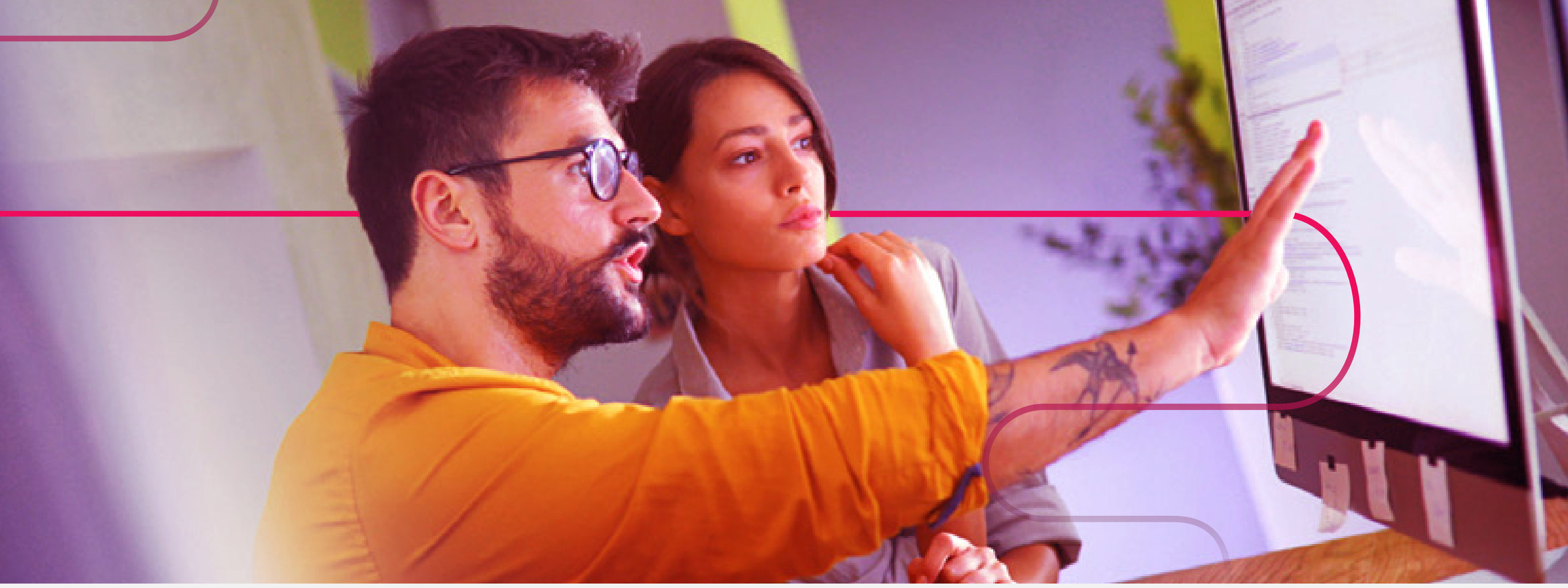
Cyberint
A Check Point Company

IMPACTFUL INTELLIGENCE OFFERING FOR MSSPs

January 2025

TABLE OF CONTENTS



1. INTRODUCTION

1.1 EXECUTIVE SUMMARY

Cyberint, a Check Point company, supports leading organizations worldwide to address their changing and growing needs for external risk identification and mitigation. As an innovative player within the cybersecurity space, Cyberint brings a unique combination of leading technology, a team of highly skilled cyber experts, and a strong focus on multiple industries.

Leveraging a unique combination of technologies, Cyberint provides external cyber risk management capabilities that tailor impactful intelligence to your attack surface. These advanced technologies are combined with highly experienced threat intelligence analysts, allowing Cyberint to offer a fresh approach to address the following challenges:

- Determine which relevant threats should be considered in order to design an effective cybersecurity defense architecture.
- Illustrate the updated cyber risk status to the board and management, as well as an action plan.
- Acquire predictive intelligence to identify intent, techniques, and tools to mitigate targeted threats before they materialize.
- Continuously monitor digital risk exposures that can be exploited by cybercriminals.
- Detect breaches as they propagate outside the organization's perimeter.
- Gain visibility into attacks targeting your brand and customers that are constantly evolving outside of your network.

We would like to thank you for giving us the opportunity to compete for your business and look forward to continuing our discussion.

1.2 ABOUT CYBERINT & IMPACTFUL INTELLIGENCE

Impactful Intelligence is defined by the following 4 dimensions:

- **Accuracy** –the intel is accurate and has very few false positives.
- **Relevance** – the threat impacts the organization, and the intel is delivered in a timely manner.
- **Actionability** – There is something the organization can do about the threat.
- **Cost effective remediation** – The cost of the unmitigated risk is higher than the cost of detection and mitigation.

Cyberint addresses the advanced external threats with a multi-tiered approach:

Proactive detection:

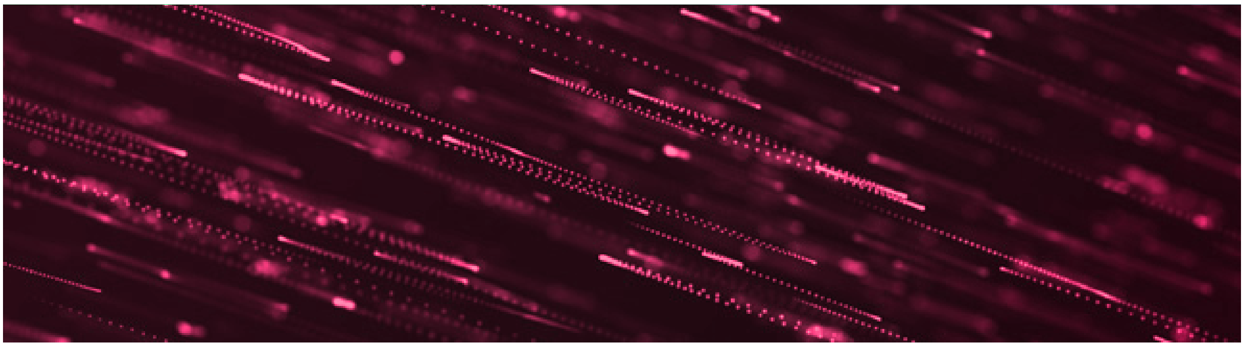
- Continuously discover the organization's external attack surface using the Cyberint ASM module to identify all the organization's Internet-facing assets and track any vulnerabilities and/or misconfigurations.
- Extract targeted threat intelligence by identifying mentions of the organization or its assets within the coverage of a plethora of sources from the open, deep and dark web, aimed at providing an early warning to an imminent risk.
- Identify the organization's suppliers and partners and monitor the associated risks.

Quick remediation:

- Real-time monitoring of unstructured data, allowing quick detection and faster response to these cyber challenges through execution of automated and managed counteractions against external malicious assets (phishing sites, phishing kits, spammers, breach evidence, etc.) to accelerate remediation.

What our customers say about Cyberint

Cyberint focuses on its customer superior experience. Some of the feedback could be reviewed in "Gartner Peer Insights" and G2 Reviews.



2. CYBERINT MANAGEMENT MSSP OFFERING

2.1 CYBERINT DEMO ENVIRONMENT (NON-COMMERCIAL USAGE)

2.1.1 CYBERINT DEMO ENVIRONMENT SCOPE

Required purchasing of Checkpoint SQU - MSSP ***ERM Program - CP-ERM-MSSP***.

In order to support the marketing of the solution to prospective customers, Cyberint comes with a demo environment which can be accessed in order to demonstrate the full capabilities of Cyberint and how it could be leveraged to handle different digital business risks.

The demo environment is equipped with the majority of Cyberint's capabilities and should be used in a non-commercial way by trained professionals.

The demo environment includes 2 tenants with the following configuration:

1. **'Vanilla' demo tenant** – An environment with a pre-existing and pre-configured demo story which presents the capabilities with a prebuilt, maintained demo story which could be presented as-is to demonstrate the full value to the customer.

2. **Ad hoc demo tenant** - Ability to analyze intelligence and execute Cyberint capabilities with relation to a specific prospect, making it possible to hold a meeting with a prospect demonstrating findings related to their organization.

The scope of the demo \ POC tenants includes:

Item	Quantity	Comments
Cyberint Tenant for demonstration and POCs	Included	• Alerts center and dashboards • Intelligence raw data access • ASM module • Phishing and Lookalike Domains module • Social media impersonation module • Report Section
Cyberint system users	2	Additional credits can be coordinated with your Cyberint representative.
Maximum number of credits for the tenant	150	Additional credits can be coordinated with your Cyberint representative.
Threat Landscape reports feed	Included	
Support	Included	Business hours
Collection time	2 weeks	Unless agreed otherwise with your Cyberint representative

The demo environment cannot be used for commercial activities and should only be used in marketing and presale activities.

2.1.2 USERS PREREQUISITES:

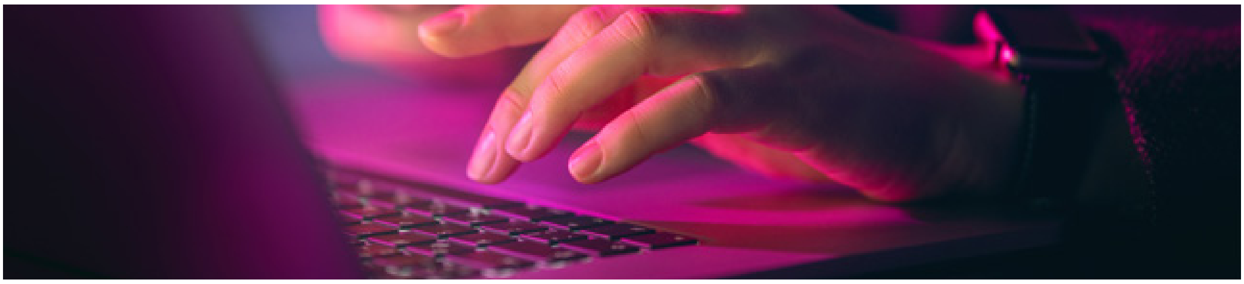
In order to use the Cyberint Demo system, the following prerequisites are required:

- Users with a technical background (presales or analysts)
- Users must complete the Cyberint training and certification process

2.1.3 DEMO ENVIRONMENT TERMS AND CONDITIONS

Subject to the consideration, terms and conditions specified herein and the Parties executing this Proposal:

- The Cyberint team will create and maintain the Demo System for the MSSP.
- The MSSP will be granted the right to operate and use the Demo System during the period of the contract.
- The Demo System is provided with a sample of demo data, which is provided "AS IS". As such, the Cyberint team does not warrant or guarantee the accuracy, availability or completeness of this information.
- For avoidance of doubt, the Demo System may be used by the MSSP solely for demo and **non-commercial purposes**. Without derogating from the generality of the above, the MSSP may not charge a potential customer in connection to the usage of the Demo System without receiving specific approval.
- Cyberint reserves the right to immediately terminate the access permissions to the Demo System granted the MSSP at any time in case of a breach by the MSSP of the terms specified herein and/or in the Agreement, all without derogating from any other and/or additional right and/or remedy Cyberint is and/or may be entitled to under the Agreement and/or the law.
- Access to the Demo System may be monitored periodically by Cyberint. Use of the Demo System constitutes consent to such monitoring. In addition, any information submitted by the MSSP to the Demo System is considered non confidential.
- As stated in the Agreement with respect to Cyberint services, the MSSP also acknowledges and agrees that all Intellectual Property Rights in and to the Demo System and/or related and/or connected thereto and any development thereof is and shall be at all times at the sole exclusive ownership of Cyberint.



2.2 CYBERINT MSSP CREDITS AND ASSETS

Credits are purchased through Check Point SQU MSSP Cyberint Edge platform
CP-ERM-MSSP-CREDITS-LVLX-Y

MSSP licensing is based on credit model, which provides flexible coverage for all organizations with different needs and coverage plans.

2.2.1 TENANT CONFIGURATION

Tenant is a specific instance of Cyberint which is tuned external risk coverage for a single organization. Each tenant includes configuration of:

- Users
- Assets
- Functionalities and modules

2.2.2 ASSETS CONFIGURATION & ASSIGNED COVERAGE PER ASSET

Cyberint support different asset types as input for the collection and risk analysis (domain, brand, keyword, person, etc.).

Each asset can consume a different number of credits, depending on the type of coverage needed for these assets.

There are 3 types of possible coverages:

Type	Description	Used credits	Assets example
ASM	Assets with ASM coverage utilizes Cyberint ASM engine to discover assets and identify posture risk in vulnerable interfaces, technologies with risky CVEs, ports, certificates and more	2	Domain IP
Threat Intelligence	Assets with Threat Intelligence (TI) coverage are checked against a database of intelligence collected from the open, deep and dark web for different risks, such as credentials, data leakage and fraud.	2	Domain Brand BIN number VIP
Digital Risk Protection	Assets with DRP coverage are being checked against phishing attempts, social media impersonation, and brand abuse in different platforms.	4	Brand VIP Domain Mobile App

Assets can use one or more of the above coverages, the actual credits used will be calculated accordingly.

For example:

- Domain which is used as a main domain of a company (i.e. used as the domain for the email address, company website and its main brand) would be configured for coverage of both ASM, Threat intelligence and Digital Risk protection.
  Example: www.company.com

- Domain which is used as a secondary domain with only web interface exposed but no associated email address would require only ASM coverage:
  Example: www.company.io

The below table summarizes the maximum credit that can be utilized for coverage of different assets types. Note all assets can be used for all types of coverages:

Asset	ASM	Threat Intelligences	DRP	Max Total Credits
Domain	Can be Enabled	Can be Enabled	Can be Enabled	8
IP address (range)	Can be Enabled			2
Subdomain	Can be Enabled			2
Cloud storage	Can be Enabled			2
Brand, company		Can be Enabled	Can be Enabled	6
BIN		Can be Enabled		8
Keyword		Can be Enabled		2
Person		Can be Enabled	Can be Enabled	6
Email		Can be Enabled		2
Mobile App			Can be Enabled	4
Sensitive Code Identifier		Can be Enabled		2
Employee Login Interface		Can be Enabled		2

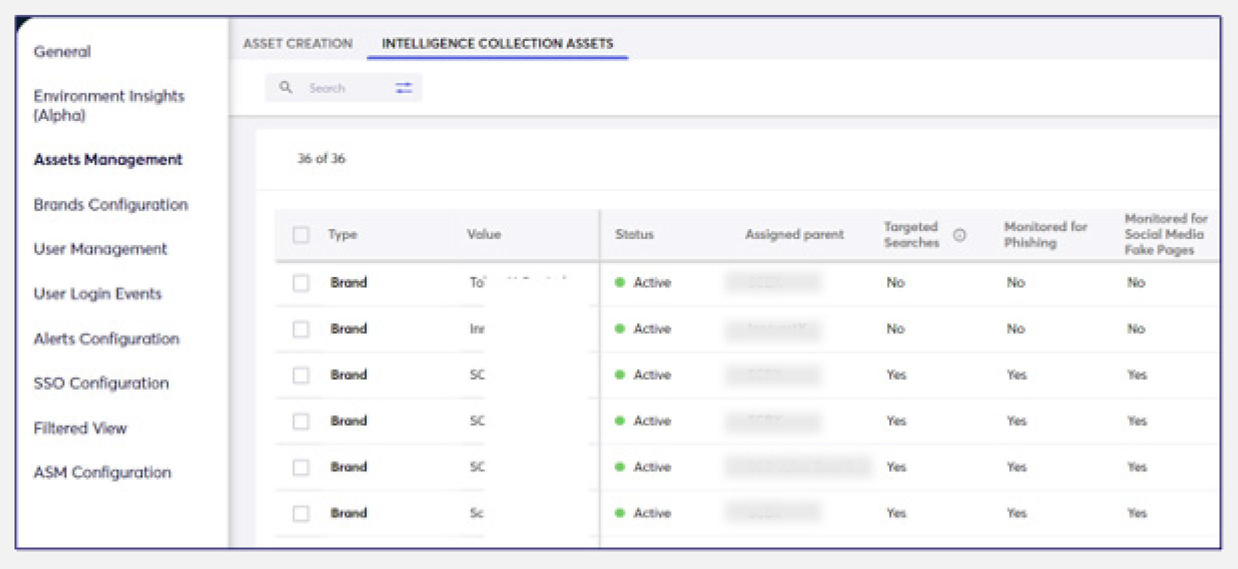
The license for each tenant includes the total number of acquired credits which can be divided between the different assets to achieve optimal coverage.

2.3 TENANT FOR REPORT GENERATION

Report generation tenants are purchased through Check Point ***SQU - Cyberint Tenant for Report Generation CP-ERM-MSSP-REPORT***

An Ad Hoc Cyberint tenant provides the ability to analyze intelligence and execute full Cyberint capabilities with relation to a specific organization, making it possible to automatically collect risks in different areas into a singular view, which allows report extraction.

Cyberint provides the option to create a tenant, upload assets and initiate an automated ASM discovery scan, CTI & Darkweb analysis, leaked credentials discovery and phishing and impersonation collection.



