SIEMs, IDS/IPS, and Antivirus Aren’t Enough: You need Human Threat Hunters

Jordan C. Lanning

5/05/2025

Introduction

The security tools vary from organization to organization. Most organizations will have at least antivirus software installed on end devices and SPF/DKIM for email authentication. Other organizations that require higher level of security attention will see Security Information and Event Management (SIEMs) that centralize alerts and logs on easy-to-read dashboards. Another technology is Intrusion Detection / Prevention Systems (IDS/IPS) which monitor network traffic or activity then generate alerts or will prevent it automatically. You can have Host-Based IDS/IPS (HIDS/HIPS) that detects unauthorized changes on the host machine. Organizations should seek to have several security systems and solutions to ensure a layered defense, but as you will see, there are always gaps in technology.

SIEMs

SIEMs like Splunk or Sentinel do a great job at actively monitoring activity in real time. These platforms produce security alerts based on rules and behavior. Security professionals can tune alert volume and sensitivity to their organization’s practices. A government contractor agency supporting military operations might need to have high sensitivity and frequent alerts for all activities. Depending on the tuning, you may produce false positives (no threat but alerted), true positives (threat), false negatives (undetected threat), and true negatives (no threat and no alert). In the contractor example, the high alert volume could produce false positives but this might be acceptable in their environment. SIEMs are primarily detective tools but can be preventative when integrated with Security Orchestration Automation and Response (SOAR) tools.

IDS/IPS

Intrusion Detection / Prevention Systems (IDS/IPS), whether host-based or network-based, will operate based on known signatures or anomalous behavior. Network-based IDS/IPS will scan network traffic based on rules and act accordingly. Host-based will do the same for host systems, but specifically with the human end user, files, or logs. Earlier we discussed alert tuning, but this applies more to IDS/IPS. SIEMs are a visual, graphical tool that can also provide playbooks based on the logs while the IDS/IPS forward alerts and logs into the SIEM for correlation and analysis. Meaning, IDS/IPS can generate false alerts at times. Specifically, if there is encrypted network traffic, IDS/IPS solutions will not be able to analyze it.

Antivirus

Antivirus (AV) software blocks viruses prior to infection on a computer. Software should be updated frequently to keep up with everchanging tactics from adversaries. AV focuses on malicious code, which means software that is designed to damage and cause unwanted actions on a computer. AV software will check potentially malicious programs according to a database of known malicious signatures, in addition to behavior analysis. However, AV tools may miss zero-days or unknown signatures – here lies another problem.

Threat Hunting

Despite these tools, attackers continue to evolve and find holes within our layered defenses. So, what is threat hunting? It is the practice through automated and human interaction with systems to identify threats that could adversely impact organizational assets prior to an event. Proactive threat hunting will include a variety of steps such as

(1) establish a hypothesis

(2) profile threat actors and avenues

(3) perform threat hunting tactics

(4) reduce the attack surface area

(5) bundle critical assets into groups or protection zones

(6) root cause analysis on security gaps

(7) update organizational intelligence feed

(8) improve detection capabilities

While AI has advanced tremendously over the years, human cyber professionals remain the foundation to organizational security. Threat hunting applies to network activities, systems, applications, and end devices. Sophos indicates that across 14 countries roughly 23% of organizations experience a cyber-attack. Your organization may have been lucky enough to never have experienced one thus far – we hope you don't. This doesn't mean one will never occur. The financial impact can be catastrophic depending on the type of attack and impact area. A small business could expect to spend hundreds of thousands to millions of dollars from financial loss, system replacements, legal fees and fines. Just because your company has not been affected doesn’t mean you are safe. You always need to be proactive to prevent unforeseen attacks.

Final Thoughts

So why would you need human threat hunters? Well, no matter how we tune our security equipment, they are never perfect. We need human threat hunters to develop hypotheses and test them within their organization. Automation tools can assist even in threat hunting, like the alerting or prevention tools, but they are not flawless – i.e. testing may stop or be interrupted prematurely due to logical errors.

What can you do? Well according to the FBI’s 2023 Internet Crime Report almost 300,000 incidents resulted from email compromise, phishing or spoofing. One simple threat hunting activity any organization can do is task internal cyber professionals with setting up phishing campaigns and developing user awareness training for employees. Use sandboxes and test antivirus efficacy in a controlled virtual environment using known safe test files. Want to take it a step further? Coordinate with the Cybersecurity and Infrastructure Security Agency (CISA) to conduct a free penetration test to provide a better overview of your security posture or hire a penetration testing team. Don’t rely on current security systems without checking them!