INFOSYS CYBER INTEL PLATFORM

Infosys®
Navigate your next

Overview

With the advent of advanced technologies and digital transformation, cyber attackers too have begun resorting to sophisticated tools and techniques to carry out data breaches and thefts. There is a dire need to understand their profiles, their methods and to assess the threat they pose to organizations.

Threat intelligence, is information that is validated and prioritized, correlated to known threat actors and attacks and specifically tailored to the enterprise in order to combat and mitigate harmful events. It facilitates teams at every level - from operations to incident response all the way to the CISO to take data-driven and proactive decisions regarding security.

Need for threat intelligence:

- **To help security products such as firewalls** - To detect and block
- **Incident response** - To set the threat context and investigate incidents
- **Vulnerability management** - To provide information on the exploits available and help in patch prioritization
- **To facilitate CISOs to take strategic decisions** on security investments by providing them with actionable insights and intelligence

As threat intelligence aids organizations to gain insightful information about incidents and threats external to the network causing serious risk to the business, integrating it with the security program is imperative. That said, there are certain challenges such as the following that pose as obstacles for having a robust threat intelligence solution:

- Threat Intel program creation from scratch can prove to be very tough and complicated as it requires niche and advanced skills and knowledge
- It involves selecting and procuring multiple products – Threat Intel Platforms (TIPs), commercial threat feeds that are complicated in nature
- Integrating feeds with the security devices – SIEM (Security information and event management), SOAR ((Security Orchestration, Automation and Response), firewall, IDS/IPS (Intrusion Detection Systems/Intrusion Prevention Systems) can turn out to be complex with no access to threat analysis tailored for the enterprise, specific to its industry

Infosys Cyber Intel Solution

The Infosys Cyber Intel solution provides comprehensive threat intelligence and analysis service. It provides machine-readable threat feeds that can be consumed by security products, access to skilled threat analysts and operational and strategic threat intelligence reports to facilitate security operations and planning. It is a service that validates and prioritizes intelligence, correlates it to the known external threat actors and attacks and provides customized reports to enterprises with regards to location, industry and regulatory environment relevant to them.

Solution Drivers

Our solution provides cyber intelligence in the following manner:

- Tactical Intel: Provides threat indicators for the SIEM and other security products to detect and block. These include IOAs (Indicators of Attack), IOBs (Indicators of Behavior), IOCs (Indicators of Compromise)
- Operational: Provides details such as the name of the threat actor, their common TTP (tools, techniques and procedures) and other related threat indicators along with information regarding remediation
- Strategic: Provides current state information to the CISO with intelligence regarding deadly threat actors and probable cyberattacks to facilitate informed decision making and combat anomalies

What we do - Our Services

Aggregated Intelligence Feeds

- Machine-readable Threat Intel
- Consumed by SIEM and other security devices
- Indicators of Attack (IOA)
- Indicators of Behavior (IOB)
- Indicators of Compromise (IOC)
- Threat Actors and Vectors
- Tools, Techniques and Procedures (TTP)

Threat Alerts and Advisory

- Alerts and advisories of ongoing threat attacks, malwares, serious vulnerabilities
- Advise on detective, remedial and preventive measures

Threat Landscape Monitoring

- Assessing the organization's exposure to threats
- Cyber risk profiling
- Tracking and alerting of expected threats
- Providing timely advisories, detailing preventive, detective and recovery measures for strategic decision making

Enterprise Threat Profiling and Assessment

- Creating and updating regularly the infrastructure and threat profile for clients
- Conducting applicability assessment against threat information derived

Malware Analysis

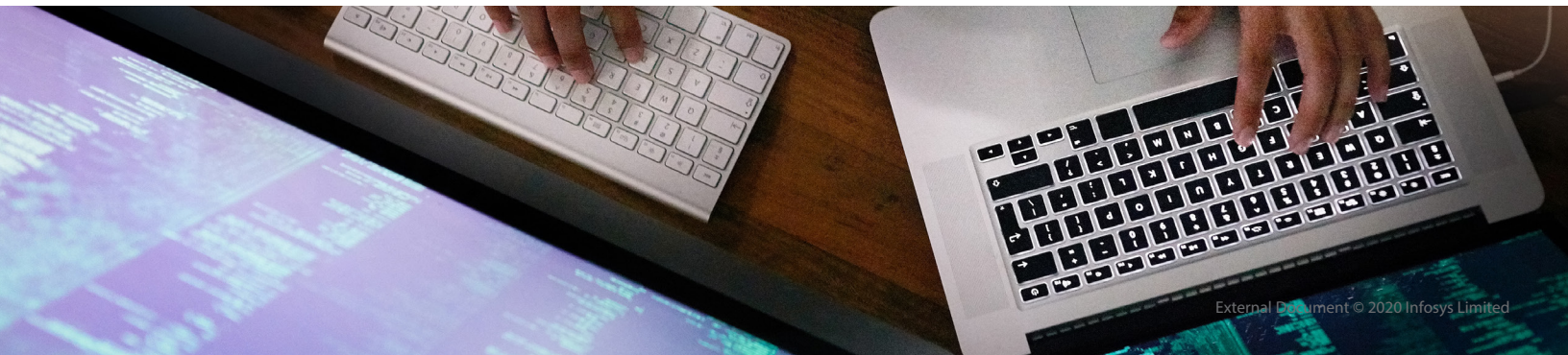
- Subscribers can submit malware sample and suspicious code for analysis
- Static and dynamic analysis
- Research environment having disassemblers and debuggers
- Dynamic analysis using sandboxing

