



External Risk Management: взгляд на компанию глазами злоумышленника

April, 2025

German Khokhlov

SE Team Lead



5,414 Ransomware Attacks Accrued in 2025

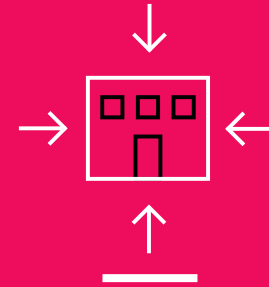
Top 3 Attack Vectors



Stolen Credentials & Identity
Theft



Phishing Websites
and Social
Impersonation



Vulnerable External
Facing Assets

Security Operations Team Challenges

Enterprises Need a Comprehensive Risk Management Platform

45

Security Tools
Used in
the Average
Enterprise

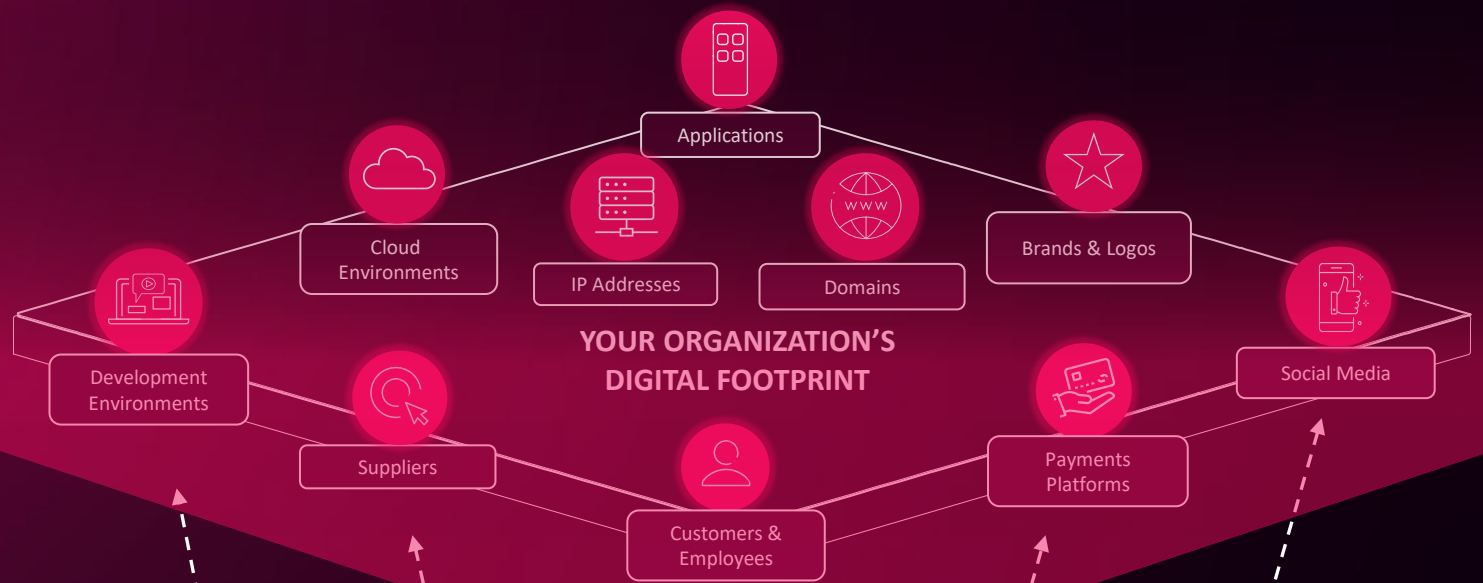
25%

of time wasted
chasing false
positives

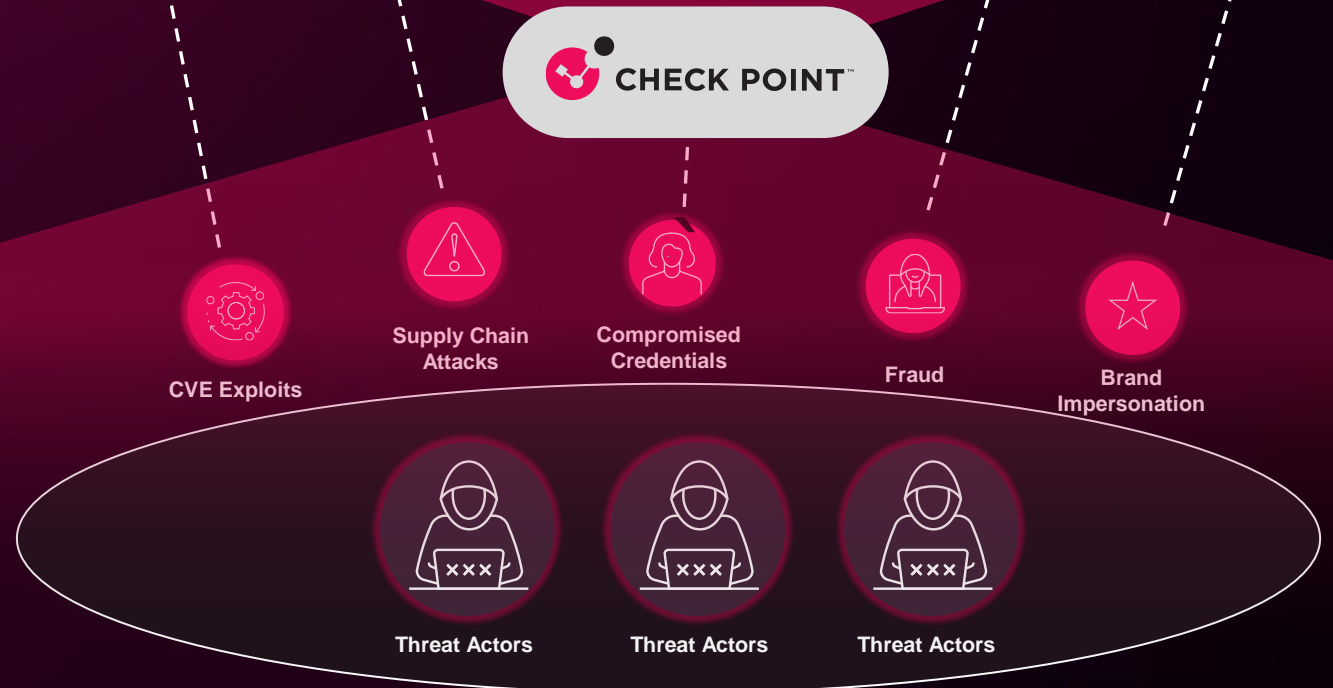
70%

of security teams
lack staff to be
effective

**WHAT ASSETS DO YOU
NEED TO PROTECT?**



**WHAT RISKS DOES YOUR
ORGANIZATION FACE?**



Comprehensive External Risk Management Solution

Attack Surface Monitoring

- Shadow IT & Asset Discovery
- Vulnerabilities & Exposure Detection
- Active Exposure Validation

Global Threat Intelligence

- Ransomware watch & Threat landscape
- Enriched IoC Feeds
- Intelligence Knowledgebase

Targeted Threat Intelligence

- Dark web Monitoring & Actor Chatter
- Credentials and Account Takeover
- Fraud & Data leakage

Brand Protection & Impersonation

- Brand & Phishing Protection
- Social Media Impersonation
- Mobile App Impersonation

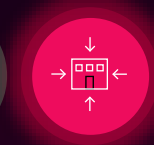
Supply Chain Intelligence

- Vendors & Technology Detection
- 3rd party Risk Management
- Alerting on Critical Risks and Breaches

