Cyber security - Do you know your SOC from your SIEM?

Submitted by: PR Artistry Limited
Thursday, 13 February 2020

Do you know your SOC from your SIEM and more importantly where security compliance and regulation fit in?

It is widely accepted that enterprise cyber-attacks are inevitable – it's not a question of if but when. However, in the age of GDPR all organisations need to have a defined approach for when a security breach occurs, or risk falling foul of regulation. Guy Lloyd at CySure looks at the tools available to keep abreast of the threat landscape and explains the importance of having a response strategy

Large scale data breaches grab headlines and 2019 has delivered its fair share of newsworthy stories. Earlier this year Capital One's security defences were breached by a lone hacker. The breach affected approximately 100 million consumers in the United States and about 6 million in Canada. The information stolen included names, addresses, phone numbers, email addresses, birth dates and self-reported income. Also exposed, in some cases, were customer credit scores, credit limits, balances, payment history and contact information. The hacker behind this breach also accessed about 140,000 Social Security numbers of potential Capital One credit card customers and about 80,000 linked bank account numbers of secured credit card customers.

This data breach ranks as one of the biggest in history and has been a costly one. It was reported that Capital One expected to suffer from $100 million to $150 million in costs related to the hack. These costs stem from notifying customers who were affected, providing these customers free credit monitoring, defending itself against legal actions and upgrading technology to fix the vulnerability.

As the saying goes, bad news travels fast and media outlets are quick to pick up on data breach stories. What we don't hear about is when security defences have proved effective. Security information and event management solutions (SIEMs) and security operations centres (SOCs) are two developments that are helping organisations stay ahead of the threat landscape.

What is SIEM?
Security information and event management (SIEM) software gives enterprise security professionals both insight into, and a track record of the activities, within their IT environment. It collects and aggregates log data generated throughout the organisation's technology infrastructure, from host systems and applications to network and security devices such as firewalls and antivirus filters. The SIEM software then identifies and categorises incidents and events, as well as analyses them. It then provides reports on security-related incidents and events, such as malware or malicious activity. Finally, it sends alerts if analysis indicates a potential security issue.

Networks are often complex and the number of interconnected systems and processes mean that SIEMs typically generate thousands of alerts daily. Many, if not most, are false positives. This is where a security operations team becomes invaluable.

Security Operations Centre
Security operations centres (SOC) monitor and analyse activity on networks, servers, endpoints,

databases, applications, websites and other systems. The aim is to look for irregular activity that could indicate a security incident or compromise. The SOC is responsible for ensuring that potential security incidents are correctly identified, analysed, defended, investigated and reported.

SIEM solutions tend to generate vast quantities of data, which must be analysed and calibrated to avoid IT teams being overwhelmed with tickets. The SOC team's goal is to detect, analyse and respond to cyber security incidents. Firstly, they must determine the real incidents from false positives. Once an event is identified they use a combination of technology solutions and a strong set of processes to address the issue.

No room for improvisation

A response strategy is vital in the aftermath of an event. When reputation, revenue and customer trust is at stake, it's critical that an organisation can identify and respond to security incidents and events.
A SOC will coordinate the primary response to any attack or loss of data. However, in the age of GDPR all organisations, regardless of size, need to have a clear strategy, in the event of an attack it is not the time to improvise.

GDPR requires breaches that are likely to have an adverse effect on individuals to be reported within 72 hours. Within this 72-hour window, a long list of activities needs to be initiated. This includes:

- A description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned
  - the number of personal data records involved and their categories
- The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained
- A description of the likely consequences of the personal data breach
- An outline of the measures taken, or proposed to be taken, to deal with the personal data breach including, where appropriate, the measures taken to mitigate any possible adverse effects.

People and processes in alignment

During a data breach is not the time to be defining an approach to a security incident and wondering about compliance and regulation. It's vital that employees know what they should do and everyone understands how their actions can affect the outcomes.

An online information security management system (ISMS) can help organisations to define their processes. CySure's Virtual Online Security Officer (VOSO) is a low cost, simple to use workflow system which guides organisations through the tasks needed to achieve alignment with security policies.

VOSO initiates and guides organisations through the required polices, processes and events in an easy to understand, phased approach that will help mitigate regulatory fines and litigation if a company suffers a data breach. The audit trail in VOSO Plus acts as evidence that organisations have implemented the process and technical controls towards protecting the business and data from internet based cyber-attacks.

Organisations need to be prepared. Now is the time to define a response strategy to ensure a security incident doesn't turn into a business disaster.

Guy Lloyd is a Director of Cysure

- ENDS -

About CySure

CySure is a cyber security company founded by experts with extensive experience in operational and risk management. The company has offices in London (UK) and California (USA) and CySure's flagship solution – Virtual Online Security Officer (VOSO) is an information security management system (ISMS) that incorporates GDPR, US NIST and UK CE cyber security standards to guide organisations through complex, emerging safety procedures and protocols, improve their online security and reduce the risk of cyber threats.

For more information please visit CySure (http://www.cysure.net)

Press contact: Mary Phillips/Andreina West
PR Artistry Limited
T: +44 (0)1491 845553
E: mary@pra-ltd.co.uk

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of PR Artistry Limited

Copyright © 1999-2024 ResponseSource, The Johnson Building, 79 Hatton Garden, London, EC1N 8AW, UK

e: info@responsesource.com t: 020 3426 4051 f: 0345 370 7776 w: https://www.responsesource.com