36 of 36

☐	Type	Value	Status	Assigned parent	Targeted Searches	Monitored for Phishing	Monitored for Social Media Fake Pages
☐	Brand	To	● Active	[redacted]	No	No	No
☐	Brand	Inr	● Active	[redacted]	No	No	No
☐	Brand	SC	● Active	[redacted]	Yes	Yes	Yes
☐	Brand	SC	● Active	[redacted]	Yes	Yes	Yes
☐	Brand	SC	● Active	[redacted]	Yes	Yes	Yes
☐	Brand	Sc	● Active	[redacted]	Yes	Yes	Yes

Figure 1 - Cyberint Tenant definition

The scope of the Ad Hoc Tenant includes:

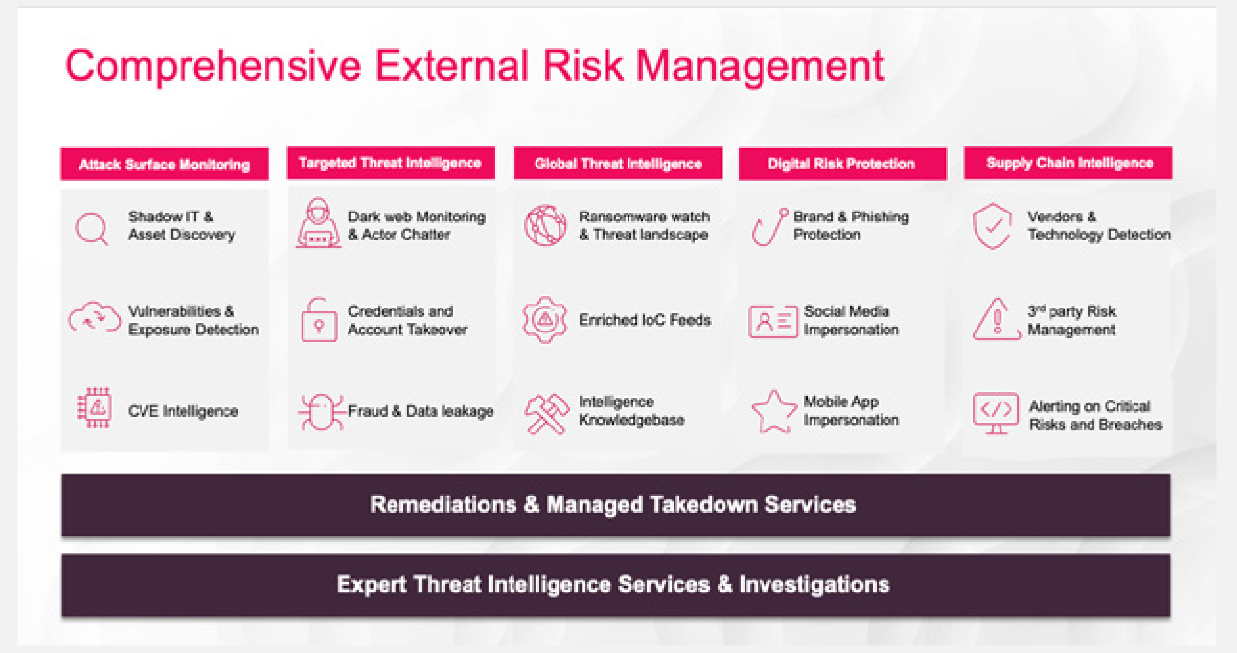
Item	Quantity	Comments
Ability to create tenants for report generation	Included	• Alerts center and dashboards • Intelligence raw data access • ASM module • Phishing and Lookalike Domains module • Report Section
Maximum number ASM assets per tenant	100,000	Additional Assets can be coordinated with Cyberint representative.
Maximum number of Threat Intelligence assets per tenant	600	Additional Assets can be coordinated with Cyberint representative.
Tenant collection period	2 weeks	During this time Cyberint will automatically collect data in its different modules. At the expiration the collection engines will stop.
Tenant availability period	4 weeks	During this time the user can access the tenant, review the collected data and generate reports.
Support	Included	Business hours

3. SOLUTION OVERVIEW

Cyberint's Impactful Intelligence solutions focus on the organization's digital environment - digital channels, online assets, digital supply chain, and brand. Cyberint goes far beyond the networks' perimeters to identify threats and mitigate them before they materialize. We leverage the most advanced technology to identify threats in the digital ecosystem and offer our experts' help to remove those threats.

Cyberint's Impactful intelligence solution is effective because it fuses threat intelligence with brand protection and attack surface management, alongside expert analysts who utilize powerful intelligence capabilities and forensic tools to fully investigate and respond to never-before-seen attacks before they can penetrate your network or have a significant impact on your organization.

Cyberint Impactful Intelligence Platform includes:



Comprehensive External Risk Management

Attack Surface Monitoring	Targeted Threat Intelligence	Global Threat Intelligence	Digital Risk Protection	Supply Chain Intelligence
Shadow IT & Asset Discovery	Dark web Monitoring & Actor Chatter	Ransomware watch & Threat landscape	Brand & Phishing Protection	Vendors & Technology Detection
Vulnerabilities & Exposure Detection	Credentials and Account Takeover	Enriched IoC Feeds	Social Media Impersonation	3rd party Risk Management
CVE Intelligence	Fraud & Data leakage	Intelligence Knowledgebase	Mobile App Impersonation	Alerting on Critical Risks and Breaches

Remediations & Managed Takedown Services

Expert Threat Intelligence Services & Investigations

Figure 2 - Cyberint's technology and services offering

The Cyberint platform focuses on protecting organizations beyond their perimeter and it includes several key modules:

1. **Attack Surface Management** - proactively and continuously discovers, monitors, and protects the organization's digital attack surface and assesses the posture risk. This module is included with the basic Tenants (Continuous Monitoring tenants and Report Generation tenants).

2. **Targeted Threat Intelligence** & Open, Deep and Dark Web monitoring - provides actionable cyber intelligence in real-time from the open, deep, and dark web, providing credential monitoring, data leakage detection and targeting risk levels. This module is included with the basic Tenants (Continuous Monitoring tenants and Report Generation tenants).

3. **Global Threat Intelligence** - Enables deeper understanding of threat actors, ransomware & cyber incidents, malware, CVEs, IoCs and more with ability to pivot around specific a IoC. F**ull functionality of this module requires the Threat Hunting license –** ***Check point SQU Additional Threat Hunting User CP-ERM-TH-USERS***

4. **Digital Risk Protection** - allowing real-time visibility of phishing and brand abuse detection including newly-created phishing sites, as well as social media profiles and applications that impersonate the customer or its employees in order to initiate an attack or illegally use the organization's brand. **This module is included with the basic Tenants (Continuous Monitoring tenants and Report Generation tenants).**

   Supply Chain Intelligence – providing threat intelligence and posture coverage for vendors and suppliers, allowing the customer to manage risks and receive proactive alerts. **This module requires** – ***Check point SQU Additional Supply Chain Monitoring # of Vendors CP-ERM-SUPPLY-STD***

Cyberint™ provides holistic coverage for multiple business risk areas. The following present the different categories and sample alert types:

DIGITAL FOOTPRINT

Map the attack surface and identify vulnerable weaknesses

Exposed Web Interfaces · Hijackable Subdomains Website Vulnerabilities · Exposed Cloud Storage Exploitable Parts · Mail Servers in Blacklist Server Connected to Botnet · Email Security Isues Certificate Authority Issues

DATA LEAKAGE & ACCOUNT TAKEOVER

Map the attack surface and identify vulnerable weaknesses

Ransomware · Compromised AcesToken Internal Information Disclosure · Malicious Insider Compromised Payment Cards · Compromised Employee Credentials · Compromised Customer Credentials

BRAND

Safeguard all facets of your online presence

Official Social Media Profle · Impersonation Intelectual Property Infringement · Unauthorized Trading · Negative Sentiment · Fake Job Posting Defafacement

ATTACKWARE

Ensure ongoing and continuous visibility of threat actors' tools

Malicious File · Reconnaissance · Automated Attack Tool · Business Logic Bypas · Target list

FRAUD

Mitigate fraud to ultimately reduce your fraud rate

Refund Fraud · Carding · Coupon Fraud · Money Laundering · Victim Reports · Malicious Insider · Extortion

PHISHING

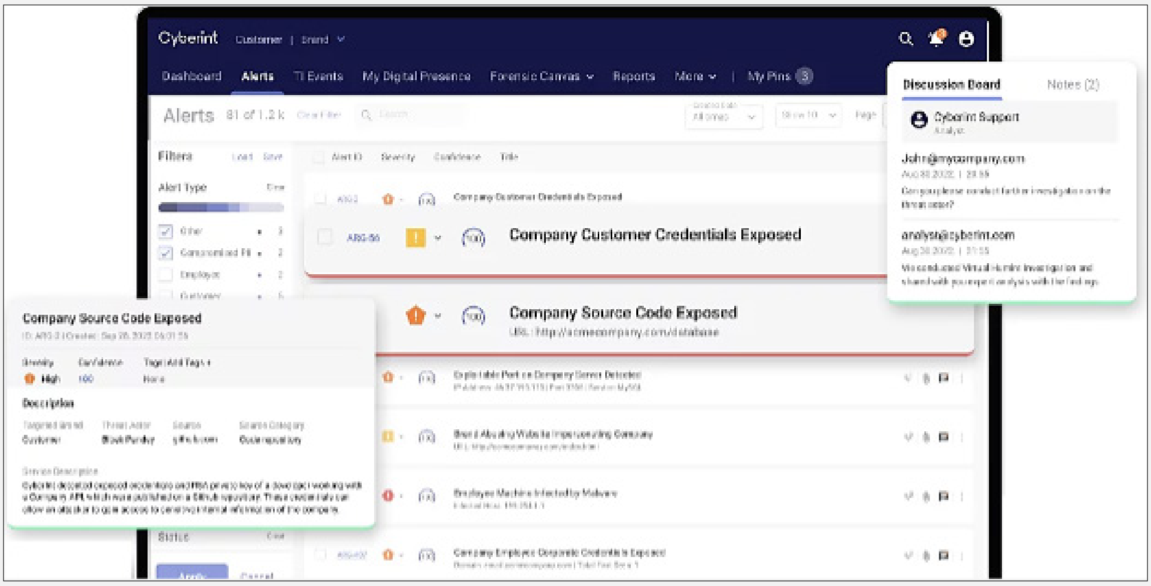
Identify & remediate phishing attack attempts before they impact

Phishing · Email · Phishing Kit · Phishing Website Lookalike Domain · Phishing Target List

Figure 3 – Cyberint's covered use cases

3.1 CYBERINT ALERTING MODULE - IMPACTFUL DELIVERABLES

The heart of Cyberint is the alert center, which provides alerts that are actionable, effective and provide a recommended path for immediate action. The Alerts are structured and can be consumed via the alert section user interface or via API integration to SIEM, SOAR or ticketing platforms.



Company Customer Credentials Exposed

Company Source Code Exposed

URL : http://acmecompany.com/database

Company Source Code Exposed

Severity: High

Confidence: 100

Tags: None

Description

Cyberint Support

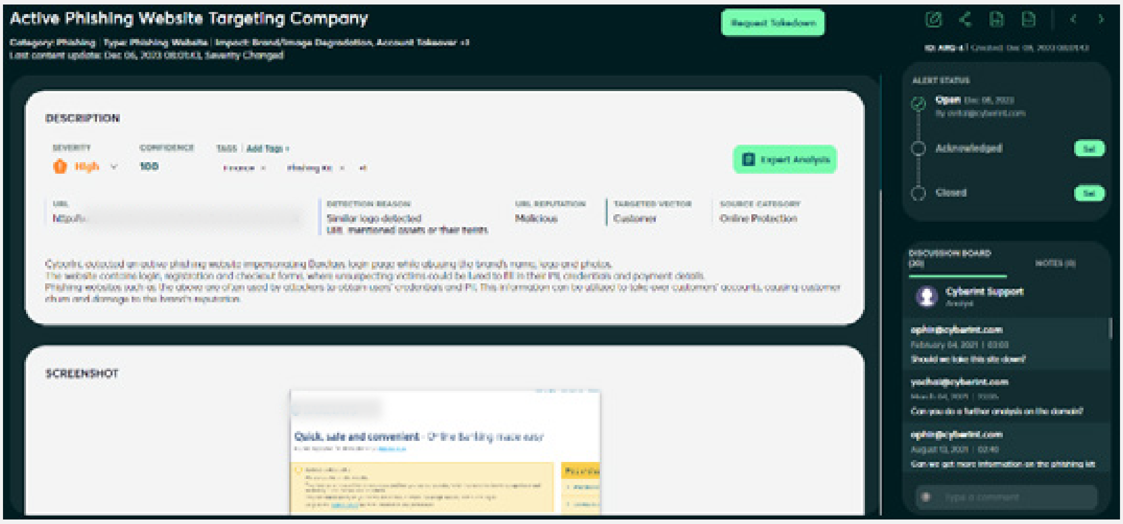
Analyst

John@mycompany.com

analyst@cyberint.com

Figure 4- Cyberint Alerts section with examples of alerts and the discussion board

As Cyberint pieces the information together, alongside Cyberint's analysts to verify and research specific threats, each detected alert includes detailed report on the findings, the related IoC, screenshots and recommendations.



Active Phishing Website Targeting Company

Category: Phishing | Type: Phishing Website | Impact: Brand/Image Degradation, Account Takeover +1

Last content update: Dec 06, 2023 08:01:43, Severity Changed

Severity: High

Confidence: 100

Detection Reason: Similar logo detected; URL mentioned assets or their terms

URL Reputation: Malicious

Targeted Vector: Customer

Source Category: Online Protection

Cyberint Support

Analyst

Should we take this site down?

Can you do a further analysis on the domain?

Can we get more information on the phishing kit

Quick, safe and convenient - Online banking made easy

Figure 5- Cyberint Alerts section with an example of an alert and the discussion board

Each Alert includes a discussion board, which allows the user to interact directly with Cyberint's expert analyst team to ask for further information and deeper investigations.

The reaction and feedback on each alert is provided by the alert status, validating acknowledgment of the alert, followed by successful remediation and feedback.

3.2 ATTACK SURFACE MANAGEMENT MODULE

Attack Surface Management has become an industry standard term for the process of continuously discovering, inventorying, and evaluating all of an organization's external digital assets. This provides visibility and protection of the business's true attack surface, mapping the digital assets you are aware of, as well as the assets you are not aware of and malicious or rogue assets.

"To protect ourselves, we must first know what to protect."

3.2.1 ASM DISCOVERY

The ASM discovery module identifies the entire organization's digital footprint, including additional domains, subdomains, IPs and cloud assets. These discovered assets are being utilized not only to identify vulnerabilities and exposure risk but also used as defined assets in the Threat Intelligence and Digital Risk protection module to identify additional areas requiring intelligence coverage. The Discovery module automates the process of asset discovery and provides up to date asset information while supporting continuous identification of the changing organization's landscape.

In order to discover the organization's assets, Cyberint uses various discovery mechanisms including: WHOIS data, DNS records, cloud search, SSL certificate analysis and more.

The discovery engine will highlight additional discovered assets, the discovery reason, and its related confidence. Assets with high discovery confidence will be automatically put into coverage that yield risk identification. Assets that have lower confidence will require the user perspective to make the coverage decision.

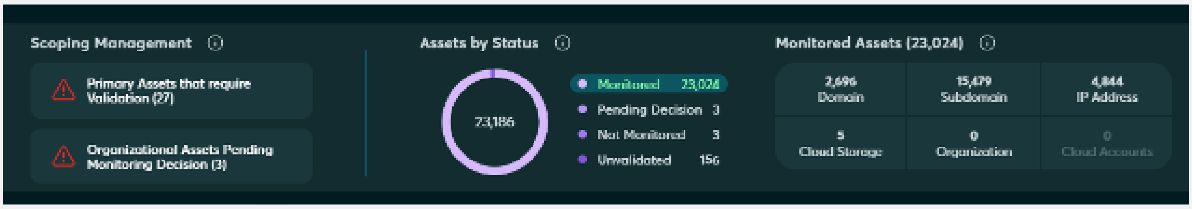


Figure 6 - Cyberint Discovery and scoping menu

3.2.2 EXPOSURE ITEMS & VULNERABILITIES SCANNING

For all monitored assets, Cyberint scans the organization's digital presence for exposure items. Cyberint dashboard displays all assets and issues in granular operational views.