Remediation

Expert Threat Intelligence Services

Example 2: Vulnerable Assets Remediation



Detection

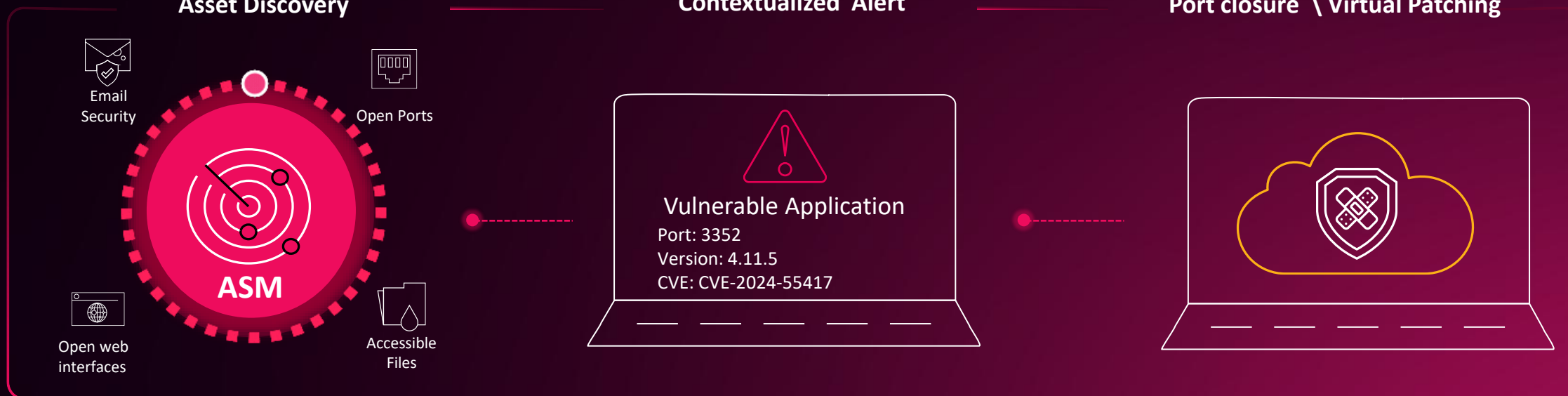
Impactfulness

Remediation

Asset Discovery

Contextualized Alert

Port closure \ Virtual Patching



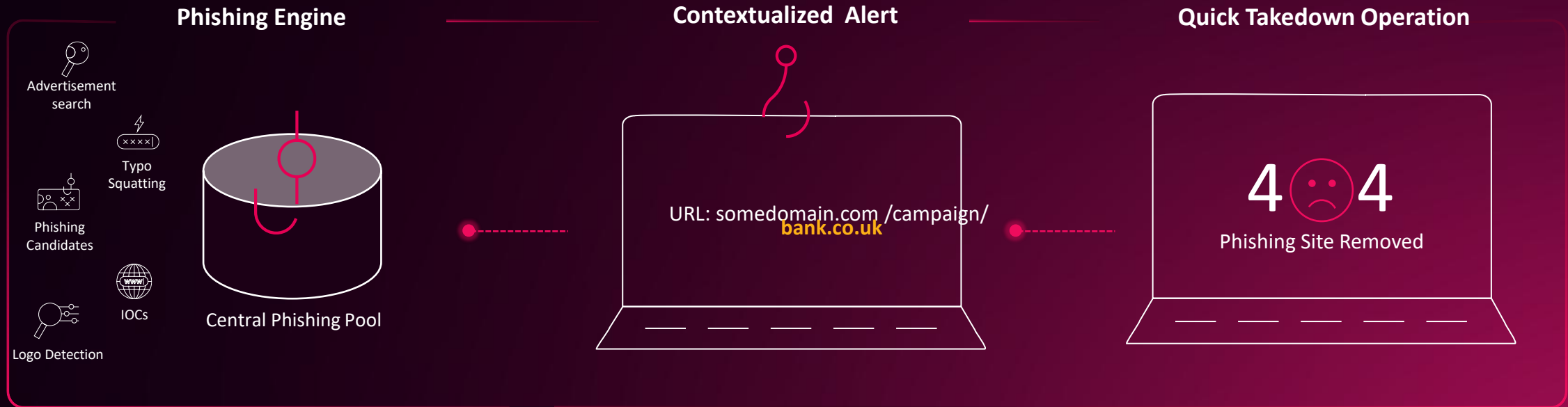
Example 3: Phishing Sites Takedown



Detection

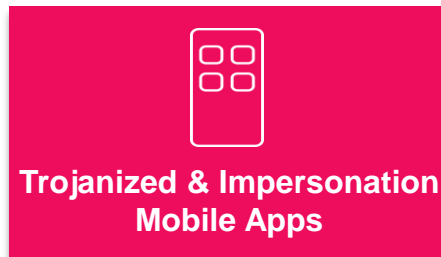
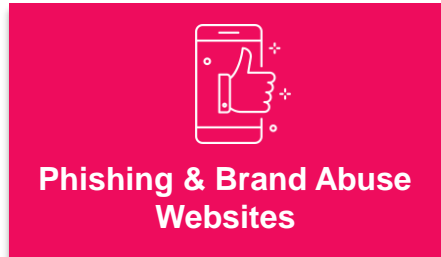
Impactfulness

Remediation



Fast and Effective Remediation and Takedowns

Malicious Content Takes Many Forms



Industry-Leading Takedown Services



Key Benefits

Add services offering based on Check Point teams of experts
Reduce the probability of account takeover and costly fraudulent activity
Protect your customer's organization from impersonation attacks that damage their brand

3 Layers Intelligence Managed Services From Expert



- Strategic threat reports
 - CVE & malware analysis
 - Ransomware & APT tracking
- Dedicated Cyber Threat Intelligence analyst
 - Deep triage & enrichment
 - Industry & regional expertise
 - Virtual Humint Operation
- Continuous triaging for defined use case
 - 1st level intelligence support
 - Customer technical support
 - Takedown Operations

