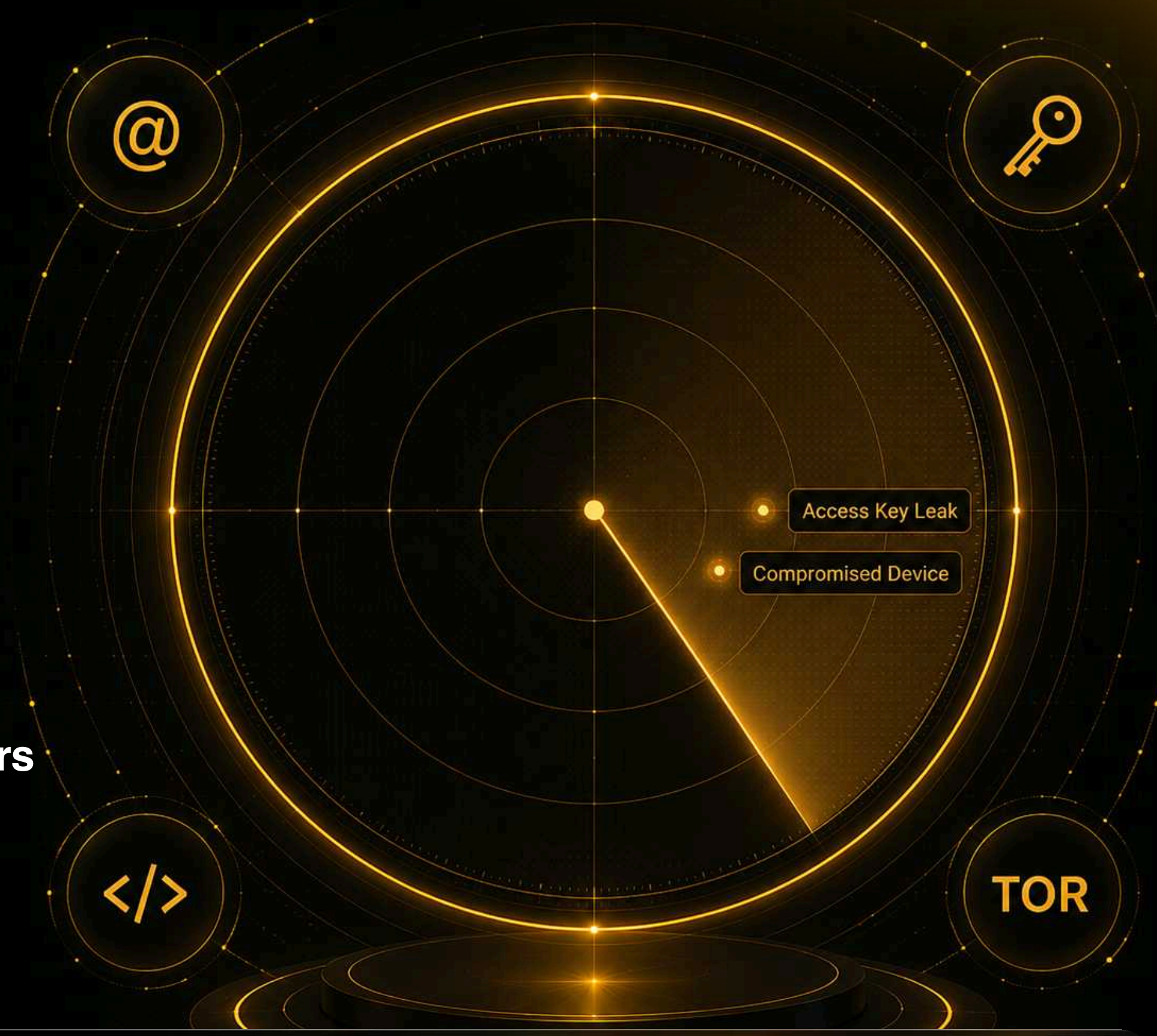


ADDRESS CREDENTIAL THEFT BEFORE LATERAL MOVEMENT BEGINS

DETECT STOLEN CREDENTIALS ON DAY ONE

Most organizations discover compromised credentials 240+ days after the theft. By then, attackers have already moved from compromised accounts into critical systems. **Passeca Signals continuously monitors darknet sources and infostealer data in real time, so you detect credential theft before the attackers move laterally.**



