

# STOP THREATS. BEFORE THEY STOP YOU.

Cloud-native sandboxing for fast malware detonation and analysis - giving your security team answers in minutes, not hours.

Instant Setup

Plug and Play

100% Private



< 3 Min

From submission to full verdict

100%

Saas - nothing to install or manage

Zero

Zero retention - nothing stored after analysis.

## THE CHALLENGE

### Modern Threats Move Faster Than Traditional Security

Today's attackers don't wait. Ransomware encrypts files in seconds. Fileless malware leaves no trace on disk. Zero-day exploits bypass every signature your tools know about. By the time your team gets an alert, the damage may already be done.

Most security teams are stuck waiting for manual analysis, for a second opinion, for tools that weren't built for the speed of modern attacks. That's the gap ThreatLab closes.



#### Analysis Takes Too Long

Hours of manual investigation for a single suspicious file - time your team doesn't have.



#### Threats Hide In Plain Sight

Evasive malware is designed to fool traditional scanners and sandbox tools.



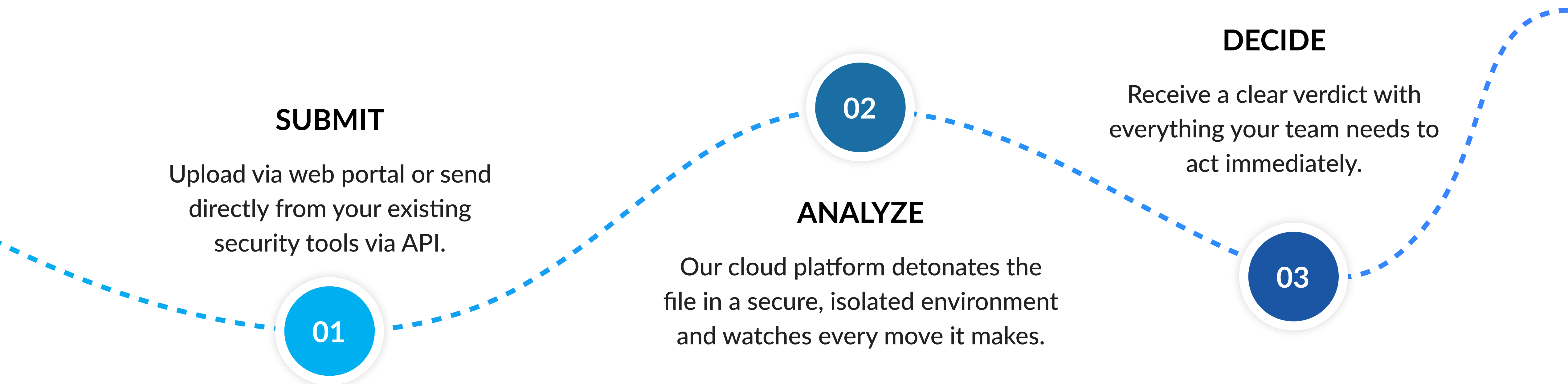
#### Infrastructure Overhead

Building your own analysis environment costs months and significant budget to maintain.

## THE SOLUTION

## ThreatLab: Instant Answers for Every Suspicious File

ThreatLab is a fully cloud-native malware analysis platform. Submit any suspicious file from an endpoint alert to a threat intelligence lead and receive a complete, actionable threat verdict in under three minutes. No hardware. No setup. No waiting.



## KEY CAPABILITIES

## Everything Your Team Needs to Stay Ahead of Threats



### Catch What Others Miss

ThreatLab runs every file through multiple layers of analysis simultaneously like behavioral, network, memory and more, so even the most evasive threats can't hide.



### Plug Into Your Existing Stack

ThreatLab connects to your SIEM and SOAR through a simple API. Automate your triage workflow without replacing a single tool you already use.



### Fileless & Zero-Day Threat Detection

Attacks that never touch disk. Scripts that exploit trusted system tools. Unknown malware families. ThreatLab is built specifically to catch what signature-based tools can't.