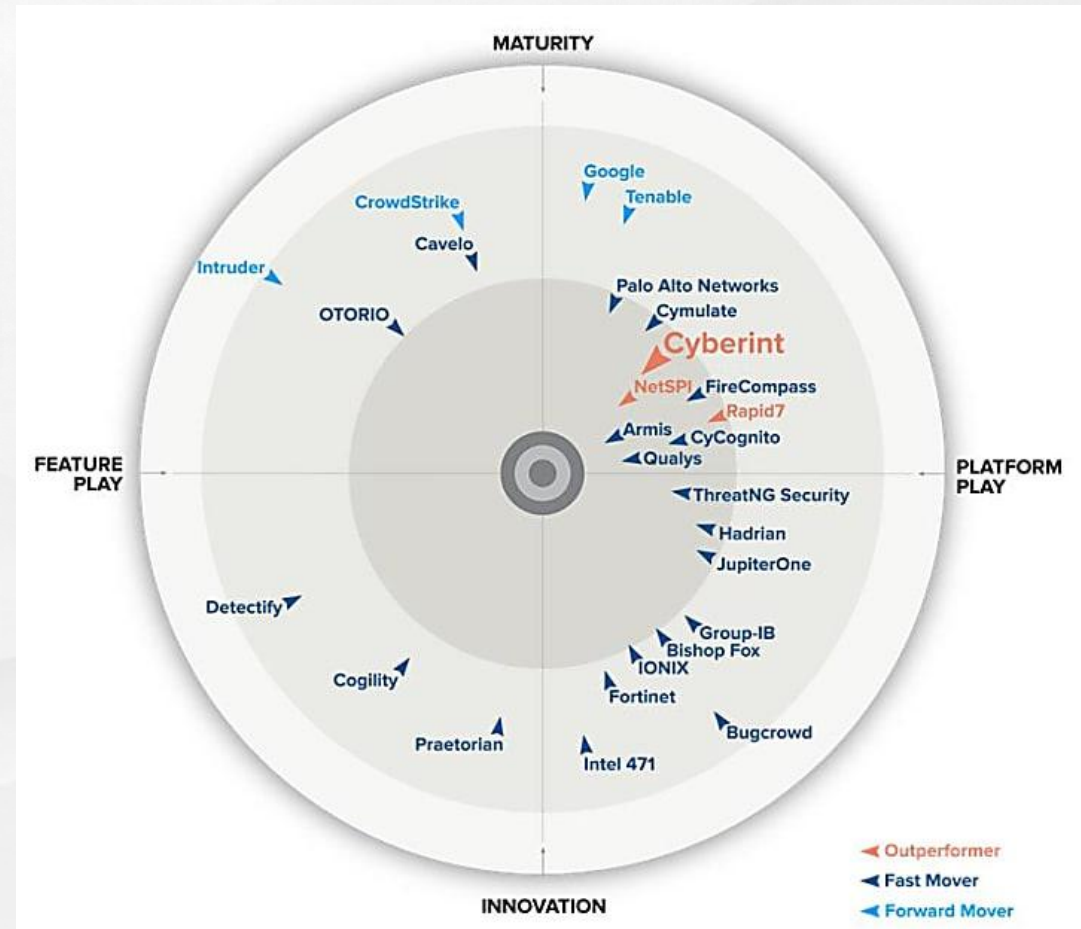
Recognition As an Industry Leader

By Industry Analysts



<https://www.g2.com/products/argos-threat-intelligence-platform/reviews>

GigaOm Report 2025 (ASM)





CHECK POINT™

Cyberint
A Check Point Company

PRODUCT DEMO



Attack Surface Monitoring > Assets

ASSETS

EXPOSURE ITEMS

TECHNOLOGIES

CERTIFICATES

QUANTUM

DISCOVERY

9 ASM Assets

2 TI Assets

B

Posture Score
Recalculate

Categories Contributing to Posture Score



Vulnerabilities 89%
Misconfigurations 5.6%
Exposed Interfaces 5.6%
Cloud Storage 0%

Exposed Ports 0%
Hijackable Subdomains 0%
Untrustworthy Server Activities 0%

Risk Reduction by Asset Severity



Very High 1
High 1
Medium 0
Low 0

Scoping Management

- Validate Primary Assets (1)
- Decide on ASM Monitoring for Assets (0)
- Decide on TI Monitoring for Domains (0)

Assets by Status



Monitored 9
Pending Decision 0
Not Monitored 0
Unvalidated 1

9 ASSETS / out of 10

Clear Filters

Search Asset Name

Status: Monitored (ASM) Monitored (ASM + TI)

ASSET	ASSET SEVERITY	ACTIVE ALERTS	EXPOSURE ITEMS	DISCOVERY INFO	PARENT ASSETS	DISCOVERY DATE	PARKED
<input type="checkbox"/> ci-proxy.azure-api.net DOMAIN Monitored (ASM)	Very High	4 alerts	5 items	100% MANUAL	N/A	Jan 14, 2025 18:09	N
<input type="checkbox"/> 20.217.212.161 IP ADDRESS Monitored (ASM)	High	2 alerts	4 items	100% MANUAL	N/A	Jan 12, 2025 11:48	N
<input type="checkbox"/> portal.site.io SUBDOMAIN Monitored (ASM)	Medium	0 alerts	3 items	100% MANUAL	N/A	Jan 14, 2025 17:17	N
<input type="checkbox"/> demo.example.net SUBDOMAIN Monitored (ASM)	Medium	0 alerts	1 items	100% MANUAL	N/A	Jan 14, 2025 17:17	N
<input type="checkbox"/> jenkins.acme.com SUBDOMAIN Monitored (ASM)	Medium	0 alerts	1 items	100% MANUAL	N/A	Jan 14, 2025 17:16	N
<input type="checkbox"/> test.example.org SUBDOMAIN Monitored (ASM)	Medium	0 alerts	1 items	100% MANUAL	N/A	Jan 14, 2025 17:16	N

Attack Surface Monitoring > ...

















