SCALING SECURITY MATURITY FOR A FAST-GROWING IDENTITY PLATFORM

aembit

LOCATION

Maryland

INDUSTRY

SaaS

EMPLOYEES

11-50

CUSTOMERS

Snowflake
Red Cup IT
Lacework

Aembit, an identity and access management platform for AI agents and workloads, was scaling rapidly. New funding, larger enterprise customers, and rising SOC 2/ISO 27001 demands created pressure for deeper security validation. Aembit needed a partner who could uncover real attacker paths, validate complex edge components, and provide predictable, repeatable security outcomes as they grew.

Dealing With Growing Pains

Aembit was in a classic high-growth bind: more customers, more components, more scrutiny, without the headcount to keep up. Larger customers required SOC 2 Type 2, ISO 27001, and quarterly pentesting. Their internal tools surfaced “unknown unknowns,” but not at the depth needed by auditors or security-conscious prospects.

Hiring couldn’t keep up with growth. Threat modeling and remediation workflows were early-stage. They needed real attacker-path validation across internet-exposed components, a predictable testing rhythm, and a partner to validate complex systems, find meaningful vulnerabilities, support their growth, and mature their security program, without slowing their release cycles.

> *“We weren’t looking for a vendor. We needed a partner who could immediately operate at our pace and our level of complexity. Software Secured gave us confidence that nothing critical was slipping through the cracks.”*
> ***— CTO & Founder, Aembit***

Scaling Security Maturity for a Fast-Growing Identity Platform

ABOUT SOFTWARE SECURED

20%

of all vulnerabilities are critical or high

26

vulnerabilities on average per pentest

3X

more vulnerabilities found than the leading competitor

How Aembit Hacked Growth

Software Secured deployed Penetration Testing as a Service to match Aembit's growing application, development speed, and security scrutiny from their client base. The quarterly testing, bi-annual edge reviews, unlimited retesting, and consulting hours that their buyers could trust.

Software Secured introduced a flexible annual pool of testing days, allowing Aembit to deploy them as needed. This optimized their pentesting budget. The engineering team had testing flexibility, and sales were enabled by knowing they could always prove security maturity with up-to-date pentest certificates.

Fast-growing teams like Aembit are like Ferraris, built for speed - pentesting shouldn't slow them down.

Aembit maintained its development velocity through the following:

- A dedicated Slack channel
- Jira integration
- Detailed vulnerability extraction into their Kanban workflows
- Collaborative retest scheduling
- Report read-outs and remediation guidance

ROI on Pentesting Dollars

1. Predictable security outcomes

Aembit moved from ad-hoc testing to a scheduled, repeatable PTaaS that aligned with compliance, customer scrutiny, and internal engineering cycles.

2. Faster audits and easier evidence collection

The Portal enabled:

- SLA-aligned remediation windows
- Historical tracking for SOC 2
- Quick extraction of metadata, rankings, and replication steps
- Central storage of reports and certificates

3. Increased engineering velocity
Actionable reports. Clear reproduction steps. Unlimited retesting. Engineering could fix issues quickly without pausing new features.

4. Sales enablement and deal acceleration
Pentest reports and retesting certificates helped Aembit:

- Answer security questionnaires
- Address client's red team findings
- Unblock deals with known vulnerabilities
- Build trust with larger buyers

5. Higher confidence across leadership

- Deeper visibility into edge components
- Validation of complex exploit chains
- Assurance that high-value issues were being found and fixed
- Architectural clarity for next-generation features

6. Cost-efficient testing at scale
The PTaaS model made the daily rate more economical, effectively giving the Aembit team an additional test per year while staying within budget constraints.

Final Words

Aembit moved beyond basic SOC 2 to a more adaptive, multi-layered pentesting cadence. They reduced the risk of missed vulnerabilities and improved customer trust and sales outcomes. SOC 2 Type 2 and ISO 27001 preparation became smoother thanks to SLA tracking, remediation timelines, and historical data in the Portal. Prospects and enterprise clients now receive retest certificates, validated reports, and evidence that Aembit's program is maturing. Deals influenced by security requirements close faster.

Aembit described Software Secured as a true security partner; communicative, transparent, and focused on meaningful vulnerabilities rather than checkbox testing.