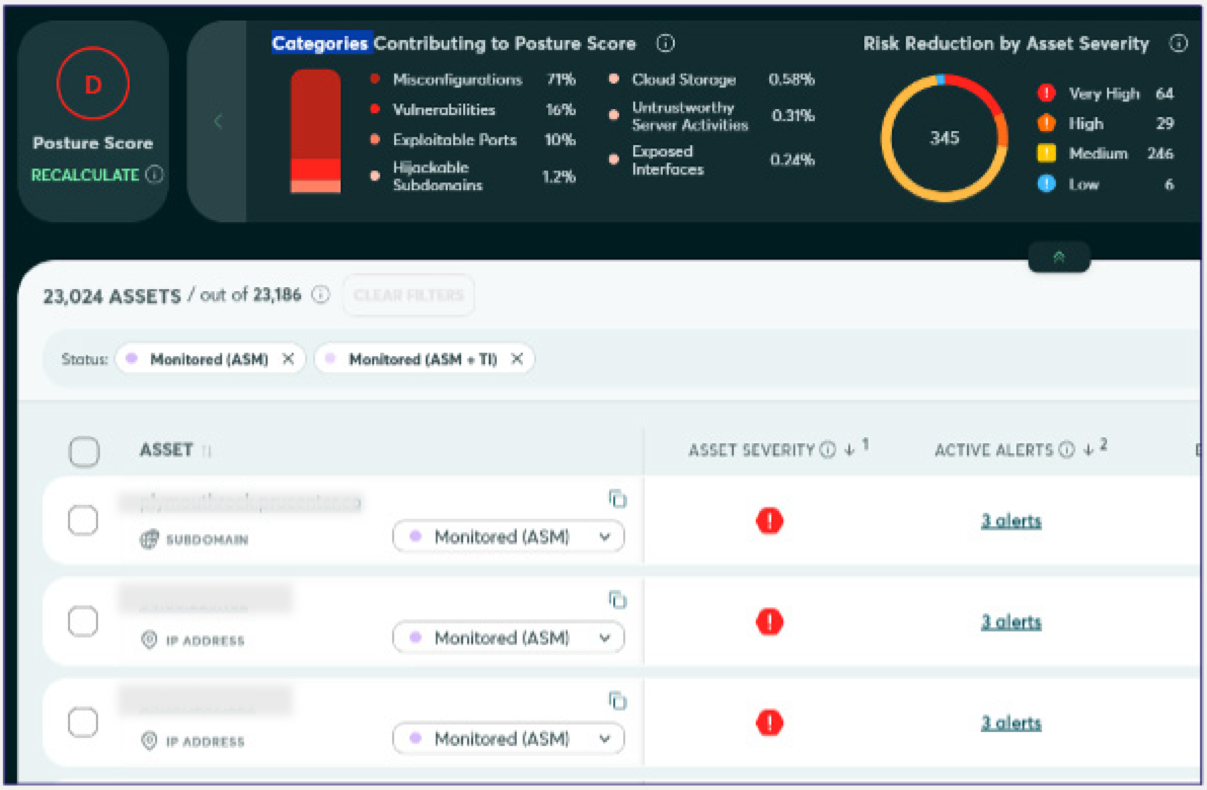
The exposure items Cyberint looks for include but are not limited to the following:

- Subdomain hijacking
- Misconfigured Cloud Assets
- Missing DNS and SPF records
- Potentially Exploitable Open Ports
- Open Web Interfaces
- Phishing and brand abuse
- Certificate Issues (CAA, SSL, etc.)
- Vulnerable technologies

3.2.3 POSTURE RISK SCORE

Based on the number of assets with identified risks, the environment's average remediation time, and the organization's size, Cyberint continuously calculates a risk score which is benchmarked against the organization itself and against organizations with a similar nature. The score is provided on scale of A to F based on industry best practices.

The posture risk score is calculated for the entire organization as well as per asset, suggesting which assets contribute most significantly to organization's level of cyber risk and thus should be dealt with first.



D
Posture Score
RECALCULATE ⓘ

Categories Contributing to Posture Score ⓘ

Misconfigurations	71%
Vulnerabilities	16%
Exploitable Ports	10%
Hijackable Subdomains	1.2%
Cloud Storage	0.58%
Untrustworthy Server Activities	0.31%
Exposed Interfaces	0.24%

Risk Reduction by Asset Severity ⓘ

345

Very High	64
High	29
Medium	246
Low	6

23,024 ASSETS / out of 23,186 ⓘ CLEAR FILTERS

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

□	ASSET	ASSET SEVERITY ⓘ ↓ 1	ACTIVE ALERTS ⓘ ↓ 2
□	[redacted] SUBDOMAIN Monitored (ASM)	!	3 alerts
□	[redacted] IP ADDRESS Monitored (ASM)	!	3 alerts
□	[redacted] IP ADDRESS Monitored (ASM)	!	3 alerts

Figure 7 – Attack Surface Monitoring risk scoring, summary of leading risk categories and highest risk assets

3.3 TARGETED THREAT INTELLIGENCE MODULE

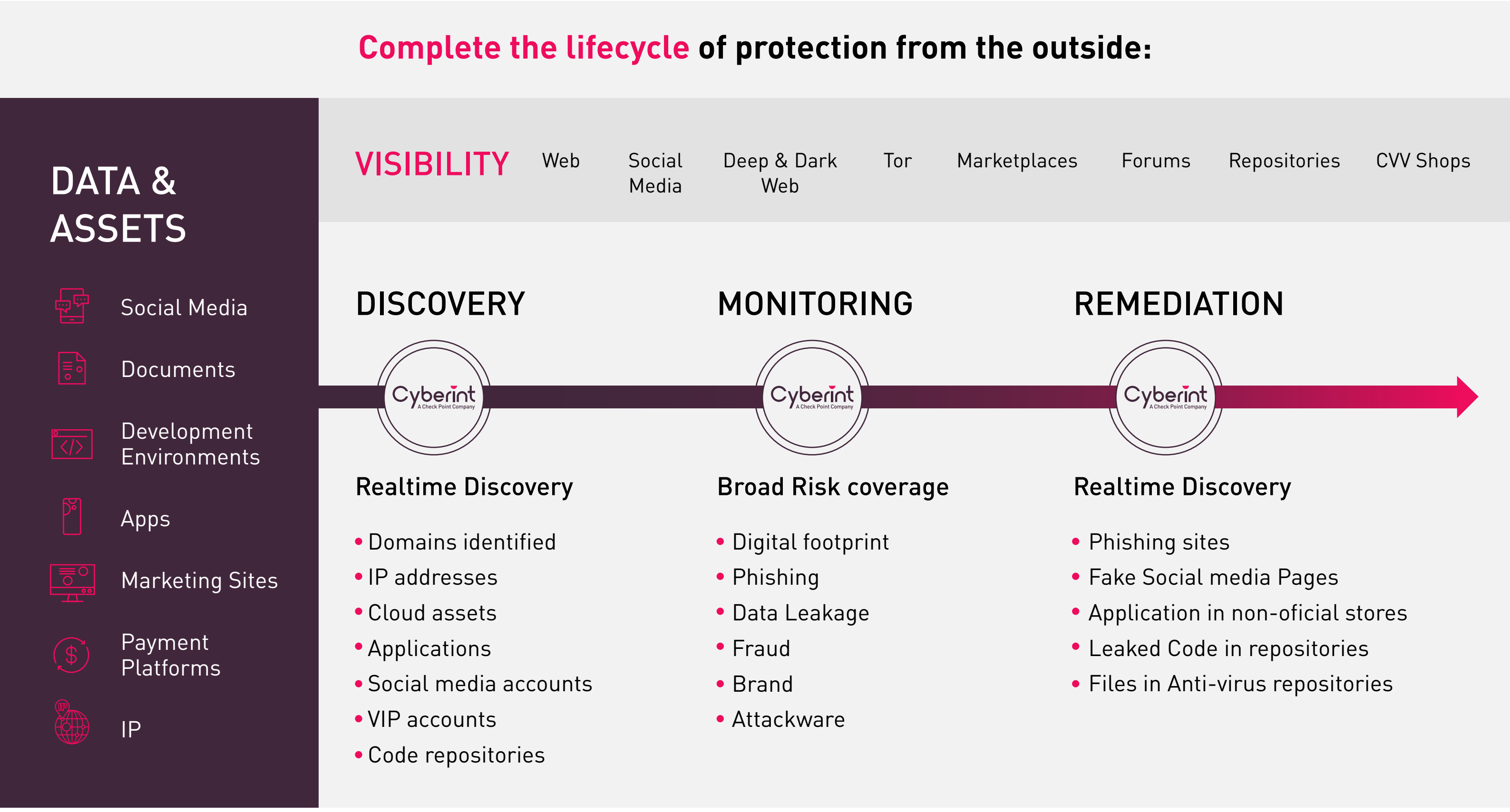
Cyberint's real-time monitoring of thousands of threat sources in the open, deep, and dark web leads to the collection and addition of millions of intelligence indicators per day to the Cyberint internal data lake.

Raw intelligence items are automatically correlated with the organization's assets (IPs, domains, brands, executives, etc.) and are categorized according to a specific use case:

- Phishing
- Malware campaigns and other attackware
- Data (documents, source code, credentials) leakage
- Brand Abuse
- VIP protection
- Fraudulent activity
- Others

Using Cyberint's proprietary machine learning algorithm, this raw intelligence is prioritized according to potential risk and impact, allowing rapid, smart and cost-effective analysis.

Automatic and semi-automatic analysis engines generate actionable intelligence alerts which are then disseminated to security teams with in-depth analysis, enriched context, threat actor profiling and more, allowing the organization to take effective action.



Complete the lifecycle of protection from the outside:

DATA & ASSETS

- Social Media
- Documents
- Development Environments
- Apps
- Marketing Sites
- Payment Platforms
- IP

VISIBILITY: Web, Social Media, Deep & Dark Web, Tor, Marketplaces, Forums, Repositories, CVV Shops

DISCOVERY

Realtime Discovery

- Domains identified
- IP addresses
- Cloud assets
- Applications
- Social media accounts
- VIP accounts
- Code repositories

MONITORING

Broad Risk coverage

- Digital footprint
- Phishing
- Data Leakage
- Fraud
- Brand
- Attackware

REMEDIATION

Realtime Discovery

- Phishing sites
- Fake Social media Pages
- Application in non-oficial stores
- Leaked Code in repositories
- Files in Anti-virus repositories

Figure 8 - Cyberint Threat Intelligence Data Flow

3.3.1 CONTEXTUALIZED THREAT INTELLIGENCE

Cyberint provides context for all intelligence alerts with the following steps:

- Collect relevant threat intelligence items from an ever-growing list of open, deep & dark web sources.
- Execute complex analysis, including the application of machine learning and natural language processing algorithms to determine raw data relevancy and significance to each customer.
- Present relevant and analyzed data via the Cyberint web interface and/or share the data with customers' external systems via out-of-the-box integrations and/or a web services API in real time.
- Highlight for each intelligence item, when applicable, the relevant context concerning threat actors, tools, and techniques.

Cyberint is being used both by Cyberint's in-house analysts as well as customers to gain insights of threats and collaboration, allowing Cyberint to effectively become an extension of the organization's security team.

3.3.2 CYBERINT UNIQUE THREAT INTELLIGENCE DIFFERENTIATORS

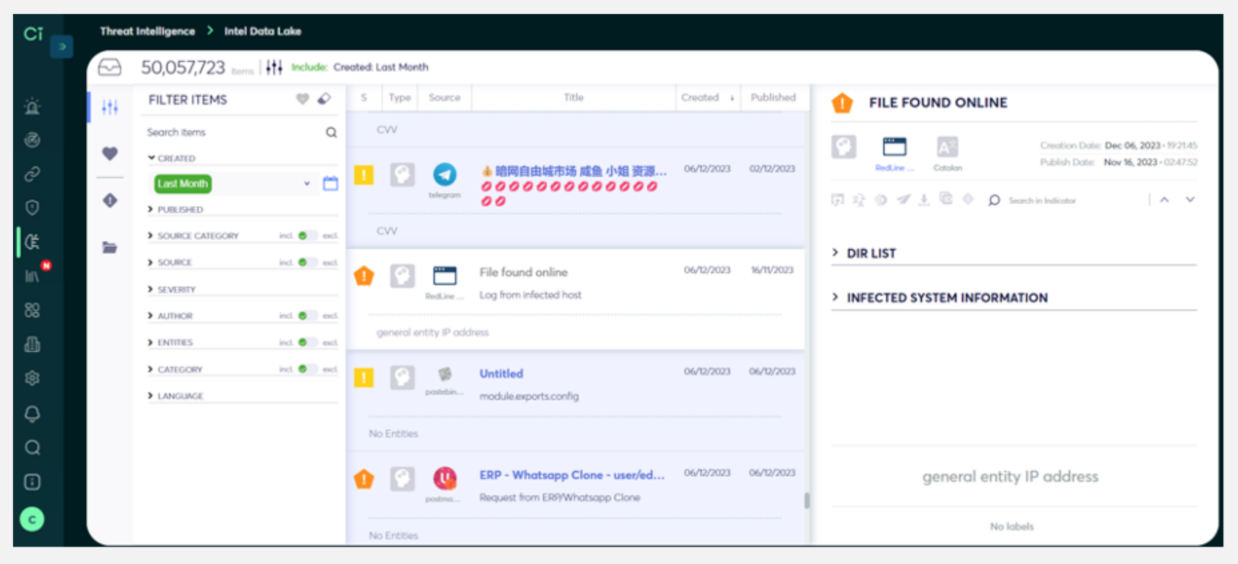
1. Cyberint provides real-time, targeted Threat Intelligence, collected from thousands of sources, as well as operational threat intelligence collected from numerous feeds to augment that data. The collected intelligence is then enriched with additional context and relevant information in the form of insights on the threat actors, tactics, techniques and procedures, as well as IoCs associated with the flagged indicator.

2. The targeted intelligence capabilities built into Cyberint rely on an array of advanced crawlers and proxies, which enable data collection from thousands of relevant sources (open web, dark web, social networks, forums, marketplaces, etc.) while maintaining anonymity.

3. These crawlers can automatically handle and bypass human authentication/trust mechanisms such as CAPTCHA. For special access forums and dark web sites, Cyberint's team of analysts and researchers create and manage avatars to gain access.

4. Cyberint is constantly evolving its list of unique sources and intel feeds supported by the system. These sources are scanned by Cyberint automated crawlers for the purpose of harvesting customer-specific information. Examples of Cyberint platform's current list of sources include Social Media feeds, online cyber-dedicated sources (XSS, breached, Exploit, hackforums, etc.), paste sites (such as pastebin.com, pastie.org, etc.) and an updated list of dark net marketplaces, chat rooms and forums, which are known locations for cyber criminals, across different industries.

5. This list of sources is updated continuously by Cyberint experts and includes regionally relevant local sources per customers' needs (e.g. we cover unique Chinese sources, Russian marketplaces, and other specific sources). In addition, Cyberint constantly adds more feeds (free and commercial) to its aggregation engine to provide a holistic view of the customer's threat landscape, using all intelligence methodologies available.



S	Type	Source	Title	Created	Published
CVV					
!		telegram	💰暗网自由城市场 咸鱼 小姐 资源... ⭕⭕⭕⭕⭕⭕⭕⭕⭕⭕⭕⭕⭕⭕⭕	06/12/2023	02/12/2023
CVV					
!		RedLine ...	File found online Log from infected host	06/12/2023	16/11/2023
general entity IP address					
!		pastebin...	Untitled module.exports.config	06/12/2023	06/12/2023
No Entities					
!		postma...	ERP - Whatsapp Clone - user/ed... Request from ERP/Whatsapp Clone	06/12/2023	06/12/2023
No Entities					

FILE FOUND ONLINE

Creation Date: Dec 06, 2023 · 19:21:45
Publish Date: Nov 16, 2023 · 02:47:52

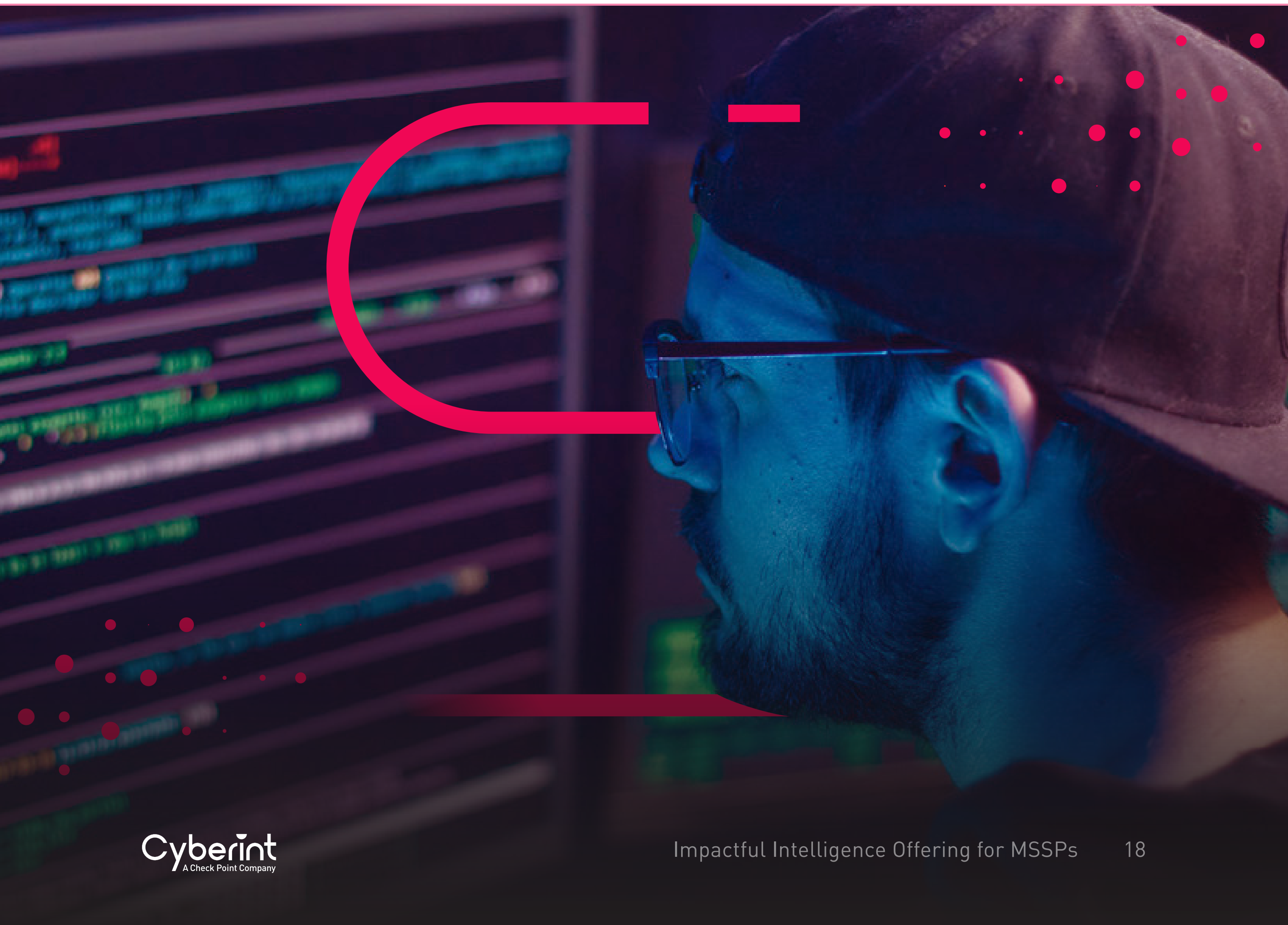
> DIR LIST

> INFECTED SYSTEM INFORMATION

general entity IP address

No labels

Figure 9 Cyberint Threat Intelligence feed



3.4 DIGITAL RISK PROTECTION MODULE

3.4.1 CYBERINT PHISHING DETECTION

Phishing is still one of the top 3 most common attack vectors. The reason for its success is twofold:

A. It is relatively simple for a novice threat actor to set up a phishing campaign.

B. It's designed to trick users to trust it - which can be achieved easily, especially in the hectic digital life we are living.

