Compromise Assessment

Establish whether an adversary is in the environment now, or has been, and close the gaps that would let the next one move.

The question it answers

Most organizations cannot say with confidence whether they are compromised. Preventive controls report on what they blocked, not on what passed. This assessment answers the question directly, on evidence, by examining the environment for indicators of compromise and unauthorized activity that evaded the controls already in place.

More than a hunt for intruders

Gaps in best practice are open invitations for a threat actor. So the assessment runs two layers in the same pass: direct indicators of compromise, and the deficiencies that would let an attacker move laterally, escalate privilege or persist.

That second layer is what separates it from threat hunting. A hunt tells you what is there. This tells you what is there and why the environment allowed it. Run over time, it is one of the most effective ways to drive down high-severity incidents.

What we collect and examine

Endpoints

Forensic collection across the estate using Velociraptor, tuned to run at speed on the hardware already on site. Execution artifacts, persistence, credential access and anti-forensic traces.

Active Directory

Security logs, privilege paths, delegation and service accounts, and the misconfigurations that turn a single foothold into domain control.

Network infrastructure

DNS, proxy and firewall logs reviewed for command and control, staging and exfiltration patterns, including traffic that looks legitimate at the perimeter.

Business applications

The systems that carry the most consequence and usually the least coverage, including applications whose logs no standard tool can read.

AT A GLANCE

TYPICAL DURATION
5 weeks, kick-off to report review

DELIVERY
Principal-level operator, start to finish

ENDPOINT TOOLING
Velociraptor, deployed for the engagement

WHERE DATA IS ANALYZED
On premise, in your tenant, or fully isolated

AGENTS REQUIRED
None retained. No new licences

WHO THIS IS FOR

- Organizations with no independent evidence of their current state, only the absence of alerts.
- Boards and regulators asking for assurance that a control inventory cannot give.
- Estates after a merger, a divestment or a rapid cloud migration, where visibility has gaps nobody has mapped.
- Teams that suspect something happened but have no incident to point at.

How an engagement runs

01 Kick-off and planning

Objectives, scope and scale are established: the critical assets, systems and network segments to examine. Agreed in writing before anything begins.

02 Velociraptor deployment

Collection tooling is deployed into your environment, under accounts your team issues. Residency and classification rules are fixed inputs from the first call, not obstacles negotiated later.

03 Data collection

Endpoint, Active Directory, network infrastructure and business application data is gathered across the agreed scope.

04 Triage of hits

Current threat intelligence supplies known indicators and adversary techniques. Automated analysis narrows the field; a senior investigator confirms or dismisses each candidate and assesses its impact.

05 Report and review

Findings are written up, then walked through with your team so every one is clear and well understood, together with the plan to act on it.

WHY ALEXSTA

- Senior hands only. The operator whose experience you are buying does the work, rather than reviewing it.
- Depth goes to the systems that carry the most consequence, including the applications no standard tool can read.
- Conclusions carry their evidence and a stated confidence level, including what the evidence does not settle.

WHAT WE NEED TO SCOPE IT

- Count of endpoints.
- Count of applications hosted and exposed to the internet.
- Number of users.
- Whether Microsoft Entra ID and Microsoft 365 are in use.

What you receive

Executive summary

A high-level account for senior management: scope, method, key findings and the actions they imply, in business terms.

Detailed findings report

Every indicator of compromise with its nature, affected systems, supporting evidence, and an analysis of the impact on security and operations.

Prioritized remediation plan

Short-term fixes for immediate threats and longer-term measures to raise the posture, sequenced by consequence rather than drawn from a catalogue.

Presentation and debriefing

A formal presentation to your stakeholders and a working session to discuss results, agree next steps and transfer what was learned.

Request an engagement

Scoping starts with a conversation, not a questionnaire. We will tell you if a compromise assessment is the wrong instrument for your question.

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