What is SOAR?

In simple terms, SOAR stands for Security Orchestration, Automation, and Response, and is a phrase which was originally coined by Gartner. It describes software capabilities which are then combined into a single platform in order to enable organisations to gather threat-related data and automate responses to the cyber-threats faced. Before analysing SOAR in more depth and examining the way in which it combines with SIEM (security information and event management), it's probably worth looking at the issues facing organisations which help to create the situation in which SOAR and SIEM can play such a vital role.

The first statistic of note is the prediction that the size of the SOAR market is due to rise by 16.3% compound annual growth rate (CAGR) between now and 2025 to hit $2.3 billion, a fact which underlines the importance of this technology and, more pointedly, the fact that it is filling what would otherwise be a gap in cyber security provision. The nature of that gap is the shortage of skilled workers within the cyber security industry – there is a security staff shortage of more than 140,000 people across Europe, the Middle East and Africa (EMEA), with more than 60% of organisations stating that they are experiencing skill shortages within cyber-security. At the same time, in North America, the shortage of skilled workers is estimated to be as high as 500,000. In addition to the difficulties which organisations face attracting and retaining the skilled operatives capable of organising effective cyber-security systems, the need for SOAR is driven by the constantly evolving nature of the threat itself. The Internet of Things (IoT), for example, presents an entire new front along which organisations and the criminals targeting them are confronting one another. According to Gartner, there are likely to be 26 billion networked devices on the IoT by the end of this year, a technological shift which means that the number of targets for cyber-criminals to choose from is increasing exponentially.

SOAR platforms greatly reduce the need for human intervention when tackling the huge range of cyber-security issues, by turning cyber-security into more of a self-operating and self-maintaining process. A platform of this kind will combine data gathering, workflow, analytics, standardisation and case management in order to facilitate highly sophisticated, automated cyber-defence capabilities. Since the system breaks down into Orchestration, Automation and Response, it's probably worth considering each of these aspects of the platform in isolation:

Orchestration

One of the biggest issues facing organisations which have to constantly adapt to new types of threat and emerging attack surfaces is the piecemeal accumulation of disparate cyber-security tools and technologies. As the cyber-security network as a whole grows so the separate parts of it become isolated and the critical information which they gather can end up being siloed within individual tools. One of the most valuable activities of any effective cyber-security teams – generating actionable insights on the basis of data gathered across a range of systems and tools – becomes difficult if not impossible.

The orchestration aspect of SOAR takes the data which is locked in individual silos and centralises it in one location for ease of analysis, which in turn leads to faster threat detection and breach response. Once gathered in this way, the information from across the entire cyber-security eco-structure forms an incredibly useful reference and learning tool

which can be cross referenced both across an organisation and with external sources of information.

In this way SOAR acts not so much as a new piece of technology but as a unifying force which works with existing technology to create a single point of access through which large swathes of data can be viewed.

Automation

One of the most difficult aspects of cyber-security operations, and the one which relates the most to the skills shortage highlighted above, is the repetitive and manual nature of much of the actual day to day work of any cyber-security centre. When alerts are generated, for example, they have to be examined one by one in order to identify genuine threats to act upon and eliminate false positives. Automation can handle a huge administrative task of this nature by examining alerts against pre-set parameters in order to weed out the false positives and isolate the genuine threats for further analysis. By enabling automation of this kind to be applied across the widest possible range of cyber-security activities, SOAR can complete tasks more efficiently and free up cyber-security team members for more strategic, proactive work.

Response

Once data has been orchestrated and automation established as a key part of an organisations cyber-security toolbox, the response to threats itself can be automated, or the weight of data and analysis gathered can be used to make any manual response both timelier and more effective. By orchestrating and integrating all aspects of an organisations cyber-security effort, SOAR makes it easier to establish a clear timeline of any events and discover and seal off any cyber-security loopholes.

SOAR can sometimes be confused with SIEM, but the two are different whilst being complementary. SIEM is software which gathers log and event data generated across the IT infrastructure of an organisation, by systems, security devices and applications. Examples might include firewall logs and antivirus events, and SIEM gathers and sorts this data, classifying it by dividing into types of potentially malicious activity, such as failed logins and malware activity. The software can be set to generate alarms when potentially threatening activity is identified, using parameters established by the cyber-security team. For example, failed login attempts might be flagged as suspicious activity but, below a certain level, could be assumed to be down to human error and a user forgetting their password. If, on the other hand, an account is subjected to hundreds of login attempts in the space of a few minutes this will be picked up and flagged as a high risk incident likely to represent malicious actors launching a brute force attack.

In simple terms, SIEM enables IT teams to take in a strategic view of the cyber-security status of an organisation by collating data from multiple sources in one place. It also means that potential breaches are likely to be spotted quickly and acted upon before the full, damaging impact is felt.

The fact that SIEM and SOAR have many surface similarities may lead organisations already invested in SIEM to question the need to utilise SOAR as well. The truth of the matter is that a combination of the two represents a much enhanced cyber-security offering.

With SIEM alone, the software can raise alerts which then have to be responded to manually by a cyber-security team. Even with some aspects of the response being automated, this can be a time consuming task, and places the cyber-security team in the less than optimal position of spending most of their time responding to events. When SOAR is used in conjunction with SIEM, on the other hand, the response to minor and repeated incidents can be fully automated, something which frees up the cyber-security team to work in a proactive manner, seeking potential threats and security gaps in the hope of finding them before any alert has to be raised. The balance between automated and human actions in response to any incidents can be determined by the boundaries set by each organisation and the SOAR platform they employ, with acts such as opening incident tickets and validating the substance and extent of any threat being fully automated before containment and remediation are either handled by SOARS itself or dealt with by the cyber-security team.