Beyond Digital **Risk Protection.**

Securing Financial Institutions from Threats Beyond the Perimeter

Cyberint

The financial sector is undergoing a digital transformation causing the amount of potential attack surface to grow exponentially. As more financial institutions are implementing mobile banking applications, threat actors are exploiting new vulnerabilities launching sophisticated ransomware attacks, malware and phishing campaigns. Even nation-state threat actors are known to target national financial institutions for geopolitical or financial reasons.

THE CHALLENGE

For financial institutions, customer and employee data protection, compliance and brand reputation are crucial for business and legal reasons. **The rise in cyberattacks aimed at financial institutions coupled with a lack of adequate resources and expertise leaves financial institutions vulnerable to cyberattacks.** They have become favorite targets for threat actors due to the high success rate and revenues combined with a low chance of being caught in the act.

All this drives the need for financial institutions to become proactive by using threat intelligence for identifying cyberattacks before any breach can occur to protect their customers, digital assets and brand reputation . A need for a security intelligence tool that can provide targeted intelligence to proactively mitigate risks and keep compliance with regulations is needed urgently.

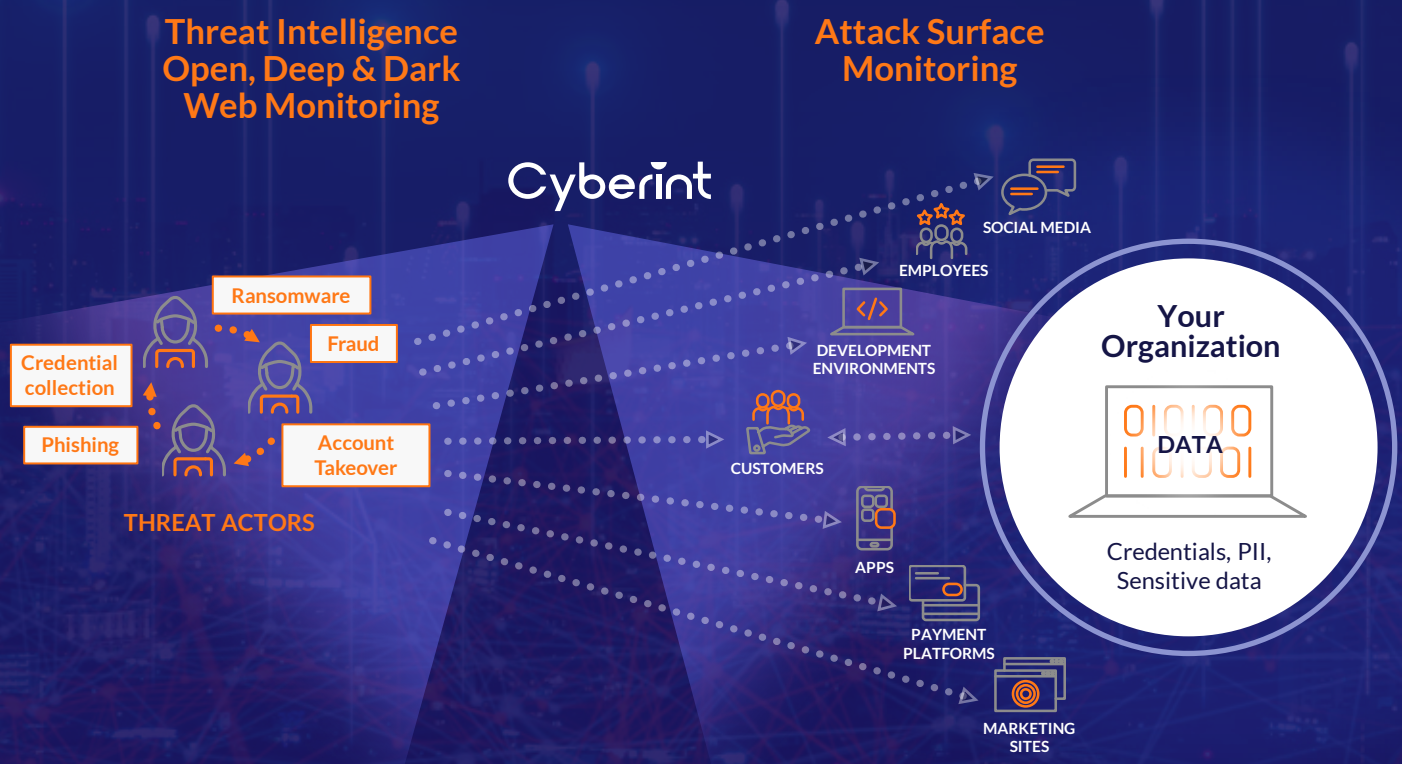
THE SOLUTION

Cyberint provides its comprehensive Digital Risk Protection (DRP) solution, turning intelligence into highly effective proactive cyber defense. The Argos Edge™ SaaS platform , Cyberint's proprietary DRP solution, collects intelligence from a broad set of open sources and analyzes potential threats.

Cyberint's solution utilizes a combination of automated and manual techniques to identify the threat actors involved and mitigate their attacks.

Financial institutions can also benefit from Cyberint's managed services team comprised of highly skilled analysts. The holistic DRP offering for financial institutions allows not only access to the Argos Edge™ platform, but also support by Cyberint's analysts that can operate as part of the organization's in-house team. Furthermore, Cyberint can also provide virtual HUMINT expertise, threat landscape research, investigation, and threat intelligence services.

