Digital Forensics and Incident Response

Where the hard cases land. Reconstruct what happened even when the evidence is cold, then contain, eradicate and recover.

The question it answers

During an incident the questions are simple and the answers are not. What got in, how far did it go, what did it take, and is it still here. Answering them takes evidence, and evidence degrades from the moment the incident starts.

When another team has already closed a case, this is often the second call, and the one that resolves it.

Two ways to hold it

Emergency response engages when something is happening now: rapid deployment, containment, forensic analysis and guided recovery for ransomware, insider activity, data breach and targeted intrusion.

An Incident Response Retainer secures priority access before you need it, with the environment understood and communication protocols agreed in advance. Retainer hours not consumed by incidents are not lost; they convert to other consulting work.

What the work covers

Rapid containment

Immediate action to stop the incident spreading: isolating affected systems, disabling compromised accounts and applying emergency measures, in the order that limits damage.

Forensic analysis

Disk, memory and cloud evidence collected and analyzed to establish root cause, attack vectors and the true extent of the compromise, to a standard that supports remediation and potential legal action.

Timeline reconstruction

The sequence of events assembled from the artifacts, including cases where the evidence is partial, degraded or was written off as unrecoverable.

Recovery and hardening

A remediation plan executed to eradicate the threat and return operations to a secure state, followed by a review that turns the incident into improvement.

AT A GLANCE

LIVE INCIDENT
40 to 80 hours, excluding the report

FINAL REPORT
16 hours, shaped to your questions

POST-MORTEM INVESTIGATION
From 32 hours, report included

DURING AN ENGAGEMENT
Daily technical updates on case progress

UNUSED RETAINER HOURS
Convert to other consulting, never lost

WHO THIS IS FOR

- Organizations in an active incident that need senior hands on it today.
- Teams holding a case that was closed without a satisfying answer.
- Boards and legal counsel needing findings that will survive scrutiny.
- Organizations that would rather agree terms and access now than negotiate them during a crisis.

How an engagement runs

01 Activation and triage

On notification the response process activates and a rapid triage establishes the scope and severity of the incident, so effort goes where it changes the outcome.

02 Containment

Immediate action to contain the incident and prevent further damage, balanced against the need to preserve the evidence the investigation depends on.

03 Incident analysis

A thorough investigation of root cause, attack vectors and extent of compromise, with digital evidence collected and analyzed to support both remediation and any legal action.

04 Remediation and recovery

A remediation plan built on the analysis: eradicate the threat, restore affected systems, and return operations to a secure state.

05 Post-incident review

Once the incident is resolved, a review establishes what happened, how the response performed, and what to change so the same path is closed.

WHY ALEXSTA

- Senior hands only. The operator whose experience you are buying does the work, rather than reviewing it.
- Evidence others consider unusable is regularly where the answer is found, including memory and artifacts recovered long after the fact.
- Conclusions carry their evidence and a stated confidence level, including what the evidence does not settle.

WHAT WE NEED TO SCOPE A PROGRAM

- Size of the environment: how many endpoints and users.
- Use of Microsoft 365, and how many users.
- Count of web applications exposed to the internet.
- Existing telemetry and log retention.

What you receive

Incident report

The nature of the incident, the response actions taken and the impact on the organization, with a timeline of events and the evidence supporting it.

Containment and remediation plan

Specific recommendations for addressing the vulnerabilities exploited, recovering systems, and closing the route that was used.

Forensic analysis report

Where the case requires it, a full forensic account of the evidence, the methods applied and the conclusions drawn, written to withstand external review.

Post-incident recommendations

Lessons learned converted into actions that raise the security posture, so the engagement leaves the organization stronger than it found it.

Request an engagement

If something is happening now, call rather than write. If nothing is happening now, that is the right moment to agree how it would work.

contact@alexsta-cybersecurity.com
+41 76 76 44884
alexsta-cybersecurity.com