- ASSETS
- EXPOSURE ITEMS
- TECHNOLOGIES
- CERTIFICATES
- QUANTUM

DISCOVERY

9 ASM Assets ⓘ

2 TI Assets ⓘ

14 EXPOSURE ITEMS / out of 14

ASSET NAME	PORT	INTERFACE	SEVERITY ↓	URL	GATEWAY ⓘ	EXPLOITABLE VULNERABILITIES	ASSET TYPE	FIRST SEEN
ci-proxy.azure-api.net	80	pyLoad		http://ci-proxy.azure-api.net/login?nex...	GW82 IP: 51.4.42.88 IPS: Enabled	2	 DOMAIN	Jan 14, 2025 18:
ci-proxy.azure-api.net	443	pyLoad		https://ci-proxy.azure-api.net/login?ne...	GW82 IP: 51.4.42.88 IPS: Enabled	2	 DOMAIN	Jan 14, 2025 18:
jenkins.acme.com	80	Jenkins		http://jenkins.acme.com	ARGENTINA-GW IP: 51.14.41.2 IPS: Enabled	1	 SUBDOMAIN	Jan 14, 2025 16:
www.site.io	443	Jira		https://www.site.io/jira/software		4	 DOMAIN	Jan 13, 2025 09:
www.acme.com	443	Jira		https://www.acme.com/login		4	 DOMAIN	Jan 13, 2025 09:
test.example.org	8080	Jira		--	BRAZIL-GW IP: 51.14.41.1 IPS: Enabled	2	 SUBDOMAIN	Jan 12, 2025 17:
20.217.212.161	80	pyLoad		http://20.217.212.161/login?next=true	gw82n IP: 51.4.42.88 IPS: Enabled	2	 IP	Jan 13, 2025 12:
20.217.212.161	443	pyLoad		https://20.217.212.161/login?next=true/	gw82n IP: 51.4.42.88 IPS: Enabled	2	 IP	Jan 13, 2025 09:

Attack Surface Monitoring > ...

- ASSETS
- EXPOSURE ITEMS
- TECHNOLOGIES
- CERTIFICATES
- QUANTUM

DISCOVERY

















9 ASM Assets ⓘ

2 TI Assets ⓘ

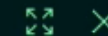
200

30

14 EXPOSURE ITEMS / out of 14

ASSET NAME	PORT	INTERFACE	SEVERITY ↓	URL	GATEWAY ⓘ	EXPLOITABLE VULNERABILITIES	ASSET TYPE	FIRST SEEN
ci-proxy.azure-api.net	80	pyLoad		http://ci-proxy.azure-api.net/login?nex...	GW82 IP: 51.4.42.88 IPS: Enabled	2	 DOMAIN	Jan 14, 2025 18:
ci-proxy.azure-api.net	443	pyLoad		https://ci-proxy.azure-api.net/login?ne...	GW82 IP: 51.4.42.88 IPS: Enabled	2	 DOMAIN	Jan 14, 2025 18:
jenkins.acme.com	80	Jenkins		http://jenkins.acme.com	ARGENTINA-GW IP: 51.14.41.2 IPS: Enabled	1	 SUBDOMAIN	Jan 14, 2025 16:
www.site.io	443	Jira		https://www.site.io/jira/software		4	 DOMAIN	Jan 13, 2025 09:
www.acme.com	443	Jira		https://www.acme.com/login		4	 DOMAIN	Jan 13, 2025 09:
test.example.org	8080	Jira		--	BRAZIL-GW IP: 51.14.41.1 IPS: Enabled	2	 SUBDOMAIN	Jan 12, 2025 17:
20.217.212.161	80	pyLoad		http://20.217.212.161/login?next=true	gw82n IP: 51.4.42.88 IPS: Enabled	2	 IP	Jan 13, 2025 12:
20.217.212.161	443	pyLoad		https://20.217.212.161/login?next=true/	gw82n IP: 51.4.42.88 IPS: Enabled	2	 IP	Jan 13, 2025 09:

