JUDGMENT Day by Alanata

Threat Intelligence pod kapotou

Zber dát z digitálneho podsvetia

Vysoká hra, kde analytici prenikajú hlboko do digitálneho podsvetia a riskujú svoje odhalenie.

Peter Kovalcik, Security Engineering Director CEE

Into the Darkness

> They don't wear capes. They don't save the world. They vanish into its shadows.

High-Risk Intelligence

Analysts who operate where others cannot go

Digital Ghosts

Creating personas that blend into criminal spaces

Behind Enemy Lines

Gathering intel without revealing true intentions

Internet Underground

Hidden Services

Not indexed by conventional search engines

Requires specialized browsers to access

Invite-Only Forums

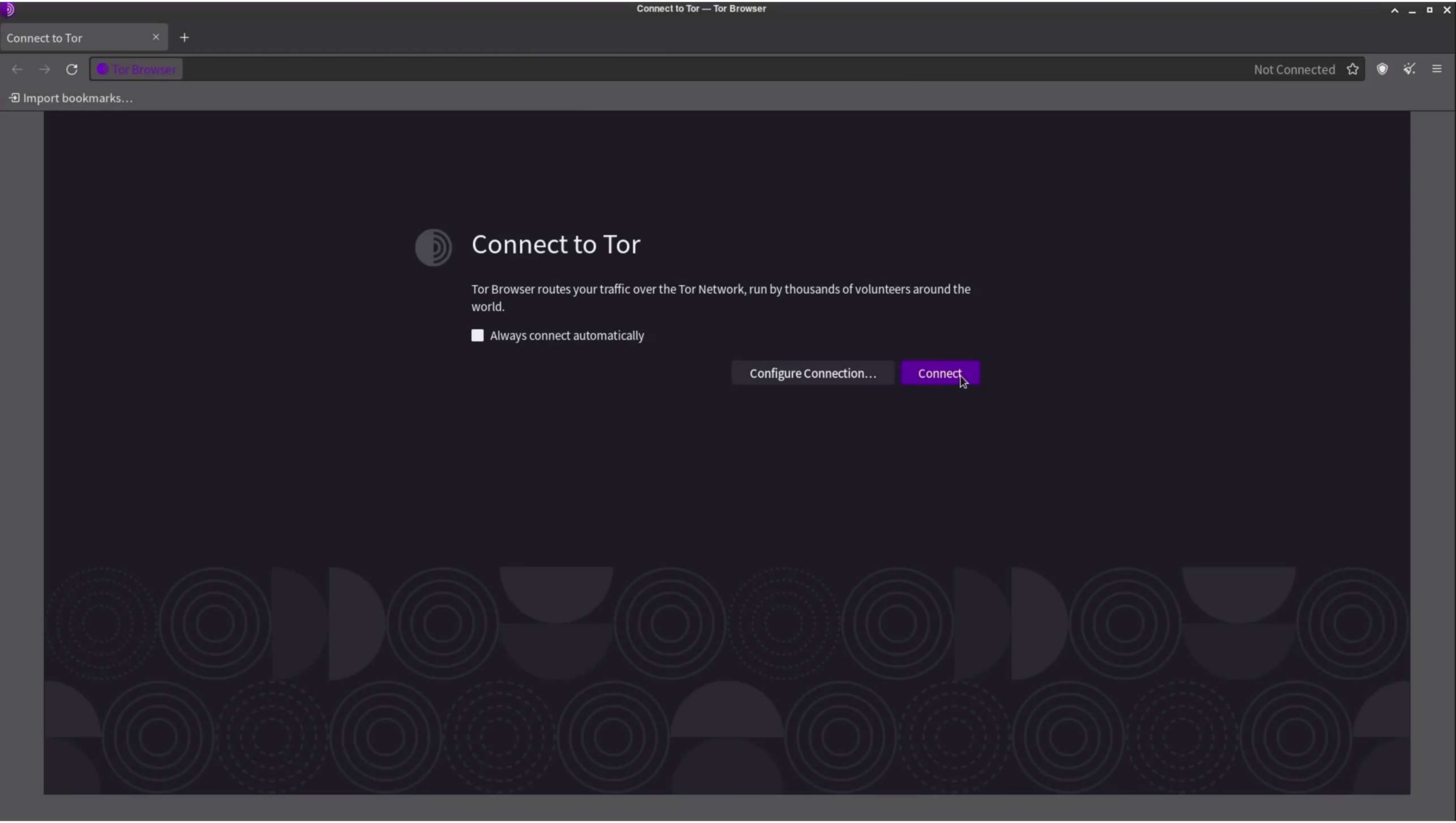
Restricted access through vetting

Multiple layers of authentication

Technical Limitations

Encryption blocks automated crawling

Constantly changing addresses



Connect to Tor

Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.

