Trellix

DATA SHEET

Threat Hunting

Don’t wait for alerts—go find the threat

Outcome & Value

- Early detection of stealthy, low-noise threats
- Enhanced visibility into adversary behavior
- Reduction in attacker dwell time
- Improved detection engineering and SOC readiness
- Validation of existing security controls and telemetry coverage

Key Deliverables

- Initial Hunting Engagement Plan
- Custom Threat Hypotheses
- Identified Indicators of Compromise (IOCs)
- Behavioral Anomaly Findings
- Tactical and Strategic Remediation Recommendations
- Final Threat Hunt Report
- Optional Threat Detection Use Case Tuning

Overview

Threat actors are becoming increasingly sophisticated, often bypassing traditional security controls and operating undetected for weeks or even months. Our Trellix Guardians Threat Hunting service is designed to close that gap.

We proactively search your environment for indicators of compromise, malicious behaviors, and advanced persistent threats that evade automated detection. By combining human expertise, deep threat intelligence, behavioral analysis, and tools like MITRE ATT&CK, our team identifies and investigates stealthy adversaries—before they escalate into major incidents.

Whether you're concerned about insider threats, emerging TTPs, or simply want to validate the effectiveness of your defenses, our service strengthens your detection capability and enhances overall cyber resilience.

When Should You Consider Threat Hunting Exercise?

- You’ve experienced a recent security incident or breach and want to ensure no residual threats remain.
- There are signs of unusual or suspicious activity that traditional detection tools haven’t flagged.
- You want to validate the effectiveness of existing security controls and telemetry coverage.
- You operate in a high-risk industry or are facing persistent targeting by advanced threat actors.
- You’re preparing for a security audit or compliance check and need assurance of threat visibility.
- You want to improve your organization’s threat detection maturity and proactively reduce risk exposure.

Optional Add-On Services

- Integration with Incident Response Retainer
- Threat Hunt-as-a-Service (recurring engagements)
- Red vs. Blue Simulation Hunts
- MITRE ATT&CK Heat Mapping for Gaps
- EDR/other Trellix Policy & Rule Tuning

Key Services

Our Guardians Threat Hunting services span intelligence-driven, hypothesis-driven, and analytics-driven approaches to identify both known and unknown threats. We tailor each hunt based on your environment, leveraging threat intelligence, behavioral analytics, and attacker TTPs to uncover hidden risks and strengthen your security posture. Below a high-level summary:

- Intelligence-Driven Hunting: Leverages global threat intelligence and IOCs to search for known adversaries in your network.
- Hypothesis-Driven Hunting: Based on TTPs from frameworks like MITRE ATT&CK, our hunters develop and test hypotheses to uncover unknown threats.
- Analytics-Driven Hunting: Uses anomaly detection, machine learning, and user behavior analytics to identify deviations from normal patterns.
- Custom Threat Scenarios: Tailored threat models based on your industry, risk profile, and infrastructure.

Our Methodology

Our threat hunting methodology follows a structured, intelligence-led approach that combines threat modeling, behavioral analytics, and forensic investigation. Using frameworks like MITRE ATT&CK, we proactively hunt for advanced threats across your environment to detect, validate, and contain malicious activity before it escalates.

1. Scoping & Planning – Define objectives, data sources, and hunting maturity.
2. Baseline Development – Understand normal vs. abnormal behavior.
3. Threat Hypothesis Creation – Based on attacker TTPs and recent threat trends.
4. Data Collection & Analysis – Use SIEM, EDR, XDR, and threat intel platforms.
5. Investigation & Validation – Correlate artifacts to validate true positives.
6. Threat Containment Support – Work with your IR team if threats are found.
7. Reporting & Recommendations – Deliver tactical and strategic remediation guidance.

For more information or to schedule a consultation, please contact us at Guardians@Trellix.com