Feb, 2022

Cyberint Pricing Model

All you need to know

Cyberint

1 CONTENTS

2 INTRODUCTION

Cyberint offers a wide range of activities and services that are built on top of the Argos platform.

The new pricing model represents the various components of the offering. The model is split into defined packages but allows flexibility thanks to the additional aspects of size and the available add-ons.

This document outlines the concept of the model, how it should be applied and FAQs

3 THE PRICING MODEL

3.1 MODEL COMPONENTS

3.1.1 Packages

The packages are differentiated by the scope of use cases and modules that they cover.

Each of the categories above are split into specific use cases, as listed in the diagram below.

Diagram 1 – packages definition

Use cases / Packages	Categories	1 - Attack Surface Monitoring	2 - Phishing & Brand Abuse	3 - Silver	4 - Gold	5 - Platinum	6 - Deep & Dark Web Monitoring
Exploitable ports	Vulnerabilities	v		v	v	v	
Exposed company web interfaces	Vulnerabilities	v		v	v	v	
Hijackable subdomains	Vulnerabilities	v		v	v	v	
Email security issues	Vulnerabilities	v		v	v	v	
CAA issues	Vulnerabilities	v		v	v	v	
Open cloud storage	Vulnerabilities	v		v	v	v	
Mail server blacklisted	Vulnerabilities	v		v	v	v	
Executive impersonation in social media	Brand Abuse		v	v	v	v	
Brand impersonation in social media	Brand Abuse		v	v	v	v	
Brand abuse websites detection	Brand Abuse		v	v	v	v	
Mobile apps impersonation	Brand Abuse		v	v	v	v	
Private access token	Data Compromise			v	v	v	v
Customer credentials exposed	Data Compromise			v	v	v	v
Customer payment cards exposed	Data Compromise			v	v	v	v
Employee credentials	Data Compromise	v		v	v	v	v
Source code disclosed	Data Compromise				v	v	v
Leaked documents (files and emails)	Data Compromise				v	v	v
Advanced sensitive information disclosure incl. PIIs, etc.	Data Compromise					v	
Refund fraud services and tutorials	Fraud					v	
Carding services and tutorials	Fraud					v	
Advanced fraudulent activities	Fraud					v	
Domain Squatting	Phishing		v	v	v	v	
Phishing websites detection	Phishing		v	v	v	v	
Phishing Beacon	Phishing			v	v	v	
Advanced phishing detection incl. phishing kits, emails, etc.	Phishing				v	v	
Credential Stuffing Tool Targeting Company	Attackware				v	v	v
Brute Force Tool Targeting Company	Attackware				v	v	v
Data Scraping Tool for Company Application	Attackware				v	v	v
Vulnerability Scanner Targeting Company	Attackware				v	v	v
Advanced attacks detection incl. attack prep, attack tools, scanners, etc.	Attackware				v	v	v

Diagram 2 – Use case by category

You can find the details of each of the use cases in the Glossary (Appendix 2).

In the table below you can see the typical customers profiles for each of the packages. This classification is a major tool for the discovery process.

1 - Attack surface Monitoring	2 - Phishing & Brand Abuse detection	3 - Silver	4 - Gold	5 - Platinum	6 – Depp & Dark web monitoring
• SMB-SME • Focused on B2B business • Has some digital footprint • Does not have research or team of TI analysts	• SMB-SME • Focused on B2C business • Suffers from phishing attacks • Does not have research or team of TI analysts	• SME-Enterprise • Focused on B2B business • May have its own team of TI analysts • Has large digital footprint • May have a central SIEM or SOAR systems	• Enterprise • Suffers from massive targeted attacks • May have its own team of TI analysts • Has large digital footprint • Has a central SIEM or SOAR systems	• Enterprise • Suffers from massive targeted attacks • May have its own team of TI analysts • Has a team of SOC analysts • Has large digital footprint • Has a central SIEM or SOAR systems	• Enterprise • Suffers from massive targeted attacks • May have its own team of TI analysts • Has a team of SOC analysts • May have a central SIEM or SOAR systems

Diagram 3 – Typical customers profiles

The activities included in each package are listed in the Proposal.