To maximize protection against phishing attacks, Cyberint is designed to cover each step in both of the attack scenarios illustrated above. Cyberint's algorithms combine automatic generation of domain permutations with open source and advanced DNS intelligence to predict with high confidence an imminent phishing attack. Together with the phishing beacon, which proactively protects against phishing sites hosted on domains that aren't flagged as suspicious, Cyberint is able to provide the broadest protection against phishing attacks.

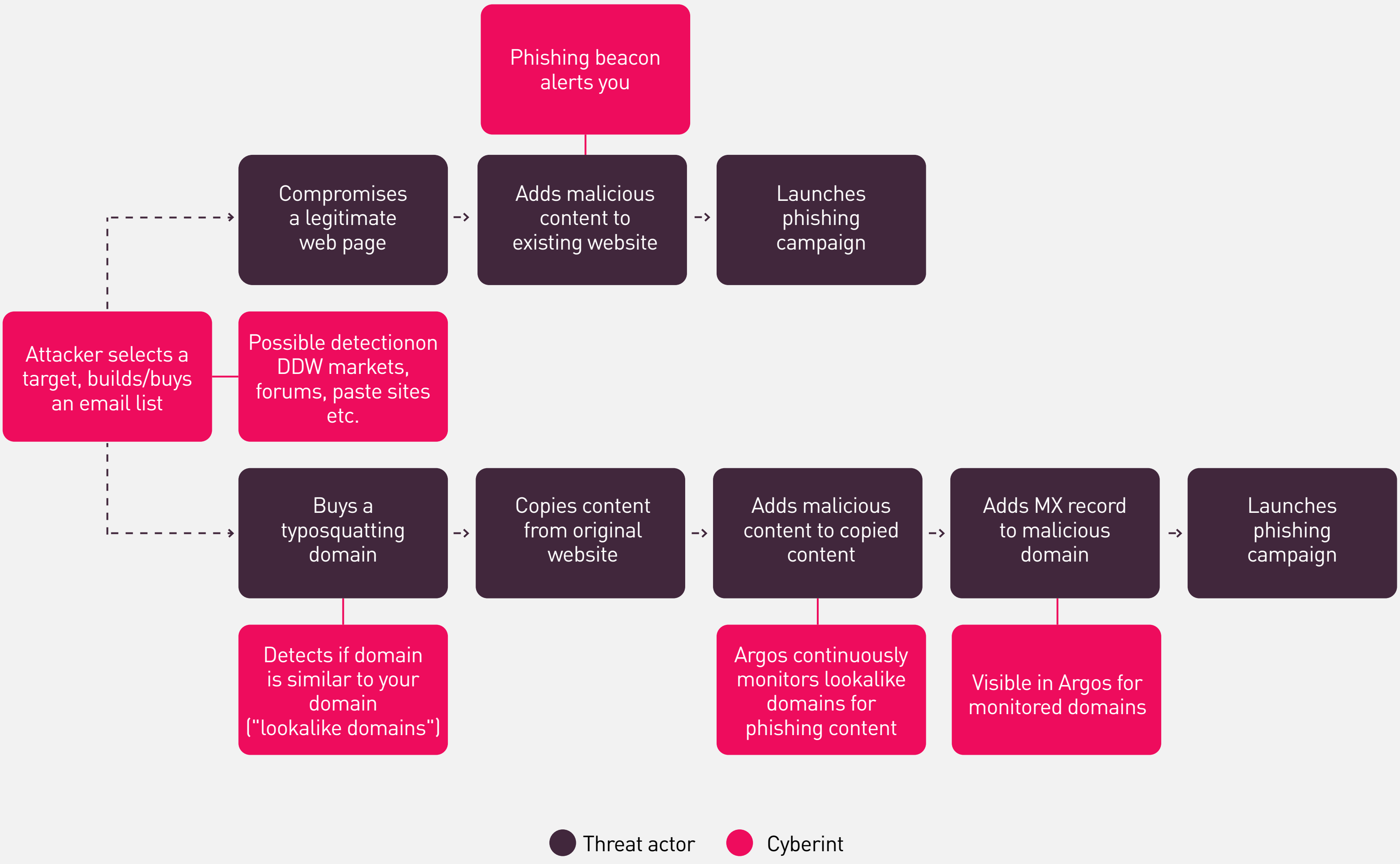
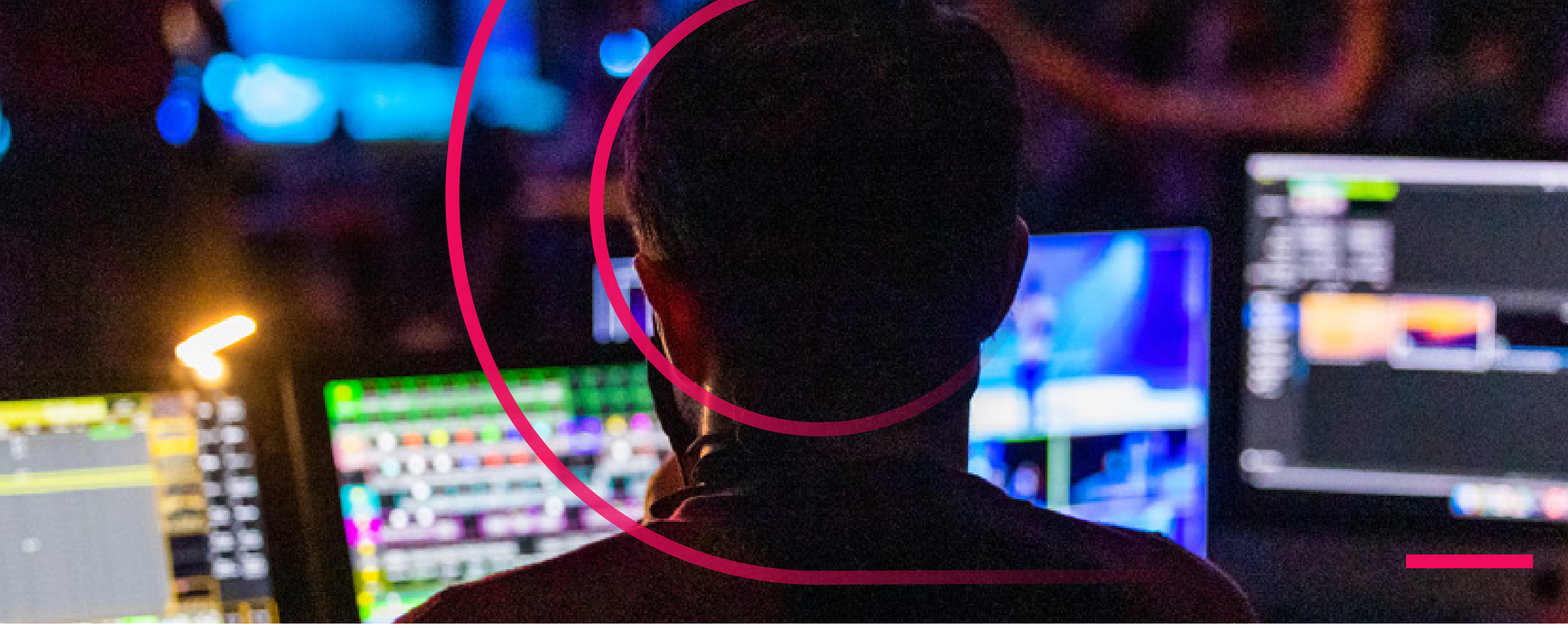

Phishing beacon alerts you
Compromises a legitimate web page
Adds malicious content to existing website
Launches phishing campaign
Attacker selects a target, builds/buys an email list
Possible detectionon DDW markets, forums, paste sites etc.
Buys a typosquatting domain
Copies content from original website
Adds malicious content to copied content
Adds MX record to malicious domain
Launches phishing campaign
Detects if domain is similar to your domain ("lookalike domains")
Argos continuously monitors lookalike domains for phishing content
Visible in Argos for monitored domains
● Threat actor
● Cyberint

Figure 10 - Phishing attack flows and Cyberint detection methods

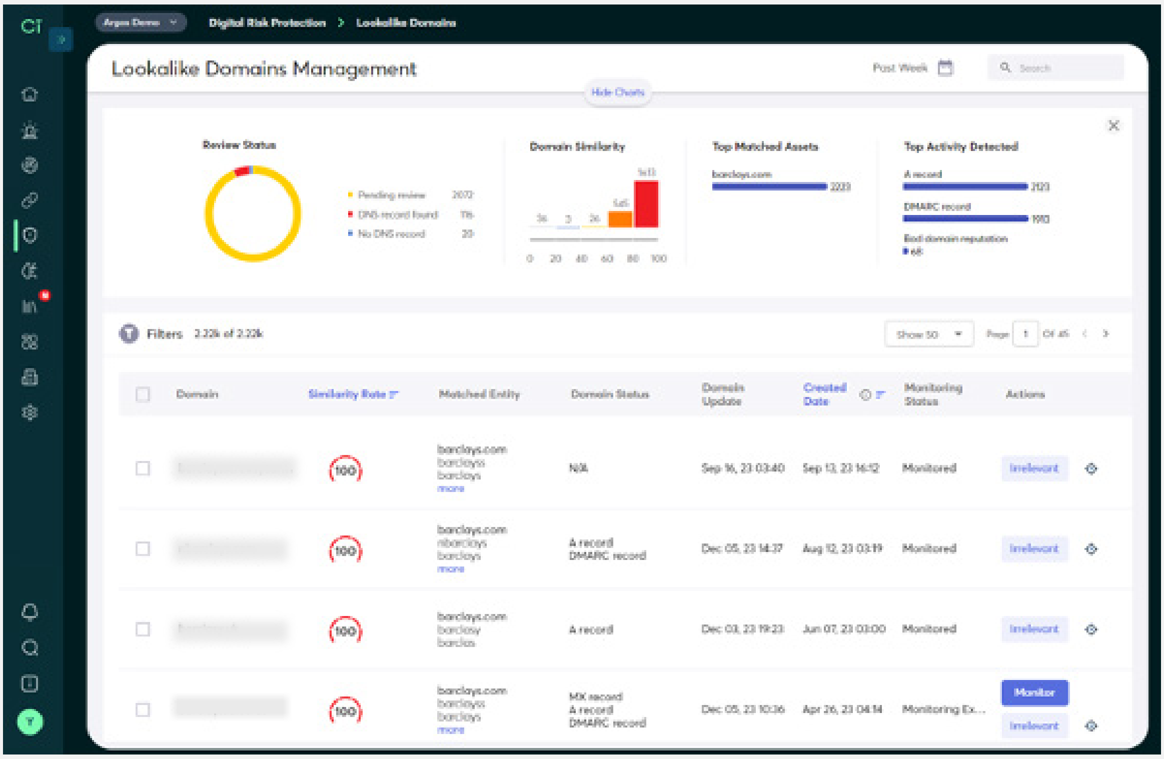


3.4.1.1 LOOKALIKE DOMAIN MONITORING

Cyberint continuously monitors for similarities between your domains and the newly registered candidates to provide a level of indication of malicious intent, and alerts you to suspicious, newly registered lookalike domains.

Each domain is tracked for A and MX records to assess the risk. Cyberint automatically looks for applications or content on the lookalike domains to check for source code or logo similarities.

Upon reaching a minimum risk threshold, Cyberint will trigger a phishing alert suggesting remediation steps.



□	Domain	Similarity Rate	Matched Entity	Domain Status	Domain Update	Created Date	Monitoring Status	Actions
□	[redacted]	100	barclays.com barclayss barclays more	N/A	Sep 16, 23 03:40	Sep 13, 23 16:12	Monitored	Irrelevant
□	[redacted]	100	barclays.com nbarclays barclays more	A record DMARC record	Dec 05, 23 14:37	Aug 12, 23 03:19	Monitored	Irrelevant
□	[redacted]	100	barclays.com barclasy barclas	A record	Dec 03, 23 19:23	Jun 07, 23 03:00	Monitored	Irrelevant
□	[redacted]	100	barclays.com barclayss barclays more	MX record A record DMARC record	Dec 05, 23 10:36	Apr 26, 23 04:14	Monitoring Ex...	Monitor Irrelevant

Figure 11 - Cyberint Look-alike domain tracking module

3.4.2 CYBERINT SOCIAL MEDIAL IMPERSONATION MODULE

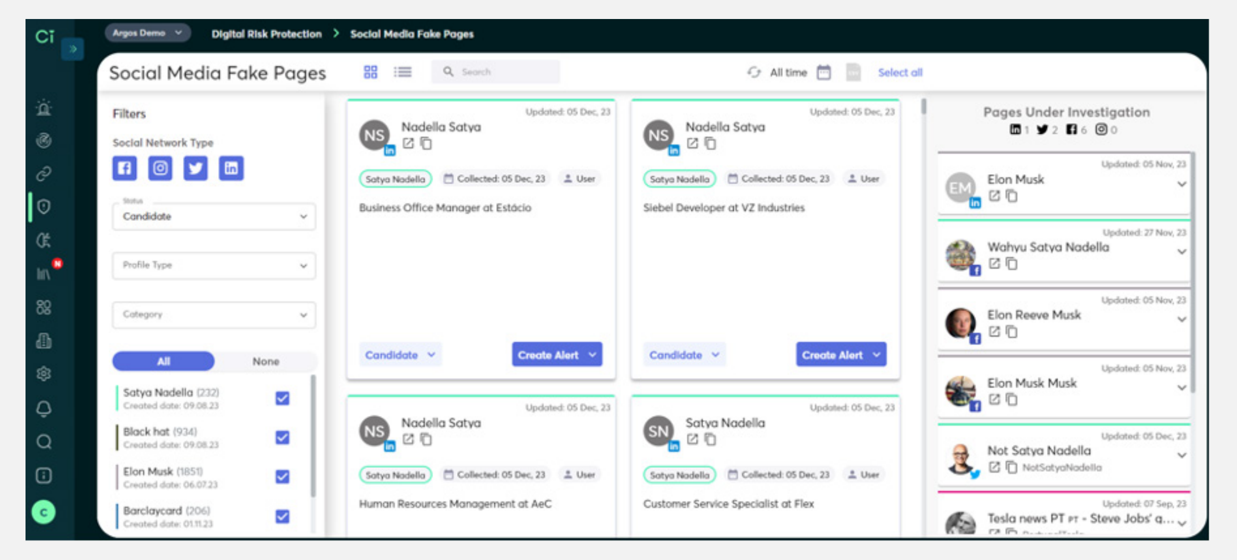
The Social Media Impersonation module continuously monitors popular social media platforms to identify fraudulent accounts that impersonate brands, organizations, and other registered trademarks, such as product names, as well as executives and important individuals.

