Cyber security long term internship

Project Title :*Threat intelligence integration and optimization*

Team ID : LTVIP2024TMID1828

Team size : 4

Team leader : Talabakthula Maha Lakshmi

Team member :Arava Anusha

Register No: 2123010

My Task

Introduction to Threat intelligence integration

security operations center (SOC) operations amplifies your ability to detect, analyze, and respond to threats in real-time. By continuously monitoring and analyzing threat intel feeds, your SOC teams can detect and thwart attacks more effectively. This intelligence enables your analysts to correlate incoming data with known threat indicators, identify patterns, and uncover hidden connections, allowing for a more comprehensive understanding of the threat landscape.For example, if a company has outbound traffic to an IP address known to be used for malicious activity, cyber threat intelligence can connect that IP address to a threat actor, and provide information about malware distributed by that attacker.

Integrating threat intelligence into your security operations center (SOC) operations amplifies your ability to detect, analyze, and respond to threats in real-time. By continuously monitoring and analyzing threat intel feeds, your SOC teams can detect and thwart attacks more effectively.

4 Types of Threat Intelligence

Tactical Threat Intelligence. This type of threat intelligence deals with the specific methods and tools used by cybercriminals. ...

- ***Operational Threat Intelligence. ...***
- ***Strategic Threat Intelligence. ...***
- ***Technical Threat Intelligence.***

CROWDSTRIKE

INTELLIGENCE AREAS

TACTICAL

Focused on performing malware analysis & enrichment, as well as ingesting atomic, static, and behavioral threat indicators into defensive cybersecurity systems.

STAKEHOLDERS:
- SOC Analyst
- SIEM
- Firewall
- Endpoints
- IDS/IPS

"Mechanic"

OPERATIONAL

Focused on understanding adversarial capabilities, infrastructure, & TTPs, and then leveraging that understanding to conduct more targeted and prioritized cybersecurity operations.

STAKEHOLDERS:
- Threat Hunter
- SOC Analyst
- Vulnerability Mgmt.
- Incident Response
- Insider Threat

"Race Car Driver"

STRATEGIC

Focused on understanding high level trends and adversarial motives, and then leveraging that understanding to engage in strategic security and business decision-making.

STAKEHOLDERS:
- CISO
- CIO
- CTO
- Executive Board
- Strategic Intel

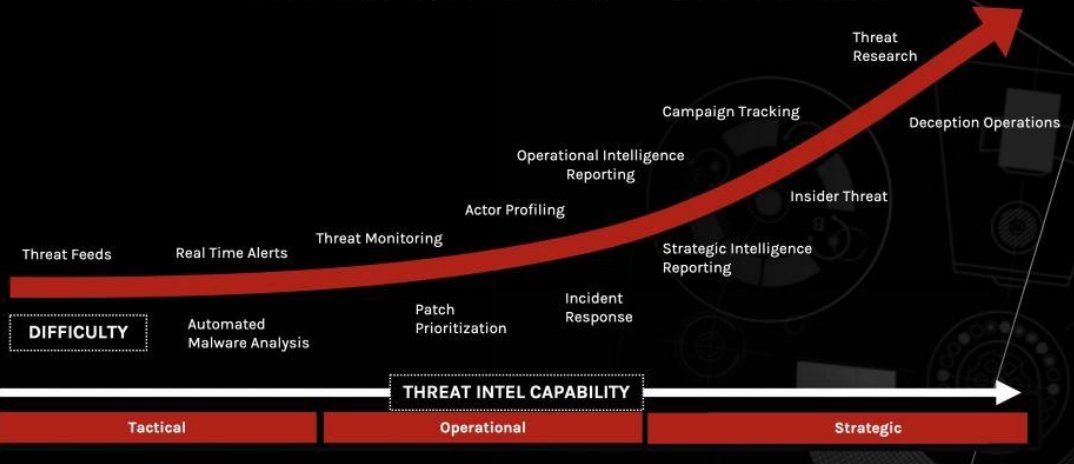
"The Owner"

CROW DSTRIKE

CROWDSTRIKE

THREAT INTELLIGENCE

WHAT USE CASES ARE RELEVANT TO YOU?



Types of threats and threat intelligence

Cyber security threats and threat intelligence can be categorized based on business requirements, intelligence sources, and intended audience. In this regard, there are three types of cyber security threats and threat intelligence.

Strategic threat intelligence

These are broad or long-term trends or issues. Review of strategic threats is often the preserve of high level, non-technical audiences such as C-suite executives. Strategic threat intelligence provides a bird's eye view of the capabilities and intents of threats, which allows for informed decision-making and prompt warnings.

Sources of strategic threat intelligence include the news media, subject matter experts, nongovernmental organization policy documents, security white papers, and research reports.

Tactical threat intelligence

Tactical threat intelligence gives structure to the procedures, techniques, and tactics of threat actors by tackling the indicators of compromise through day-to-day intelligence events and operations. It's intelligence that's meant for a more technical audience, such as security professionals, system architects, and network administrators.

Operational:

Operational threat intelligence focuses on the tools (malware, infrastructure, etc.) and techniques that cyber attackers use to achieve their goals. This type of understanding helps analysts and threat hunters identify and understand attack campaigns.

THE END