ASM > Inventory > CPX



ci-proxy.azure-api.net | Domain | ID:48728156 | No Description

Monitored (ASM)

4

Posture Alerts

DISCOVERY ORIGIN

ci-proxy.azure-api.net | Domain

DESCENDANTS

0

DIRECT CHILDREN

0

QUANTUM GATEWAY

Name: GW82 | IP: 51.4.42.88 | IPS: Enabled | Destination IP: 172.16.2.5

Risk

Discovery Details

Exposure Items (5)

Mail Servers In Blocklist (0)

Email Security (0)

Exposed Web Interfaces (2)

Certificate Authority (1)

SSL/TLS (2)

Technologies (5)

Certificates (0)

Status History

4

SECURITY POSTURE ALERTS

0

TARGET LEVEL ALERTS

0

DATA EXPOSURE ALERTS

Security Posture Alerts (4)


SEE ALL

TITLE	ALERT ID	SEVERITY	CONFIDENCE	CREATED DATE
Exploitable Vulnerability Found On Company Asset	CPX-7		90	January 14, 25
Vulnerable Technology Detected On Exposed Compa...	CPX-9		90	January 15, 25
Missing Company Domain CAA Records Detected	CPX-5		90	January 14, 25
Exposed Company Web Interface	CPX-3		80	January 14, 25



Username

Password

 SIGN IN


Exploitable Vulnerability found on a Company Asset

Category: Vulnerabilities | Type: Vulnerabilities
Last content update: Jan 15, 2025 17:31:12, Severity Changed


Apply IPS Protection

ID: CPX-7 | Created: Jan 14, 2025 22:48:05

ALERT STATUS




Open Jan 14, 2025
By system



Acknowledged

Set



Closed

Set

DISCUSSION BOARD (0) NOTES (0)

Cyberint Support
Analyst



No comments have been added yet

 Type a comment

SEVERITY
 Very High

CONFIDENCE
90

TAGS | Add Tags +
None

CVE	ASSET	PORTS	TECHNOLOGY	VERSION	VENDOR
CVE-2024-21644 7.8 ⓘ	ci-proxy.azure-api.net	443	pyload	*	pyload

QUANTUM GATEWAY	AVAILABLE IPS PROTECTION
GW82	pyLoad Information Disclosure (CVE-2024-21644) (Inactive)

CONFIDENCE REASON	TARGETED VECTOR	SOURCE CATEGORY
Detected by Active Exposure Validation	Business	Attack Surface Monitoring

Argos Active Vulnerability Scan has detected and exploitable vulnerability on an exposed company asset. Evidence supporting this exploitability is detailed in the section below.

pyLoad is the free and open-source Download Manager written in pure Python. Any unauthenticated user can browse to a specific URL to expose the Flask config, including the 'SECRET_KEY' variable. This issue has been patched in version 0.5.0b3.dev77.

Security vulnerabilities are flaws in a software product that can be exploited to compromise an application or system. Active exploits aim to disrupt performance, steal data, and hijack computer resources, putting accessible systems and assets at risk.

RECOMMENDATIONS

Patching exploitable vulnerabilities should be prioritized.

The remediation process should encompass at least one of the following actions: (i) Implement the vendor's patches. In many instances, this will involve the deployment of a patch or an

Establishing Vulnerability Based on a Company Asset

Quantum Gateway: GW82

Apply IPS Protection



Apply IPS Protection

The IPS protection *pyLoad Information Disclosure (CVE-2024-21644)* will be applied on your Quantum Gateway: **GW82**.

The operation may take a few minutes to complete. Click "Apply" to confirm.

