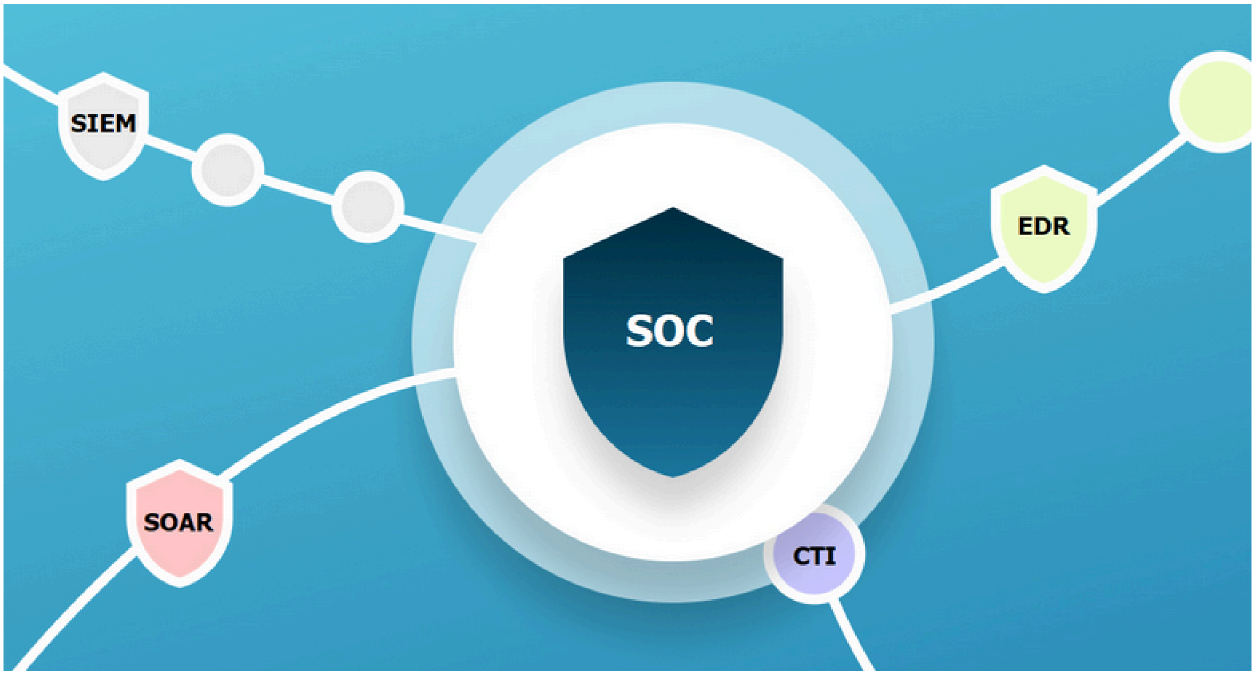
Threat Intelligence and SOC Integration

By: Ryan Stewart

Due to its inherent characteristics, threat intelligence seamlessly integrates into various Security Operations Center (SOC) products. This integration enhances the effectiveness of threat intelligence, especially when applied to Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), Endpoint Detection and Response (EDR), and Firewalls—all essential components within the SOC framework. Each of these products possesses distinct capabilities, and their combined outputs yield the most impactful results.



For optimal results, it is **crucial** to **merge** the **threat intelligence flow** with the security products under the SOC framework, providing unparalleled visibility both **inside** and **outside** the organization.

In the context of **SIEM**, integrating the logs collected with the threat intelligence feed minimizes false information and establishes elimination criteria, enhancing the overall quality of outputs. This refined data enables SOAR products to generate higher-quality outputs by reducing the occurrence of false information in the SIEM.

Integrating threat intelligence with **EDR** proves advantageous in detecting risks on **end users**' devices. By incorporating threat intelligence into EDR, it enables more precise and detailed detection on systems, particularly by leveraging users' **web traffic feeds**.

Firewalls, essential for monitoring and managing external traffic, offer another compelling example of SOC and Threat Intelligence integration. By feeding threat intelligence into firewall products, these systems can respond swiftly to potential threats. Creating specific rules for identified malicious IP addresses allows the firewall to p**romptly block any traffic** from those sources, enabling the detection and elimination of risks before triggering alerts within the broader SOC security tools. This proactive approach enhances the overall security posture of the organization.