be based on real time intelligence, whilst ensuring that the response to those events is measured, effective and not a knee-jerk reaction that could introduce further problems, such as causing a system outage.

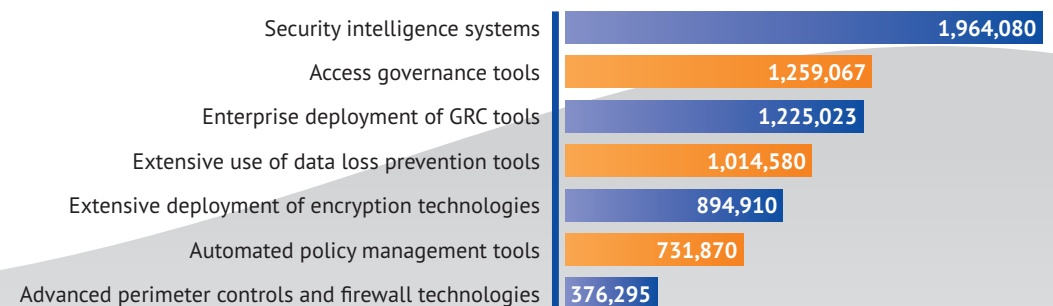
By being able to prioritise actions, organisations are able to cut response times dramatically and ensure that they are able to contain even the most critical security threats.

Technology that provides visibility across the network, and all devices, applications, and users that access the network, not only allows organisations to take immediate action to counter threats as they occur, but also enables them to forensically analyse events to look for patterns of behaviour that have occurred so that controls and policies can be put in place to prevent them from occurring again. In this way, security intelligence platforms provide predictive intelligence capabilities so that they are actually able to anticipate events before they occur.

With such information at their fingertips, organisations will be better able to improve their overall security posture and upgrade their ability to achieve compliance, governance and assurance objectives.

As well as this, they will be able to achieve cost savings in their efforts to counter cyber crime. As shown in **Figure 6**, security intelligence systems provide the greatest cost savings of seven categories of tools included in a recent survey by the Ponemon Institute. It also found that the use of such platforms provides organisations with the greatest return on investment at 21%.

Fig 6.
Cost savings with the use of security tools in US\$



Source: Ponemon Institute

Sample use cases for security intelligence platforms

EVIDENCE

Advanced threat management

- Close attackers' means of entry
- Automatically remove malware
- Detect breach before data loss or cybercrime occurs
- Expose compromised credentials
- Contain breaches through ability to see a series of events over time that lead to the extraction of valuable data
- Investigate entire lifecycle of an attack from initial compromise, through traversal of the network to data extraction to a command and control server

Compliance management

- Comply with regulatory requirements for log collection, review, archiving, and reporting
- Search and retrieval of logs for analysis and forensic investigation
- Keep track of and manage privileged users
- Monitor file integrity

Continuous monitoring

- Support overall operational and security risk management strategy
- Regulations increasingly mandating continuous monitoring
- Achieve real time actionable intelligence for improved decision-making
- Validate security controls

Forensic investigation

- Gain required evidence to support investigations
- Support electronic discovery
- Reconstruct a series of events to determine root cause

Fraud detection

- Detect and flag fraud that evades fraud detection technology by discerning activity from logs, such as bank withdrawals from multiple locations
- Take real time remedial decisions, such as disabling affected account
- Analyse behavioural patterns to detect all suspicious activity
- Detect fraudulent insider activity

Insider threat detection

- Monitor privileged users
- Provide detailed contextual information to isolate and contain threat
- Prevent, detect, and respond to insider threats
- Prevent data leakage, IT sabotage, and fraud

Monitor remote and critical infrastructure facilities

- Monitor industrial automation, SCADA and remote facilities such as electricity substations, many of which may be unmanned
- Detect changes made remotely where physical controls such as keypads are bypassed
- Take remedial action to rollback changes

Network behaviour anomaly detection

- Detect communication patterns indicative of botnet callbacks to a command and control server
- Prevent data extraction
- Enhance performance of other network controls, such as intrusion prevention systems to better identify and control network threats

Support for multiple locations

- Provide centralised control of multiple branch office and remote locations at a fraction of the cost of separate systems
- Provide visibility across entire enterprise operations
- Ease compliance with regulations across an enterprise

Web application defence

- Detect, identify, and prevent breaches
- Automatically blacklist malicious URLs and web applications
- Prevent attacks targeting web servers

What technology components are needed?

