LORCA NEEDS ACCELERATOR: INTEGRATION CHALLENGES FACED BY SECURITY OPERATIONS CENTRES

LORCA

Security operations centres (SOC) are the central hubs for information security teams and are responsible for detecting and responding to cyber security threats. SOCs face three main challenges.

Firstly, a lack of experienced analysts means they take too long to respond to threats.

Secondly, the expansion of the network perimeter is making it harder to maintain visibility.

Lastly, the fusion of digital and physical worlds, thanks to the rise of connected devices, means that SOCs are increasingly integrating their operations with other areas of the business – adding operational complexity.

To overcome these challenges, SOCs will have to transform their approach to people, processes and technology. SOCs of the future will exploit automation to transform their analysts from reactive alert responders to active defenders of the network.

They will pursue advancements in network visibility to contend with the disappearing network perimeter. They will also begin to fuse their operations with operational technology (OT), information technology (IT) and cyber threat intelligence (CTI) teams.

LORCA brought together cyber industry leaders, policymakers and innovators to explore how these shifts will affect SOC professionals and to understand what tools they'll require.

HELD UNDER THE CHATHAM HOUSE RULE, OUR DISCUSSION UNVEILED A RANGE OF INSIGHTS, CHALLENGES AND OPPORTUNITIES...

1 SOCs need automation that integrates with people.

2 To retain staff, SOCs need automation solutions that support skills development in analysts.

3 Current data storage approaches impede threat investigation.

4 To improve threat investigation capabilities, SOCs need to extract more value from network data.

5 Coordinating response activities requires alternatives to standard operating procedures and playbooks.

6 To reduce complexity, SOCs are calling for greater integration across existing tools.

7 Threat intelligence platforms should span the wider business.

8 Culture clash: SOCs need new approaches to training.

SOCS NEED AUTOMATION THAT INTEGRATES WITH PEOPLE

In most SOCs, a tier one analyst's role consists of completing tickets and collecting and analysing log data.

These are mundane, time-consuming tasks that frustrate analysts and increase a SOC's mean time to resolve (the average time from when an incident is opened until it's closed). As one attendee put it, "a SOC analyst's purpose is to be a decision maker but if they're doing admin, they don't have time to make decisions".

SOCs are turning to automation such as next-generation security incident and event management (SIEM) and security orchestration automation and response (SOAR) platforms to reduce resolution times and increase efficiency.

Automating certain tasks frees up analysts' time, improves end-to-end threat reactiveness and creates space for analysts to be trained in more proactive roles like threat hunting.

But attendees expressed concern that "(SOCs) can lose the human eye with automation" and that they would prefer to "automate certain tasks rather than automate certain flows".

Currently, many SIEM and SOAR vendors focus on minimising the human interaction as much as possible but this can lead to automation replacing old inefficiencies with new ones.

> **“A SOC analyst’s purpose is to be a decision maker but if they’re doing admin, they don’t have time to make decisions”**

For example, an organisation may choose to automate its workflows so that suspicious activity on an endpoint, such as a user logging in from an unknown location, automatically blocks the user from accessing the network.

If this access request is from a genuine user, the tool will be responding to false positives and analysts will spend their time overriding automated responses.

Innovators creating automation platforms should aim to augment – not replace – the analyst.

TO RETAIN STAFF SOCS NEED AUTOMATION SOLUTIONS THAT SUPPORT SKILLS DEVELOPMENT IN ANALYSTS

Attendees mentioned that automation "is as much about improving the retention of staff as it is about SOC effectiveness". SOCs are contending with cyber talent shortages and unhappy analysts. Analysts are unhappy in their roles because of their ever-increasing workload and lack of career progression. Automation allows SOCs to retain these skilled analysts by reducing their mundane workload and providing opportunities for development.

But automation isn't a panacea. It creates new maintenance overheads such as automation scripts that need to be kept in sync with changes being made in other interfacing systems. SOCs can use this to increase staff retention by giving analysts new opportunities (like learning advanced scripting).

Automation in stages

Since there are different levels of automation maturity such as ticket enrichment, compliance checking and end-to-end threat management, SOCs will have to go on a journey to using automation to retain talent. And innovators should be mindful of this journey. Solutions that plug into a SOC's automation journey will be better received, as they can be adapted to. current and future goals in terms of skills and automation maturity.

CURRENT DATA STORAGE APPROACHES IMPEDE THREAT INVESTIGATION

Digital transformation initiatives have complicated enterprise architectures and expanded network perimeters. They can also create blind spots on corporate networks.