□ Always connect automatically

Building a Fake Identity

Choose a Specialization

Access broker, data trader, exploit developer

Create Backstory

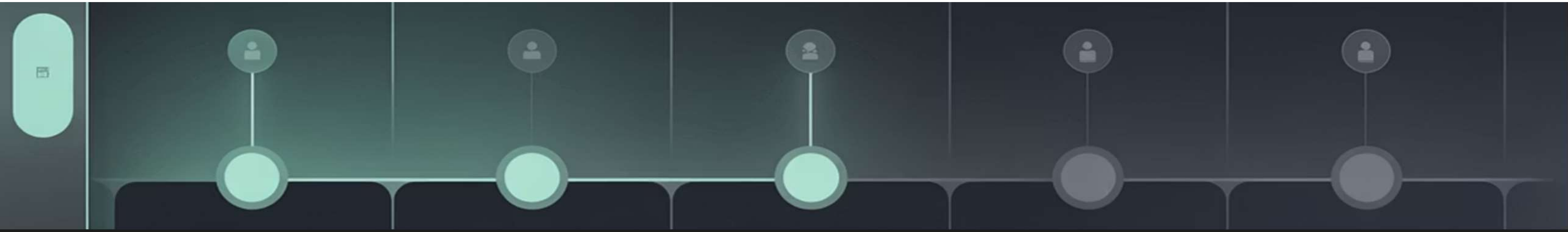
Believable history that can't be easily verified

Establish Credentials

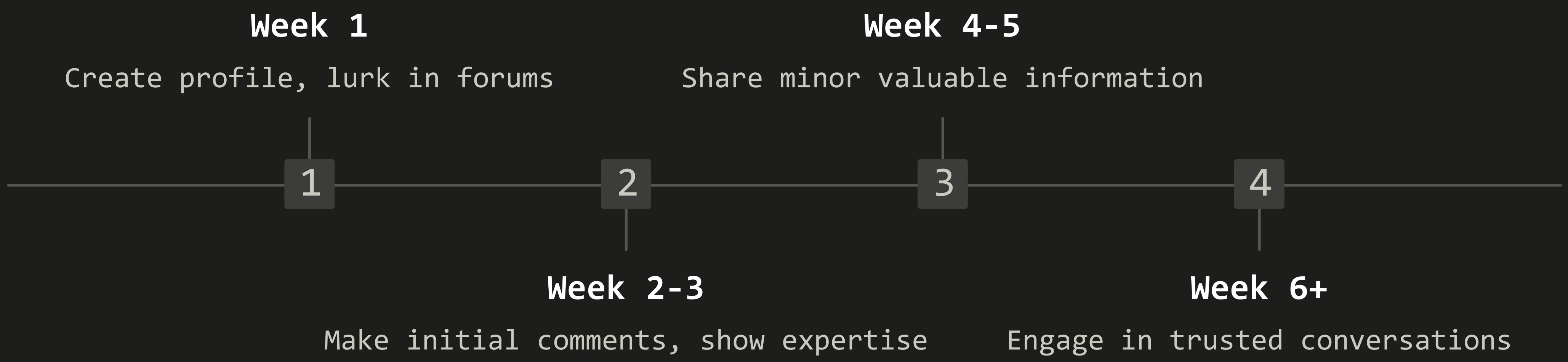
Start small, build reputation gradually

Maintain Character

Stay in persona at all times



Aging the Persona



1 **Week 1**

Create profile, lurk in forums

2 **Week 2-3**

Make initial comments, show expertise

3 **Week 4-5**

Share minor valuable information

4 **Week 6+**

Engage in trusted conversations

> Patience is your firewall.

Profile 1: The Data Leaker

Username: breachnotify777

Digital middleman offering corporate leaks to data buyers and media.

Formal, Aggressive Tone

"250GB dump from EU retail chain. Seeking serious buyers only."

Proof Strategy

Provides screenshots and small samples, never complete packages.