SECURITY INTELLIGENCE TOOLS have evolved from security information and event management (SIEM) and log management systems. The term SIEM was coined roughly a decade ago and refers to technology that provides capabilities for the real time and forensic analysis of all events occurring from the alerts and logs generated by all devices connected to the network and applications that run on it. SIEM systems provide the ability to capture all network events and to correlate and analyse all information to uncover abnormal system behaviour that is indicative of security risks, threats or incidents, turning event data into actionable information.

Over the years, some vendors have evolved SIEM and log management systems into security intelligence platforms that provide comprehensive tools for providing full visibility into events across the network stack. Such complementary capabilities include file integrity monitoring, configuration monitoring, network and user monitoring, and network forensics. They provide contextual information through capabilities such as geolocation (regarding where a user is), the entitlements a person has been given and what device they are using so that those that have been targeted or compromised can quickly be identified and incidents and threats remediated.

The following components are required for a security intelligence platform for providing the actionable insight needed for effective security and risk management:

Log management and analysis

Log management is defined by **NIST** as an approach to dealing with large volumes of computer-generated log messages (also known as audit records, audit trails, event logs). Logs are verifiable records of events that have occurred over the network that provide evidence of activities such as failed login attempts or escalation

of privileges and entitlements. Log management covers log collection, centralised aggregation, long-term retention, log analysis both in real time and in bulk after storage, as well as log search and reporting.

In order to be effective, log sources must be included from all parts of the network, devices that attach to it, and applications and controls running on the network. These sources include anti-malware applications, intrusion detection and prevention systems, file systems, firewalls, routers, servers, and switches. To overcome challenges in dealing with the diversity of sources and formats of log records, all data collected must be normalised to provide a unified view of events.

For security and compliance purposes, log records need to be kept in a highly secure, centralised storage facility so that records are archived for forensic and compliance purposes. The system should provide intuitive, quick search capabilities across all records, with the ability to retrieve any records required.



▶ **Advanced analytics**

Once logs have been collected and normalised, they need to be correlated to find all logs that are related to one specific event so that patterns can be recognised and the entire picture can be gauged and events can be classified. Advanced analytic techniques include statistical and behavioural pattern matching, utilising machine-based learning regarding what constitutes normal behaviour based on context related to users, applications, devices, and configurations. It is essential that the system is capable of analysing massive volumes of data—so-called big data—owing to the sheer volume of information generated across networks today and the speed with which those volumes are growing as networks expand to encompass an ever-growing array of devices, endpoints and applications.

Advanced analytics capabilities should be capable of deriving context related to the identity of users against log events for more effective forensic analysis and incident response. The ability to infer the identity of users is essential to detect and respond to the use of compromised credentials, the misuse of privileged accounts, insider theft, data exfiltration, and compliance violations. It also helps in determining the most effective response when behavioural anomalies are exposed. To provide the context required regarding user identities, the system should interface with authentication and access control systems.

Continuous monitoring

So that all activity across the network, hosts, users and endpoints can be captured in real time to provide full visibility and awareness of all network events, it is necessary that the security intelligence platform be able to perform continuous monitoring of network, host, user activity, file integrity, and configurations. Continuous monitoring not only ensures that the organisation is aware of all events in real time, but is increasingly a requirement of regulatory mandates and best practice standards.

