CyberKnight

Unified Threat Intelligence

Many organizations are taking a threat-led approach to cyber security, seeking to understand what is in the threat landscape that can cause harm to their businesses, and using that information to improve their ability to prevent or mitigate those risks. To achieve this, companies are seeking to create and deliver Cyber Threat Intelligence (CTI) capabilities. However, many find it a really challenging endeavor, to select the right type of intelligence sources and feeds, consolidate those feeds into one platform, normalize and filter the feeds of interest, enrich and make sense of the collected feeds, and finally curate and prepare the feeds for dissemination and consumption by other security systems and practices.

"Cyber Threat Intelligence is the process of collecting, processing and analysing information regarding adversaries in cyberspace, in order to disseminate actionable threat intelligence, by understanding adversaries' motivations, capability, and modus operandi, to inform cyber security mitigation measures."

There are a myriad of vendors claiming to provide the right threat intelligence service; as a result, prospective customers struggle to build an effective collection strategy with threat intelligence feeds that align with their threat profile and business risk.

For this reason, CyberKnight has built a Unified Threat Intelligence solution offering, to help our customers in their journey to build a CTI program:

1. The first milestone in any CTI program is to define a CTI strategy. However, in order to define the strategy, a customer needs to conduct an information security threat assessment to understand their threat profile. After this exercise, customer will better know the threat landscape and the risk their business is exposed to; for instance, who are the potential threat actors that would be keen on targeting their business, what are their tactics, motives, origins, or the regions and industries they operate in?

Based on a thorough threat assessment, a customer can identify the objectives that will help structure the proposed CTI program:

- What key outputs the CTI program will deliver
- What information the program will collect which caters to the intelligence requirements of the relevant stakeholders on strategic, operational or tactical
- Which threat actor groups the program will focus its attention on
- With which security devices and tools must it integrate (SIEM, SOAR, EDR...etc.)

2 The second steppingstone is to choose the right CTI feed provider. There are several feed providers in the market, and each one focuses on different threat actor groups, intelligence types, use cases and industry sectors. Customers should pick the feed(s) that provide(s) the most relevant intelligence that aligns with the corporate strategy and fulfills the business requirements of all relevant stakeholders participating in the CTI program.

There are 3 types of threat intelligence:

Strategic
is to assist senior management in making informed business decisions by providing them with an understanding of threats to the company.

Tactical
is more technical in nature and consists of analysis of indicators of compromise (IOCs) to allow the security operations center (SOC) and security analysts to more effectively triage alerts and distinguish active attacks that require escalation from background noise.

Operational
commonly in the form of tools, techniques and procedures, aims to understand threat actors and their likely attacks against the department.

Apart from the above categories, threat intelligence itself can be collected from various sources and channels across the internet (web, social, mobile, email etc.) in the open, deep, or dark web. Customers need to subscribe to the right threat intelligence feed provider to align with their business risk requirements and cover their threat intelligence profile.

