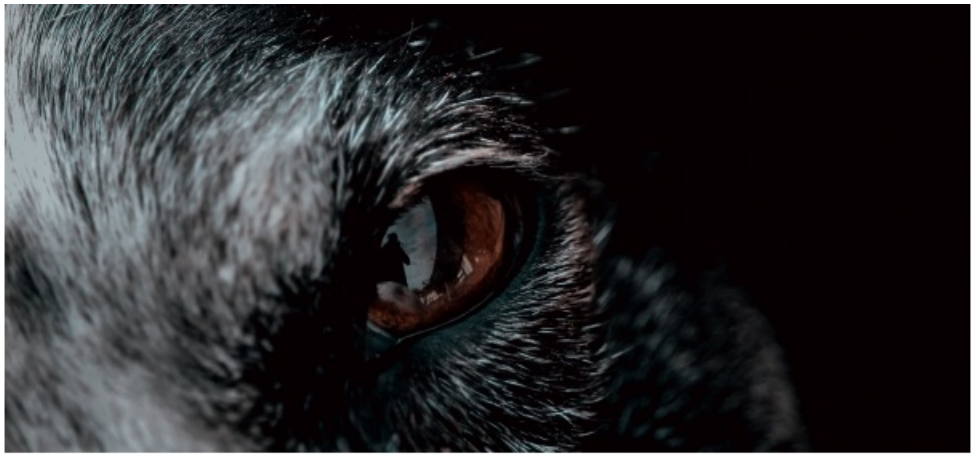
Article

Jul 2021

The server that cried wolf

Preventing alert fatigue by eliminating misalignment.



I call it alert fatigue. Having proven an alert is innocuous multiple times leads you to believe that it's always innocuous. And in some cases that may be true, however when dealing with security events, as we know, it only takes one missed or mishandled event for a breach to occur. You'd really be surprised just how much isn't being captured or how many alerts are skimmed over and closed. While we would like to believe that the people handling the events and incidents coming from our infrastructure have a deep understanding of the security ramifications, for a few reasons, it simply isn't realistic.

This sounds pretty awful, negligent even, but the fact of the matter is that this is commonplace, and I would argue given the circumstances, rightfully so. Any member of the public would find it absurd to discover car mechanics, their staff and their apprentices alongside their normal workload were now appointed to also handle car crash investigations, monitor traffic safety cameras and design safer roads.

Sure, maintaining cars, engines and in some cases safety features, they would have some great insights, but without the bandwidth, proper training, understandings of methodology, best practice, frameworks and years of experience, you couldn't expect a manageable outcome. And while bizarre it may be, I believe many organisations and MSPs do exactly this with their approach to network security.

> **"The fact of the matter is security related events and alerts should be handled by the appropriately trained staff from the very start"**

While taking the typical steps forward such as implementing better security, MFA, audit logging, reviewing privileged changes in your cloud infrastructure weekly, setting up a SIEM, installing EDR, meeting compliances etc will add visibility and help secure your organisation against the simpler attacks, each implementation generates alerts, events and logs.

This is where the situation becomes tricky. In typical tiered support, that influx of events and alerts are filtered through the least experienced team members, typically generalized support technicians to allow the more experienced members bandwidth to deal with the larger issues. Even when these alerts land in the queue of more technical team members, they aren't typically trained in security, it's actually not their job to understand kill chains, exploits, investigation techniques and threat hunting. Combine this with a high volume of already extremely technical work, and it becomes clear why some things may be misdiagnosed repeatedly and alert fatigue sets in.

Organisations are starting to realise this. Not only would it be unfair to expect someone with years of experience building, maintaining and troubleshooting infrastructure, software and endpoints to be able to monitor your security or handle digital forensics and incident response but the overall organisational security would suffer as a result. As mentioned in my previous article in this series, The Telescoping Nature of Cyber Security, the growth of cyber security is exponential, and the misalignment of roles and responsibilities are now starting to become a blind spot some organisations don't realise they have.

Which begs the question, what short of restructuring can address this? Is it a matter of more training for junior members, or immediate escalation to more technical staff? I would argue neither. The fact of the matter is security related events and alerts should be handled by the appropriately trained staff from the very start, and based on AustCyber's Cyber Security Sector Competitiveness Plan, the industry is starting to agree:

https://austcyber.com/resources/industryroadmap

As organisations and Managed Service Providers alike have started to recognise this blind spot, so too have we. Starting with a small team of Cyber Security consultants, we have now grown to operate a global 24-hour in-house Security Operations Centre, provide Virtual Managed Security services, assistance with compliance and auditing, technical mergers and acquisitions consulting, project services and assistance with major incident remediation.

If you'd like to learn more about our offering or have a chat about what we could do to help secure your organisation, please don't hesitate to reach out to andrey.derevyanko@waterstons.com or info@waterstons.com.au