Picture credit: AdobeStock

PARANOID POSTURE MANAGEMENT

Martin Jakobsen *explains how automation is enabling better detection and response*

241 days, or almost eight months. According to IBM, that's the typical length of time that data breaches go unnoticed. That's a huge problem. The longer it takes to detect a breach, the greater the likelihood that the impacts could escalate to catastrophic levels.

Modern cybercriminals work to remain under the radar of security teams and tools, dwelling within networks for prolonged periods in order to eventually inflict maximum damage on their victims. Through subtle, gradual movements and actions, they'll begin working to elevate their network privileges, move laterally across systems, plant backdoor and persistence mechanisms and exfiltrate large volumes of sensitive or personal data.

The average cost of a data breach is as much as $4.44-million for a reason. If threat actors are successful in capturing administrator credentials, taking control of key systems and disabling defences, then they can execute potentially devastating ransomware attacks. Those costs aren't just down to ransoms themselves. Recovery from such attacks can also be incredibly time-consuming and costly, potentially requiring a complete rebuild of the network and system infrastructure.

Early detection of potentially malicious activity is therefore vital. It's no longer adequate for companies to simply focus on preventing threats. Indeed, in the current threat landscape, no organisation is ever 100 percent protected, with threat actors actively searching for and exploiting unknown, unprotected vulnerabilities.

Cybercriminals work to remain under the radar of security teams in order to inflict maximum damage

We see this year after year. In 2024, for example, Google Threat Intelligence Group (GTIG) found evidence for 75 zero-day vulnerabilities being exploited by cybercriminals seeking to bypass security measures. Businesses today must look to establish multi-layered defences, moving beyond just prevention and equally prioritising detection, response and recovery.

To build adequate detection and response capabilities as part of a broader cybersecurity strategy, organisations need to establish a security operations centre (SOC) – the centralised function or team responsible for improving the overall cybersecurity posture. From monitoring endpoints, identities and apps to on-prem and cloud networks, they play a key role in surfacing, mitigating and minimising potential risks and breaches.

Given that it currently takes 241 days on average to detect a breach – and the longer a breach takes, the greater the damage can be inflicted – SOCs would be right in working to improve their threat detection efforts. Rather than only addressing high-severity alerts, many security teams need to adopt what can only be described as a more paranoid posture, assuming that breaches rarely announce themselves clearly, and that even low-fidelity or ambiguous signals may matter.

Naturally, a paranoid posture means evaluating more events in greater detail to spot threats earlier. However, this approach can potentially result in highly challenging or unsustainable workloads. In any line of work, role, or indeed walk of life, a bit of pressure isn't necessarily a bad thing. When the balance is right, it can keep us focused and motivated. Yet for many cybersecurity professionals, that balance was lost a long time ago.

Inundated with alerts, many are struggling to keep their heads above water daily. In fact, Microsoft research suggests that data security teams typically only get to 60-70 percent of alerts, leaving potentially 30-40 percent unchecked.

It's a precarious position for organisations to be in. Leaving a single alert completely unchecked might be the difference between becoming a ransomware victim or not. Yet the reality in many SOCs is that the resources simply aren't there and many stones are left unturned.

Security professionals themselves recognise this risk, and that concern is taking a personal toll. One study revealed that 71 percent of SOC analysts said they felt burned out on the job, with nearly 70 percent commenting that teams are understaffed. 64 percent of analysts also say manual work eats up more than half their time, with reporting and monitoring cited as the least favourite aspects of their jobs.

The message is clear: many analysts are stressed and unhappy, creating a scenario in which mistakes are more likely to occur. In a survey of IT security professionals, 83 percent admitted that either they themselves or someone else in their department had made errors due to burnout that had led to a security breach. More than three-quarters (77 percent) also stated that stresses at work directly impacted their ability to safeguard customer data. Evidently, many SOCs are struggling, with current methods having become antiquated and unmanageable. And the current situation is not helped by the sheer volume of false positives. According to the 2025 SANS Detection & Response Survey, almost three-quarters of organisations list false positives as their number one challenge in threat detection.

Not only is this highly inefficient, dramatically heightening workloads, but it also creates significant risks for organisations. Should the volume of overall alerts become unmanageable, then security professionals may miss actual threats while responding to false alarms.

Indeed, research shows that 73 percent of security professionals in SMEs have missed, ignored or failed to act on critical security alerts, owing to a lack of staff or time.