The following social media platforms are covered:

- Instagram
- Facebook
- Twitter
- LinkedIn

The Social Media Impersonation Module operates on the customer-configured brand and person keywords which have impersonation enabled.

Upon identification of impersonation, an alert is triggered to support remediation.



Status: Candidate

Satya Nadella (232) Created date: 09.08.23 ☑
Black hat (934) Created date: 09.08.23 ☑
Elon Musk (1851) Created date: 06.07.23 ☑
Barclaycard (206) Created date: 01.11.23 ☑

Nadella Satya — Updated: 05 Dec, 23 — Satya Nadella — Collected: 05 Dec, 23 — User
Business Office Manager at Estácio

Nadella Satya — Updated: 05 Dec, 23 — Satya Nadella — Collected: 05 Dec, 23 — User
Siebel Developer at VZ Industries

Nadella Satya — Updated: 05 Dec, 23 — Satya Nadella — Collected: 05 Dec, 23 — User
Human Resources Management at AeC

Satya Nadella — Updated: 05 Dec, 23 — Satya Nadella — Collected: 05 Dec, 23 — User
Customer Service Specialist at Flex

Elon Musk — Updated: 05 Nov, 23
Wahyu Satya Nadella — Updated: 27 Nov, 23
Elon Reeve Musk — Updated: 05 Nov, 23
Elon Musk Musk — Updated: 05 Nov, 23
Not Satya Nadella — NotSatyaNadella — Updated: 05 Dec, 23
Tesla news PT PT - Steve Jobs' q... — Updated: 07 Sep, 23

Figure 12 - Social Medial impersonation detection module

3.4.2.1 BRAND IMPERSONATION

Threat actors impersonate trusted brands on social media for a variety of reasons. The purpose may be to drive traffic to a phishing site, where unsuspecting users are subsequently fooled into giving up credentials and other sensitive data. The goal may be to pass off trojanized applications or counterfeit goods as legitimate. Or, in some cases, the objective may simply be brand abuse, impersonating an established brand in order to degrade its value.

Cyberint's Social Media Impersonation Module monitors for impersonation of organizations, brands, products, and other registered trademarks. Customers can manually set all of the keywords they would like to monitor upon deploying this module.

3.4.2.2 EXECUTIVE IMPERSONATION

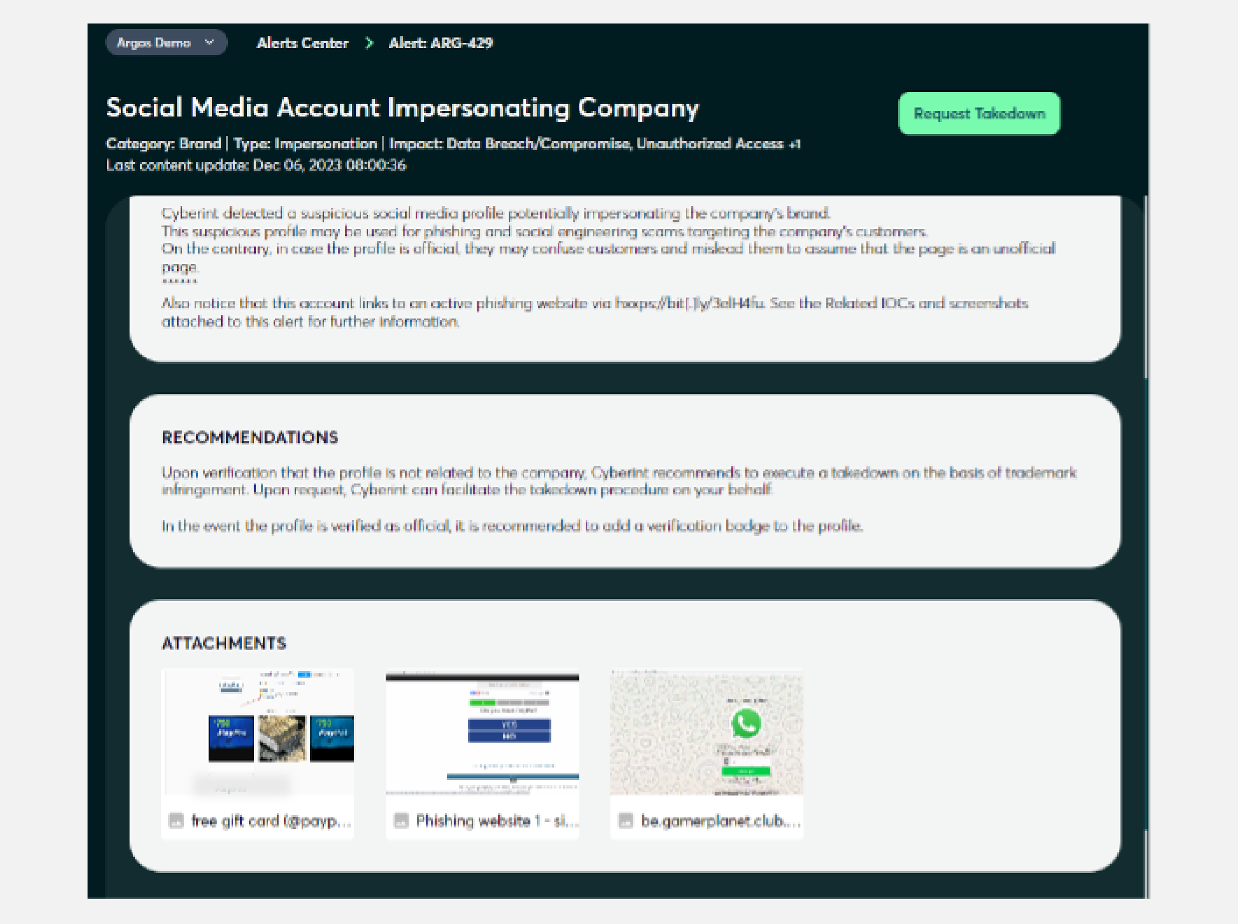
In addition to impersonating brands, attackers often impersonate executives within major organizations, such as the CEO, CFO, CISO, or other senior management personnel. In some cases, the attackers impersonate executives in order to have fraudulent invoices paid, effectively stealing money directly from the organization. In other cases, threat actors impersonate executives to recruit legitimate candidates for fake jobs, eventually sharing malware-infected files with the victims to compromise their machines and environments.

The Cyberint solution's Social Media Impersonation Module monitors for impersonation of executives across major social media platforms, simply using the first and last names of the executives whom the customer would like to safeguard against impersonation.

3.4.2.3 ALERTING AND REMEDIATION

When a suspicious profile is detected, it is added to the Social Media Impersonation Module dashboard for review. If the account is, in fact, authentic, it can be marked as such from the dashboard. Similarly, innocuous profiles can be marked as irrelevant. The profiles that represent real threats are marked as Suspicious and/or converted into an Alert.

Once a social media profile has been converted into an Alert, it will then appear under the Alerts screen and additional actions can be taken. This includes submitting a takedown request, which can be done within the Cyberint platform with a few clicks. Cyberint's dedicated takedown team handles takedowns across all social media platforms in scope for monitoring.



Social Media Account Impersonating Company

Category: Brand | Type: Impersonation | Impact: Data Breach/Compromise, Unauthorized Access +1
Last content update: Dec 06, 2023 08:00:36

Cyberint detected a suspicious social media profile potentially impersonating the company's brand.
This suspicious profile may be used for phishing and social engineering scams targeting the company's customers.
On the contrary, in case the profile is official, they may confuse customers and mislead them to assume that the page is an unofficial page.
******
Also notice that this account links to an active phishing website via hxxps://bit[.]ly/3elH4fu. See the Related IOCs and screenshots attached to this alert for further information.

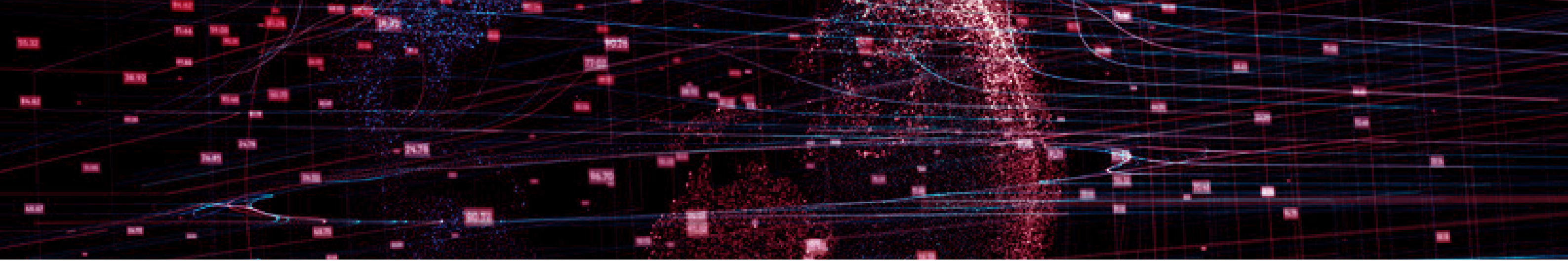
RECOMMENDATIONS

Upon verification that the profile is not related to the company, Cyberint recommends to execute a takedown on the basis of trademark infringement. Upon request, Cyberint can facilitate the takedown procedure on your behalf.

In the event the profile is verified as official, it is recommended to add a verification badge to the profile.

ATTACHMENTS

Figure 13 - Impersonation Alert



3.5 GLOBAL THREAT INTELLIGENCE MODULE

Check point SQU - Additional Threat Hunting User CP-ERM-TH-USERS

Infosec teams must keep up with trending global threats and the latest attack campaigns. In the chaos of threats like malware, evolving TTPs, IoCs and newly discovered CVEs, monitoring all relevant threats is never easy. Finding the relevant threats that pose an urgent risk can be sometimes like finding the needle in a haystack. Threat Intelligence Analysts need to effectively analyze global threats and quickly identify the immediate risks to their organization.

Cyberint provides customers with an up-to-date threat landscape that is relevant to their region and sector and sheds light on the modus operandi of the threat groups active in that specific landscape. This module helps to eliminate unnecessary information and highlights the specific threats that should remain in focus to take preventative actions.

With Cyberint Global Treat Intelligence Module one can:

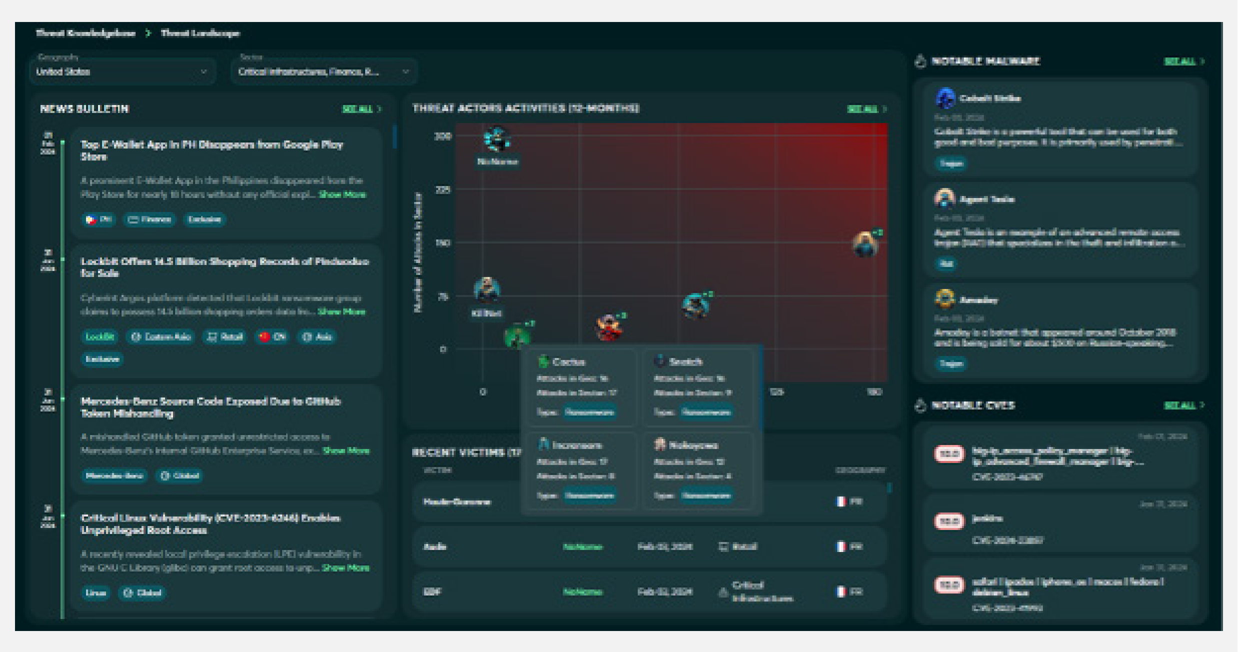
- Search for specific threat entities (such as malware, threat actors and threat groups).
- Learn about each threat through an exclusive summary provided by the Cyberint Research Team.
    - Victimology- find Threat Actor's victims by their sector and country.
    - TTPs – discover the tactics, techniques and procedures used by specific threat actors, mapped to the MITRE ATT&CK matrix.
    - CVEs – gain open, deep and dark web intelligence on every documented CVE, along with a risk score that estimates the likelihood of exploitation.
    - IoCs – research the latest indicators of compromise, including domains, IP addresses, file hashes, and more.
- Threat Reports
- Filter and sort by region and industry to examine a specific threat landscape
- Integrate specific IOCs
- Initiate forensic investigations

The Global Threat Intelligence module has 2 main licensing options:

1. Regular user license – provides a preview of all the intelligence entities with limited ability to drill down.
2. Threat Hunting user license – provides full access to the intelligence entities as well as access to Cyberint's Threat Intelligence Data Lake and the Forensic Canvas module.

3.2.3 POSTURE RISK SCORE

The Cyberint threat landscape dashboard provides extended information on threats that are targeting the organization based on the geography and the sector.



Top E-Wallet App In PH Disappears from Google Play Store

A prominent E-Wallet App in the Philippines disappeared from the Play Store for nearly 18 hours without any official expl... Show More

PH · Finance · Exclusive

LockBit Offers 14.5 Billion Shopping Records of Pinduoduo for Sale

Cyberint Argos platform detected that LockBit ransomware group claims to possess 14.5 billion shopping orders data fro... Show More

LockBit · Eastern Asia · Retail · CN · Asia · Exclusive

Mercedes-Benz Source Code Exposed Due to GitHub Token Mishandling

A mishandled GitHub token granted unrestricted access to Mercedes-Benz's Internal GitHub Enterprise Service, ex... Show More

Mercedes-Benz · Global

Critical Linux Vulnerability (CVE-2023-6246) Enables Unprivileged Root Access

A recently revealed local privilege escalation (LPE) vulnerability in the GNU C Library (glibc) can grant root access to unp... Show More

Linux · Global

Cactus: Attacks in Geo: 16, Attacks in Sector: 17, Type: Ransomware

Snatch: Attacks in Geo: 16, Attacks in Sector: 9, Type: Ransomware

Incransom: Attacks in Geo: 17, Attacks in Sector: 8, Type: Ransomware

Nokoyawa: Attacks in Geo: 12, Attacks in Sector: 4, Type: Ransomware

Haute-Garonne · FR

Auchan · NoName · Feb 03, 2024 · Retail · FR

EDF · NoName · Feb 03, 2024 · Critical Infrastructures · FR

Cobalt Strike, Feb 05, 2024: Cobalt Strike is a powerful tool that can be used for both good and bad purposes. It is primarily used by penetrati... Trojan

Agent Tesla, Feb 05, 2024: Agent Tesla is an example of an advanced remote access trojan (RAT) that specializes in the theft and infiltration o... Rat

Amadey, Feb 05, 2024: Amadey is a botnet that appeared around October 2018 and is being sold for about $500 on Russian-speaking... Trojan

10.0 · big-ip_access_policy_manager | big-ip_advanced_firewall_manager | big-... · CVE-2023-46747 · Feb 01, 2024

10.0 · jenkins · CVE-2024-23897 · Jan 31, 2024

10.0 · safari | ipados | iphone_os | macos | fedora | debian_linux · CVE-2023-41993 · Jan 31, 2024

Figure 14 – Cyberint Global Threat Landscape Dashboard

The threat landscape dashboard presents:

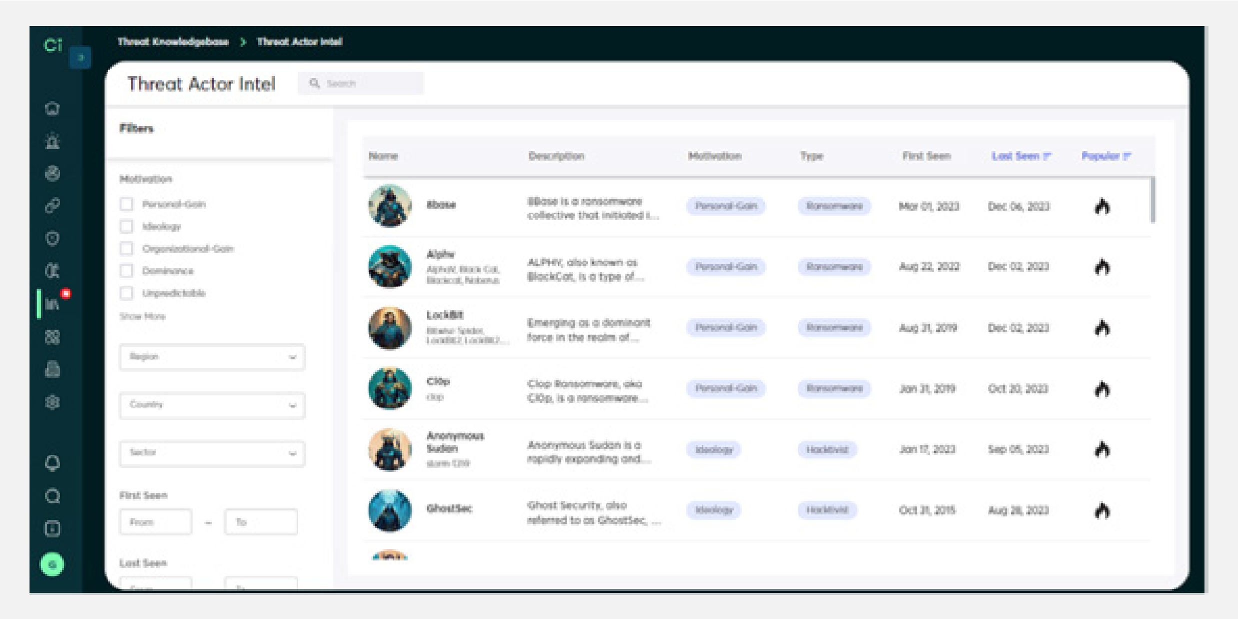
- Cyber news related to the organization's geography and sector.
- A graph presenting the most active threat actors.
- List of recent victims in the geography and region.
- Most notable strains of Malware.
- Most notable CVEs.