Argos Edge™ | PROTECTION BEYOND THE PERIMETER



Argos Edge™ | THE ALL-IN-ONE SOLUTION

ATTACK SURFACE MAPPING

The attack surface mapping module identifies the financial institution's digital footprint and monitors assets beyond the perimeter to provide transparency based on defined threat severity to prioritize response to detected threats and vulnerabilities.

THREAT INTELLIGENCE COLLECTION & ANALYSIS

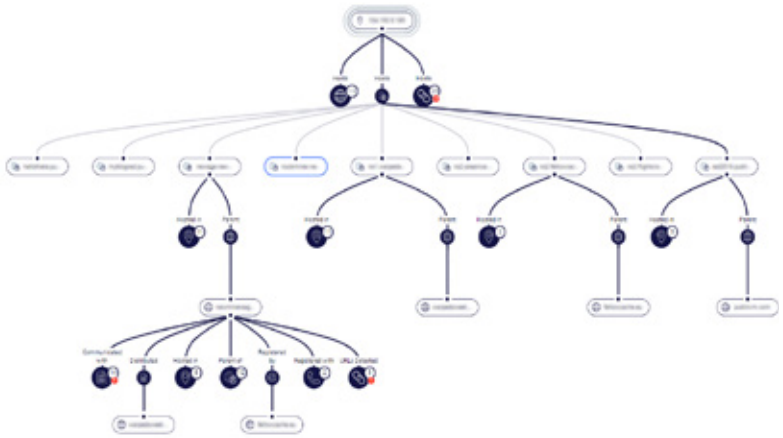
The platform's engines collect and analyze huge amounts of open-source data from the surface, deep and dark web in real time to generate actionable intelligence alerts for the financial institution's cybersecurity professionals to get actionable insights. The harvested data are benchmarked against the financial institution's assets such as IPs, domains, brands or executives. This data is also categorized by type of threat, such as phishing, malware campaigns, credential stuffing, data leakage and fraudulent activities. The proprietary machine-learning algorithm prioritizes the analyzed data by risk factor and impact for optimal insights and follow-up.

PROACTIVE DEEP AND DARK WEB MONITORING

The Argos Edge™ platform's algorithm leverage data from thousands of sources to monitor threat actors. **This allows financial institutions to safeguard their business information** against data leakage, breaches and the illegal selling of data on a broad range of deep and dark websites, forums and in dark web chat rooms. The continuous monitoring of deep and dark channels enables the financial institution's security team to detect potential information leakage, obtain contextual analyses of current and pending cyberattacks and receive actionable alerts.

FORENSIC CANVAS

The forensic canvas module enables a deep dive into the attributes of specific entities for further investigation. It identifies and analyzes threat actors and their tools, tactics, and procedures (TTPs) for indicators of compromise (IOCs). By integrating multiple services into a unified investigation platform, various types of connections, WHOIS services, passive DNS, social discoveries, and malicious codes can be mapped for DRP. Its easy usability enables quick contextualizing and insight into a specific threat or suspicious act based on generated and analyzed data.