Apart from the use cases coverage, each package includes also different products and service elements as seen in the following table:

Use Cases *Modules*	*1 - Attack Surface Monitoring*	*2 - Phishing & Brand Abuse*	*3 - Silver*	*4 - Gold*	*5 - Platinum*	*6 - Deep & Dark Web Monitoring*
Alerts Center	v	v	v	v	v	v
API Access	v	v	v	v	v	v
News Ticker	v	v	v	v	v	v
Number of users	2	2	3	5	10	3
Phishing beacons domains			1	3	5	
Raw intel access (targeted)				v	v	v
Services						
Ongoing Intelligence Expert Triaging				v	v	
Cyber Investigation & HumINT Operations hours (yearly)				40	60	
Takedowns (annual)	0	25	10	25	50	

Diagram 4 – Packages scope

Access to raw data (targeted data)
Customers that would like to engage their analysts with their targeted data that is generated in the Argos platform, can purchase a standalone package that includes the use cases of package #3 (Bronze). This package does not include the alerts mechanism.

3.1.2 Sizing

Each of the packages comes in various sizes to support various customer types.

- The size of the company is determined by the required # of Monitored Assets (for packages #1,3,4,5) and # of brands (for package #2).
- Monitored Assets are an organization's digital resources that can be targeted by or exposed to cybersecurity threats - these can include organization names and brand/product names, domains/subdomains, IP address, employee names and email addresses, social media profiles, general keywords (e.g., confidential classification keywords, payment card bin number (6-8 digits)).

3.1.3 Add-ons

The customer can choose to add additional components, either increase existing amounts or adding add-ons that are not originally included.

The available add-ons are:

- Additional Users
- Additional Assets (in bulks of 100)
- Additional phishing beacons
- Additional takedown requests
- Additional analyst hours
- Access to Forensic Canvas
- Access to raw data (targeted data)
- Premium support

4 DISCOVERY FLOW

Steps	*Question*	*Purpose*
1. Determine which use cases are relevant for the underlying customer	The type of business you employ – B2B or B2C?	is attack surface mapping enough or more thorough coverage is needed (package #1 or #3 or higher)
	Do you manage your business through portals with your users?	potential target for phishing and fraud (packages #2 or #3-5)
	What types of attacks do you experience?	Determine the overall needed use cases
	Do you have you own team of analysts and/or researchers?	Need access to non-managed, raw data
	Is there a ticketing \ SOAR system in place?	To determine the ability and interest to integrate with the existing cyber technologies in place
	Are there any compliance requirements?	Understand reports, need for an entry level package (packages #1-#2)
	Is there an existing TI/DRP solution?	
2. Determine the organization sizing	What is the # of Monitored Assets and the # of monitored brands?	
3. Determine which modules and add-ons are required.	Do you have a takedown tool or mechanism in place?	
	Do you have a takedown tool or mechanism in place?	Do you need takedowns – more than in the needed package?
	How many users do you need to access Argos?	Does the current package amount is sufficient?
	Do you have a team of investigators?	Do you need access to raw, can I suggest the Forensic canvas data?
	How many websites \ brands do you have?	Can we add more phishing beacons?
	Are there any specific needs for VIP or specific investigations?	Do we need to add VIP reports, do we need to add additional investigation hours?
4. Determine the price	Based on the above 3 steps	

Diagram 5 – Discovery Flow

5 APPENDIX 1: FAQ

Q: What are Monitored Assets?

A: Monitored Assets are the organization's digital resources that can be targeted by or exposed to cybersecurity threats - these can include organization names and brand/product names, domains/subdomains, IP address, employee names and email addresses, social media profiles, general keywords (e.g. confidential classification keywords, payment card bin number (6-8 digits)).

Q: What is the difference between targeted data and non-targeted data?

A: Targeted data is the data that is accumulated in Argos and that is assigned to a specific customer, based on its setup, assets and keywords. Non-targeted data is the data that is not labeled nor assigned to a specific customer. It can be found under News (for OSINT data), historical search (future), etc.

Q: What is Attack Surface Monitoring?

A: The ability to get full visibility into the organization's digital presence uncovering known and unknown assets and access points. The My Digital Presence (MDP) module in Argos covers that aspect. The relevant use cases for this module are mainly under the "Vulnerabilities" category.

Q: What is a customer needs specific use cases that fall under packages #1-#3, but does not have its own analysts and requires some level of managed service?

A: The customer can purchase additional analyst hours if additional analyst coverage on top of the package required.

Q: What if a customer does not need all use cases that are in scope of the nearest chosen package?

A: If the package scope does not correlate completely with the customer's needs it can be handled by applying discounts.

Q: What is included in the "Access to targeted data" package?

A: The customer is given access to the raw intel module, to review, printout, share, and comment on intelligence items. The customer is entitled to 2 users and up to 500 assets.