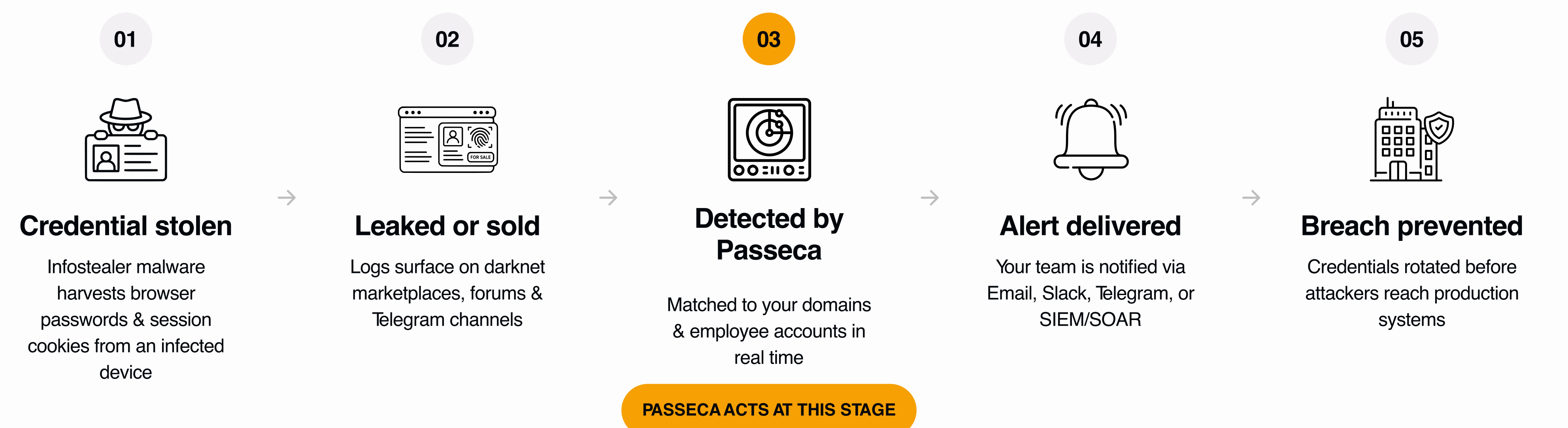
**#1**
Initial access vector in modern breach chains

**240+ Days**
Average dwell time before detection, industry-wide

**Hours**
Time to detection with Passeca Signals

**€67/mo**
Starting price — scales with your team

The attack chain passeca interrupts



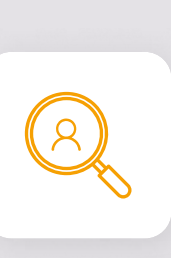
The intelligence gap

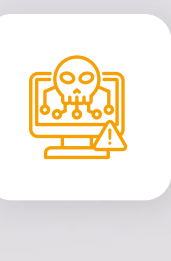
Attackers may already have access to your systems, APIs, and customer data — often for weeks before you find out. Most monitoring tools miss infostealer logs entirely and ignore the personal accounts employees use for work.

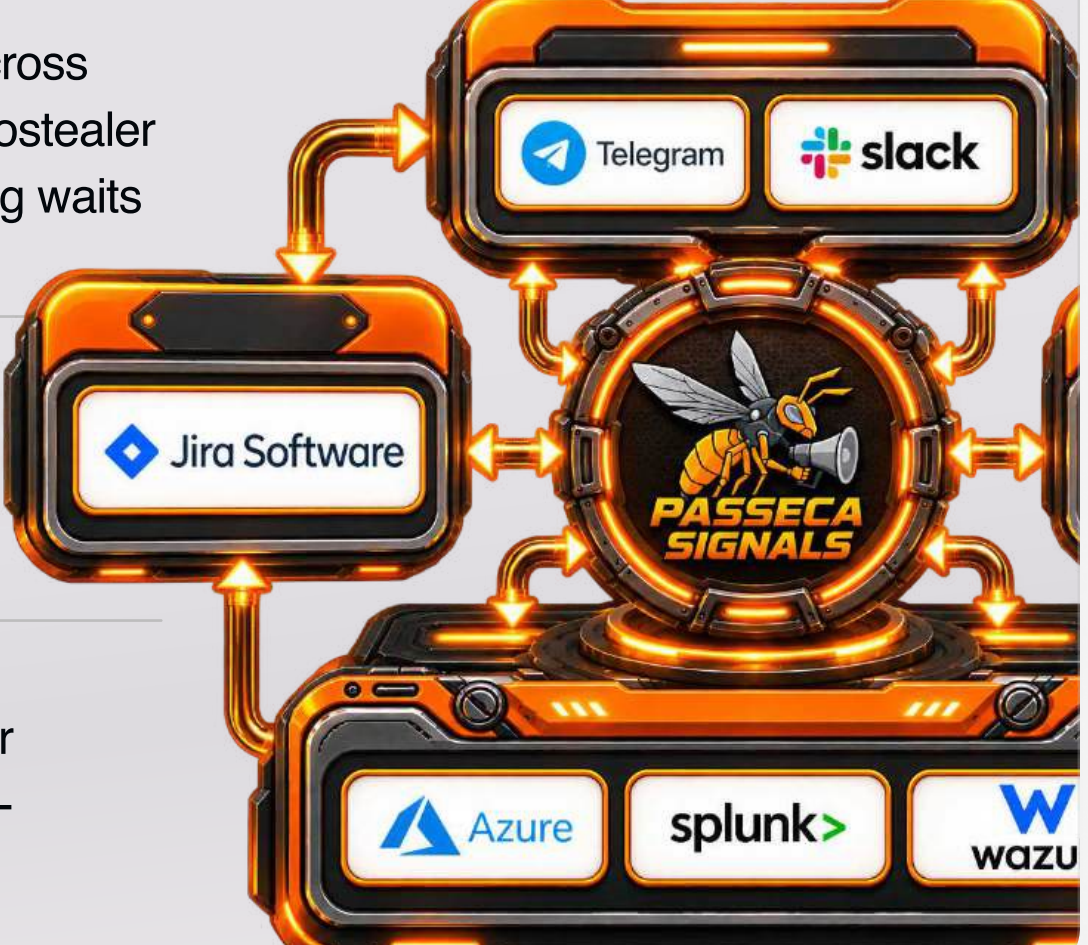
**Most organizations have hidden credential exposure that attackers are already exploiting.**

