INCIDENT DISCOVERY

Detailed Insight into Your Infrastructure

Overview

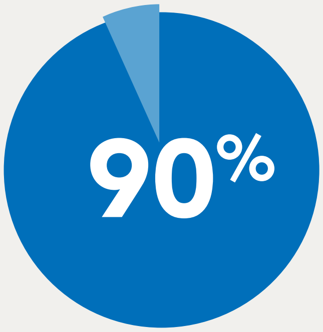
Optiv's Incident Discovery service examines your organization's IT infrastructure with a focus on identifying signs of a potential compromise, active breach activity or malicious tools that an attacker could initiate later. This service uses automated and manual approaches to identify indicators of malicious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

During the assessment, Optiv's expert malware engineers and breach investigators take a holistic look at your computing environment, including workstations, laptops, servers, logs and network traffic. Through the use of 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 in engagements includes:

- 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 the assessment, Optiv's experts act with your best interest in mind, preserving digital fingerprints and advising you of next steps.



of businesses suffered some sort of computer hack **over the last 12 months**

FIND OUT WHAT'S IN YOUR NETWORK

Contact us for more
details about our
Incident Discovery service.
800.565.5091
www.optiv.com

Our Approach

Optiv works with your organization to perform the following:

1. **Environment Discovery:** Identify the critical infrastructure and data flows that support the business.
2. **Agent Deployment:** Deploy Advanced Malware Protection (AMP) 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 devices at key ingress/egress points and/or collect ingress/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, compromised user accounts, etc. 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:

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

HIGH-LEVEL CHECKS:

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 Incident Discovery 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 even more technical detail so that findings are clearly communicated 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 | optiv.com

Optiv is a market-leading provider of end-to-end cyber security solutions. We help clients plan, build and run successful cyber security programs that achieve business objectives through our depth and breadth of cyber security offerings, extensive capabilities and proven expertise in cyber security strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers. For more information, visit www.optiv.com or follow us at www.twitter.com/optiv, www.facebook.com/optivinc and www.linkedin.com/company/optiv-inc.