THREAT HUNTER

Mossé Security's Threat Hunter technology allows organisations to detect active threat actors who have bypassed network security defenses. With Threat Hunter, a single senior security analyst can review hundreds of machines per day for previously unseen indicators of compromise.

OVERVIEW

Threat Hunter is a force multiplier for organisations looking to proactively hunt for active threat actors on their networks.

The technology allows a senior security analyst to collect and identify anomalies across thousands of machines within minutes.

Ranging from high-fidelity signatures to data visualisation and statistiscal analysis identification techniques, we offer a variety of innovative threat hunting techniques.

Several licensing options available – call us today.

FEATURES

- **Big Data Analytics:** We can hunt for indications of compromise across thousands of machines within minutes. With Threat Hunter, a single security analyst can typically review over two hundred machines per day.
- **Data Visualization:** Using data visualization techniques, we scan for compromised IT systems and current threat actors. Histograms and network graphs help visualize potential anomalies.
- **Statistical Analysis:** Mathematics and statistics enable us to detect abnormal behaviors on the network that traditional signature-based detection techniques are unable to uncover.
- **Signatures:** Regularly updated OpenIOC, STIX and YARA rules are integrated into Threat Hunter to better detect advanced persistent threats on the network.
- **Rapid Framework:** Our flexible interface allows for new hunting modules within minutes that are easily shareable with your team members

BENEFITS:

Strategy:

Threat Hunter assists business executives and CISOs in better understanding the threat actors targeting their organisations. With this additional knowledge, they can reassess their cyber security risks and optimise IT security spending.

Rapid Response:

When an intrusion occurs, speed is paramount to mitigate damage. Threat Hunter helps organisations rapidly assess how many assets on their network have been compromised. A single analyst can review over 200 machines per day.

Due Diligence:

Threat Hunter helps organisations evaluate whether there may be active threat actors on their network that traditional security defenses have failed to stop.

Mossé Security, 454 Collins Street. Melbourne, 3000, Victoria, Australia
www.mosse-security.com contact@mosse-security.com