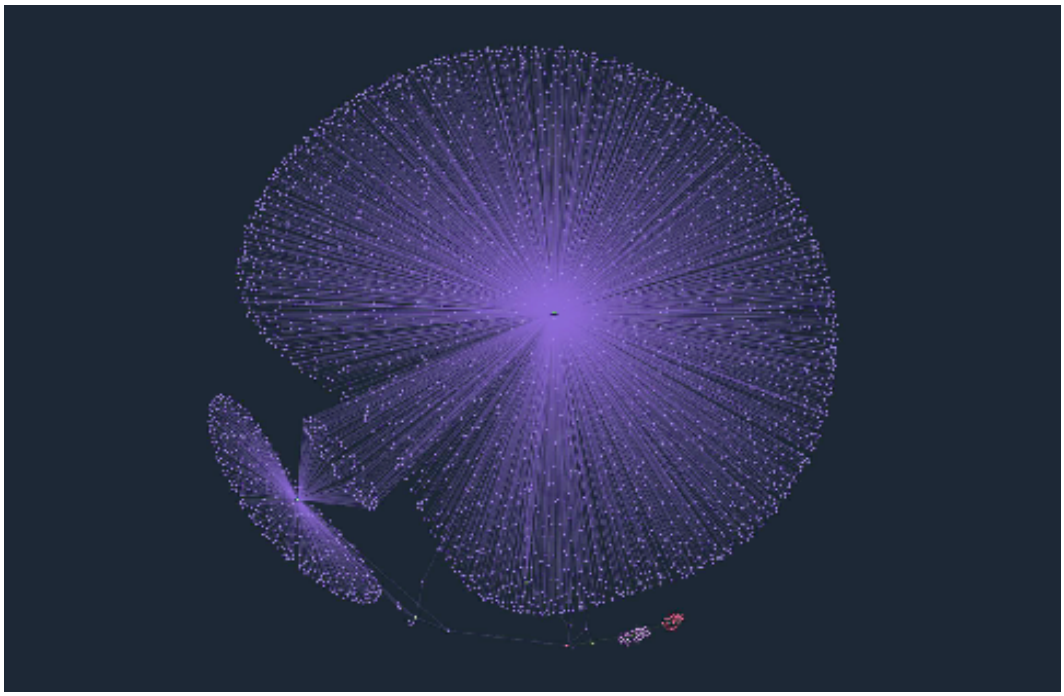

Real-Time Third-Party Supply Chain Cyber Risk

COGILITY

Introduction

To effectively manage cyber risk for external entities — such as third parties supplying critical services, equipment, and supply chain logistics — each entity must be continuously enumerated and evaluated against a dynamic set of vulnerabilities, and threat intelligence data streams, and then evaluated with variable impact assessments considering full context, historic exposure — anticipating future risk. Currently, many of the existing solutions rely on manual entity enumeration and focus on 'point-in-time' reporting that does not effectively scale to be able to monitor millions of entities. Cogility has developed a system and several component processes for automatically enumerating each entity's infrastructure, cloud assets, technologies, related technologies, vulnerabilities, and system compromise signals for any given scope of entities. The proposed solution can be scaled to assess every commercial entity in the United States in a near real-time manner.

Current State

At present, many solutions for addressing supply chain risk rely on enumerating an entity's internet-facingexposure by active (e.g., OWASP Amass) and passive DNS (e.g., SecurityTrails) enumeration. The DNS enumeration results are decomposed into IP addresses and scanned using technologies like NMap for activescans or queried against internet scanning datasets such as Shodan.io. This methodology often misses many assets or contains false positives due to shared infrastructure or stale DNS records. In addition, active scans are frequently lacking in quality and integrity as many cyber security products block scan attempts. The combination of these factors reduces the signal resolution, quality, and confidence, requiring manual intervention or interpretation that is not sustainable in a scalable process. This process is also inherently challenged by utilizing a small set of initial selectors (i.e., company name and domain name, or other key features used to join sets of data) to then query a variety of dependent structured datasets. This requires that each additional set of data be integrated into the enumeration and analysis model in a dependent data model, and queried at some regular interval, which leads to significant challenges in scaling the overall process.

