Challenges in IT Security Incident Management

An International Data Group (IDG) Research survey conducted in the early days of the pandemic shows that IT teams are increasingly burdened with a heightening volume of IT incidents and outages, which results in customer attrition and costly service interruptions. This is in addition to managing complex and ever-changing IT systems with many different technologies. As their organizations strive to capture the digital-led market, IT Ops, NOC, DevOps, and SRE teams confront several problems, according to the report.

To address needs and dangers, businesses frequently adopt new security products and services. How to integrate these multiple offerings—many of which are provided by separate vendors—into the existing infrastructure to enable a unified security approach is a significant consideration. Here are some of the difficulties that businesses may confront in IT security incident management:
Too many security tools: Many organizations make the mistake of installing too many security products and services, which leads to a typical security integration issue. **"One of the largest issues facing cybersecurity operations today is the sheer variety of heterogeneous security solutions. Each new security solution must be integrated with dozens of others, producing an ever-increasing number of unique integrations that must be handled between each—growing at an impossible scale,"** says Anupam Joshi, Senior Manager, Cyber security services, Skillmine Technology Consulting.

Lack of interoperability: Many security technologies today use proprietary interfaces and data communication languages. While many companies now provide open application programming interfaces (APIs), these APIs aren't always constructed on the same standards. Hence, specific, proprietary code is still required to combine product A with product B.
Multiple security communities are working to address the issue of interoperability, with an emphasis on building more common data models, open standards, and open-source tooling that can be utilized across vendors and toolsets. By depending on standard APIs and data formats, security teams will be able to swap out one tool more simply for another, making it easier to introduce new tools and improve security.

Limited visibility: New security solutions focus on developing behavioral models to better understand network traffic and behavior, and then use that data to detect aberrant activities. These models must inspect and analyze all the network traffic to be effective. Models will not be accurate or effective if the tools only view a portion. This is mostly a concern with network devices and appliances, but if a new network device is placed in front of current technology, it may block traffic and reduce visibility. The solution is to deploy network tools per virtual local area network or network segment, such that a single tool has complete visibility over the network segment it is guarding.

Rise in false alarms: New security technologies are also more focused on claiming to be able to identify assaults rather than offering accurate and dependable information. Therefore, as you add additional tools, the number of warnings rises, and the overall number of false positives rises. The solution is to use a security incident and event management system that correlates data from numerous sources and only alerts on activity that consistently alarms across several tools.

Shortage of skills: For practically every facet of security, demand simply outnumbers supply. This includes the ability to incorporate a variety of security tools and services. A fundamental difficulty today is a shortage of educated personnel who can manage the integration of security solutions and assess what measures need to be performed. Having more tools necessitates more time and knowledge, and this frequently results in a considerable resource drain.

“With a massive increase in the scope of cybersecurity post the pandemic, it is important for businesses to adopt a multi-layered approach towards security. In fact, a successful IT security incident management rests on the pillars of patience, proactiveness, and ability to formulate solutions,’ Anupam Joshi adds.