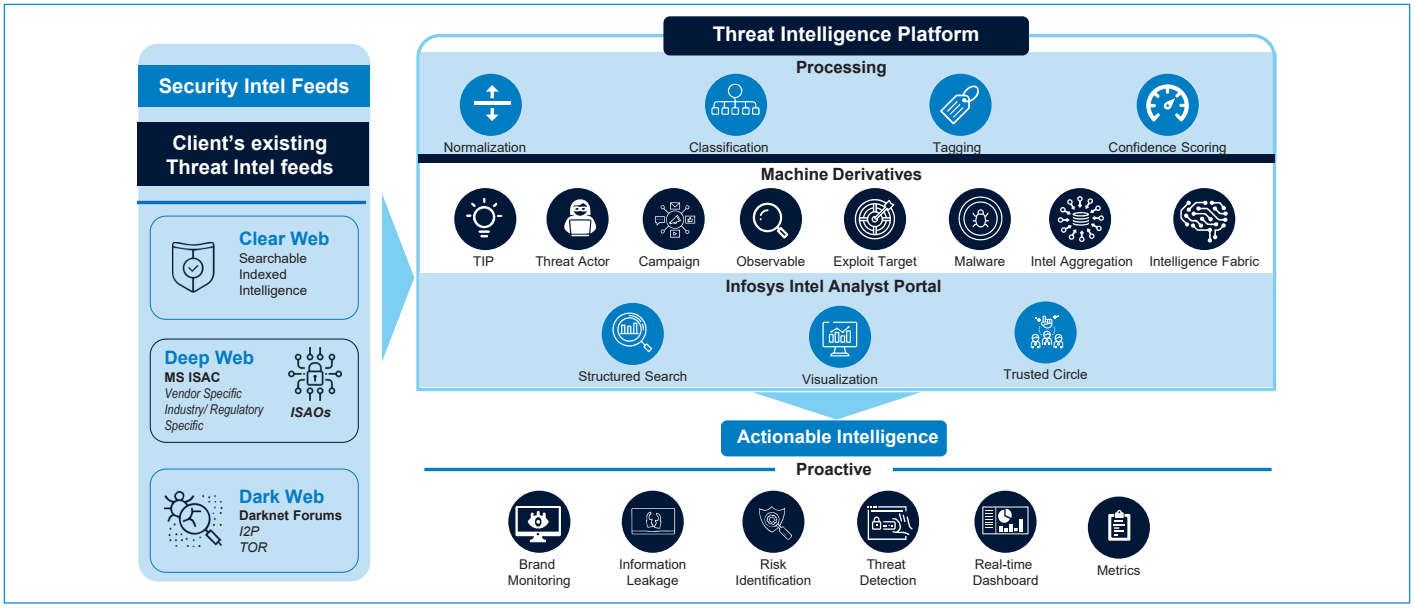
Brand Monitoring

- Search the indexed Web, Deep Web and Dark Web to detect
- IP Leakage
- Credential exposure
- Defacement
- Impersonation
- Cyber squatting
- Social media monitoring

Analyst Access

- Access to threat analysts who can perform additional investigations and specific analysis
- Assistance in deciphering if isolated incidents are part of a more pervasive attack
- Access to dedicated threat analyst in preferred time zone





Threat Reports – Service Outcome

Most of the threat indicators, when initially collected, are large in volume, disorganized, unstructured and isolated - typically inoperable. Infosys Cyber Intel service ensures that the threat indicators provided are contextualized, analyzed and assessed to deliver high-quality threat reports. We provide the following reports according to relevance and urgency:

Weekly Threat Reports

- Contains details of currently active global threats, a description of their TTPs, their threat indicators and vulnerabilities they exploit
- Contains top vulnerabilities seen, their CVEs, the systems they target, associated threat indicators, exploitability of the vulnerabilities and recommendation in the form of mitigation measures
- Operational Intelligence for consumption of security operations and vulnerability management teams. Enables them to be alert of possible attack from the malware, and patch the vulnerabilities

Monthly Threat Reports

- Threat Exposure report that contains brand monitoring details
- Describes the IP leakage, credential leakage, list of typosquatted domains and vulnerabilities pertaining to the organization's stack
- Consolidated operational intel report that enables customers to reduce their exposure

Threat Landscape Report

- Quarterly strategic intel report to the CISO to increase situational awareness and help perform effective security planning
- Provides information and trends related to common threats (eg: targeted phishing attacks), threat actors (eg: APT groups), their TTPS (mapped to MITRE ATT&CK) and their intentions.
- Lists data breaches by sector along with high level recommendations
- Lists top vulnerabilities that are being exploited

Ad Hoc Reports

- Provided out-of-cycle in case of major security incident such as massive credential leakage or IP leakage.
- Also provided for critical ongoing security attacks or exploitable vulnerability that may be discovered
- Enables the security teams to very quickly assess the damage and resolve the incident.

Business Value

- Attain a comprehensive threat intelligence and analysis service with Infosys Cyber Intel platform
- Get a combination of technologies (TIP, Feeds), threat analyst services and system integration as a single pre-integrated package
- Achieve a quicker path to security maturity compared to having a home-grown program
- Take informed and data-driven security decisions to create a robust security framework

For more information, contact askus@infosys.com

Infosys®
Navigate your next