THREAT HUNTING AND INCIDENT RESPONSE

Bag Your Prey

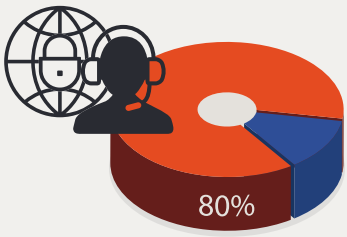
Optiv's Threat Hunting service proactively examines your organization's IT infrastructure with a focus on identifying signs of a potential compromise, active breach activity or malicious tools that an attacker could initiate later. This service uses automated and manual approaches to identify indicators of malicious activities and provide you with awareness regarding the safety of your computing environment and if your systems have been compromised. Optiv can also identify whether malicious third parties have unauthorized access to your systems.

During a threat hunt, breach investigators and malware reverse engineers examine your computing environment, including workstations, laptops, servers, logs and network traffic. Using manual and automated tools, our experts identify threats including those that frequently bypass standard security controls, such as antivirus and intrusion detection tools. Examples of malicious activity we typically find include:

- Malware
- Advanced Persistent Threats (APT)
- Viruses
- Backdoors
- Botnets
- Rootkits
- Data exfiltration
- Command and control traffic
- Unpatched vulnerabilities that are open doors for attackers

All data that Optiv collects is compared against numerous behavioral analysis and threat intelligence databases and activity baselines to identify suspicious or malicious processes, network connections and traffic patterns for evidence of compromise. During a threat hunt, Optiv's experts act with your best interest in mind, preserving digital fingerprints and advising you of next steps.

WHY THREAT HUNTING:



More than 80 percent of all breach victims learn of a compromise from third-party notifications, not from internal security teams.

In most cases, advanced threats have been present in an organization for months prior to detection, yet those organizations are still caught by surprise when the breach is discovered.

As cyber adversaries continue to change, modify and evolve their tactics, a proactive approach is essential to protecting your enterprise.

90 percent of businesses suffered some sort of significant security incident **over the last 12 months**.

Find out what's in your network.
Contact us for more details about our Threat Hunting service | 800.565.5091
www.optiv.com

Our Approach

1. **Environment Discovery:** Identify the critical infrastructure and data flows that support the business.

2. **Agent Deployment:** Deploy advanced endpoint security monitoring agents to targeted hosts and environments.

3. **Live Information Analysis:** Monitor and analyze data from AMP agents to identify suspicious or malicious activity.

4. **Network Traffic and Log Collection:** Place network monitoring devices at key ingress and egress points and/or collect ingress and egress packet captures and logs from critical systems and devices.

5. **Static Information Analysis:** Analyze collected data for undetected malicious activity, suspicious network connections, malicious processes or services, suspicious artifacts and compromised user accounts. Examine outbound network traffic to identify systems that attempt to communicate with known bad domains, IP addresses, network address blocks or suspicious regions. Compare all data against proprietary and third-party advanced threat intelligence sources.

6. **Reporting and Analysis:** Compile data from the assessment into a technical report of findings and recommendations. The methodology includes identification of gaps in security controls within the environment and recommendations for containment and remediation of threats.

7. **Presentation of Findings:** Publish the technical report of findings and hold a technical presentation to select client personnel to review the report findings and recommendations.

Target Data Sources:	High-Level Checks:
1. Workstations and laptops used by sensitive business units such as executives, developers, network/systems administrators, accounting, finance and other entities with privileged access 2. Internal DNS systems 3. Windows domain controllers 4. Point of sale servers 5. Firewall ingress/egress logs 6. Proxy logs 7. VPN logs 8. Security appliance logs	1. Unusual amounts of data being transmitted from a given host or to a given destination 2. Suspicious activity patterns 3. Unusual ports, protocols or services 4. Unusual DNS activity 5. Communications originating from your network destined for systems with known connections to "botnets" or other malicious activity 6. Geo-mapping of network ingress/egress activity 7. Workstation scans for artifacts of ongoing or past compromise 8. Malicious applications

Deliverables

A typical Threat Hunt report contains the following components:

- **Executive Summary –** High-level narrative that explains the work performed, what was assessed, what was found and what it means to the business.
- **Summary of Findings and Recommendations –** Detailed description of identified malicious activity, compromised infrastructure, at risk data, recommended next steps for containment and remediation, and a graphical map showing the location of discovered external connections.
- **Detailed Findings Matrix –** Highly detailed matrix that shows technical details of each finding including description, impact, risk severity and difficulty of remediation.
- **Appendix –** The appendix contains additional detail that clearly communications findings to technical staff for remediation.

The Optiv Advantage:

Optiv can help businesses in every industry connect information security policies, procedures and practices with business goals. Our security leadership experts, backed by our team of consultants, can provide the experience you need to take your program to the next level.

Expert Minds

Optiv's security professionals are dedicated to helping you achieve results and realize value. Our team of 1,000+ highly skilled client managers and security practitioners work hard to deliver superior results and cutting-edge research to solve your complex, real-world security problems.

Leading Best Practices

Our knowledge of leading best practices helps Optiv formulate security recommendations tailored to meet your specific business objectives.

Client-first Culture

Optiv's passion for security and our commitment to quality results means we focus on the right solutions to meet your specific needs.

Proven Methodologies

Optiv has developed proven methodologies to help ensure superior outcomes for your projects and programs.

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.