# "Day One" – Breach Response

## Digital Forensics & Incident Response (DFIR)

Thank you for downloading this Abacode resource. Carahsoft is the distributor for Abacode cybersecurity solutions.

To learn how to take the next step toward acquiring Abacode's solutions, please check out the following resources and information:

For additional resources:
carah.io/AbacodeResources

For additional cyber solutions:
carah.io/Cybersecurity

For additional Abacode solutions:
carah.io/AbacodeProducts

To purchase, check out the contract vehicles available for procurement:
carah.io/AbacodeContracts

To set up a meeting:
Abacode@carahsoft.com
703-871-8505

# "DAY ONE" - BREACH RESPONSE
## DIGITAL FORENSICS & INCIDENT RESPONSE (DFIR)

## IMMEDIATE INCIDENT RESPONSE

*Without a question, time is of the essence when dealing with cybersecurity incidents as downtime translates to financial losses.*

*However, the urgency to restore services needs to be balanced with the need to find out how the incident occurred and what steps need to be taken from the regulatory compliance standpoint.*

*Abacode's Day One DFIR Consulting Services focus on the following five areas to gain control over an incident or suspected breach on Day One.*

**RAPIDLY RESPOND** TO CYBER ATTACKS
Combining the deployment of host-based, cloud-based, and network forensic tools, we are able to identify targeted and impacted systems and develop a forensic analysis plan on Day One.

**ANALYZE** DATA EXFILTRATION RISK
Reporting requirements depend on the level of access threat actors gained on systems hosting controlled data. Abacode detects indicators of compromise in systems hosting confidential data on Day One.

**DETECT** UNAUTHORIZED ACTIVITY
Threat actors build persistence mechanisms to retain access to compromised environments. Abacode's US-based Security Operations Center provides a 24/7 cybersecurity monitoring service to detect and disable threat actors from Day One.

**COORDINATE** DFIR RESPONSE TASKS
Successful incident response management requires effective communication among the different teams involved. Abacode serves as liaison between IT, legal, insurance, executive team, etc. on Day One.

**QUICKLY RESTORE** NORMAL OPERATION
By accelerating the identification of all impacted systems and quickly gathering any relevant forensic evidence, Abacode can build a prioritized restoration plan and begin restoring impacted systems from Day One.

**REMEDIATE** EXPLOITED VULNERABILITIES
Breaches and incidents occur when vulnerabilities are exploited by threat actors. Abacode identifies and corrects these vulnerabilities and provides measures to mitigate the risk of reinfection from Day One.

## PROGRAM HIGHLIGHTS

- Day one response time SLA - not to exceed 12 hours
- Program includes one hour per quarter of vCISO consultation
- Annual auto renewal terms and conditions at no additional fee

## INCIDENT RESPONSE PROGRAM SERVICE

- The most accelerated program for day one breach isolation and containment
- Forensics expert personnel
- Immediate technical analysis using advanced threat hunting tools
- Agreement meets required controls for incident response plan

### Abacode DFIR Pricing:

**$1,950** Administrative Fee (paid in advance)

**$7,800** Program Cost (paid at time of an incident/breach)

## CONTACT

US Office: 866-596-9020

CyberConnect@abacode.com