Q: What is included in the "Research module"?

A:

- Global search (access to Cyberint data lake)
- Customer's own targeted data under Raw Intel

6 APPENDIX 2: GLOSSARY

Use Case	Domain	Packages	Helps with	Description
Exploitable Ports	Vulnerabilities	1,3,4,5	Reducing the risk in unnecessary/vulnerable exposed ports.	Exploitable ports are doorways to internal applications and services that allow external connections. Ports that should be open or ports with vulnerabilities can be detected by attackers, who could potentially spread malware or gain access to the server, and more.
Exposed Web Interface	Vulnerabilities	1,3,4,5	Reducing the risk in unnecessary/vulnerable exposed applications.	Exposed web interface is a website that hosts an internal or sensitive system. If publicly accessible, it could be exploitable by an attacker who could leak sensitive information or gain access to an internal system.
Hijackable Subdomains	Vulnerabilities	1,3,4,5	Uncover and reduce the risk of a domain takeover by an attacker	Hijackable subdomain is a vulnerability that allows at attacker to take control of a subdomain through a third-party service. The attacker utilizes an abandoned link in the records of that domain to gain control of its content. This can be used for phishing, user login interceptions, and more.
Email Security Issues	Vulnerabilities	1,3,4,5	Complying with best practices of email security configurations. Very relevant for clients who suffer from phishing emails.	Email security issues are misconfigurations in email authentication standards. We recommend enforcing SPF and DMARC to reduce the success of an attacker in initiating a phishing campaign and damaging the brand's reputation. These mechanisms lay the foundation for authenticate emails coming from legitimate domains.

Use Case	Domain	Packages	Helps with	Description
CAA Issues	Vulnerabilities	1,3,4,5	Complying with best practices of certificate authority authorizations configurations. Very relevant for clients who suffer from phishing websites that have valid certificates and therefore look legitimate.	Certificate authority issues are misconfigurations in certificate authorization standards. If not enforced, these may allow an attacker to issue a legitimate certificate for an illegitimate website. This can help an attacker exploit trust relationships between domains or carry out phishing campaigns.
Exposed Cloud Storage	Vulnerabilities	1,3,4,5	Reducing sensitive data exposure and risk in unnecessary exposed cloud storage.	Exposed cloud storage accounts are a misconfiguration in the access control rules of the cloud provider. This may result in unrestricted listing, reading or writing to the storage that might lead to security or privacy issues, e.g., data leakage, web resource infection, ransom demand and more.
Mail Server Blacklisted	Vulnerabilities	1,3,4,5	Identifying mail servers whose emails are not received and are possibly affected by malware.	Mail servers in blacklists are listed in block lists as servers known to distribute spam, phishing attacks and other forms of malicious email. Emails sent from these mail servers might not reach their recipients or get flagged as spam. In addition, this could indicate that the server is infected with malware or part of a wider botnet infection.
Executive Impersonation	Brand Abuse	2,3,4,5	Relevant for clients who seek early detection of social impersonation of executives.	Social accounts that impersonate an executive may be used to tarnish a person's name and leverage their identity to damage their reputation and utilize their identity.
Brand Impersonation	Brand Abuse	2,3,4,5	Relevant for clients who want to protect themselves from brand reputation issues.	Social accounts that impersonate a brand may be used for phishing, and social engineering scams targeting the brand's clients.
Brand Abuse Website	Brand Abuse	2,3,4,5	Relevant for clients who suffer from sites that abuse their brand.	Websites that are built by the threat actor, using the brand's name, logo to assets, to advertise, tarnish the brand or advance the threat actor's agenda.