From each of the sections, the user can drill down further for additional information.

3.5.2 GLOBAL INTELLIGENCE KNOWLEDGE

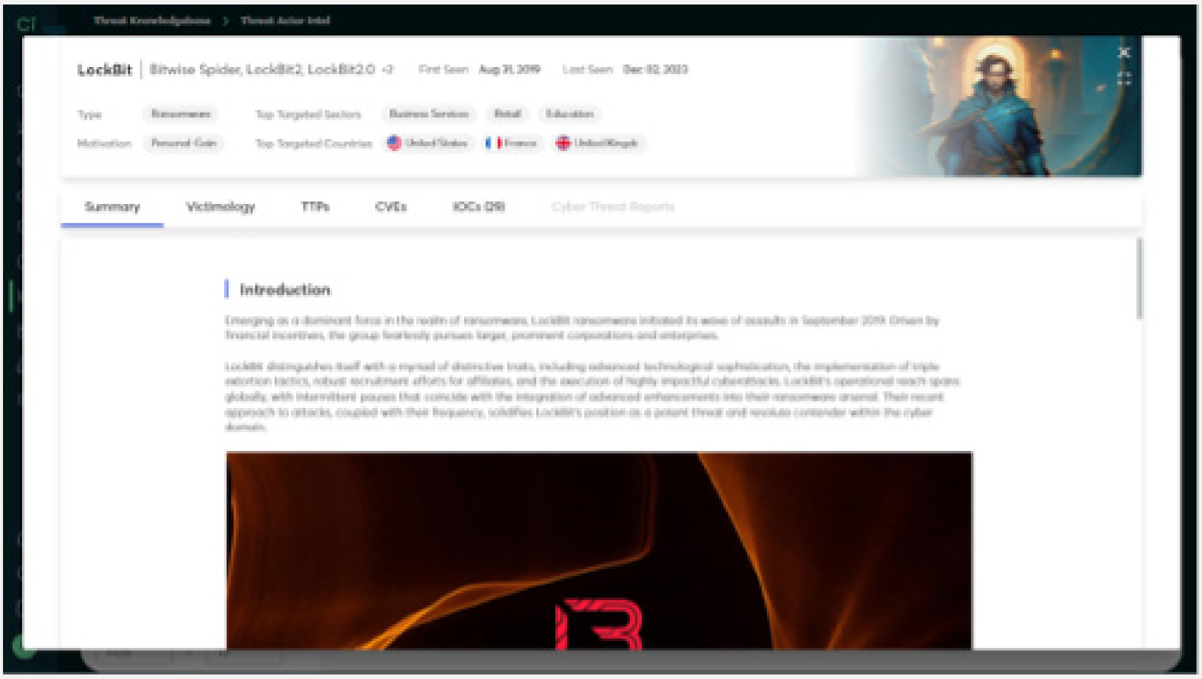
3.5.2.1 THREAT ACTOR KNOWLEDGEBASE

This capability provides essential information related to a specific threat actor or threat group, including their motivations, the regions and industries they target, and associated TTPs and IoCs. It's an excellent starting point when conducting strategic risk assessments, proactively preparing defenses against relevant threats, launching red team engagements or tabletop exercises, and attributing a security incident after it has been resolved.



Name	Description	Motivation	Type	First Seen	Last Seen	Popular
8base	8Base is a ransomware collective that initiated i...	Personal-Gain	Ransomware	Mar 01, 2023	Dec 06, 2023	🔥
Alphv ALPHV, Black Cat, Blackcat, Noberus	ALPHV, also known as BlackCat, is a type of...	Personal-Gain	Ransomware	Aug 22, 2022	Dec 02, 2023	🔥
LockBit Bitwise Spider, LockBit2, LockBit2...	Emerging as a dominant force in the realm of...	Personal-Gain	Ransomware	Aug 31, 2019	Dec 02, 2023	🔥
Cl0p clop	Clop Ransomware, aka Cl0p, is a ransomware...	Personal-Gain	Ransomware	Jan 31, 2019	Oct 20, 2023	🔥
Anonymous Sudan storm-1359	Anonymous Sudan is a rapidly expanding and...	Ideology	Hacktivist	Jan 17, 2023	Sep 05, 2023	🔥
GhostSec	Ghost Security, also referred to as GhostSec, ...	Ideology	Hacktivist	Oct 31, 2015	Aug 28, 2023	🔥

Figure 15 - Threat Actor Search Capabilities



LockBit | Bitwise Spider, LockBit2, LockBit2.0 +3 First Seen Aug 31, 2019 Last Seen Dec 02, 2023

Type: Ransomware Top Targeted Sectors: Business Services, Retail, Education

Motivation: Personal-Gain Top Targeted Countries: United States, France, United Kingdom

Introduction

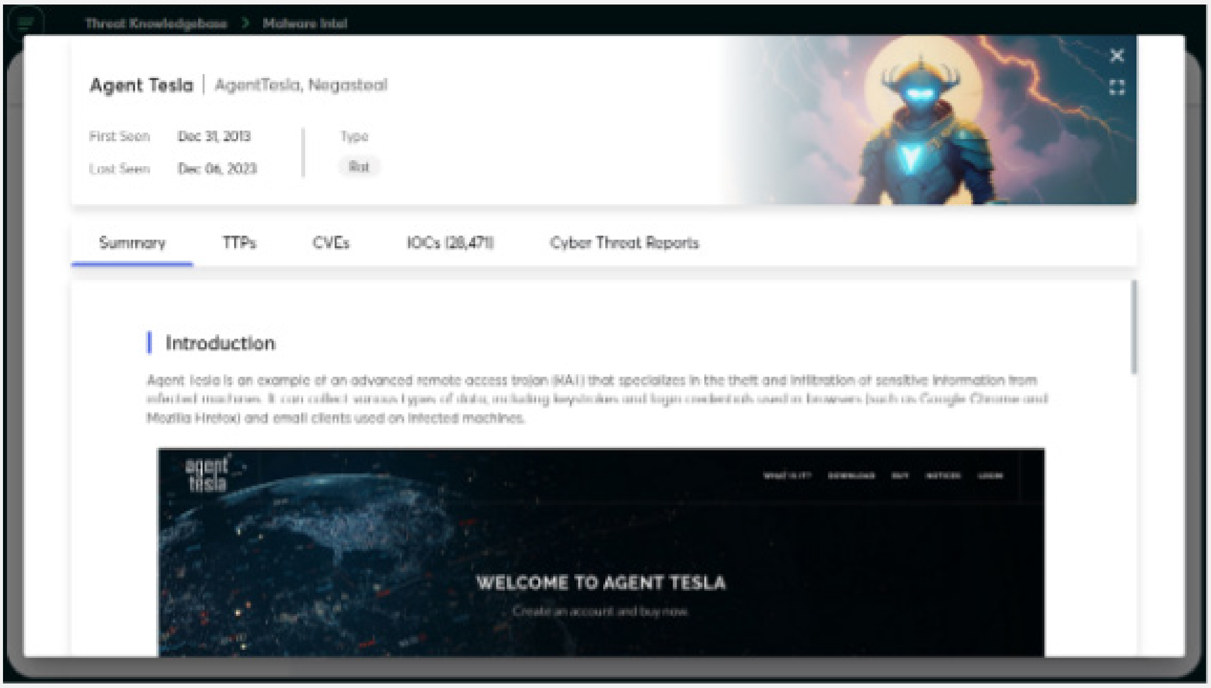
Emerging as a dominant force in the realm of ransomware, LockBit ransomware initiated its wave of assaults in September 2019. Driven by financial incentives, the group fearlessly pursues larger, prominent corporations and enterprises.

LockBit distinguishes itself with a myriad of distinctive traits, including advanced technological sophistication, the implementation of triple extortion tactics, robust recruitment efforts for affiliates, and the execution of highly impactful cyberattacks. LockBit's operational reach spans globally, with intermittent pauses that coincide with the integration of advanced enhancements into their ransomware arsenal. Their recent approach to attacks, coupled with their frequency, solidifies LockBit's position as a potent threat and resolute contender within the cyber domain.

Figure 16 - Threat Actor entity full information

3.5.2.2 MALWARE KNOWLEDGEBASE

Through the Malware Intelligence module, we offer an instantly accessible overview of crucial details pertaining to distinct strains of malware. These cards are consistently updated as new information is gathered. This encompasses details such as the delivery approach, potential consequences, tactics, techniques, and procedures (TTPs), Common Vulnerabilities and Exposures (CVEs) exploited by that type of malware, as well as identified indicators of compromise (IoCs). Additionally, you will find links to relevant reports published by the Cyberint research team. These Malware Cards serve as an excellent starting point for evaluating whether a specific malware instance poses any potential risks to your organization.



Agent Tesla | AgentTesla, Negasteal

First Seen Dec 31, 2013

Last Seen Dec 06, 2023

Type Rat

Introduction

Agent Tesla is an example of an advanced remote access trojan (RAT) that specializes in the theft and infiltration of sensitive information from infected machines. It can collect various types of data, including keystrokes and login credentials used in browsers (such as Google Chrome and Mozilla Firefox) and email clients used on infected machines.

Figure 17 - Malware Entity Information

3.5.2.3 CVE INTELLIGENCE MODULE

Cyberint's CVE Intelligence Module provides Infosec teams with impactful CVE intelligence for effective vulnerability triaging and patching strategy planning, from hundreds of open, deep, and dark web sources.

Background

As part of the global digital transformation and remote/hybrid workplace shift, security teams are facing a larger attack surface that relies on more 3rd party products, which leads to more vulnerabilities to handle.

- There are currently more that 200K published CVEs. Security teams often struggle to prioritize them.
- One of the most common practices to prioritize CVE patching is by their CVSS score.

- However, research reveals that only 5% of CVEs are ever exploited in the wild. CVSS doesn't aggregate the actual intelligence-based risk factors for each vulnerability, as it only considers how severe the impact of the vulnerability will be if it is actually exploited. CVSS is not enough to accurately understand risk.

- Multiple customers and prospects shared that it is essential to understand which vulnerabilities are being actively exploited by threat actors, which vulnerabilities have publicly available PoCs or sample exploit code, and so on. This intelligence is critical to an effective patch management program.

- "Researching a single CVE can take us between 4 hours to 2 days."

Module Overview

Cyberint CVE intelligence API (CVE API requires dedicated, annual license) provides a much-needed CVE enrichment layer to help make informed decisions when you conduct vulnerability triaging and plan your patching strategy. The API can be integrated with your Vulnerability Management System, SOAR, and CMDB and includes:

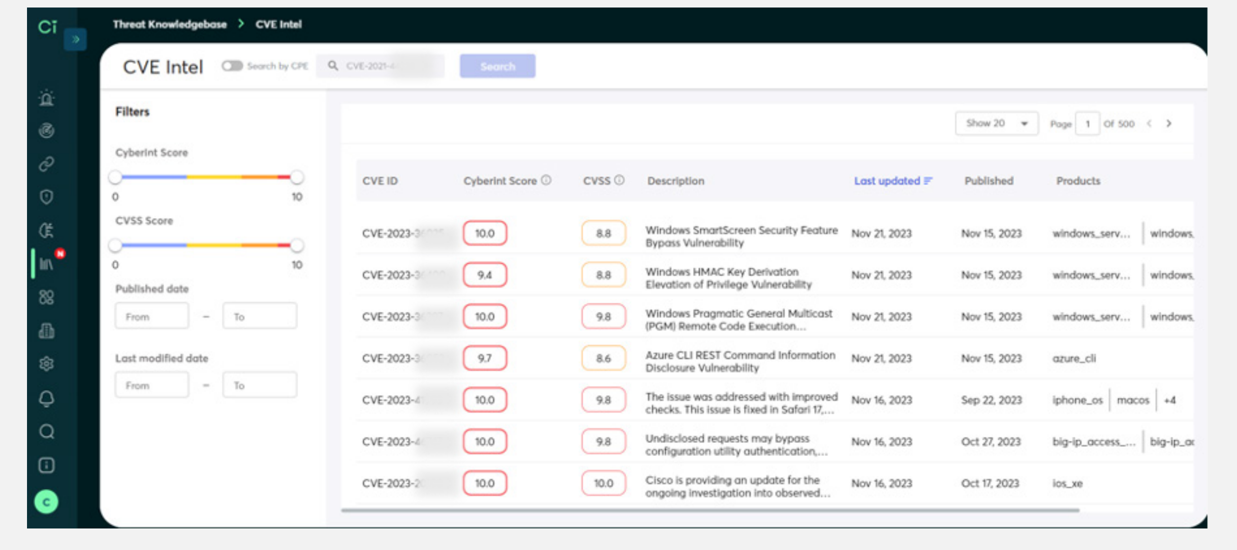
1. Cyberint Score, an intelligence-based risk score that reflects how probable it is that a specific vulnerability will be exploited, along with many other important factors such as CVSS.

2. Aggregated CVE intelligence analysis including risk factors (is it exploitable?), related Intel-Items, mentions, trends, and more.

3. Cyberint Research Team analysis and recommendations regarding the most trending CVEs among threat actors.

4. CVE Threat Intelligence, indicating if a CVE is being exploited in the wild, whether exploit code is offered for sale by threat actors on the Darknet or discussed on Telegram, and so on.

5. The CVE's official information, description, CVSS, CWEs, related products (CPE) and more.



CVE-2021-4[redacted]

Filters

Cyberint Score: 0 – 10

CVSS Score: 0 – 10

Published date: From – To

Last modified date: From – To

CVE ID	Cyberint Score	CVSS	Description	Last updated	Published	Products
CVE-2023-3[redacted]	10.0	8.8	Windows SmartScreen Security Feature Bypass Vulnerability	Nov 21, 2023	Nov 15, 2023	windows_serv... windows
CVE-2023-3[redacted]	9.4	8.8	Windows HMAC Key Derivation Elevation of Privilege Vulnerability	Nov 21, 2023	Nov 15, 2023	windows_serv... windows
CVE-2023-3[redacted]	10.0	9.8	Windows Pragmatic General Multicast (PGM) Remote Code Execution...	Nov 21, 2023	Nov 15, 2023	windows_serv... windows
CVE-2023-3[redacted]	9.7	8.6	Azure CLI REST Command Information Disclosure Vulnerability	Nov 21, 2023	Nov 15, 2023	azure_cli
CVE-2023-4[redacted]	10.0	9.8	The issue was addressed with improved checks. This issue is fixed in Safari 17,...	Nov 16, 2023	Sep 22, 2023	iphone_os macos +4
CVE-2023-4[redacted]	10.0	9.8	Undisclosed requests may bypass configuration utility authentication,...	Nov 16, 2023	Oct 27, 2023	big-ip_access_... big-ip_ac
CVE-2023-2[redacted]	10.0	10.0	Cisco is providing an update for the ongoing investigation into observed...	Nov 16, 2023	Oct 17, 2023	ios_xe

Figure 18 - CVE Intelligence Module

CVE sources used to calculate the risk score

We use multiple sources to provide the most comprehensive intelligence on CVEs which includes:

- Chatter in Chat Apps and Forums (e.g. Telegram)
- Exploit Repositories (e.g. Exploit-db)
- Paste Sites
- Darknet
- Malware Analysis Tool
- Social Media (Twitter)
- Code Repositories (Github)
- FIRST-EPSS
- NVD
- CISA KEV

3.5.2.4 KNOWLEDGEBASE DASHBOARD AND NEWS BULLETIN

The purpose of this dashboard is to serve as a homepage for the customer’s threat landscape, providing guidance to the user about which threats are most relevant to their organization. It helps the user to identify which entities they should focus on and learn more about, given the constantly changing global arena with many different kinds of actors and threat groups.

