CybrHawk
Transforming Cybersecurity

# THREAT HUNTING
## FROM CYBRHAWK

The pursuit of cyber threats is an important cyber defense operation. In comparison to conventional threat management initiatives, such as firewalls, intrusion detection systems (IDS), malware sandboxes (computer security) and SIEM systems, this is “the method of proactively and iteratively scanning across networks to identify and isolate advanced threats which bypass existing security solutions.”

SECURITY **ASSESSMENT**

**Threat Detect** & Response

**CLOUD** SECURITY

Threat hunting has historically been a manual process in which a security analyst sifts theories regarding potential threats such as, but not limited to, Lateral Movement by Threat Actors across various data information using their own experience and expertise with the network.

www.cybrhawk.com

Nevertheless, risk hunting can be partially automated, or machine-assisted, to be even more effective and efficient. In this scenario, the analyst uses machine learning and user and entity behavior analytics (UEBA) using tools to warn the analyst about potential risks. These potential risks are then investigated by the analyst, tracking suspicious behavior within the network.

Thus hunting is an iterative process, meaning that it must be continuously carried out in a loop, beginning with a hypothesis. The hypothesis can focus efforts on known exploits, potential bad actors or assets and data of value. Using security data, industry reports and other intelligence, the hypothesis is formed, and the hunt team sets out to prove or disprove its validity.

Cyber vulnerability hunts often use automated as well as manual tools and techniques to identify a breach before it is detected. Three kinds of theories exist:

- Analytics-Driven: 'Machine-learning and UEBA, used to develop aggregated risk scores that can also serve as hunting hypotheses Situational-Awareness Driven. '
- Crown Jewel analysis, corporate risk assessment, corporate-level intelligence-driven trends.
- Threat intelligence reports, threat intelligence feeds, malware analysis, vulnerability scans.

Through digging through vast amounts of network data, the analyst examines their theory. The findings are then processed so that they can be used as a basis for potential hypotheses to enhance the automated portion of the detection system.

The concept of Detection Maturity Level (DML) expresses the probability of detecting risk indicators at various semantic levels. High semantic indicators like goal and strategy or tactics, techniques and procedure (TTP) are more valuable than low semantic indicators like network artifacts and atomic indicators like IP addresses. Generally, SIEM methods only provide measurements at relatively low levels of semantics. Therefore, SIEM tools need to be built to provide indicators of threats at higher linguistic levels.

**Indicators:**

Compromise Indicator-An Indicator of Compromise (IOC) informs you there has been an intervention and you are in a proactive state. Through looking inward at your own data from transaction logs and/or SIEM information, this sort of IOC might be possible.

Concern Indicator-Using Open Source Intelligence (OSINT) information can be collected from publicly available sources for use in cyber-attack detection and risk hunting.