Passeca signals delivers

Continuous monitoring across darknet marketplaces, infostealer logs & Telegram — nothing waits for a scheduled scan

Employee personal-account visibility most tools miss entirely

Direct integration into your SIEM/SOAR and incident-response workflow



What you get with Passeca Signals

**Infostealer intelligence**

- Compromised credentials, browser passwords & session cookies
- Infected endpoints with timestamps, URLs, geolocation

**Identity threat intelligence at scale**

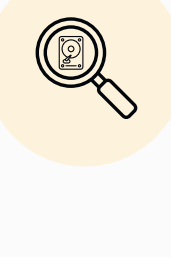
- Email/password pairs, tokens, identity & access records
- Marketplaces, cybercrime forums, Telegram, paste sites

**Exposure intelligence**

- Continuous protection for domains, emails, shadow IT
- Exposure scoring + credential-to-domain matching

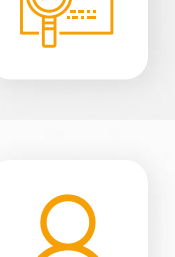
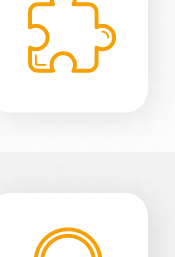
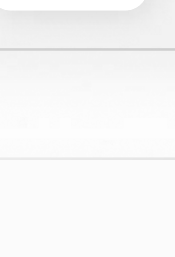
**Real-time alerts & integration**

- Email, Slack, Telegram notifications + RESTAPI for bulk retrieval
- Native SIEM/SOAR integrations — JSON, webhook, polling

**Investigation toolkit**

- Raw infostealer logs for forensic deep-dives + time-series risk data
- Optional analyst-supported investigation workflows

Why passeca signals stands apart

Feature	Signals TI	Generic monitoring
 Infostealer monitoring Breadth of sources covered	✓ Extensive	✗ Limited or none
 Raw infostealer logs Forensic-level visibility	✓ Full logs	✗ Summary only
 Private email credential monitoring Personal GitHub / DockerHub / cloud accounts	✓ Covered	✗ Missed entirely
 Real-time detection Time to alert	✓ Day one	✗ 7–30 day delay
 SIEM/SOAR ready Automation & workflow fit	✓ Native	✗ Manual
 Analyst support Deep-dive investigations	✓ Optional	✗ Self-service only

Passeca signals pricing

FOR END ORGANIZATIONS

- Starting from €67/month — scales with company size
- Custom pricing for 1,000+ employees

FOR MSPS & RESELLERS

- Unlimited API access — flat rate, unlimited domains, full raw data, reselling rights

Why compromising your cybersecurity is no longer a choice

- Infostealers remain the leading cause of initial access in modern breach chains
- Personal accounts are a blind spot most monitoring solutions miss entirely
- Waiting for a breach to confirm exposure is no longer a viable strategy
- Regulatory expectations are rising — NIS2, DORA, GDPR, SOC 2, and ISO 27001 increasingly expect organizations to detect credential exposure early and demonstrate effective security monitoring.



Where your organization is most exposed

**Devops & cloud teams**

Engineers use personal GitHub, DockerHub, OAuth/SSO, and AWS accounts — credentials get exposed on home machines, and attackers pivot to production.

Passeca detects: private-email credential leaks before lateral movement.

**Sensitive data access**

Employees sign up for SaaS tools — CRM, analytics, HR — on personal accounts, and session cookies get stolen, exposing company data.

Passeca detects: session hijacking & unmanaged SaaS account compromise.

**Supply chain risk**

Third-party vendors, contractors, and consultants use personal email to access corporate tools and systems.

Passeca detects: vendor account compromise & shadow IT exposure.

**Compliance support**

GDPR, SOC 2, and ISO 27001 require evidence of breach detection and timely response

Passeca detects: forensic evidence, automated alerts, compliance reporting.

WHERE IDENTITY THREAT INTELLIGENCE BECOMES ACTION.

01
Check your exposure
run a free, instant scan of your domain for exposed credentials.

02
Schedule a demo
see real-time detection in action with live darknet data.

03
Request a report
get statistics and samples of your domain exposure intelligence.

Check Your Exposure →

Schedule a Free Demo



info@passeca.com

signals.passeca.com

Passeca Signals — where identity threat intelligence becomes action