Cross-Forum Distribution

Posts across multiple platforms to establish reputation.

Brand Positioning

Signature: "I don't steal. I publish." Distances from acquisition.

Profile 2: The Access Broker

Username: netripper91

Forum Type: Hacking & RDP access forums (e.g., Exploit.in, XSS.is)

Former sysadmin who "got tired of the 9–5 life" and now sells RDP/VPN access for profit.

Language Style

Short, blunt, technical: "Selling"

Proof Strategy

Provides screenshots and small samples, never complete packages.

Cross-Forum Distribution

Posts across multiple platforms to establish reputation.

Brand Positioning

Signature: "I don't steal. I publish." Distances from acquisition.

Gaining Access Is an Art

Vouching

Build relationships with existing members

Leverage trust from one forum to another

Seeding Rumors

Plant information that generates interest

Create value that makes others seek you out

Offering Value

Share non-sensitive information to build credibility

Demonstrate skills without compromising position

Strategic Patience

Wait for invitations rather than forcing access

Accept minor setbacks as part of operation

How Threat Intel Platforms Operate

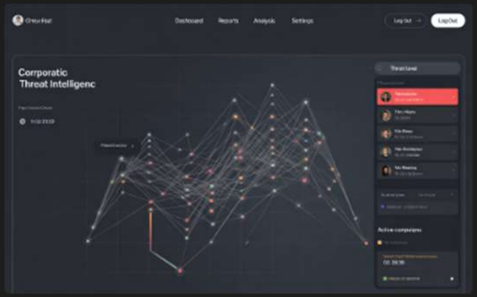
Human-led intelligence gathering, not just software automation

Crawl

Automated systems scan accessible areas of the dark web, collecting data from forums, marketplaces, and other digital spaces

Infiltrate

Human analysts access restricted spaces using specialized techniques and established personas

