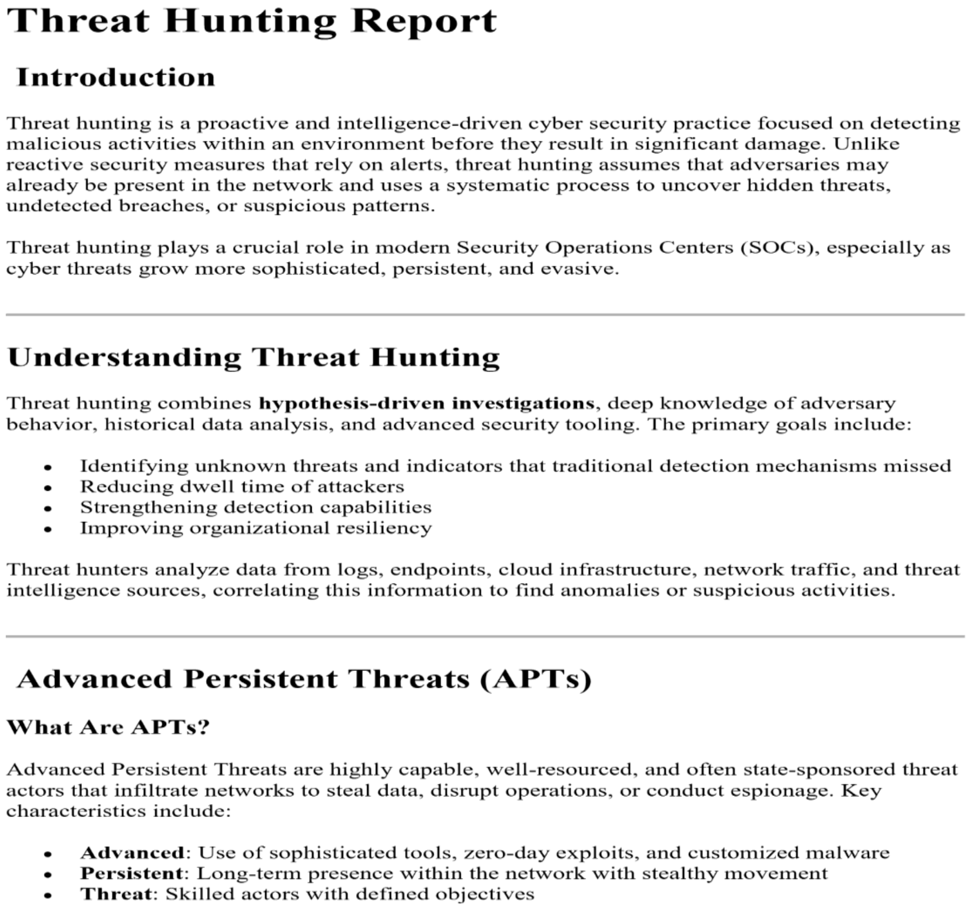

Threat Hunting Report

Introduction

Threat hunting is a proactive and intelligence-driven cyber security practice focused on detecting malicious activities within an environment before they result in significant damage. Unlike reactive security measures that rely on alerts, threat hunting assumes that adversaries may already be present in the network and uses a systematic process to uncover hidden threats, undetected breaches, or suspicious patterns.

Threat hunting plays a crucial role in modern Security Operations Centers (SOCs), especially as cyber threats grow more sophisticated, persistent, and evasive.

Understanding Threat Hunting

Threat hunting combines **hypothesis-driven investigations**, deep knowledge of adversary behavior, historical data analysis, and advanced security tooling. The primary goals include:

- Identifying unknown threats and indicators that traditional detection mechanisms missed
- Reducing dwell time of attackers
- Strengthening detection capabilities
- Improving organizational resiliency

Threat hunters analyze data from logs, endpoints, cloud infrastructure, network traffic, and threat intelligence sources, correlating this information to find anomalies or suspicious activities.

Advanced Persistent Threats (APTs)

What Are APTs?

Advanced Persistent Threats are highly capable, well-resourced, and often state-sponsored threat actors that infiltrate networks to steal data, disrupt operations, or conduct espionage. Key characteristics include:

- **Advanced**: Use of sophisticated tools, zero-day exploits, and customized malware
- **Persistent**: Long-term presence within the network with stealthy movement
- **Threat**: Skilled actors with defined objectives

SOC Radar

It offers comprehensive SOC teams to identify & analyze threats in real time. It reduces time spent on minimal intelligence & it offers comprehensive visibility for proactive hunting.

MITRE ATTA&CK Navigation

This ATT&CK Navigation was used as an interactive web tool used to visualize MITRE ATTA&CK techniques which made it easier to understand heat maps. It also supports strategic security decision making. This navigation was used to examine 3 APT from the Groups. They are Moonstone Sleet, Hexane and Blue Mockingbird.