

DIGITAL FORENSICS AND INCIDENT RESPONSE

PRAGMATIC REACTION, DELIBERATE RESPONSE

Cybercriminals have more resources and time to focus on finding a way in than you have in stopping them. Falling prey to an incident is a matter of when, so relying on the right response team is crucial.

Provided as an on-demand crisis response service as well as retainer-based program, Avertium's Digital Forensics and Incident Response (DFIR) helps you to rapidly assess, contain, eradicate and recover from a security incident to minimize impact and return you to normal operations.

Because superior DFIR extends beyond technical expertise, Avertium's skilled incident handlers help you and your executive team to navigate potential legal and reputational liabilities while driving to identify and resolve the root cause.

TYPES OF INCIDENTS WE ENCOUNTER

Avertium tackles each unique incident with the right tools, methodologies, and people to meld to the distinct challenges presented and ensure we react quickly and appropriately to your situation.

- » Ransomware
- » Advanced Persistent Threats
- » Banking Trojan Outbreaks
- » Malware and Worm Outbreaks
- » Business Email Compromises
- » Spear Phishing Attacks
- » Drive-by Downloads
- » Insider Threat
- » Social Engineering
- » Unauthorized Access
- » Data Exfiltration

INITIATE AND PLAN

Emergency response w/n two hours; Gather details and create action and communications plan

ACTIVATE AND DEPLOY

Prompt project initiation; Gain the required access, deploy tools, activate investigation

INVESTIGATE AND ANALYZE

Monitor threat activity, collect forensic artifacts, analyze actions to determine incident timeline, root cause, scope

REMEDiate AND RECOVER

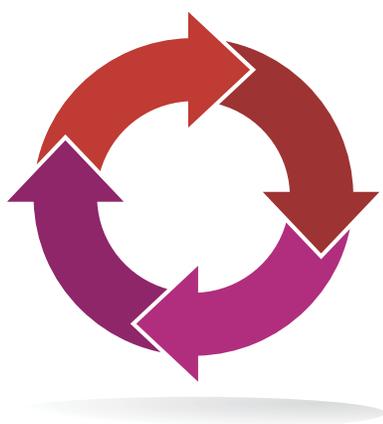
Collaborative comprehensive strategy to return to normal operations and build long-term defenses

THE AVERTIUM ADVANTAGE

MORE RIGOR - Avertium takes command to fully analyze and address the spectrum of technical, legal, regulatory and business impacts of the incident, expertly weighing each to facilitate containment and eradication in the short-term and deploy practical recovery strategies aligned with your objectives in the long-term.

MORE RELEVANCE - Our investigators relay the nature and potential ramifications of the incident to your technical staff and business stakeholders in a way that makes sense, paving the way for faster and more efficient incident handling.

MORE RESPONSIVENESS - Our in-house 24/7/365 CyberOps Centers of Excellence stands ready to mobilize our incident responders and forensic investigators at a moment's notice to join you in the trenches, rapidly activating response strategies tailored to your needs.



FULL INCIDENT RESPONSE LIFECYCLE

As the leading provider of accessible managed security and security consulting services to the midmarket and enterprise, we offer a comprehensive array of solutions that support the full incident response lifecycle:

- » Plan Development:
 - Incident Response
 - Business Continuity
 - Disaster Recovery
- » Digital & Mobile Forensics
- » Tabletop Exercises
- » Managed Security
- » Penetration Testing

DELIVERABLES

Avertium stays in contact in the near term with regular touchpoints, then provides a full understanding of the incident to avoid reoccurrence once all information is gathered:

- » Daily or Weekly Update
- » Post-Incident Report and Briefing

ABOUT AVERTIUM

Avertium brings enterprise-level security to mid-sized and larger organizations challenged by the cybersecurity talent shortage, rapidly evolving threat landscape and budgetary constraints. The company's acclaimed show-no-weakness approach to extended detection and response (XDR), governance and compliance, and strategic advisory services is redefining the managed security services category. From financial services and manufacturing, to technology and healthcare, more than 2,500 companies rely on Avertium's more rigorous, more relevant, and more responsive delivery of cybersecurity services. Backed by growth equity firm Sunstone Partners, Avertium operates CyberOps Centers of Excellence in Arizona, Colorado, and Tennessee. **Avertium. Show No Weakness.®**