Cyber Defense Assurance Program

A multi-year, threat-informed program that keeps defenses calibrated to the adversaries most likely to target the organization, and proves they work.

The question it answers

A point-in-time engagement describes a moment. Between engagements the estate changes, the adversary changes, and the assurance quietly decays until the next one restates it.

This program removes that gap. The assessment work runs continuously rather than annually, and every finding is carried through to closure instead of being handed over and hoped for.

Your team operates. Ours engineers.

The client's team runs the environment day to day. Principal-level experts design, engineer and advise at a depth an internal SOC cannot reasonably self-supply, through an embedded Virtual Principal Consultant who knows the estate rather than learning it again each engagement.

The program is assembled from the services in this catalog and calibrated to the organization, so the mix reflects the actual threat profile rather than a fixed package.

What runs inside the program

Continuous compromise assessment

Collection and threat-intelligence-led triage across endpoints, Active Directory, network infrastructure and business applications, run on a cycle rather than once, so a foothold is found in weeks rather than at the next annual review.

Monthly perimeter testing

External vulnerability scanning of the perimeter and its assets, open-source intelligence research for exposed or leaked credentials, and penetration testing of internet-facing applications.

Detection and hunting engineering

Hypothesis-driven hunts against your own telemetry, with each finding converted into real-time detection content your team keeps and runs.

Readiness and response

Response plans and handling guides kept current, exercises to pressure-test them, and priority access to the DFIR team.

AT A GLANCE

TERM
Multi-year by design

CADENCE
Continuous assessment, monthly testing

OPERATING MODEL
Your team operates, our experts engineer

EMBEDDED ROLE
Virtual Principal Consultant

FINDINGS
Carried through to verified closure

WHO THIS IS FOR

- Organizations whose risk does not pause between annual engagements.
- Internal SOCs needing principal-level design and engineering they cannot justify hiring full time.
- Boards that want assurance demonstrated on a cadence rather than asserted once a year.
- Estates that change faster than a point-in-time assessment can describe.

How the program runs

01 Baseline

The environment, its technology and its threat exposure are profiled in detail, together with the systems whose loss would matter most. This establishes where assurance actually stands today rather than where it is assumed to stand.

02 Design

The program is calibrated to the adversaries most likely to target the organization, and the mix of assessment, testing and engineering is set against that profile. Agreed in writing before anything begins.

03 Run

Assessment, perimeter testing and engineering cycles run on their agreed cadence, with the Virtual Principal Consultant embedded alongside your team throughout.

04 Close

Findings are worked through with the teams that own them, in working sessions rather than by handover, so each one is understood and closed rather than logged.

05 Recalibrate

The program is reviewed against the changed threat landscape and the changed estate, so what it covers next year reflects next year rather than the year it started.

WHY ALEXSTA

- Senior hands only. The operator whose experience you are buying does the work, rather than reviewing it.
- Assurance is demonstrated continuously, so the answer to whether defenses work is never more than a cycle old.
- Every cycle leaves capability behind: detection content, documentation and a team that understands both.

WHAT WE NEED TO SCOPE IT

- Size of the environment: endpoints and users.
- Use of Microsoft 365 and Entra ID, and how many users.
- Count of applications exposed to the internet.
- The security technologies already in place.
- Desired program duration.

What you receive

Rolling assessment reporting

Each cycle reported with its findings, supporting evidence and impact, so the picture is cumulative rather than a series of unrelated snapshots.

Detection content

Real-time use-cases built from what the hunts and assessments find, written to run in your own tooling and owned by your team.

Remediation carried to closure

A prioritized plan worked through with the teams that own each item, in sessions that confirm the fix is understood and in place.

Executive assurance reporting

A standing account for leadership of what has been tested, what was found, what was closed and what exposure remains.

Request an engagement

A program only makes sense if the cadence matches your risk. Tell us how your estate changes and we will propose the mix, or tell you that point-in-time engagements are enough.

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