Attack Surface Monitoring

Cyberint

> “I have a level of assurance and trust that Cyberint's team is always there for me. The feeling that they always have my back is invaluable and has given me the confidence that we have enough visibility and can be proactive in dealing with different cyberthreats.”
>
> Mark Frogoso,
> CISO at GCash

Exploitable ports, exposed company web interfaces, hijackable subdomains and SSL/TLS issues - these are just a few of the threats that organizations face from the ever-expanding numbers of attack surfaces.

Organizations fight back, but it often results in a siloed approach where security teams shoot in different directions. That means that multiple solutions generate siloed alerts.

Unlike other solutions, **Cyberint**’s holistic and integrated approach combines external Attack Surface Monitoring (ASM) and advanced threat intelligence. The two modules work together to seamlessly and continuously infuse and enrich the Argos Edge™ to provide a comprehensive solution from ongoing discovery of assets to monitoring and identifying business risks and helping in remediation.

Attack Surface Monitoring Capabilities - identifying weaknesses and vulnerabilities that no other solution can

How Argos Edge™ Attack Surface Monitoring Protects you from External Threats

A HOLISTIC AND INTEGRATED APPROACH

Gain full and automatic visibility into your digital assets with the combined approach of Argos Edge™ attack surface monitoring and advanced threat intelligence platform.

AN AGILE AND FLEXIBLE DRP OFFERING

Start by identifying and monitoring your organization’s attack surfaces. Expand to other Digital Risk Protection (DRP) related challenges as they evolve in the different stages of your security maturity journey.

ADVANCED DISCOVERY AND ACCURATE ATTRIBUTION OF ASSETS

Continuously discover and monitor a wide range of asset types, that are accurately attributed to the company, for identifying unknown assets and shadow-IT.

SIMPLICITY THAT DOES NOT COMPROMISE DEPTH

Get actionable, focused and relevant alerts in real time for complex security challenges with our AI-powered technology.

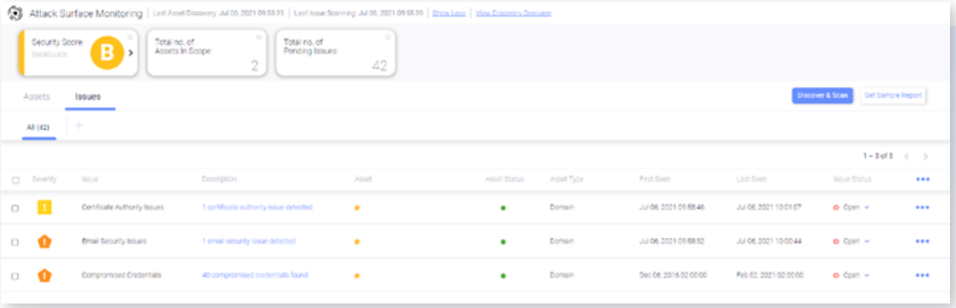
Full Coverage and Operational Control

Control your presence in the digital environment with Argos Edge™ Attack Surface Monitoring's two critical components.

DISCOVERY AND SCANNING

Continuously uncover and map all externally-facing assets. Scan for issues and vulnerabilities threatening to harm your organization.

- Automate the discovery of your digital assets
- Configure periodic remapping of your organization's digital presence to revalidate and update assets
- Identify and categorize critical assets
- Recognize assets that are no longer attached to the company as well as new assets
- Enable historical tracking of your digital presence



Attack Surface Monitoring | Last Asset Discovery: Jul 06, 2021 09:55:35 | Last Issue Scanning: Jul 06, 2021 09:55:35 | Show Less | View Discovery Overview

Security Score: B

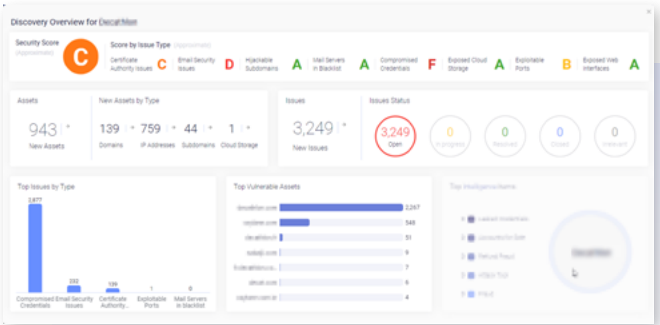
Total no. of Assets In Scope: 2

Total no. of Pending Issues: 42

□	Severity	Issue	Description	Asset	Asset Status	Asset Type	First Seen	Last Seen	Issue Status
□	!	Certificate Authority Issues	1 certificate authority issue detected	★	●	Domain	Jul 06, 2021 09:58:46	Jul 06, 2021 10:01:07	Open
□	!	Email Security Issues	1 email security issue detected	★	●	Domain	Jul 06, 2021 09:58:32	Jul 06, 2021 10:00:44	Open
□	!	Compromised Credentials	40 compromised credentials found	★	●	Domain	Dec 06, 2016 02:00:00	Feb 02, 2021 02:00:00	Open

MANAGEMENT

Fine-tuning and prioritizing all assets discovered to allow for optimal handling and management. Continuously monitor for new issue.



