TRUE OR FALSE?

David Atkinson *outlines how to combat SOC alert fatigue*

Cyber security tools have become crucial in the arsenal against digital threats, diligently monitoring user behaviour, network traffic, and system operations to spot and mitigate risks before they turn into major incidents. However, the myth of 'the more, the better' persists across organisations, leading to a reliance not on a singular cyber security tool, but a multitude – under the assumption that an increase in tools equates to heightened security. In fact, this sentiment is shared by 78 percent of cyber security professionals, according to the latest research by SenseOn.

Despite CISOs investing in even more security tools, there has already been over 30-million records breached so far in 2024. This contradiction reveals a reality, where instead of strengthening corporate defences, investments have often been channelled into buying point products to resolve isolated issues, leading to over complicated stacks of security tools. That can easily lead to an 'alert fatigue' phenomenon, compromising the effectiveness of threat detection across the organisation and causing burnout.

Solutions focusing on a single point might generate up to thousands of alerts in a week, with just a small percentage proving to be accurate. This deluge of notifications significantly burdens those responsible for checking each alert, leading to hours spent sifting through false positives.

Not only does this cost businesses money, but it also makes SOC teams unhappy. Some might look to change jobs or even explore new careers as a direct result of alert fatigue. SOC analysts also carry concerns over the potential of overlooking critical security incidents amid the barrage of repetitive or redundant alerts. If a malicious alert is mistakenly dismissed as just another false alarm amid daily noise, organisations run the risk of a catastrophic breach.

> WHEN CONFIGURING A SYSTEM TO ALERT LESS OFTEN, THERE'S A RISK OF EXCLUDING REAL THREATS

The reality is that every false positive alert undermines the ability to respond to true positives consistently and quickly. Alert fatigue can also translate to the loss of trust in security operations across the entire organisation, as every time the security team has to interrupt everyone's workflows due to an alert – and it turns out to be a false alarm – employees get annoyed and start to take security events less seriously.

Tuning out false positives isn't easy. After all, an environment that is 'too quiet' can be just as dangerous. When configuring the system to alert less often, there's always a risk the team will exclude real threats from detection. The solution is two-fold. Firstly, SOC teams need to find a way to dynamically filter false positives alerts from the alert queue. Secondly, make it less stressful and faster to investigate real alerts. This is possible by investing in proactive defence, automating threat detection at endpoints and integrating AI into cyber security platforms.

Automating threat detection at endpoints requires a new approach to data collection. To gain context into real threats, analysts need a unified source of data collection that can pull together network, endpoint and user information into a single case. SOC teams need a single solution that collects and correlates all endpoint data with information from their network and cloud environments. Then, by using advanced AI-powered anomaly detection engines, it can discern genuine threats from noise, significantly reducing the incidence of false positives. Leveraging automation for data correlation and aligning with MITRE ATT&CK frameworks can significantly boost SOC productivity.

To maximise the benefits of AI-powered cyber security platforms, it's important for teams to understand the normal patterns of user and device behaviour. Moving beyond simple rule-based alerts to incorporate user and entity behaviour analytics helps SOCs spot anomalies that could signal a threat much faster. This dynamic approach, which adjusts to the evolving environment of an organisation, improves the precision of threat detection and reduces the occurrence of false alarms.

In any IT environment with more than a few dozen users and different detection methods, there's so much data flowing into SOC from various siloed sources that the alert fatigue phenomenon is simply unavoidable. With threat actors becoming smarter and more technologically capable, the amount of noise cyber security teams have to sift through will only grow louder – and so will the problem of alert fatigue. Before SOC teams burn out, and an ignored alarm escalates into a catastrophic data breach, organisations need to invest in AI-powered cyber security to streamline and enhance their detection capabilities. It's simply not worth wondering if an alarm is a real threat or a false positive. The stakes are too high and teams need to be certain, every time ●

> **The amount of noise cyber security teams have to sift through will only grow louder – as will the problem of alert fatigue**

Dave Atkinson is Founder and CEO of SenseOn. He has over 15 years' experience working within the UK's specialist military units and government environments, where he was the first cyber operative.

Picture credit: AdobeStock