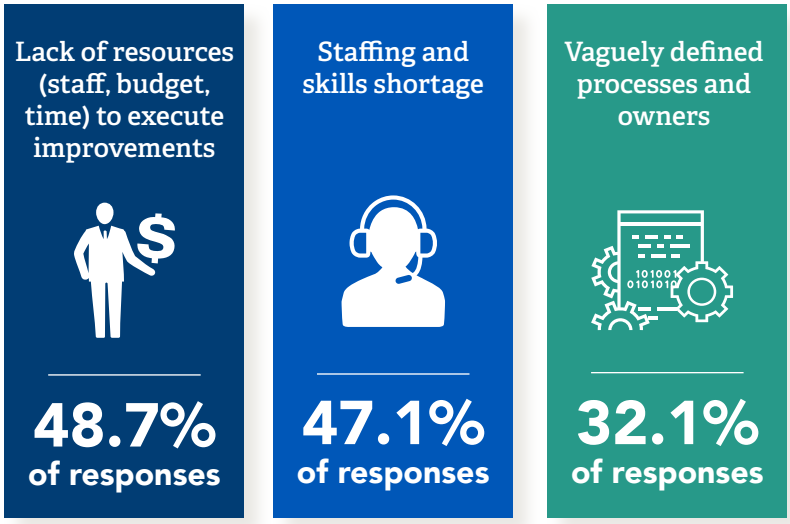
Digital Forensics

Find, Analyze and Preserve the Evidence You Need

A critical but often overlooked capability when responding to incidents is forensic analysis. Whether the incident is a ransomware infection, a data breach, or a malicious attack on a server, tactical decisions need to be made quickly. These decisions potentially include the preservation and collection of digital evidence.

2017 SANS IR Survey: Top Three Impediments Facing IR Teams



Going beyond the collection, however, it is difficult to find qualified individuals capable of conducting thorough digital forensic investigations (see above SANS survey data). There are also many pitfalls that may compromise your investigation before you even get started. One common mistake responders make is immediately shutting down an affected system; this can destroy volatile data or critical evidence that may only be available in memory.

Working with a partner that has years of experience and knowledge actively assisting organizations with forensic investigations is essential. Optiv's Enterprise Incident Management (EIM) team can help guide you through the critical initial steps of forensic analysis investigations including data collection, analysis and preservation.

How Do We Do It?

DISCOVERY
We identify important data sets for imaging, analysis and processing that inexperienced or understaffed teams may forget during incidents.

IMAGING
We assist with live imaging, memory capture and "dead box" imaging from a variety of systems during an engagement.

ANALYSIS
We conduct analysis of memory dumps and imaged systems to identify malware, AUP violations, breaches and other issues that may arise during an incident.

RECOMMENDATIONS
We provide recommendations for bolstering your forensic capabilities in the event of future incidents.

COMMUNICATION
In reportable situations, we allow for your organization to inform your customer base of any potential issues and assisting your legal counsel with case generation.

Partner With Optiv to Strengthen Your Investigation

Throughout the entire investigation, Optiv works directly with your legal counsel to build the strongest case possible. Once the investigation is complete, Optiv educates and provides first responders with the necessary tools and information they need to preserve and collect evidence in a defensible manner to expedite future investigations. Additionally, Optiv can recommend measures organizations can take to fill gaps in their forensic analysis capability. By partnering with Optiv, you also receive the following benefits:

Full Lifecycle Support: Optiv's EIM team has experts with the experience and knowledge required to conduct the full lifecycle of a digital forensic investigation from collection to analysis.

Experience Across Your Technology Stack: Optiv's EIM team has conducted large enterprise investigations involving smartphones, tablets, laptops, workstations and servers.

Sophisticated Investigation Methodology: Optiv's EIM team utilizes leading technology solutions available in the market to uncover the data needed to support investigations.

Consistent and Transparent Crisis Communications: Optiv's experts work side-by-side with your team members to ensure proper handling and storage of evidence, recovery of volatile data, documentation and coordination between technical and legal teams.

Forensic Investigation To-Do List

- Isolate the infected/suspect machine from the network
- Document observed behavior
- Capture memory and disk images
- Generate network captures
- Engage your legal team to gain support for your investigation
- Limit communications about the incident until your legal team is engaged
- Reference your incident response (IR) plan and any documented playbooks or SOPs that may guide your IR triage processes
- Review your obligations as dictated by your cybersecurity insurance provider
- Prepare notes to share with your forensic/IR retainer support partner
- Document any seized evidence with a chain of custody form

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