carahsoft

WaveStrong
Information Security Professionals

Digital Forensics and Incident Response

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASA SEWP V, E&I Carahsoft Cloud Solutions & Services Distributor Contract and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with WaveStrong, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/learn

Join Events & Webinars:
carah.io/events

Discover Technology Solutions:
carah.io/wavestrong

Learn About Procurement:
carah.io/opensourcecontracts

Connect With Our Team:
wavestrong@carahsoft.com
(703) 871-8548

WaveStrong
Information Security Professionals

Digital Forensics & Incident Response (DFIR) Services

Rapid Response. Deep Visibility. Proven Containment

Introduction

WaveStrong delivers enterprise-grade **Digital Forensics and Incident Response (DFIR)** services designed to help organizations **detect**, **contain**, **investigate**, and **recover** from **cyber incidents** with speed and precision. Our DFIR team combines advanced tooling, threat intelligence, and forensic rigor to minimize business impact and strengthen long-term resilience.

Core Capabilities

1. Incident Response (IR)
- 24x7 breach response and triage
- Ransomware containment and eradication
- Business Email Compromise (BEC) response
- Insider threat investigations
- Cloud and hybrid environment incident handling (AWS, Azure, M365)

2. Digital Forensics
- Endpoint and server forensic analysis
- Memory (RAM) forensics
- Disk imaging and artifact analysis
- Log correlation across SIEM, EDR, and network sources
- Chain-of-custody compliant evidence handling

3. Threat Hunting
- Proactive compromise assessments
- MITRE ATT&CK-aligned threat detection
- Advanced adversary behavior analysis
- EDR/XDR telemetry deep dives

4. Malware Analysis
- Static and dynamic malware analysis
- Reverse engineering (where required)
- Payload behavior and persistence analysis
- Indicators of Compromise (IOCs) extraction

5. Ransomware Response
- Rapid isolation and containment
- Root cause and patient-zero identification
- Data exfiltration analysis
- Support for recovery and restoration strategy

Engagement Models

- **Retainer-based DFIR (recommended)**
  - ❑ Guaranteed SLA response times
  - ❑ Pre-negotiated rates
  - ❑ Priority access to IR experts
- **On-demand Incident Response**
  - ❑ Emergency engagement
  - ❑ Rapid mobilization within hours
- **Proactive Services**
  - ❑ Compromise assessments
  - ❑ Threat Hunting programs
  - ❑ IR Readiness and tabletop exercises

DFIR Lifecycle Approach

1. Preparation
- ✓ IR Playbooks and Runbooks
- ✓ Tabletop exercises
- ✓ Logging and telemetry readiness assessments

2. Detection & Analysis
- ✓ Alert triage and validation
- ✓ Threat Intelligence enrichment
- ✓ Scope determination and impact assessment

3. Containment
- ✓ Network Segmentation
- ✓ Credential resets and access control
- ✓ Endpoint quarantine

4. Eradication
- ✓ Malware removal and persistence elimination
- ✓ Vulnerability remediation

5. Recovery/ Post Incident Review
- ✓ System Restoration
- ✓ Monitoring for reinfection or residual threats
- ✓ Executive and technical reporting
- ✓ Lessons learned and control improvements
- ✓ Compliance and legal support

Identify and understand security risks in your environment

Protect your data and risk exposure by putting safeguards in place

Detect threats and vulnerabilities in a timely manner

Key Deliverables:
- ❖ Executive Summary Report (business impact, timeline, recommendations)
- ❖ Technical Forensics Report (IOCs, TTPs, attack vectors
- ❖ Remediation Plan (prioritized actions)
- ❖ Compliance Support Docs (HIPAA, PCI, CJIS, etc.)
- ❖ Legal Ready evidence packages

WaveStrong
Information Security Professionals

Rapid Response. Deep Visibility. Proven Containment.

WaveStrong delivers enterprise-grade Digital Forensics and incident Response (DFIR) services designed to help organizations, detect, contain, investigate, and recover from cyber incidents with speed and precision. Our DFIR team combines advanced tooling, threat intelligence, and forensic rigor to minimize business impact and strengthen long term resilience.

Core Capabilities

Incident Response
- 24x7 breach response and triage
- Business Email Compromise (BEC) response

Digital Forensics
- Endpoint and server analysis
- Cloud and hybrid IR (AWS, Azure, M365)

Threat Hunting
- Proactive compromise assessments
- MITRE ATT&CK-aligned detection

Malware Analysis
- Static and dynamic malware analysis
- Reverse engineering (when needed)

Malware Analysis
- Static and dynamic malware analysis
- Reverse engineering (when needed)

Ransomware Response
- Rapid isolation and containment
- Root cause identification

Contact Us

For more information about how WaveStrong can help you to implement the best DFIR program, reach your WaveStrong DFIR specialist at info-dfirsvcs@wavestrong.com.

Please visit us at www.wavestrong.com or via email at info-dfirsvcs@wavestrong.com