The dashboard is constantly updated with the latest entities, news items of relevant events and incidents (like breaches and ransomware attacks) as collected by the Cyberint Research team to provide the customer with effective situational awareness of the threats around him.

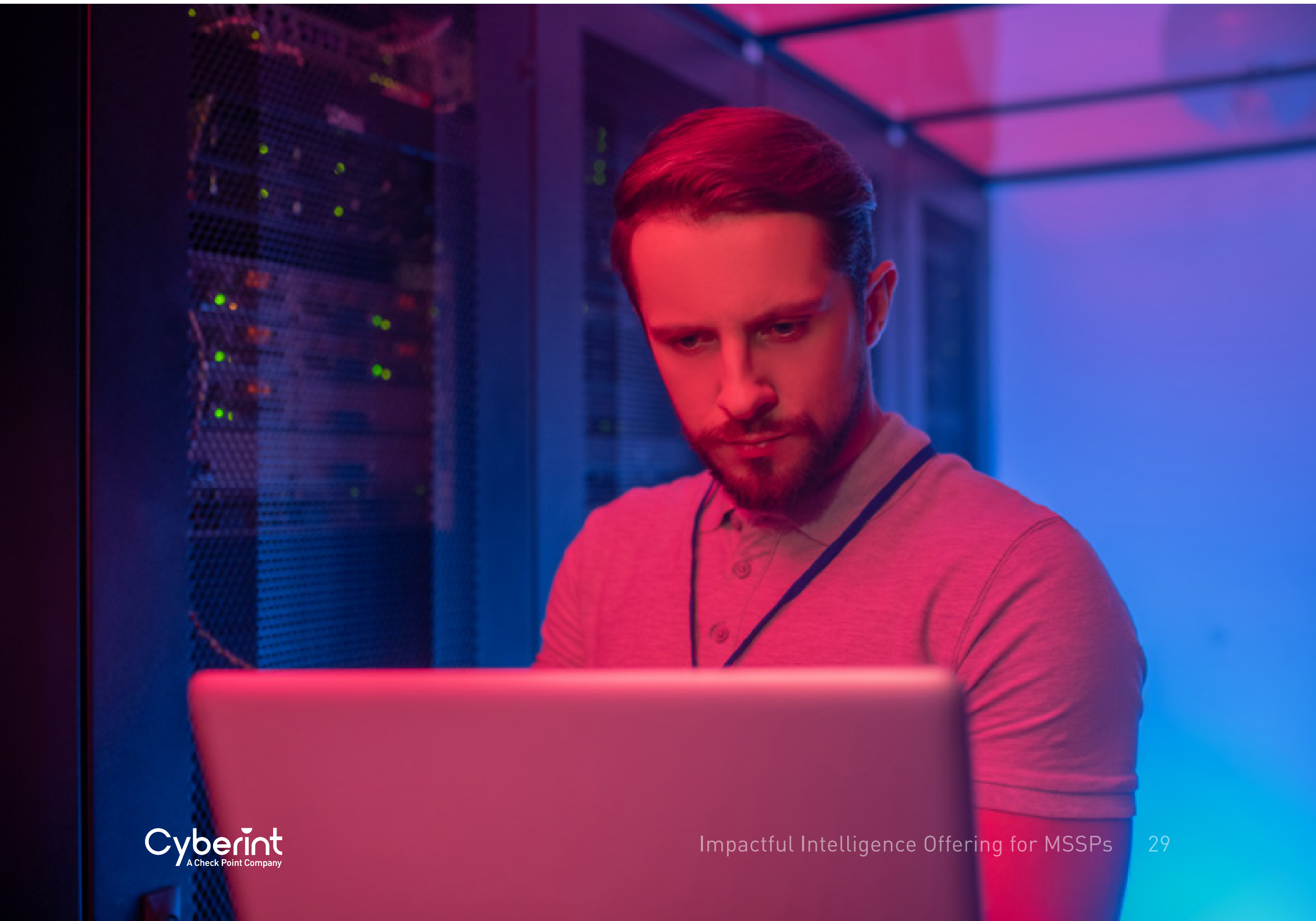
3.5.3 CYBERINT RESEARCH TEAM AND THREAT REPORTS

Cyberint's Cyber Research Team explores the frontier of the cyber threat landscape to maintain strategic visibility of trending threats. The Cyber Research Team analyzes vast amounts of data to create strategic threat intelligence reports, enabling decision makers to identify meaningful trends, and gain a broader and deeper perspective of the digital risks targeting their organization. The reports include periodic analysis of current sector risks, notable threat actors, TTP analysis, and more.

Some of the research report could be found in Cyberint blog: https://cyberint.com/blog/

Cyberint
New InfoStealer in Town:
The Continental Stealer
New InfoStealer in Town-The Continent...
CYBERINT WEEKLY >REPORT
Cyberint Weekly Review - Week 43
Cyberint
F5 BIG-IP Vulnerability CVE-2023-46747
F5 BIG-IP Vulnerability
Cyberint
Q3 RANSOMWARE
Ransomware Landscape - Q3

Figure 19- Cyberint research team report samples



3.6 CYBERINT INTEGRATIONS

3.6.1 INTEGRATIONS

Cyberint includes out of the box integrations with multiple SIEM, TIP, SOAR, Ticketing and FW platforms, to allow effective injections of Cyberint alerts. Many of the integrations could be found in the respective stores of the products.

The integration includes multiple APIs including (some APIs and integration requires a dedicated annual license):

- Alerts
- IOC
- CVE
- Credentials
- Takedowns

The following list is a sample list of some of the available integrations.

SOAR \ TIP	SIEM	Ticketing \ CMDB	Firewall / Cloud
XSOAR	IBM QRADAR	Jira	Palo Alto - Panorama
FortiSoar	Splunk	ServiceNow	Forcepoint
Chronicle SOAR (Siemplify)	Azure Sentinel	Axonius	AWS
Threat Connect	ArcSight		Azure
Cyware			

In addition, an API is available for other integrations which are currently not available out of the box.

3.6.2 SSO INTEGRATIONS

Cyberint supports Single Sign On (SSO) with Okta, Google Workspace, Azure AD & OneLogin to allow secure log-in without the needed for username and password input from the end-user.

4. ADD-ON MODULES & CAPABILITIES

4.1 WHITELABEL TENANT

Cyberint offers a whitelabeled version of the product for MSSPs that wish to provide a fully branded experience to their accounts. This capability is most valuable for mature MSSPs that plan to sell Cyberint at scale and deploy many tenants where end-users at the client organization wish to have hands-on access to the solution.

4.2 COINS FOR TAKEDOWNS & SPECIALIZED SERVICES

Required purchasing of Checkpoint SQU - ***Remediation and Investigation Coins CP-ERM-COIN***

Cyberint provides multiple remediation options upon detection of risks.

1. **Takedown** – removal of risks in the case of phishing, VIP impersonation, brand abuse, data leakage and more.

2. **Purchase of credentials** / payment cards from marketplaces.

3. **Specific investigations** – utilizing Cyberint's threat intelligence experts for deeper investigation, including virtual HUMINT operations.

In order to execute the above, "Cyberint Coins" need to be utilized. Each operation will utilize a different amount of coins according to its complexity and cost. The table below provides the remediation types and coins usage.

Activity Type	Coins Usage
Takedown of Phishing identified via Cyberint Alert	4
Takedown of Phishing reported by the customer	6
Takedown of Mobile application cost	4
Takedown of Social media cost	6
Takedown of Source code, AV, other	6
Investigation Hour	8
Purchase of credentials \ payment cards from marketplace	6

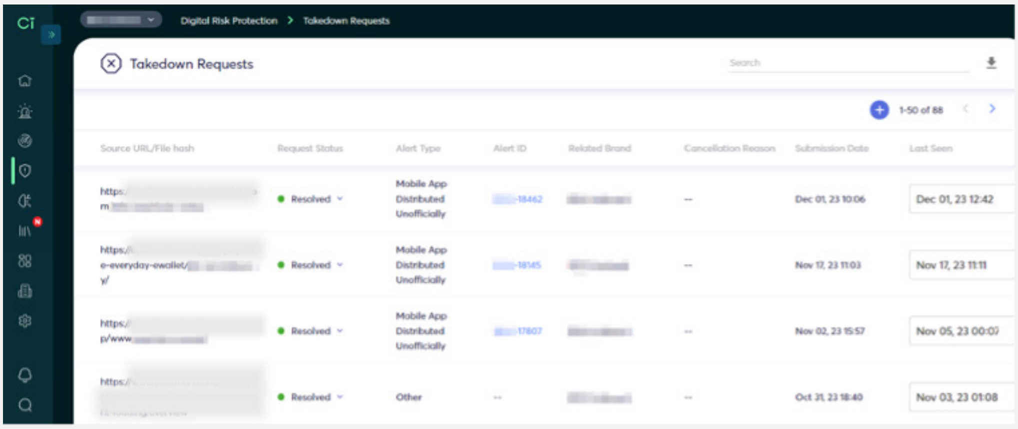
4.2.1 TAKEDOWNS

Upon detection of a malicious site, Cyberint can initiate a take-down process which involves, as necessary, notification to the relevant providers to remove the misleading content, blocking of domains, and updates to public blacklists.

Cyberint handles hundreds of takedown requests per week from various customers and can influence the different hosting and service providers to act quickly. Upon receiving the request for the removal of illegitimate content that is infringing upon the customers' trademarks, and/or used for malicious purposes, Cyberint takes action immediately. Cyberint supports the following takedowns:

- Phishing sites.
- Impersonating social media accounts.
- Mobile Applications in official and non-official stores.
- Source code in code repositories.
- Files in Anti-Virus engines.
- Data leaks in some file sharing sites.

The takedown request is initiated via Cyberint alert section and the "Takedown request" screen allows customers to monitor the progress as presented in the picture below:



Source URL/File hash	Request Status	Alert Type	Alert ID	Related Brand	Cancellation Reason	Submission Date	Last Seen
https:/ [redacted] m [redacted]	● Resolved	Mobile App Distributed Unofficially	[redacted]-18462	[redacted]	--	Dec 01, 23 10:06	Dec 01, 23 12:42
https:/ [redacted] e-everyday-ewallet/ [redacted] y/	● Resolved	Mobile App Distributed Unofficially	[redacted]-18145	[redacted]	--	Nov 17, 23 11:03	Nov 17, 23 11:11
https:/ [redacted] p/www. [redacted]	● Resolved	Mobile App Distributed Unofficially	[redacted]-17807	[redacted]	--	Nov 02, 23 15:57	Nov 05, 23 00:07
https:/ [redacted]	● Resolved	Other	--	[redacted]	--	Oct 31, 23 18:40	Nov 03, 23 01:08

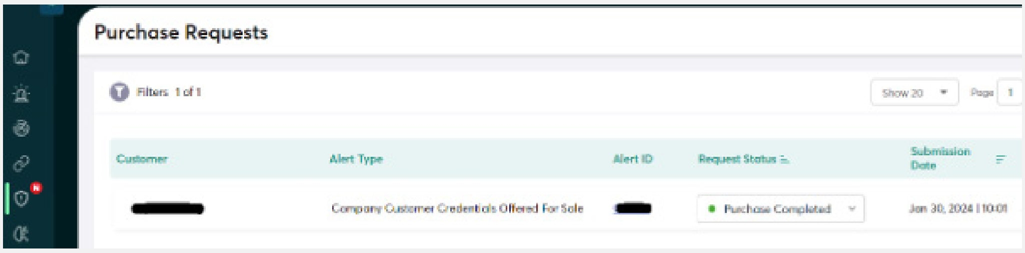
Figure 20 - Cyberint Takedown request status page

4.2.2 PURCHASE OF CREDENTIALS

Darkweb marketplaces as Russian Market, 2Easy and more offer credentials for sale, obtained through various illegal activities. Cyberint alerts on the above and the remediation option is to acquire those credentials before anyone else can do so.

The acquisition is done anonymously via Cyberint's covert darkweb operations and is executed via "purchase credentials" button in the respective alert types.

Credential purchase will consume "Cyberint Coins" and can be tracked via the Credentials Purchase Requests screen.



Customer	Alert Type	Alert ID	Request Status	Submission Date
[redacted]	Company Customer Credentials Offered For Sale	[redacted]	● Purchase Completed	Jan 30, 2024 I 10:01

Figure 21 - Credential purchase tracking screen

4.2.3 MANAGED HUMINT OPERATIONS

Cyberint provides a valuable human element when it comes to research, investigation, and threat intelligence operations. The Virtual HUMINT capabilities, e.g. live interaction with threat actors, enable deeper contextualization which is required for effective mitigation.

HUMINT operations provide the following value:

- Assessing veracity and imminence of a threat
- Obtaining TTPs, motivation, accomplices
- Gathering IoCs for investigation and mitigation

4.3 THREAT HUNTING LICENSE

Threat Intelligence Events collected within this module are prefiltered to display only raw intelligence which is relevant to the organization. This allows focused hunting and identification of threats that are related to the organization. Prefiltering is done through configuring the Cyberint platform with assets that belong to the organization, such as domains, keyword terms, brand names, VIP names, and so on. Once configured, Cyberint begins hunting through all sources for relevant intelligence items, flagging only relevant events within the targeted threat events view.

The user can create **custom threat hunting** rules in order to generate alerts for specific identified use cases.

For advanced threat hunting, Cyberint provides a dedicated user license with access to sophisticated features.

A threat hunting user can utilize the following capabilities.

4.3.1 FULL ACCESS TO THE GLOBAL INTELLIGENCE KNOWLEDGEBASE

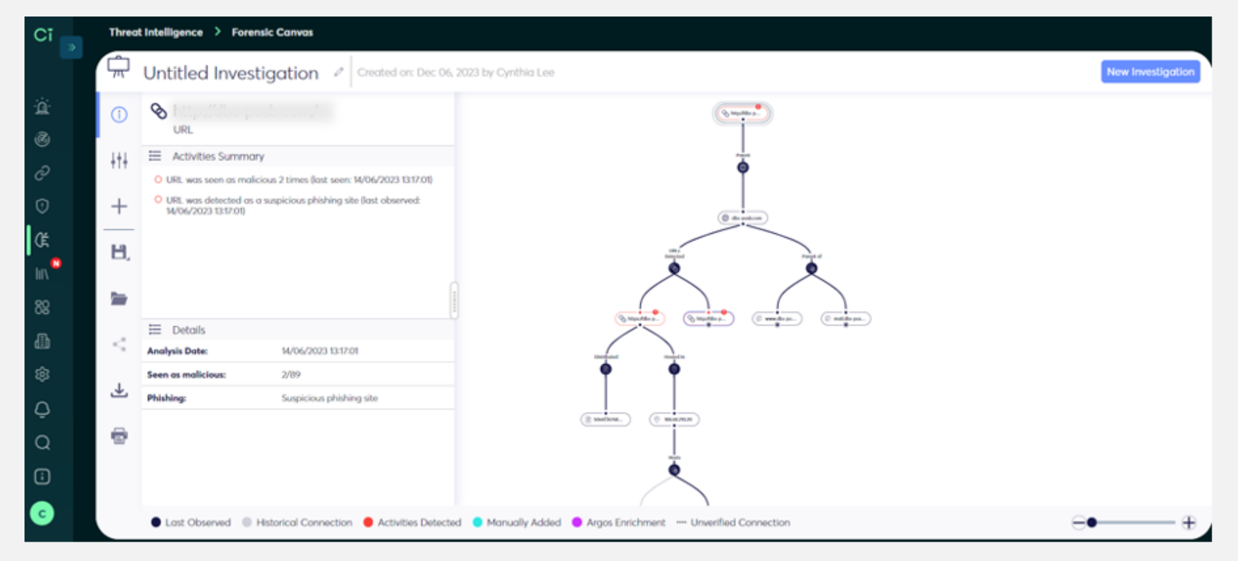
Threat hunting users have the ability to view not only the main summary but also the underlying intelligence, TTPs, victimology, and more, and pivot between entities.

4.3.2 ACCESS TO CYBERINT DATA LAKE

Full access to the Cyberint datalake of open, deep and darkweb collection, with the ability to use complex query language and analyze any available information. While regular users receive only access to the “raw data” related to the assets configured in their tenant, the data lake offers unlimited visibility into all collected intelligence items and threats.

4.3.3 CYBERINT FORENSIC CANVAS MODULE

To provide threat hunters with a tool to perform deep-dive investigations on suspicious intelligence items, Cyberint created the Forensic Canvas module within the Cyberint platform. Utilizing the data gathered from multiple sources, Forensic Canvas provides a detailed and interactive graphical visualization of the indicator in question. Forensic Canvas has been designed as an intuitive interface for investigation reporting and correlation.



