THE NEED FOR BETTER INCIDENT RESPONSE TOOLS

No matter how much security organizations put in place, breaches are inevitable. Organizations from all sectors today are under constant pressure to identify successful attacks and respond quickly in order to minimize damages from breaches. While the ability to alert on a suspicious activity exists, the real challenge is to understand what the alert stands for and how to best respond. Struggling with lack of context, complex tools, and even the skills to properly investigate are at the heart of the problem. According to a recent report by Mandiant, the average time attackers were present on a victim's network before being remediated is 205 days. This lag time between breach and response is critical. Security teams need to be able to validate the alert, figure out the attack surface and perform root-cause analysis in order to mitigate the incident before it becomes a full-blown breach. IT departments are adjusting to this changing threat landscape by rebalancing their resources from fortifying security controls to rapid detection and response initiatives.

LOGS DON'T SOLVE VISIBILITY DEFICIENCY

Organizations cannot investigate what is happening in their network if they cannot see it. The traditional approach was derived from a handful of data feeds – i.e. forwarding log events from various security tools, such as FW and IPS, into a security information and event management (SIEM) solution. Unfortunately these data sources are no longer adequate on their own. The security team can use SIEM to see high-level statistics based on log and alert data (e.g. metadata), but they cannot dive into the details that are crucial for the investigation, such as files and the actual content within network conversations. Solutions limited only to metadata are not investigations tools.

TODAY'S CHALLENGES WITH EXISTING FORENSICS SOLUTIONS

When trying to extend visibility beyond metadata in order to support effective investigations, organizations adopt network forensics solutions that are designed to retain and analyze full packet capture (PCAP) data. However, in most real-life scenarios, today's existing solutions have proven to have unacceptable ROI:

1. Complexity of use: These tools require advanced skillsets only a few team members possess. The current recognized shortage of skills in cybersecurity creates a major bottleneck in facilitating forensics investigations. Organizations must support users who lack deep expertise, so that security professionals at all levels can handle more complex investigations, escalate fewer tickets and resolve incidents faster.
2. Storage requirements: Recording traffic at an enterprise-scale is restricted by costly storage investments to only several days. A quick calculation shows that a 10GbE link will require about 110TB of storage for recording a single day of traffic. While most security breaches take months to discover, the value of traditional solutions that entail full packet capture is clearly diminished

This reality creates a difficult situation. While conventional approaches do not get the job done, the cost and complexity involved in the adoption of forensics solutions are making them infeasible in most environments. Organizations are left without the ability to investigate the constant alerts triggered by their own security measures. To overcome today's forensics challenges, security teams must arm themselves with better tools to get access to the detailed information they need, but also save effort and time in the process.