- Track an issue's lifecycle from detection to resolution
- Calculate a security score to assess and prioritize risks
- Automatically close resolved issues
- Enable historical snapshots of issue handling
- Report capabilities including ad-hoc and periodic reports

How Argos Edge ™ Attack Surface Monitoring Works

From automated discovery to managing real-time issues and providing a security risk score, leading organizations across a wide range of industries choose **Cyberint** for its attack surface monitoring solution.

Discovery

Step 1

Uncover & Map

Uncover your digital presence and map all externally facing digital assets. This includes domains, subdomains, cloud storage and more. Argos Edge™, **Cyberint**'s proprietary platform, collects information from multiple open, deep and dark web data sources for a holistic approach to discovering your organization's digital presence: and alllow you to also detect Shadow IT.

Step 2

Scan & Detect

Scan and detect your company's digital presence for issues and vulnerabilities such as leaked credentials, malware infections, exploitable open ports, vulnerable web interfaces, and more. The **Cyberint** dashboard displays all assets and issues in a granular operational view.

Step 3

Assess the Risk

Calculate a security score by comparing current threats against your organization's current best practices and how it currently manages its issues. By placing the security score in context, you can better evaluate the risks your organization faces at all times.

Management

Step 4

Monitor & Reiterate

Prioritize and act on all assets and issues discovered. Present them to your security team in an operational view that enables handling, managing issue statuses and assignments, and asset management. Remove and add assets while also setting different priorities for your most critical assets.

Step 5

Prioritize & Act

Map the organization's on an ongoing basis to discover new assets and act upon any vulnerabilities or threats identified.

Argos Edge ™ Attack Surface Monitoring Prioritizes a Wide Variety of External Threats

EXPLOITABLE PORTS

Detect potentially exploitable ports before attackers do and prevent the leak of sensitive information or access to an internal system. Identify exposed applications that attackers can use to steal private or regulated data.

EXPOSED COMPANY WEB INTERFACES

Continuously monitor and scan exposed web interfaces that can be exploited by threat actors to leak sensitive information. Automatically discover third-party technologies with known vulnerabilities that interface with your organization's digital presence.

EMAIL SECURITY ISSUES

Track and manage misconfigurations in email authentication standards. Safeguard against phishing campaigns that can spread malware within your networks and access internal information. Defend against phishing campaigns targeting customers that cause churn and damage brand reputation.

CERTIFICATION AUTHORITY AUTHORIZATION (CAA)

Monitor misconfigurations in certificate authorization standards that allow threat actors to issue a legitimate certificate for non-legitimate websites. Identify the resulting risks threat actors use to exploit the trust relationships between domains to execute phishing campaigns.

Cyberint

BLACKLISTED MAIL SERVERS

Discover IP addresses listed in blacklist repositories of DNSBL servers. Identify IP addresses that have been flagged due to suspicious or spam activity.

HIJACKABLE SUBDOMAINS

Continuously uncover subdomains that have been hijacked and could be used to conduct complex phishing attacks on your organization's employees and customers. This extends to hijacked sessions of logged-in users in any service using vulnerable domains.

OPEN CLOUD STORAGES

Track and continuously update your monitoring of exposed cloud storage accounts. Safeguard against threat actors that modify and inject your data with malicious content, putting your entire organization - its employees, customers, partners and systems - all at risk.

COMPROMISED CREDENTIALS

Protect both your employee and customer credentials dark web by malicious actors seeking to gain access to internal data. Defend against illicit access of web services to execute spear phishing attacks on key employees and gain access to entire organizational systems.

SSL/TLS ISSUES

Defend your organization against vulnerabilities that could lead to various attacks that exploit weak cipher suites, keys and more. These attacks can then lead to traffic interception or data exchange decryption, allowing Man-in-the-Middle attacks to impersonate a server or leak data from communication between the client and server.

WEB APPLICATION SECURITY ISSUES

Identify misconfigurations of security headers leaving your organization unprotected against Man-in-the-Middle attacks, cross-site scripting, data corruption, sensitive data exposure and various attacks.

About Cyberint

Cyberint believes in making the digital world a safer place to conduct business by protecting our customers from cyber threats beyond the perimeter. We do this by providing a rich set of external Digital Risk Protection solutions – both automated and tailored with human expertise – along with Threat Intelligence. **Cyberint** serves leading brands worldwide including Fortune 500 companies across industries such as finance, retail, helathcare, eCommerce, gaming, media, and more.

Contact information:

www.cyberint.com | sales@cyberint.com | blog.cyberint.com