THE AVERAGE COST OF A DATA BREACH IS AS MUCH AS $4.44-MILLION FOR A REASON

This is the reality facing many SOCs today. With threat indicators potentially appearing as simple or small anomalies, a paranoid approach to security is required. Yet under-resourced analysts who are mentally and operationally exhausted, suffering from alert fatigue, are at much greater risk of letting genuine risks slip through growing cracks.

To avoid this becoming the norm, firms must ensure their SOCs are adequately supported with the right tools and resources, so that any existing or emerging security gaps can be bridged and avoidable risks can be addressed in a timely manner. The answer to this often lies in automation – and the statistics speak for themselves.

According to IBM, companies that leverage AI and automation within their security operations typically resolve breaches 80 days faster than those that don't. Additionally, it also found that security AI and automation usage can cut the cost of an average data breach by $1.9-million.

There are several reasons for this. Crucially, automated security operations can lift the burdens on SOCs' shoulders by not only dramatically increasing the throughput of alerts, but also enriching each and every event with relevant threat intelligence.

These are among the key benefits that Security Orchestration, Automation and Response (SOAR) tools can provide to organisations. By integrating with Security Information and Event Management (SIEM) systems and collecting alerts and data from various sources, SOAR can remove many of the manual overheads that typically slow analysts down.

Rather than having to spend valuable time and effort gathering context, security professionals receive cases that are pre-populated with the data they need – be it telemetry, threat intel, relevant correlations or patterns, entity mapping or otherwise. They have a more complete picture from the outset, acting as a springboard for faster and more confident decision-making. It's a method that dramatically cuts down the time from detection

to containment with individual alerts. Yet that alert enrichment also allows analysts to more easily identify broader trends that may otherwise go unnoticed. Events that once would have been dismissed as low-fidelity now feed into a broader, correlated view of activity. When automation aggregates alerts across multiple systems, subtle anomalies can be pieced together as indicators of a larger campaign.

IT'S NO LONGER ADEQUATE FOR COMPANIES TO SIMPLY FOCUS ON PREVENTING THREATS

In this sense, leveraging SOAR has become a no-brainer for analysts. This kind of correlation is fundamental to a paranoid detection posture, where individual low-signal events are rarely viewed in isolation but instead assessed as part of a wider behavioural pattern that may indicate an emerging attack. And the benefits don't end there.

SOAR solutions can also deliver automated guidance to analysts, providing structured investigation and remediation pathways that ensure standardised and logical responses are implemented in response to each and every alert, reducing the potential for variability in response and human error.

Rather than relying on a handful of playbooks, SOCs can use many highly tailored remediation and response sequences simultaneously that cover an expansive range of threats and scenarios. Further still, rules can be implemented in which cases can be closed and containment enacted automatically by SOAR tools under specific conditions when predetermined criteria are met. Today, these capabilities are more useful than ever. It's estimated that there is a global workforce shortage of 4.8-million cybersecurity professionals, with the latest (ISC)2 Cybersecurity Workforce Study also revealing that many teams are worried that their organisations are not adequately protected against cybersecurity threats due to a shortage of key skills. 88 percent note that their organisations have experienced at least one significant cybersecurity consequence in the last year because of a skills shortage and 69 percent have experienced more than one.

Due to resourcing constraints, most SOCs end up tuning out all low-severity alerts in order to prioritise critical and high-severity ones. With severe resourcing constraints, this is the only logical outcome, but it leaves organisations exposed.

Automation helps to bridge this gap, handling repetitive, low-value yet time-consuming tasks so that analysts may focus their attention on addressing genuine and complex threats. By capturing and correlating more data and connecting dots at speed, patterns can be surfaced earlier, increasing the likelihood of spotting the initial point of compromise before an attacker gains momentum.

In practice, paranoid posture management is not about assuming every alert represents an imminent breach. It is about maintaining the visibility, context and analytical depth required to spot early indicators before attackers gain momentum.

IBM's statistics show the immense value that can come from this approach. At a time in which the volume and sophistication of threats continue to tick up, technologies such as these have become imperative. You still need adequate analysts, but with the right combination of solutions, the burden on them can become dramatically reduced ●

Martin Jakobsen is CEO of Cybanetix.

71 percent of SOC analysts say that they feel burned out on the job