In terms of host and network activity monitoring, the system should provide full session packet capture to provide a complete record of network activity for real time threat defence and to aid in forensic investigations. At a network and host level, events that should be recorded include process and service activity, network connections, endpoint and removable media activity, and user activity monitoring of any user or process that authenticates to a host. This monitoring will aid organisations in their ability to detect anomalous, unauthorised, or suspicious behaviour and activity, and to prevent data loss through exfiltration or via removable media and other endpoints. In particular, privileged user activity should be monitored to reduce the insider threat.

User-aware file integrity monitoring is an essential component for preventing inappropriate access to data, thwarting data transfer and stopping breaches by showing when sensitive files are created, viewed or modified in any way according to the context of which users or user groups are accessing what. It can also be used to flag abnormal application behaviour to prevent vulnerabilities from being exploited. Configuration monitoring ensures that no errors or vulnerabilities are introduced through inappropriate changes to configurations or mistakes made in order to strengthen configuration and change control.



▶ Automated remediation

Automated remediation capabilities enable organisations to automatically and immediately respond to alerts from the real time analysis activities signalling anomalous behaviour has been detected or a policy has been violated, reducing the need for manual intervention. It is essential that remediation be automated given the exceptionally high volume of threats and incidents faced by organisations and the number of alerts generated, which are far too great for time-consuming, resource-intensive manual remedial processes to be effective. Automation allows immediate actions to be taken, such as blocking suspicious IP addresses, quarantining rogue users or devices, or preventing specific processes from executing.

However, it is essential that the security intelligence platform does not introduce extra risk through automating the remedial action process, such as causing essential systems to be shut down, which is a fear that prevents many organisations from automating such processes. Therefore, built-in checks with layers of authorisation before remedial action is actually taken are essential to ensure that the action taken is the correct one and does not have unintended consequences. To aid making remediation

decisions, it is also useful for the security intelligence platform to provide predetermined rules that look at the behavioural patterns associated with a breach, including the tools, techniques, and procedures used by attackers in situations already seen. These are known as indicators of compromise and can allow organisations to better determine what of the alternative automated responses will be the best course of action to take.

Forensics

Security intelligence systems should provide the ability not just to investigate events in real time, but to delve into historical data to discern patterns and to find evidence related to events that have occurred, tying activity back to behaviours exhibited by specific individuals. For this, log and event records must be stored in a highly secure, tamperproof repository, with good search capabilities across both structured and unstructured data, covering activity at both the network and host level. For best results, the system should provide visualisation capabilities that allow the organisation to pivot data and drill down into the details.

Centralised management

To ensure an organisation gains visibility and insight across the entire network, a security intelligence platform should provide centralised management so that all event logs are collected, stored and analysed in one central location to provide one single view across all security events. This allows for policies to be set and managed from one central enforcement point, so that all out-of-policy alerts can be triggered and handled from one point of management, sent on to the relevant personnel and all actions taken recorded by the management console. This provides the audit trail that is necessary for generating management reports and for proving compliance with regulations, best practice guidelines, and internal governance needs. For automating proof of compliance, it is useful for pre-built report templates to be included, based on requirements of specific regulations that organisations face.

Summary

SECURITY INTELLIGENCE PLATFORMS provide visibility across the network and all hosts, users, devices, and applications that connect to it, of all security events impacting the organisation, along with the context needed to drive effective decision-making and response. Collecting and analysing information from across the network and all security controls in use, they allow organisations to ensure that no stone is

left unturned in their battle to detect, contain, and respond to the security threats that they face. Those organisations that deploy security intelligence platforms will ensure that they have the actionable insight that they need to prioritise all actions and to keep their valuable data out of the hands of attackers, as well as shielding themselves from the unwelcome attention of regulators and public scorn.

Where next?

Bloor maintains a Technology page on their website with further information regarding [Security Analytics](#).

The author of this eBook is [Fran Howarth](#), Senior Analyst for Bloor's security area.

Fran's [website page](#) has a rundown of her experience and you can discover other papers and articles she has written.



2nd Floor
145-157 St John Street
LONDON EC1V 4PY
United Kingdom

Tel: +44 (0)207 043 9750
Web: www.BloorResearch.com
email: info@BloorResearch.com