Maintaining network visibility is now one of the top three issues that SOCs face today. SOCs need to be able to collect and store data in greater volumes – and for much longer – to detect threats, conduct investigations and respond to events.

But while cloud storage provides affordable options for retaining large volumes of data, log ingestion and processing by third party tools can become expensive and act as a disincentive to keeping all data. SOCs are trying to keep costs down by prioritising the data they store. For instance, one attendee mentioned that they retain data that's key for producing threat alerts, but they don't store all the contextual data that's needed for investigation and response.

Some established and emerging SIEM vendors have developed alternative pricing models that help keep costs down, and SOCs are likely to start adopting these solutions. Innovators with solutions that can significantly reduce data storage costs, circumvent the need for storage altogether or help SOCs retain only the most vital data will allow SOCs to improve their investigation and response capabilities.

TO IMPROVE THREAT INVESTIGATION CAPABILITIES SOCS NEED TO EXTRACT MORE VALUE FROM NETWORK DATA

Many SOCs rely on SIEMs for alerts to potential threats, but analysts can struggle to get meaningful value from this data. Extracting value from log data not only requires analysts to understand each platform, but also to understand the context of the data.

Without this context, conducting investigations and responding to threats is more difficult.

Vendors have developed cloud workload protection platforms (CWPP), network detection and response (NDR) or extended detection and response (XDR) tools that help organisations improve network detect and response activities inside – and outside – the cloud.

These tools have advanced analytics and automated response functions that can provide context to the data (which means the analyst spends less time on understanding the context).

But while these tools can boost efficiency, they bypass the real problem: analysts still need to conduct manual investigations.

There's an opportunity for innovators to develop solutions that help analysts extract value from data for manual investigations (such as transformation to common standards, which can reduce complexity).

Vendors offering application programming interface (API) querying platforms may have success, as this method allows analysts to query data at the source rather than waiting for logs to come back.

> **Vendors offering application programming interface (API) querying platforms may have success**

For example, an analyst may be alerted to an anomaly in a software-as-a-solution by the SIEM, but an API query will help the analyst understand what data is in that SAAS solution, how it's being secured or what is happening to it.

COORDINATING RESPONSE ACTIVITIES REQUIRES ALTERNATIVES TO STANDARD OPERATING PROCEDURES AND PLAYBOOKS

An organisation's attack surface can include suppliers, Internet of Things devices, multi-cloud platforms and a remote workforce. This means that to secure the corporate network, SOCs need to have a better understanding of the wider business.

For example, they need to collaborate with physical security teams to understand the security and safety dependencies in OT and work with risk management teams to understand the organisation's exposure to security weaknesses in the supply chain.

Attendees said this need for collaboration means that "fusion is absolutely necessary". Cyber fusion centres (CFCs) are SOCs that have integrated their operations with CTI, cyber incident response (CIR), Internet of Things and risk management teams.

Fusion presents challenges

Fusion improves collaboration and communication, but not every organisation will be mature enough to see the need for it. Adopting this model will depend on the scale and goals of the organisation.

One potential barrier is coordinating response activities across IR, OT and SOC teams. Traditional methods like standard operating procedures and playbooks may not be able to deal with the complexity that collaboration brings.

For instance, two assets on the same site will not necessarily behave the same way. Given that creating highly detailed playbooks for each asset and scenario is unrealistic, codifying responses in this situation is difficult. Escalation of incidents also presents a problem, as assigning responsibilities is difficult when there's overlap between team members' roles.

> **Cybersecurity vendors have an opportunity to create innovative alternatives to SOPs and playbooks by developing solutions or services that are suited to a more complex operating model**

To overcome these barriers to fusion, SOCs need new approaches to governance and response activities. Cybersecurity vendors have an opportunity to create innovative alternatives to SOPs and playbooks by developing solutions or services that are suited to a more complex operating model.

TO REDUCE COMPLEXITY, SOCS ARE CALLING FOR GREATER INTEGRATION ACROSS EXISTING TOOLS

SOCs have too many tools, and these tools don't always work well together. This causes inefficiencies: having multiple vendors with multiple tools results in tasks being duplicated and more noise in the data.

To overcome this problem, SOCs try to streamline their use of tools. In response, well-established vendors are vying to become a one-stop-shop for security platforms by centralising information and giving analysts a single viewpoint to help them make accurate decisions more quickly.