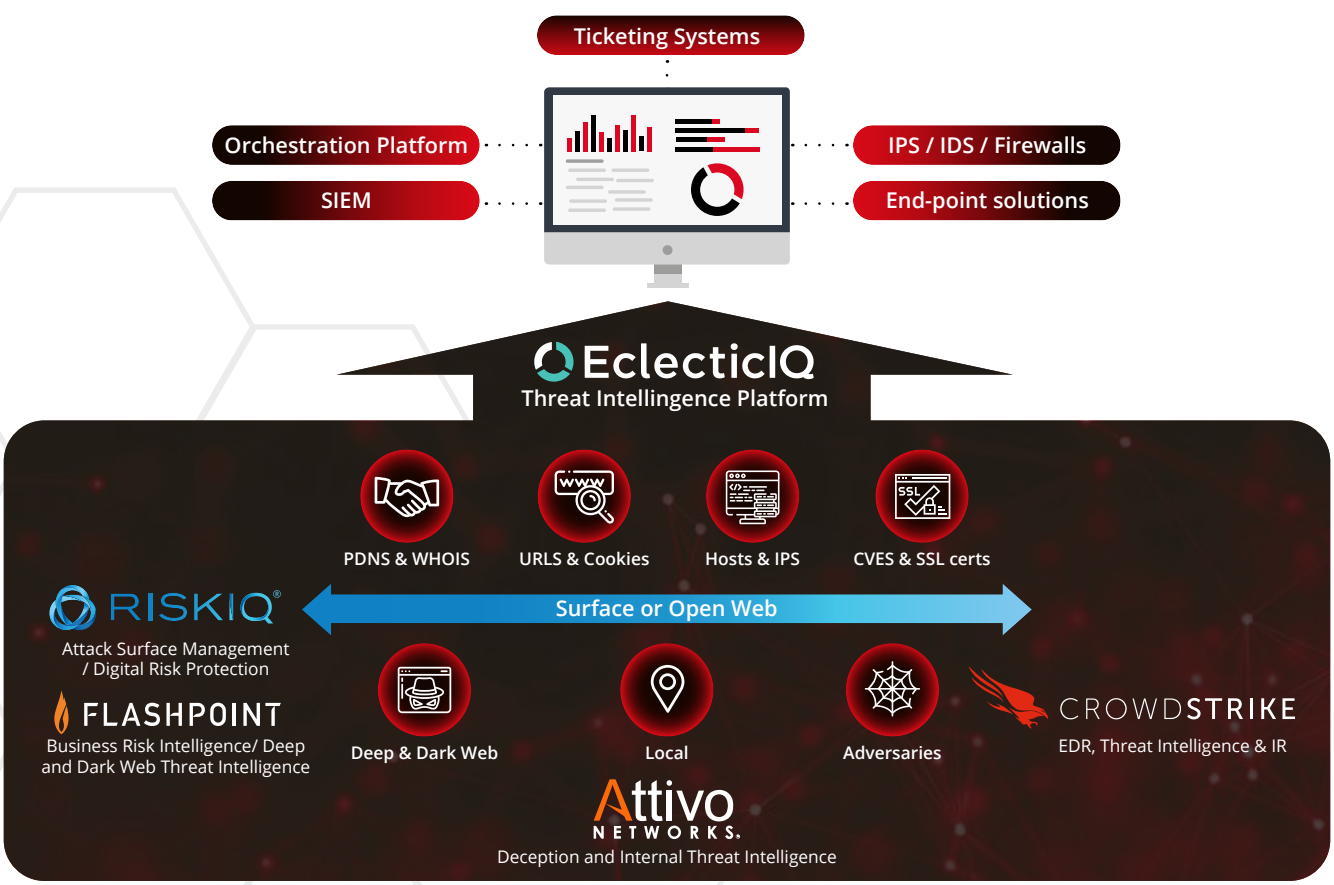

Figure 1- CyberKnight Unified Threat Intelligence Program

To simplify building the CTI data collection plan, CyberKnight has partnered with market-leading providers to support with architecting a comprehensive threat intelligence program, that can fulfil most customer requirements and threat intelligence needs.

CyberKnight can assist from the initial phase of conducting cyber threat assessment, identifying the right threat profile, and identifying the right threat intelligence feed types.

On the technology front, CyberKnight has partnered with the following vendors, to ensure full coverage for most of the CTI use cases, categories, and channels that most of the customers would be considering:

EclecticIQ

EclecticIQ is an analyst-centric threat intelligence platform (TIP). It ingests intelligence data from open sources, commercial suppliers, and industry partnerships into a single collaborative analyst workbench. The EclecticIQ platform eliminates manual and repetitive work, allowing analysts to identify the most critical threats, take timely actions, advise the organization on how to respond and collaborate with industry peers. The platform is based on industry best practice, compatible with STIX and TAXII. It is developed with CTI workflows and tradecraft at its core. With EclecticIQ's knowledge base, you start with lots of information and as you use the platform, that information is distilled down into more relevant intelligence. EclecticIQ can ingest feeds from most threat intelligence sources out of the box, including those provided by Cyberknight: FlashPoint, RiskIQ, Crowdstrike. EclecticIQ has built-in integrations with many technology companies, operating in spaces such as orchestration, SIEMs, end-point security, firewalls, ticketing systems, etc. Those integrations enable EclecticIQ to disseminate curated, validated and actionable intelligence feeds to those tools, which enhance the quality of incidents triggered by those technologies, reduce the noise and increase the ability to take risk-aware decisions.

RISKIQ®

Offers attack surface management intelligence leveraging on its wide Internet scale datasets that it collects from the open and surface web spaces. Virtual user technology is used to discover web assets, and go beyond simple crawling, by visiting websites using different browsers, varying click patterns and time on page to behave as a human user would. Using a network of tens of thousands of these virtual users, they scan the entire internet and collect telemetric data to produce a dynamic index of the web attack surface. This process illuminates websites, URLs, web page content, ASNs, IPs, and nameservers, WHOIS, Passive DNS, SSL certificates, newly observed domains, CVEs, session cookies etc. RiskIQ adds value to the other consolidated feeds as all its collected intelligence, help CTI analysts to map threat actors attacking infrastructure in open and surface web, and the technical indicators

Crowdstrike produces different types of intelligence (strategic, operational, or tactical) that focuses primarily on adversaries such as nation-states threat actors, cyber-criminal or hacktivists groups. A detailed view is provided into actor profiling, exposing their motives with strategic intelligence reporting based on campaigns and regional threat landscape, tools and tradecraft analysis, and reporting. Crowdstrike combines automated and human-led malware analysis, malware search and finished threat intelligence into a seamless solution which can be consumed via portal access, through analyst access and via intelligence feeds. CrowdStrike provides the option to design threat modeling for the prospects through priority intelligence requirements and to submit CTI RFIs based on customer ad-hoc investigation requests to fill the intelligence gap requirement.

Flashpoint provides intelligence that is grounded in the deep & dark web, as well as, closed illicit groups. Fueled by a combination of sophisticated technology, advanced data collections, and human-powered analysis, Flashpoint tailors its offerings to customer requirements. From bolstering cyber and physical security, to detecting fraud and insider threats, Flashpoint partners with customers across the private and public sectors to help them rapidly identify threats and mitigate their most critical security risks.

Attivo stands guard inside the network, using high-interaction deception and decoy technology to lure attackers into engaging and revealing themselves. Through misdirection of the attack, organizations gain the advantage of time to detect, analyze, and stop an attacker. Attivo provides “eyes inside the network” visibility and accurate detection alerting based upon decoy engagement or attempts to use deceptive lures, early in the attack cycle. High-fidelity alerts are substantiated with threat intelligence about the threat, adversary, forensics details about their IOCs and TTPs

CyberKnight’s complete Unified Threat Intelligence offering addresses any customer’s CTI requirement, regardless of the varying use cases. The UTI concept is an easy and practical approach that can help our strategic customers, build an efficient and relevant threat intelligence practice, within minimal time, however achieving significant and relevant outcomes.