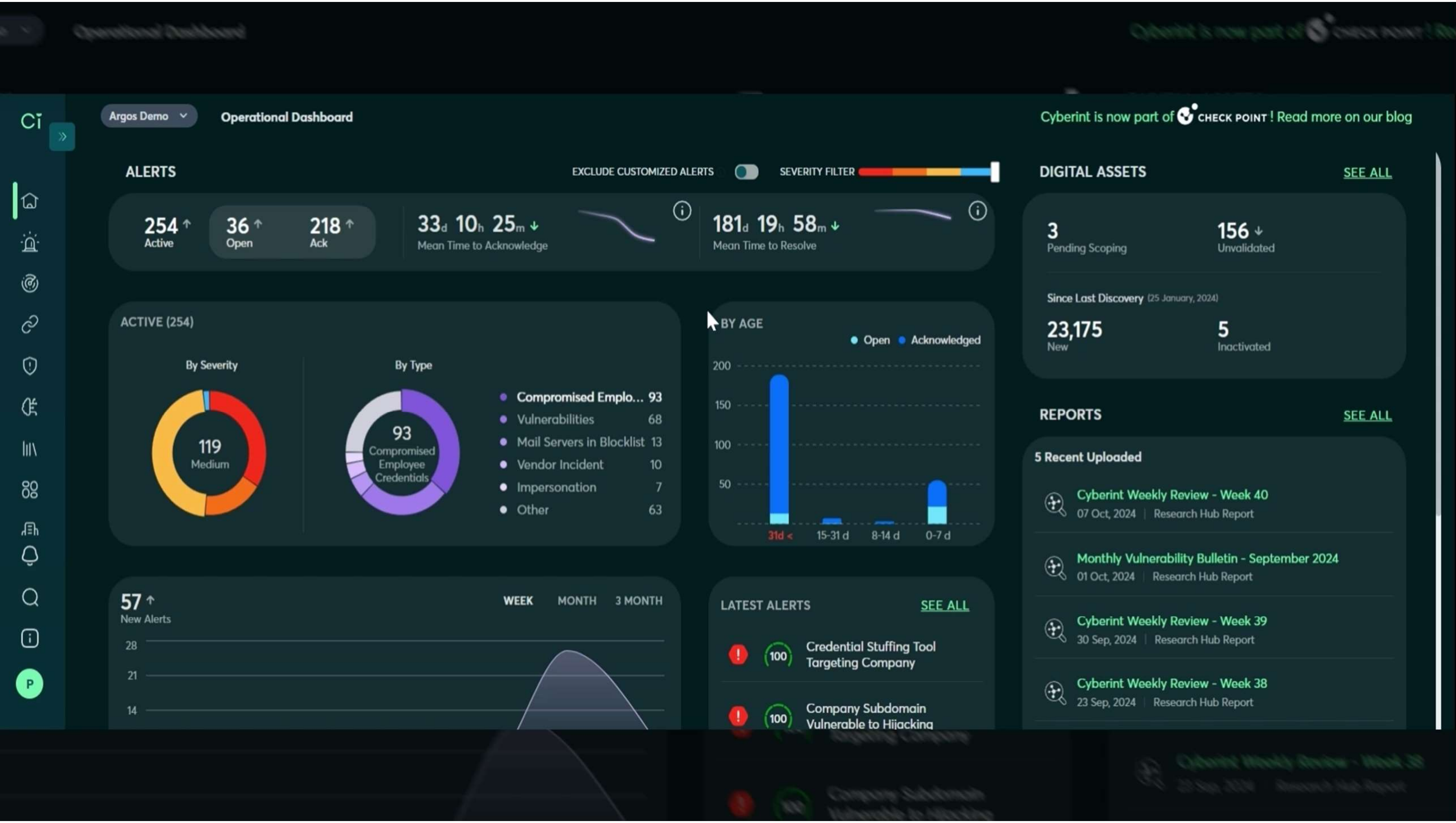


Analyze

Teams correlate findings with known threats, identifying patterns and potential risks to organizations

Alert

Platforms deliver actionable intelligence to clients, enabling proactive defense against emerging threats



Cyberint is now part of CHECK POINT ! Read more on our blog

ALERTS

EXCLUDE CUSTOMIZED ALERTS

SEVERITY FILTER

254 ↑ Active

36 ↑ Open

218 ↑ Ack

33d 10h 25m ↓ Mean Time to Acknowledge

181d 19h 58m ↓ Mean Time to Resolve

ACTIVE (254)

By Severity

119 Medium

By Type

93 Compromised Employee Credentials

● Compromised Emplo...	93
● Vulnerabilities	68
● Mail Servers in Blocklist	13
● Vendor Incident	10
● Impersonation	7
● Other	63

BY AGE

57 ↑ New Alerts

LATEST ALERTS

SEE ALL

! 100 Credential Stuffing Tool Targeting Company

! 100 Company Subdomain Vulnerable to Hijacking

DIGITAL ASSETS

SEE ALL

3 Pending Scoping

156 ↓ Unvalidated

Since Last Discovery (25 January, 2024)

23,175 New

5 Inactivated

REPORTS

SEE ALL

5 Recent Uploaded

Cyberint Weekly Review - Week 40
07 Oct, 2024 | Research Hub Report

Monthly Vulnerability Bulletin - September 2024
01 Oct, 2024 | Research Hub Report

Cyberint Weekly Review - Week 39
30 Sep, 2024 | Research Hub Report

Cyberint Weekly Review - Week 38
23 Sep, 2024 | Research Hub Report

Mistakes That Burn You

Timing Errors

Posting too frequently or at wrong hours

Language Tells

Using wrong slang or outdated terminology

Behavioral Patterns

Inconsistent actions raising suspicion

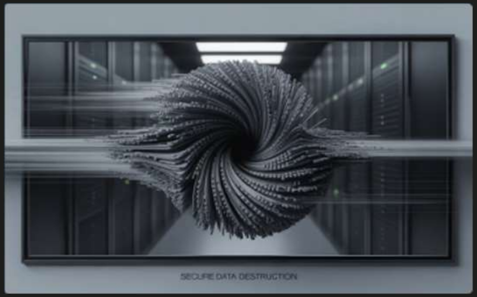
Technical Leakage

VPN failures revealing true location

Emergency Burner Shutdown

Immediate Disconnect

Halt all operations instantly



Destroy All Traces

Delete credentials and conversation logs

Rotate to Backup

Switch to secondary persona if available

Vanish Without Drama

No explanations or goodbyes

To Summarize

Before the Breach Comes the Whisper

The most dangerous threats don't knock.

They whisper your name... in places you've never seen.

Hidden Forums

Malicious actors plan attacks beyond your visibility.

Identity Compromise

Your organization's weaknesses are being quietly cataloged.

Silent Infiltration

By the time you detect them, they've already been inside.