EXTERNAL ATTACK SURFACE MANAGEMENT

See your perimeter the way an attacker does.

Surface your exposures before they become entry points — continuous attack surface monitoring that streams straight into Microsoft Sentinel.

WATCHES	SURFACES	STREAMS TO	OUTPUT
Dark web, CT logs & lookalikes	Leaked creds · typosquats · impersonation	Microsoft Sentinel	High signal, low noise

WHAT ATTACKERS SEE FIRST

Every organisation has an attack surface beyond its perimeter. **Leaked credentials traded on dark web forums and Telegram channels.** Newly issued TLS certificates for lookalike domains.

Attackers map this surface before they strike. Most defenders only learn about it after.

22% **of breaches begin with stolen credentials — still the most common initial access vector.**

— Verizon DBIR 2025

THE SOLUTION

Observer watches the channels attackers watch

Dark web forums, Telegram leak feeds, TLS transparency logs, lookalike domain discovery — findings surfaced to your SOC before they reach the attack stage. **High signal, low noise.**

01

Credentials Monitoring

Continuous crawling of dark web forums, Telegram channels, and leak repositories for credentials matching your domains and user identities.

02

Typosquatting Detection

Detects domains designed to impersonate your brand — homoglyphs, character substitutions, alternative TLDs. Visual similarity analysis enables rapid identification of phishing sites, fraud, and brand abuse.

03

Certificate Transparency Monitoring

Detects newly issued certificates associated with your organisation, flagging phishing campaigns and brand impersonation attempts as they're set up.

NATIVE TO THE MICROSOFT SECURITY STACK

Extends your Microsoft operations — it doesn't sit beside them

Findings flow into the tools your SOC already runs, correlating with the rest of your detection and response telemetry.

Microsoft Sentinel NATIVE
Findings stream into your SIEM and correlate with the rest of your telemetry.

Microsoft Entra ID NATIVE
Domain ownership verified through your tenant — onboarding in minutes.

Defender XDR NATIVE
Unified incident triage alongside endpoint, identity & cloud signals.

API DESIGNED FOR
Direct integration for custom SOC workflows & Microsoft Copilot agents.

CHANNELS WATCHED

- Dark web forums
- Telegram leak channels
- Public credential dumps
- Certificate Transparency (CT) logs
- Lookalike domain discovery

> **One stream. Three monitoring surfaces. Straight into Microsoft Sentinel.**

WHY CHOOSE NOIBIT

Built by the people who do the reconnaissance

01 **Built by offensive security specialists**

Observer started as Noibit's internal reconnaissance tool — battle-tested against live engagements before it became a product.

02 **Actionable Exposure Intelligence**

Gain visibility into exposed identities and the associated accounts and services. Exposure insights are delivered without storing plaintext passwords or raw leak datasets in your systems.

03 **Native to your Microsoft stack**

Findings stream into Sentinel and correlate with the rest of your detection and response telemetry.

04 **High signal, low noise**

Findings reach your SOC before they reach the attack stage — prioritized and ready to act on, not raw alert volume.

CREDENTIALS & CERTIFICATIONS

- ✓ **ISO 27001 · NIS2 · DORA**
  Certified information security, aligned to EU regulation.
- ✓ **ISO/IEC 27701**
  Privacy information management.
- ✓ **ISO 9001**
  Quality management system.

Observer surfaces what's exposed. Your team closes it before it becomes an entry point.

Talk to us about Observer.

noibit.com