Access Approved. Access Denied. Access Automated.

Cybersecurity is more challenging than ever, and it's not just because the threats are more challenging. The problem lies with enterprise security processes. It's well reported that security teams are understaffed. Cybersecurity professionals are hard to find and expensive to hire. Yet the threats to corporate networks proliferate.

When networks were simpler with well-defined perimeters, tools like firewalls and IPS systems were reasonably effective. Today's environments, however, are larger, complex, hybrid concoctions that are populated by mobile and remote devices. They present more attack surfaces than ever before. Complexity is the bane of security.[1]

With seasoned security staff difficult to find, many companies try to boost their defenses by investing in more security tools. Indeed, many vendors have jumped on the security bandwagon. However, these tools often have narrow differentiation from one another, and each generates more data, if not alerts, that must be monitored.

To help, security vendors developed Security Information and Event Management (SIEM) platforms. These systems aggregate data from firewalls, switches, IPS solutions, and other sources to identify deviations from patterns and baselines. If an issue is detected, they might order other security systems to prohibit a questionable activity or notify analysts so they can take action.

Problem solved? Here are some sobering facts.

According to one study, 27 percent of IT professionals receive over one million alerts daily and 55 percent see more than 10,000.[2] SIEMs eliminate most from consideration, but even SOCs (security operations centers) struggle to determine which remaining incidents are real threats and which are just noise, or false positives.

These are breathtaking numbers. For each potentially menacing alert, a security analyst must do a deep dive by cross-referencing data from other tools, consulting with established policies, reviewing information from threat intelligence services, and deciding upon appropriate action. An army of security professionals couldn't process 10,000 alerts daily, if not a million, let alone an understaffed, overworked security team.

---

[1] https://blogs.cisco.com/security/using-a-playbook-model-to-organize-your-information-security-monitoring-strategy

[2] www.imperva.com/blog/27-percent-of-it-professionals-receive-more-than-1-million-security-alerts-daily/

It's no surprise that security analysts suffer from alert fatigue.[3] Examining just a few dozen alerts is very laborious. By far and away, most are false positives, but analysts must be vigilant for the one needle in the haystack, even at the end of a grueling eight-hour shift. The risk is overlooking an intrusion that will have dire consequences for the organization.

More help arrived with a new generation of security solutions—security orchestration, automation, and response (SOAR) systems. These automate some of the routine tasks of security teams. SOAR platforms reduce the load on security professionals by eliminating processes that require human intervention, enabling analysts to concentrate on other work. They also can speed incident response. They might, for example, instruct firewalls to block traffic from a source launching an attack well before analysts are aware of the issue.

Yet the problem remains. Even with SOAR, there are too many alerts overwhelming analysts. Is there a solution whereby security staff can identify only true threats and intervene as necessary? The answer starts with compliance and risk management workflows.

Compliance Proactive, Security Reactive

Compliance and risk management are, in effect, about erecting walls, which means they're inherently proactive. In context of compliance mandates, network access is configured around the priorities in the environment. What should have access to a resource and what shouldn't? How risky is that open port? How removed from the Internet should a particular asset be? Based on the answers, we take measures like segmenting our networks and assigning permissions with access control lists. We manually makes changes as needed to keep compliance current and to manage risk.

Dynamic networks demand scores of changes daily, which is why many enterprises go further by automating change management. Based on referenceable policies, automated change management implements requested changes, such as adding or denying access, without the need for staff. These systems efficiently ensure compliance is up-to-date, more so than when policies reside in static Word or Excel files and modifications require manual processing. Automating changes strengthens risk management, economizes on labor, and provides documentation for the inevitable audit.

Security teams, on the other hand, respond when the walls are breached, making security defensive and reactive. When security suspects an incident is occurring, it creates a ticket for networking to remove access and firewall rules based on available intelligence. Networking either processes the ticket with other emergency changes or just puts it in the standard queue. Neither guarantees a prompt response.

---

[3] https://www.alienvault.com/blogs/security-essentials/alert-fatigue-and-tuning-for-security-analysts

Here's the rub. If we can automate change management to reduce vulnerabilities, can we automate security responses when a breach occurs? Automated impact analyses may inform us that rules need to be changed, but the changes still need to be done by staff. Can changes be automated?

Automate Cybersecurity

Automated incident response is possible when change management is integrated with security solutions like SIEMs and SOAR platforms. Tickets associated with security incidents would pass through a different workflow that conducts automated impact analysis. If the impact to the network is negligible, the close out would be automated. Otherwise, tickets go to networking for emergency network access removal.

It makes sense to leverage automated access changes for security and incident response. You would extend the same facets of automation you already use for compliance and risk management. We at Tufin see customers that are not only removing rules for cleanup or optimization, but also for consolidation into a security incident response process to manage change requests. They leverage existing analysis solutions (and investments) by integrating all the information these tools create or aggregate from threat intelligence services, and take action based on the playbook within their SOAR platforms. Their security teams are more likely to respond to actual threats and attacks, without the need to sift through countless alerts and false positives.

When enterprises automate cybersecurity, they respond more quickly to threats, reduce the burden on security staff, and enable effective and consistent action across both security and networking teams to mitigate attacks. You might already have tools within your environment to smartly manage access changes; why not leverage them for security processes?