But replacing their existing tools with these one-stop-shop solutions requires more investment and time spent training analysts to use new platforms. SOCs prefer to integrate their existing tools, which they already know work effectively.

This need for integration is likely to increase as SOCs fuse operations with other teams. For example, they may need to integrate OT feeds into their existing SIEMs. Vendors developing new solutions should be mindful of this problem.

Creating tools that don't integrate well with existing platforms means they're less likely to be adopted. Meanwhile, innovators that directly address this problem across the IT, OT and risk management landscape will add real value to SOCs.

THREAT INTELLIGENCE PLATFORMS SHOULD SPAN THE WIDER BUSINESS

Combining security and threat landscapes is a main driver for adopting a fusion centre model. It allows organisations to build a comprehensive threat posture, which ultimately drives the right security behaviours.

For example, deception-based attacks that allow attackers to enter the corporate network and stay below the radar are on the rise in the banking sector.

To better identify these covert attacks, threat intelligence teams need to correlate threats across the business landscape. This can span insider threat, fraud and bribery, for example.

This information helps intelligence teams correctly interpret the cause of anomalies. As one attendee commented, “intelligence is not one team, it’s the whole organisation”.

But there are barriers to creating actionable, business-led threat intelligence.

Combining data from across the business results in huge amounts of information that needs to be collected and analysed before it can be used as intelligence. Sorting through the noise can be difficult and time-consuming.

One attendee raised a concern that organisations are already drowning in too much data, and intelligence fusion would only require more analytics and more time invested by people.

Secondly, incorporating intelligence from suppliers is key to having a comprehensive view of a threat posture. However, most organisations take an assurance-based approach to risk management when onboarding or managing suppliers. This means that real-time threat intelligence is not always shared across the supply chain.

> “organisations are already drowning in too much data, and intelligence fusion would only require more analytics and more time invested by people”

To deal with these challenges, SOCs will need tools that allow for data across the organisation and the supply chain to be collected, normalised, analysed and easily interpreted. These tools need to be accessible not only to SOCs, but to other teams and potentially other organisations.

CULTURE CLASH: SOCS NEED NEW APPROACHES TO TRAINING

Greater collaboration will require teams with different cultures and priorities to work together. For example, OT teams are concerned with safety, reliability and availability threats while cybersecurity teams are concerned with confidentiality, integrity and availability. SOC managers need to break down siloes between different teams and navigate the internal political landscapes of their organisations.

Security culture programmes can reduce insider threat by changing the security behaviour of staff. Attendees mentioned that these programmes could be adapted to address fusion centre challenges. In this scenario, an employee's awareness of threats across the IT/OT landscape could act as a human firewall to minimise the organisation's exposure to threats.

There is also an opportunity to cross-train staff and enable employees to progress laterally by learning skills from other teams. This training would help address the cyber talent shortage by providing progression opportunities for staff while helping teams learn more about each other's roles.

Attendees already have tier one to tier three SOC training in place. But this training is not suited to fusion centres as it isn't sensitive to different working cultures and doesn't allow for the development of additional skills.

CONCLUSION: IT'S TIME TO INTEGRATE

SOCs are ready to undergo a transformation from inefficient, reactive and siloed security operations to automated, proactive and collaborative fusion centres.

This will improve MTTRs and free up analysts to take on more proactive roles, detect threats across the network and defend cyber physical systems more effectively.

This transformation will require SOCs to integrate their people, processes and technology.

There will be barriers along the way. As SOCs align their strategies and cultures with other teams in the wider business, they will have to develop the capabilities of SOC analysts and navigate internal political landscapes.

Fusing operations will require SOCs to redefine their roles and responsibilities and begin to consume intelligence from across the attack surface. They will have to contend with a more complex operating model and will be more dependent on other teams.

This means they must streamline their technology and simplify the security estate.

Innovators have an opportunity to support this transformation. They can offer:

- cultural change and training programmes to improve collaboration
- services that support the redesign of processes and procedures
- automation that helps SOCs use people's time more effectively
- SIEMs and threat intelligence platforms with integration capabilities

SOCs that successfully integrate will reap the rewards. Security will grow in importance within organisations, security postures will improve and SOC analysts will have more job satisfaction – which means they'll be more likely to stay in the role.

CONNECT WITH US

lorca.co.uk
info@lorca.co.uk

Twitter: @LORCACyber
LinkedIn: LORCA Cyber

FIND US

Plexal, The Press Centre Here
East, 14 East Bay Lane
Queen Elizabeth Olympic Park
London, E20 3BS

LORCA BY plexal