### Reports Your Whole Team Can Use

From a one-page executive summary to a detailed forensic breakdown - ThreatLab reports are designed for every audience, from the CISO to the analyst on the floor.



### Instant Attack Context

Every verdict comes mapped to the MITRE ATT&CK framework - so your team immediately understands what the threat was trying to do and where to focus your response.



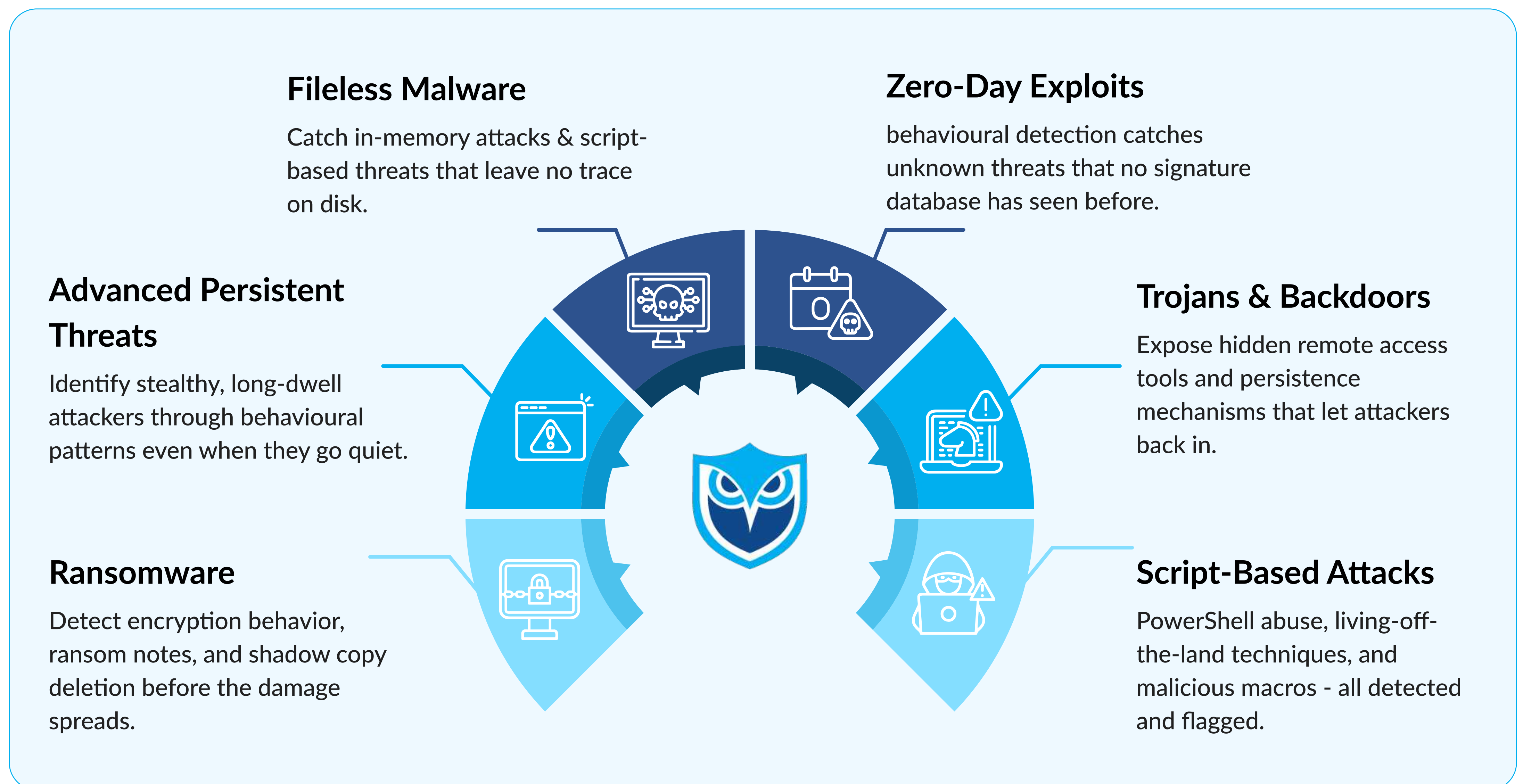
### Full Network Visibility

See every connection a threat attempts to make - command and control servers, data exfiltration, suspicious DNS lookups. Stop threats from phoning home before they do.