Threat Intelligence > Forensic Canvas

Untitled Investigation

Created on: Dec 06, 2023 by Cynthia Lee

New Investigation

[redacted]
URL

Activities Summary

- ○ URL was seen as malicious 2 times (last seen: 14/06/2023 13:17:01)
- ○ URL was detected as a suspicious phishing site (last observed: 14/06/2023 13:17:01)

Details

Analysis Date:	14/06/2023 13:17:01
Seen as malicious:	2/89
Phishing:	Suspicious phishing site

● Last Observed ● Historical Connection ● Activities Detected ● Manually Added ● Argos Enrichment ┄ Unverified Connection

Figure 22 - Cyberint Forensic Canvas Module

This allows discovery of attack infrastructure, both past and present, and uncovers potential Threat Actors' profiles and identities. Common uses of Cyberint's Forensic Canvas module include pivoting from data points and IoCs to potential threat items, as well as reversing threat investigations to identify digital attack infrastructure.

4.4 ACTIVE EXPOSURE VALIDATION

Cyberint's Active Exposure Validation (AEV) capability is an extension of the Attack Surface Management module. While the ASM focuses on discovering external digital assets, fingerprinting what technologies are running on each asset, and detecting outdated software with known CVEs, the AEV feature makes active attempts to exploit digital assets. This automated exploit testing capability identifies the exposures that can be easily exploited, thus highlighting some of your organization's most critical risks that must be remediated immediately.

4.4.1 TEST KNOWN CVES FOR EXPLOITABILITY

Go beyond standard CVE detection with active attempts to exploit known vulnerabilities. The traditional approach to CVE detection—that is, fingerprinting technologies and running an automated CPE lookup in a CVE database to see whether known vulnerabilities existing with the software and specific version number—produces a large quantity of unvalidated results. Some environmental factors or mitigating security controls may prevent exploitation of a CVE, even when the software is out of date.

The Active Exposure Validation capability addresses this limitation by actively attempting to exploit CVEs using advanced automation. If the CVE is exploitable, an Alert is issued with full context, including the exact payload used to exploit the asset, so you can share evidence with relevant stakeholders and remediate the vulnerability as quickly as possible.

4.4.2 CHECK YOUR WEB APPS FOR SECURITY ISSUES

Run thousands of tests on your digital assets to find common issues in your organization's web applications that would not be listed in a CVE database. Test for SQL injections, directory traversals, cross-site scripting, and other common web app vulnerabilities.

4.4.3 REAL-TIME ALERTS FOR STREAMLINED REMEDIATION

Receive an enriched alert the moment an exploitable risk is detected. Leverage integrations to feed alerts to your SOC tools or ticketing system. Accelerate remediation and eliminate high risk exposures.

4.5 SUPPLY CHAIN INTELLIGENCE MODULE

Check point SQU Additional Supply Chain Monitoring # of Vendors CP-ERM-SUPPLY-STD

The Cyberint Supply Chain Intelligence module helps customers measure, manage, and mitigate risks introduced through vendors and other digital suppliers.

4.5.1 DISCOVERY OF DIGITAL SUPPLIERS

Through the external attack surface discovery process, Cyberint detects the software, services, and technologies running on externally facing assets, which enables the platform to automatically identify which vendors produce those technologies. These vendors and digital suppliers are added into the Supply Chain Intelligence module as suggestions to simplify and accelerate the process of creating a vendor inventory.

Any vendors and 3rd party suppliers not identified through the automated discovery process can be manually added into scope for cyber risk monitoring.

4.5.2 CONTINUOUS MONITORING

Cyberint monitors the vendors, partners, and suppliers that have been added into scope for cyber risks along 4 different dimensions:

- Exposures –indicates the number of external risks and attack vectors that the 3rd party is exposed to, including open ports, malware infections, leaked credentials, and more.

- Hygiene – an estimate of the 3rd party's security hygiene and posture, based on the version of software running on externally-facing assets, the presence of CVEs, the versions of protocols like TLS, issues related to SSL certificates, and so on.

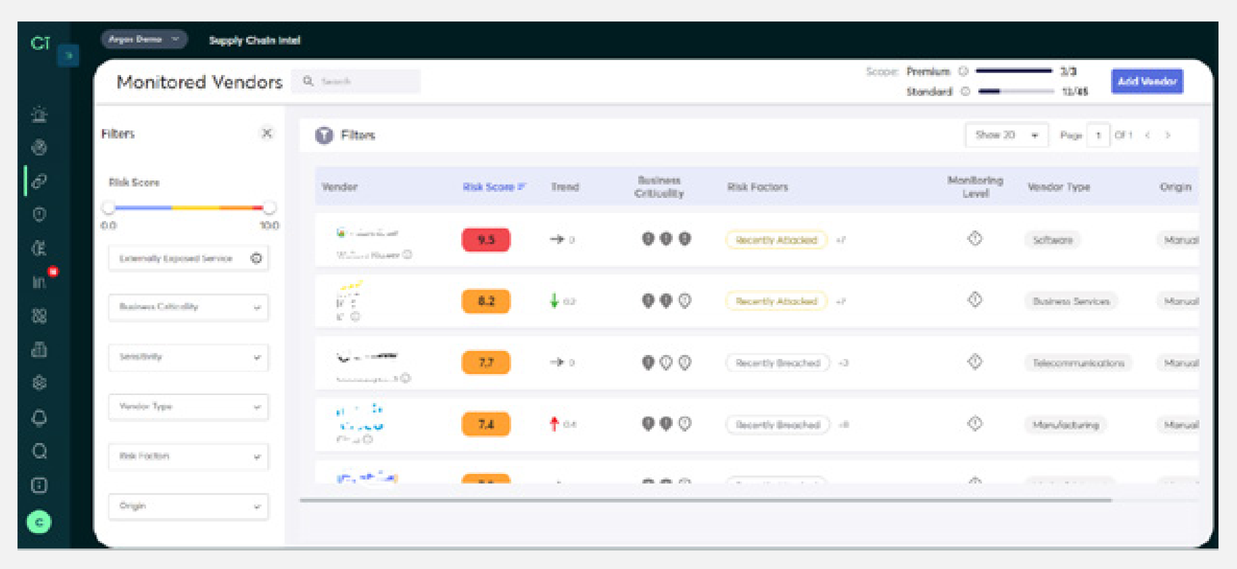
- Targeted Level – uses deep and dark web threat intelligence to check for mentions of the 3rd party's brands, products, domains, and assets in threat actor forums or underground marketplaces. This is a measure of how targeted the 3rd party is by bad actors.

- Breach History – using historical data—from public media reports to proprietary threat intelligence collected by Cyberint over the past decade—the vendor is assigned a risk score based on their cybersecurity track record.

- Vendor Monitoring is continuous and ongoing so major security events, such as ransomware attacks and data breaches, are detected in real-time.

4.5.3 ALERTING

For 3rd party vendors and suppliers that are in scope, Cyberint issues alerts in real time when major security events are detected. Examples include cyber attacks, ransomware incidents, and data breaches. When a major event like this occurs, Cyberint immediately issues an alert, which can then be shared via API with any integrated platforms, e.g. SIEM, SOAR, or XDR.



Vendor	Risk Score	Trend	Business Criticality	Risk Factors	Monitoring Level	Vendor Type	Origin
[illegible]	9.5	→ 0	●●●	Recently Attacked +7	◇	Software	Manual
[illegible]	8.2	↓ 0.2	●●○	Recently Attacked +7	◇	Business Services	Manual
[illegible]	7.7	→ 0	●○○	Recently Breached +3	◇	Telecommunications	Manual
[illegible]	7.4	↑ 0.4	●●○	Recently Breached +8	◇	Manufacturing	Manual

Figure 23 - Cyberint Supply Chain Intelligence page

4.6 RISK INTELLIGENCE (IOC) FEED

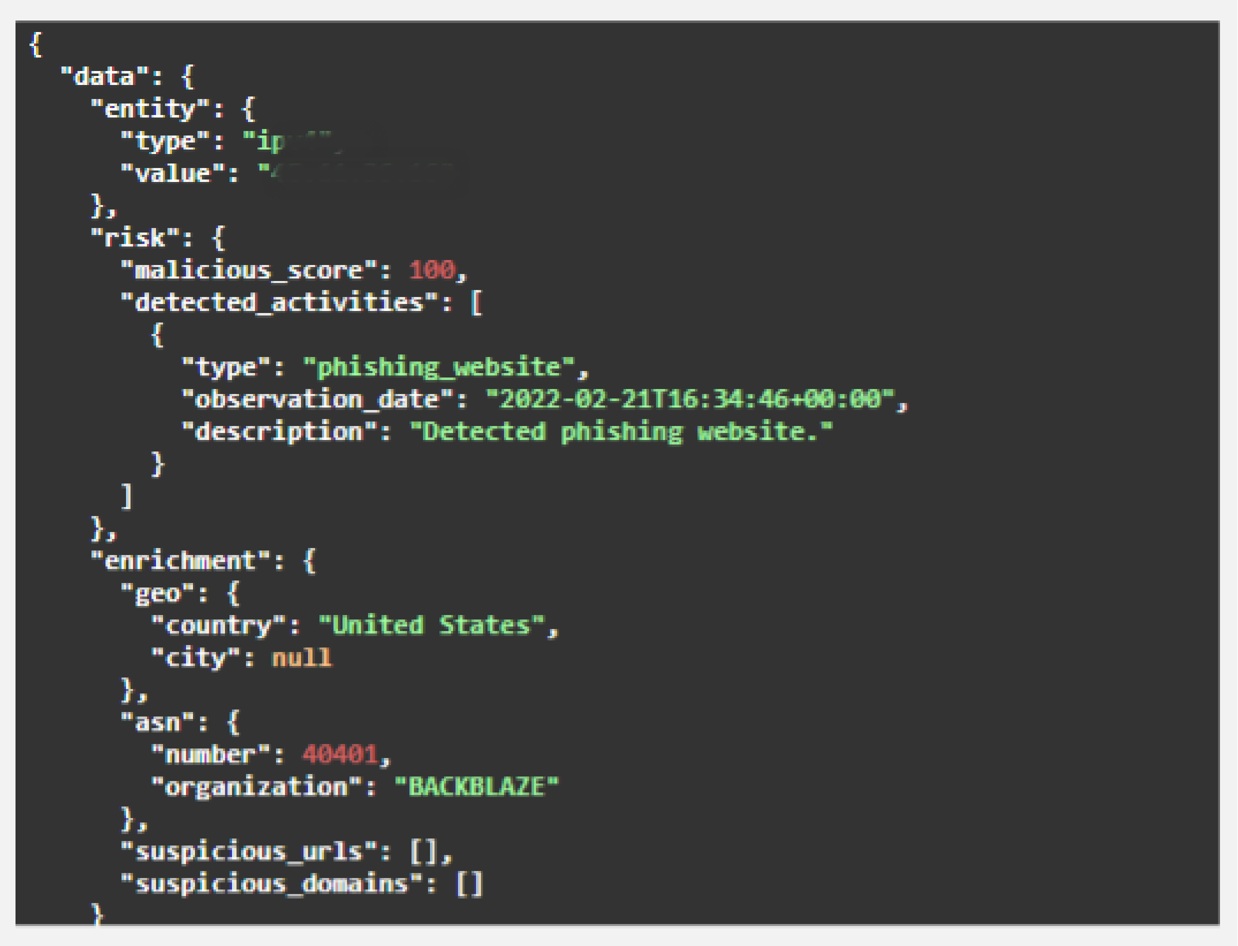
IOC feed and API requires dedicated, annual license. As part of Cyberint threat intelligence abilities, Cyberint collects and analyzes IoCs from different sources. These include Antivirus repositories, Darkweb mentions, machines infected with an Infostealer, social media reporting and more.

Cyberint provides the ability to analyze IoCs in 2 main ways:

4.6.1.1 IOC ENRICHMENT API

Cyberint provides an API which allows queries regarding a specific suspected IoC such as an IP address, URL, Domain, or Hash.

Each request is conducted via http to Cyberint API and receives a JSON format response with the available information. For example, the answer for the specific IP address “45.11.36.16” will be that it is a phishing website with the details:



```
{
  "data": {
    "entity": {
      "type": "ip[redacted]
      "value": "[redacted]
    },
    "risk": {
      "malicious_score": 100,
      "detected_activities": [
        {
          "type": "phishing_website",
          "observation_date": "2022-02-21T16:34:46+00:00",
          "description": "Detected phishing website."
        }
      ]
    },
    "enrichment": {
      "geo": {
        "country": "United States",
        "city": null
      },
      "asn": {
        "number": 40401,
        "organization": "BACKBLAZE"
      },
      "suspicious_urls": [],
      "suspicious_domains": []
    }
```

Figure 24 - Cyberint IoC API format

The API could be used by different SIEM and SOAR platforms in order to provide complete alert handling cycles.

4.6.1.2 IOC FEED

The IoC module also makes it possible to extract the IoCs as a feed in the format of a downloadable file. The file could be ingested in the SIEM for internal correlation of activities.

The feed allows querying on different categories, such as:

- Malware payload
- C&C server
- Infected machine
- Botnet
- Phishing website
- Payload delivery
- Credit card skimming

4.7 PHISHING BEACON

Some phishing sites are created using valid domains by adding a new URL with the phishing page, making look-alike domain detection methods ineffective.

To identify such phishing cases, Cyberint has created the Phishing Beacon technology, which is a small snippet of hidden code implemented within the customer's main webpages or public facing login pages. Once implemented and configured, the beacon will alert Cyberint any time that the page is copied and hosted on any other domain.

With the Phishing Beacon in place, Cyberint's customers have seen increased detection of phishing sites with high accuracy.

Pricing: Phishing beacon is licensed according to the number of subdomains in which it is placed. The root of a domain is considered one subdomain.

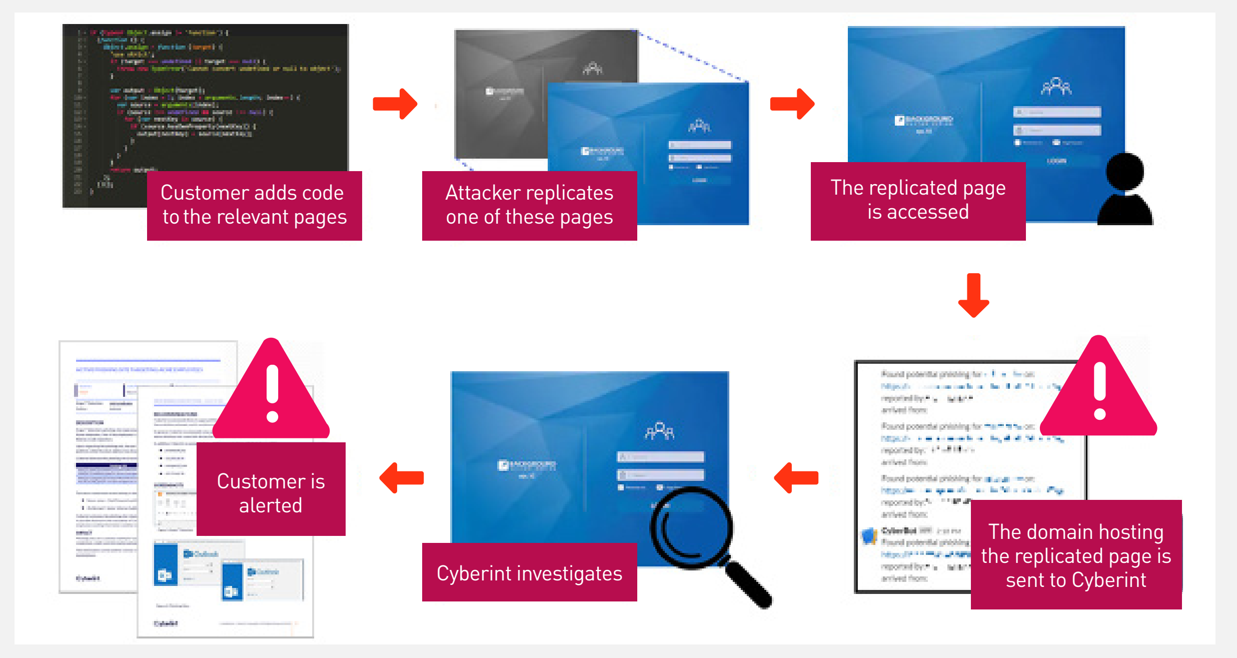

Customer adds code to the relevant pages
Attacker replicates one of these pages
The replicated page is accessed
The domain hosting the replicated page is sent to Cyberint
Cyberint investigates
Customer is alerted

Figure 25 - Phishing Beacon operational flow

CONTACT US

ISRAEL

Tel: +972-73-226-4555
5 Shlomo Kaplan Street
Tel Aviv 6789159

USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1,
Singapore 079120

PHILIPPINES

Tel: +63 2 8465 9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas
Makati City 1223, Metro Manila

UK AND IRELAND

Tel: +44 20 7628 4211
85 London Wall, 4th Floor,
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F,
1-2-8, Toranomon Minato-ku, Tokyo 105-0001

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://cyberint.com / checkpoint.com/erm