Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
The operation-centric strategy

Yossi Naar, Cybereason

Often, IT teams are obliged to defend their organisations from within silos as their arsenal is largely composed of tools designed to protect specific assets. In other words, one solution may be deployed to ensure that cloud workloads are locked down, while another may focus primarily on preventing attacks on endpoints.

Predictably, this shapes the defending organisation’s strategy, forcing it to view attacks as individual, isolated events. In a threat environment where cyber criminals leverage a multitude of techniques and target numerous users as well as devices simultaneously, such a view will inevitably leave teams blindsided.

Consider the recent SolarWinds supply chain attacks (http://bit.ly/3uHq06U). For months, threat actors were active on systems across various organisations, leaving traces of their presence as they conducted malicious activity. Yet this evidence was swiftly buried under an interminable stream of uncorrelated alerts. Without the context essential to piece together the individual attacks, the scale of the global operation went undetected.

Regrettably, the vast majority of traditional security tools available are alert-centric. They endlessly spew notifications, warning of every instance of suspicious activity within the system, without truly offering valuable insight. Rather, the burden is placed on the defenders to assess just how each event is related to another.

It is simply inefficient by design. Each event demands manual intervention, heightening the risk of human error and significantly limiting the capacity for an organisation to scale securely. Addressing individual attacks might well set back an adversary, but the fix would only be temporary.

Securing complex network infrastructures with an alert-centric, siloed approach provides cyber criminals with generous leeway to burrow themselves deep into the network – any attempt to detect, track or eliminate an attack becomes near impossible. By treating the symptom and not the cause, companies fall into an unrelenting spiral. Every year, more money is spent on security, and still they remain one step behind cyber criminals.

For a defender to effectively remediate an attack, they must be quick to spot the threat and adeptly counter it. More importantly, they need to ensure that the organisation is prepared to fend off the next day’s onslaught.

Security teams need the ability to react and eradicate a threat in minutes, as opposed to days or weeks. They need to think, adapt and act faster than an attacker can adjust their tactics. An operation-centric approach can facilitate this as it enables defenders to envisage the attack from its foundations right up to its outstretched grip on affected endpoints. Through multi-stage visualisations, defenders gain real-time insight into the minutiae of an attack across all devices and users. In turn, they can respond promptly and appropriately before an attack develops into a breach.

Moreover, an operation-centric approach authorises the use of automation in a number of response options to further speed up the remediation time. In doing so, security teams are empowered to shift critical resources from alert response to strategic, time-saving security initiatives.

Finally, the intelligence offered needs to actionable for it to be useful. Unfortunately, traditional products lack the capacity to process and store valuable data, nor can they make this data accessible at a moment’s notice for investigation. By filtering out potential key indicators of an attack, organisations leave themselves vulnerable.

Adopting an operation-centric approach is critical to reducing time spent on detection and remediation so that time and resources can be redirected to more effective security initiatives. With this approach, organisations can turn the tables against their adversaries and become future-proof.