PHISHING DETECTION & TAKEDOWN

The phishing detection & takedown module identifies and mitigates phishing attack **attempts before they can cause damage to the financial institution's reputation.** The module not only monitors, but also deploys other methods for detecting newly registered domains, phishing repositories, phishing kits, phishing emails, and traffic quickly and efficiently. Upon detection of e.g., a malicious phishing site, a takedown process is initiated that can also consist of notifying the relevant providers to remove the detected misleading content, block the domains, and update their public blacklists.

Cyberint's innovative Phishing Beacon is a singular phishing detection & takedown module, which provides real-time insights into phishing sites cloned from e.g., a bank's legitimate website content. The rapid detection allows these phishing sites to be taken down quickly to eliminate any resulting risk to that bank's assets and its reputation.

- The Phishing Beacon's single-line of code is added to the bank's web pages.
- Threat actors are prone to clone such web pages for e.g., phishing attempts, brand damage.
- The Phishing Beason detects the first-time rendering of such a cloned web page and automatically sends an alert to investigate that web page.
- Once it has been determined as being malicious, an alert is sent to the bank for follow-up.

Argos Edge™ | FEATURES & BENEFITS

All-Round Protection

Comprehensive DRP powered by AI provides a single pane to thwart digital risks and a human-machine approach

Real-Time Protection

Protecting financial and banking data across all touchpoints in real time

Brand Protection

Safeguarding all facets of the financial institution's online presence

Phishing Detection

Identifying and remediating phishing attack attempts before they can have a negative impact

Fraud Detection

Mitigating and preventing of fraud to reduce monetary loss

Digital Footprint Detection

Identifying and mapping the attack surface and identifying vulnerable weaknesses to follow the digital footprints of threat actors

Cyber Risk Insights

Ensuring ongoing and continuous visibility of cybercrime tools used by threat actors. Identifying leaked Information and ransomware risk

BUSINESS VALUES

- **High accuracy enabled** by actionable, focused, and relevant data
- **High ROI due to mitigation of fraud** that helps to reduce internal costs
- **Increased SOC efficiency** by saving security team's time and resources
- **Brand protection** to prevent customer churn and loss of reputation
- **Prevents compliance issues** regarding various statutory rules and regulations

Cyberint

SELECTED USE CASES

Identifying Fraud | Bank Credit Cards Sale on the Deep and Dark Web

Cyberint's Argos Edge™ detected on various deep and dark web forums multiple posts containing the details of stolen customer credit cards, including credit card numbers, CVVs and expiration dates, together with the personal details of the cardholders. The bank was proactively prepared and the compromised credit cards were blocked to prevent any malicious usage of the credit cards.

Identifying Phishing | Active Phishing Site

Cyberint's Argos Edge™ detected that a threat actor had copied the bank's website code and had created several cloned websites for illicit purposes.
The Cyberint analysts managed to obtain the phishing kit and were able to identify the involved threat actors and non-actors. This allowed our client to take quick action by proactively taking down the copycat sites, thus preventing account takeover, unauthorized access, brand reputation damage and user data compromise.

Identifying Malware Alerts | Bank Trojan

Cyberint's Argos Edge™ detected the presence of the bank Trojan Anubis that was targeting the bank's two official Android applications for stealing the financial information of the bank's customers. After mitigation, Cyberint also recommended that the bank would inform its customers about the dangers of using unofficial APK files in Google Play and opening suspicious emails and attachments that could contain unknown APK files.

ABOUT CYBERINT

Cyberint provides **Digital Risk Protection and Threat Intelligence** to protect organizations from cyber threats beyond the perimeter by providing a rich set of external digital threat protection solutions, all automated by or tailored with human expertise.

Its proprietary **Argos Edge™** custom platform provides targeted insights into threat actor activity, brand protection, phishing attacks, data leakage and exploitable attack surfaces.

Cyberint's customer base encompasses enterprises, including Fortune 500 companies, in the finance, retail, e-commerce, gaming and media sector.

Beyond Digital **Risk Protection.**

Contact information:

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

Cyberint