## THREAT COVERAGE

## Built for the Full Spectrum of Modern Malware

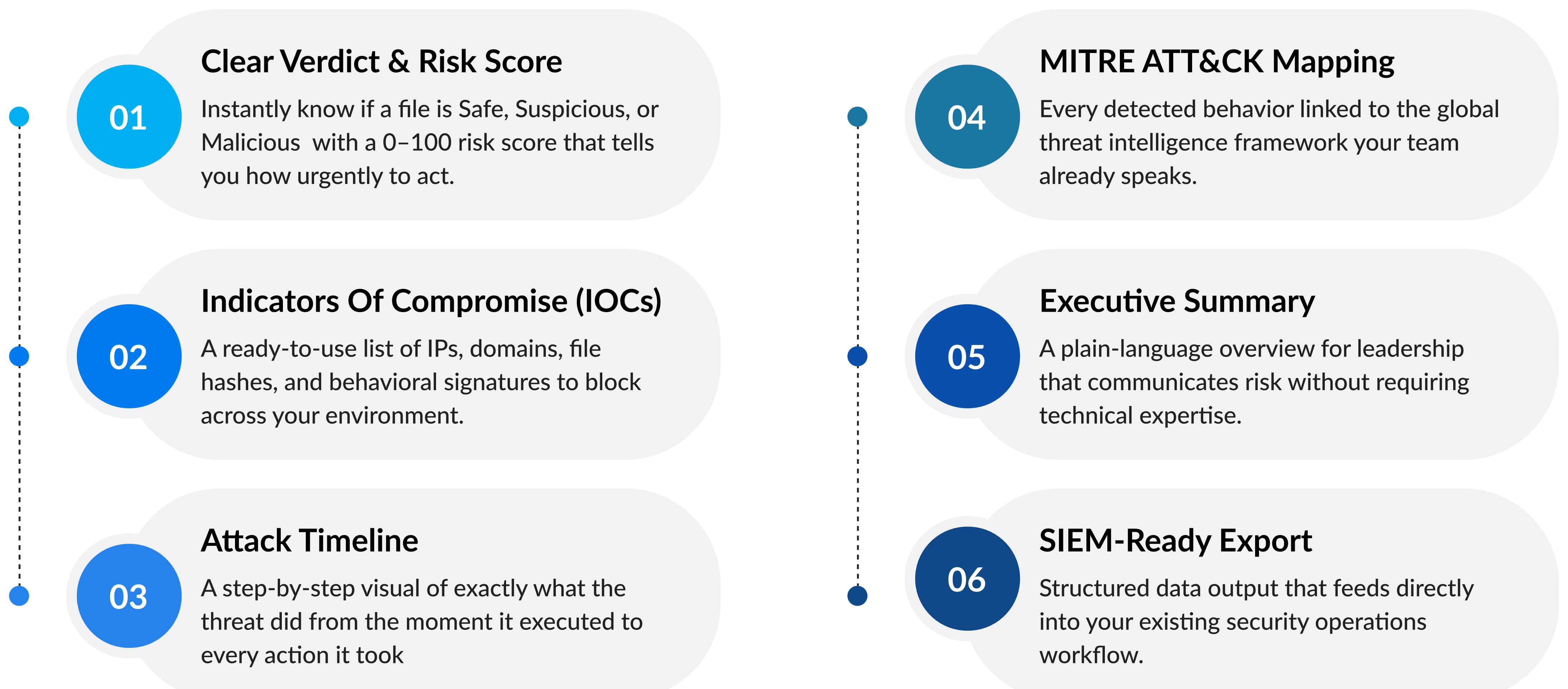
From everyday commodity threats to nation-state-grade attacks, ThreatLab is purpose-built to analyze them all, across both Windows and Linux environments.