Cogility Supply Chain Risk

To overcome the challenges related to signal quality, confidence, resolution, and scalability; Cogility has inverted the data model and processes internet scale telemetry in a set of components arranged in a set of hierarchical complex event processing models, which are outlied in the remaining sections below. This process represents a change in basic approaches from structure, store, and query methods to an event stream processing method that handles internet scale analysis in near real-time and allows for processes such as entity enumeration to be a continuous discovery process rather than a set of queries based on assumptions for a point in time.

Component 1 - Entity Enumeration Model

The purpose of the entity enumeration model is to continuously define what internet-facing exposures and extents of related selectors are attributable to a given entity for a certain period. Entity enumeration begins with a defined scope, such as all entities in a target country contained in a database. Key selectors are mapped from this dataset into the enumeration models based on a set of streaming data sources such as domain registrations, IP address registrations, SSL certificate transparency data streams, etc. This component defines what selectors are valid for the entity and for what period the selectors are accurate. The output creates a dynamic model of each entity's overall attack surface and key selector sets over time.

Component 2 – Technology Signals Processing Model

Technology signals processing utilizes a variety of internet-scale data streams from multiple datasources. These data streams, such as internet port scanning, are active and passive internet sensors. Each technology signal is streamed against the enumerated set of selectors from Component 1 – Entity Enumeration. The HCEP (Hierarchical Complex Event Processing) model also uses these data streams to perform validation and identify additional entity selectors to recursively be added to the entity enumeration set of selectors, thereby continuously improving the signal quality for both component sets. While the signal processing is a continuous data stream, the results of the model, both real-time and historical

(in the event new data is exploited or discovered that applies to a historical time period, such as the forensic discovery of previous threat actor activities) can be recursively updated when new telemetry sources are identified, even if those sources cover a historical timeframe.

Component 3 – Continuous Targeting Cycles Model

Components 1 and 2 are applied to both the entities intended to be defended and the threat actors that seek to exploit these entities. The exact entity enumeration process utilized to continuously map internet-facing infrastructure and key selectors linked to the entities to defend also applied to an initial set of known threat groups' operations and infrastructure. The same sources streamed into the models as part of the Technology Signals Processing component are also streamed against adversary entity enumeration models, thereby scaling and sustaining threat group entity enumeration. Mapping the infrastructure over time in both cases allows for the union of NetFlow signals analysis to be applied to identify key events that take place when these two targeting cycles share collection features.

Component 4 – Signals Analysis Model

Utilizing HCEP, the overall outputs of all components are streamed against a set of patterns that classify each activity, vulnerability, and feature with a risk score. These signals are processed to identify specific vulnerabilities and threat actor activities that seek to exploit the vulnerabilities. By processing NetFlow signals, this method also covers the detection of threat actors' post-exploitation activities, such as data exfiltration, persistent latent compromises, and exploitation of vulnerabilities internal to entities, such as phishing attacks.

Conclusion

Existing methods for monitoring supply chain risk have five key weaknesses:

1. **Lack of depth – often limited to basic network scans.**
2. **Not continuous or real-time – rely on queries run at intervals.**
3. **Do not consider both threat actors and targets.**
4. **Does not scale.**
5. **Lacks context, data provenance, and risk-scoring transparency.**

The Cogility supply chain risk model is based on real-time streaming data and HCEP to overcome challenges that industry solutions have failed to address. In addition, the Cogility supply chain risk solution is built entirely in Cogynt, with the ability to rapidly adapt to changing threat landscapes, new data feeds, private datasets, and tailored risk scoring to meet the operational objectives and tasking of many distinct roles within one unified platform.