Apply

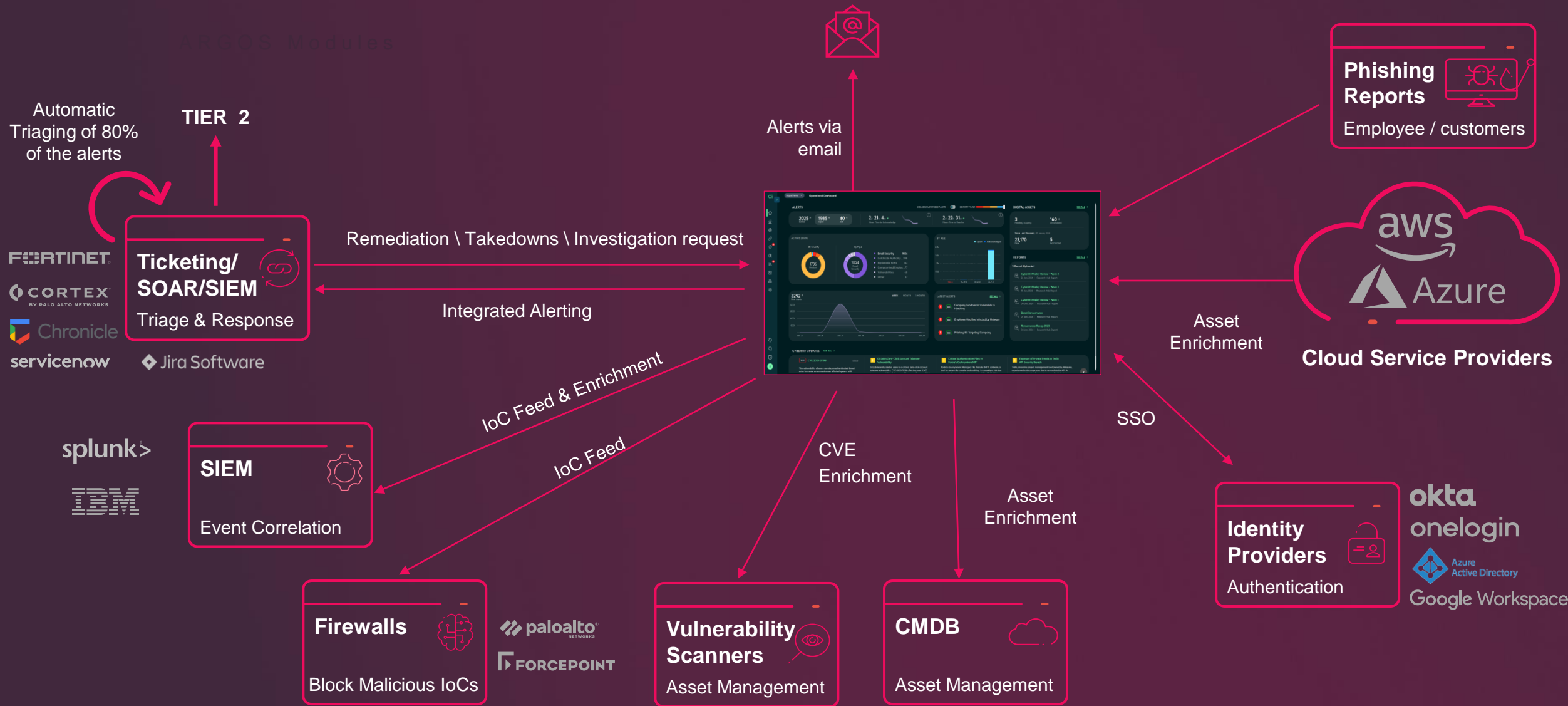
[Cancel](#)

Recommendations

Recommendation 1: Update the IPS protection rules to the latest version.

Recommendation 2: Enable the IPS protection on the Quantum Gateway.

ERM Unified & Impactful End To End Approach





Thank You