## REPORTING

## From Analysis to Action in One Report

Every ThreatLab analysis produces a structured, ready-to-act report, no interpretation required. Your team gets everything they need to make a confident decision, immediately.



PRIVACY & TRUST

Your Intelligence Stays Yours

When you analyze a threat, you're often submitting your most sensitive data, internal documents, proprietary software, confidential communications. ThreatLab is built around one principle: that data belongs to you, and only you.

**Your Data Never Leaves Your Hands**

Every file you submit and every result we generate- stays exclusively within Techowl's infrastructure. We never share, sell, or expose your data to any third party. Period.

**Built For Enterprise Security Standards**

ThreatLab is designed to meet the rigorous data governance and compliance requirements of enterprise security teams. All data is encrypted in transit and at rest.

**Dedicated Environment, Just For You**

Your organization gets its own isolated analysis environment. Your submissions, reports, and findings are completely separate from every other customer always.

**No Setup. No Risk. Just Results.**

Because ThreatLab is fully cloud-native, there are no on-premise components to secure, patch, or maintain. Your risk surface stays exactly where it was before you added ThreatLab.

WHO IT'S FOR

Built for Every Security Function

**Security Operations (SOC)**

Stop spending hours on manual file triage. Get a complete verdict in minutes and keep your queue moving.

**Endpoint & EDR Integration**

Connect ThreatLab to your EDR and endpoint security tools to automatically analyze suspicious files and alerts the moment they surface.

**Threat Hunting**

Proactively detonate suspicious files and IOCs to uncover threats before they become incidents.

**Incident Response**

Understand what a threat did, how it spread, and what it touched - in the time it used to take just to triage.

WHY THREATLAB

The Advantage That Matters

|                          | Techowl ThreatLab            | Traditional Approaches                |
|--------------------------|------------------------------|---------------------------------------|
| Time To First Result     | ✔ Less Than 3 Minutes        | ✔ Hours To Days                       |
| Infrastructure Required  | ✔ None - Fully Cloud-Native  | ✔ Significant (Servers, VMs, Storage) |
| Maintenance Overhead     | ✔ Zero - Fully Managed       | ✔ Ongoing Patching And Updates        |
| Data Privacy             | ✔ 100% Private, Zero Sharing | ✔ Often Relies On Shared Cloud Pools  |
| Evasive Threat Detection | ✔ Multi-Layer Behavioral AI  | ✔ Limited To Known Signatures         |
| Time To Deploy           | ✔ Minutes                    | ✔ Weeks To Months                     |
| MITRE ATT&CK Mapping     | ✔ Automatic, Every Report    | ✔ Manual, If At All                   |

Part of the TechOwl Security Platform

|                                                                                                                                               |                                                                                                                                                    |                                                                                                                                                    |                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <br><b>TechOwl</b><br>SHIELD<br>Attack Surface Monitoring  | <br><b>TechOwl</b><br>DMARC+<br>Email Trust Assurance           | <br><b>TechOwl</b><br>TPRM<br>Third-Party Risk Intelligence   | <br><b>TechOwl</b><br>CSPM<br>Cloud Security Visibility                 |
| <br><b>TechOwl</b><br>Phishlens<br>Employee Risk Readiness | <br><b>TechOwl</b><br>ThreatPulse<br>Threat Signal Intelligence | <br><b>TechOwl</b><br>ThreatLab<br>Advanced Threat Detonation | <br><b>TechOwl</b><br>Simulens<br>Continuous Breach & Attack Simulation |

### See ThreatLab in Action

Start your free trial today. No credit card. No setup. No commitment.