Use Case	Domain	Packages	Helps with	Description
Mobile Apps Impersonation	Brand Abuse	2,3,4,5	Relevant for clients with mobile apps who want to protect their brand and clients.	Impersonating mobile apps can be used to spread malware on behalf of the company, gain sensitive information, and more.
Private access token	Data Compromise	1,2,3,4,5	Relevant for clients who have various systems with different access methods and want to identify when access tokens are leaked online.	Private access tokens are used as an authentication method for various platforms. Stealing these tokens may provide an attacker with access to highly sensitive data, to the network itself or to management platforms.
Customer credentials exposed	Data Compromise	3,4,5	Identifying compromised customer (our clients' clients) accounts and taking appropriate measures to protect the clients and the brand.	Compromised customer credentials that were used to login to a company interface have been detected. The credentials seem to have been obtained via malware, which has infected the customer's machine and is sending any user inputs to the malware operator, specifically exfiltrating credential pairs used to log into various platforms including the company's. Customer credentials can be used by threat actors to carry out fraudulent activities, exposing the company to both financial and legal claims.
Customer payment cards exposed	Data Compromise	3,4,5	Identifying exposed payment cards to stop illegitimate use and protect the clients and the brand.	Compromised customers payment cards have been detected. Compromised payment card details, especially when combined with exposed PII, can be abused by threat actors for illegitimate and fraudulent activities.
Employee credentials	Data Compromise	1,2,3,4,5	Reduce the risk of exploitation of employee credentials to access internal systems.	Compromised employee credentials could be used by an attacker to access sensitive or internal information. Even historical leaks with older credentials, can be exploited to access a legacy platform or, if reused with slight modifications, a pattern can be formed to apply a brute force attack.
Source code disclosed	Data Compromise	4,5	Reduce the exposure of sensitive code.	Detection of publicly available code that might expose sensitive data that could be leveraged by threat actors.

Use Case	Domain	Packages	Helps with	Description
Leaked documents (files and emails)	Data Compromise	4,5	Identify cases of exposed files and reduce their exposure.	Online leaked documents can contain internal and sensitive information of the company.
Advanced sensitive information disclosure incl. PIIs, etc.	Data Compromise	5	Identify cases of exposed personal information data.	PIIs, Fullz, etc., which are exposed and are sometimes already offered for sale. It may disclose address, date of birth, driving license, phone number, social security number, and other personal information that could be used for attacks and fraudulent activities on the victim's behalf.
Refund frau d services and tutorials	Fraud	5	Relevant for clients who suffer financially due to fraudulent refund frauds.	Refund fraud services and tutorials are methods of abusing the company's refund policy to receive a refund. They are disseminated by the threat actor who gains from this.
Carding services and tutorials	Fraud	5	Relevant for clients who suffer from carding frauds.	Carding services and tutorials are methods of hacking cards and accounts and gaining goods illegally.
Advanced fraudulent activities	Fraud	5	Relevant to clients complaining about vari ous fraud incidents.	More advanced and less common fraudulent activities.
Domain Squatting	Phishing	2,3,4,5	Relevant to clients complaining about phis hing attacks or who are worried about brand abusing websites	Domain squatting prevents phishing campaigns through early detection of suspicious activities in newly registered domains that correlate with the company's brand or assets
Phishing Website	Phishing	2,3,4,5	Relevant to clients who suffer from phishing website attacks.	Phishing websites impersonating the company are a common method of social engineering leveraged by attackers to obtain sensitive data including credentials, payment information and PII. This information may be used for account takeover, unauthorized transactions, identity theft and various criminal activities. Stolen accounts are often traded in dark web marketplaces and can quickly reach a wide audience of attackers. Thus, the risk is increased if the accounts are not quickly identified and secured.

Use Case	Domain	Packages	Helps with	Description
Phishing Beacon	Phishing	3,4,5	Relevant to clients who want to reduce the impact of cloned websites on their business and brand.	Early detection of a replica of an official site by a threat actor, in his attempt to create a phishing/brand abusing site, with the beacon.
Advanced phishing detection incl. phishing kits, emails, etc.	Phishing	4,5	Relevant to clients who have phishing attacks with more complex techniques.	Detection of various forms of phishing that are not the standard phishing website but more advanced techniques including phishing kits, phishing emails, and more.
Credential Stuffing Tool Targeting Company	Attackware	4,5	Relevant to clients who want to protect their clients' accounts.	Credential stuffing is the automated injection of exposed credentials to gain access to an account.
Brute Force Tool Targeting Company	Attackware	4,5	Relevant to clients who suffer from brute force.	Brute force tools are used to gain access to a platform using aggressive technics that could cause denial of service.
Data Scraping Tool for Company Application	Attackware	4,5	Relevant to clients who want to identify and prevent attack tools that crawl and scrape their content.	Data scraping tools are used to gain information on a site to later attack, manipulate and abuse it.
Vulnerability Scanner Targeting Company	Attackware	4,5	Relevant to clients who want to identify vulnerability scanner tools.	Vulnerability scanners allow attackers to detect security weaknesses that could be leveraged for an attack.
Advanced attack detection incl. attack prep, attack tools, scanners, etc.	Attackware	4,5	Relevant to clients who wish to have hermetic coverage of attack detection.	More advanced and less common attack tools and attack chatter.