Anomali Enterprise: An Operational Model for Breach Analytics and Intelligence

OVERVIEW

The current widely adopted methodologies for computer security operations are failing. According the to 2015 M-Trends report, the average time for an organization to detect an intrusion is 205 days and 69% of the victim organizations only learned of the breach after being notified by an external 3rd- party[1]. This means that on average the adversary is likely operating in your environment for more than 6 months before discovered. With dwell times like this, it is not surprising that the scale of data breaches continues to grow with an estimated 700M records compromised and $400M in losses according to the 2015 Verizon DBIR Report[2]. In the face of this situation, a new approach to security strategy and operations must be adopted. An approach in which more focus is placed on operational relevance, reducing adversary dwell time and speeding incident response activities.

Thus far security systems have focused on building a passive approach to monitoring, detection and protection. Some of these approaches are borne out of an engineering mindset where so long as an organization can implement enough safe guards the system will be secure. Other practices are borne out of an infection-control approach, attempting to block the fast-spreading slowly evolving virus or worm models. Much of the security industries best practices and compliance standards are built to address only these two worlds.

The approach for addressing current threat actors is ridged, non-adaptive and relies on a small finite amount of investigation approaches. Due to change management processes, configuration changes slowly, typically at the scale of days or weeks. Many only allow for time-based threat discovery from the current point in time into the future. This passive approach to detection and defense frequently misses the advanced attack threat actor for months. To fill this void, the threat analyst practices conform to the current methodology, frequently called “hunting.”

The new approach needs to be supported by creating a more dynamic system that aggressively drives active investigation for breaches by continuously updating security detection controls with new intelligence and active searches over historical data for intruder activity.

A path forward can be seen through the improvements in new analytic models that guide workflows and enable interoperability. These models include intrusion lifecycle models, attributional models, intrusion response models, and data description models.

Anomali Enterprise is a breach analytics and intelligence model that aims to unify and integrate for a holistic approach to cyber security that significantly improves enterprise risk exposures.

The Anomali Enterprise Model allows for constant automated improvement of security controls enabling the sharing of other orgs hunting procedures and partial automation to gather information for human review.

Intrusion Lifecycle Models

The Cyber Kill Chain

Intrusion Lifecycle models like the Cyber Kill Chain™ allow Security Operations Centers (SOCs) to quickly map detection and protection controls to an adversary's capabilities aligned to the stages common to most attacks.[3] These stages include Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives. When applied correctly, the Cyber Kill Chain enables defenders to start to map out various adversary's playbooks to ensure coverage through detections, preventions, and mitigations.

Figure 1: Cyber Kill Chain

Mandiant's Attack Lifecycle Model

Mandiant's Attack Lifecycle Model[4] is used for modeling typical APT style intrusions involving hands on keyboard, interactive operations. Its phases are similar to the Cyber Kill Chain. The Mandiant Attack Lifecycle includes a cycle that represents the adversary performing internal reconnaissance, expanding access, maintaining persistence, and escalating privileges. All of these stages are typical events seen with targeted intrusions, especially where the goal is long term access

.

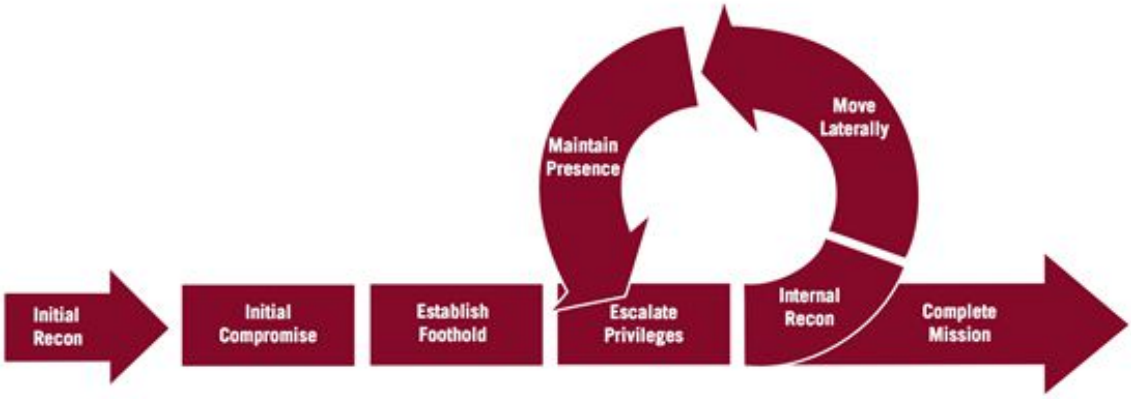


Figure 2: Mandiant's Attack Lifecycle Model

Threat Hunting

Most Threat Hunting methodologies can be seen as an application of intrusion lifecycle models. They are designed for detecting post compromise activity in large enterprise environments. Threat Hunting methodologies start with the assumption that adversaries are already operating in the environment, utilizing data mining and breach analytics to find them. They focus on the phases of Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives. Hunting methodologies are most effective in aiding defenders in finding Installation, C2, and Actions on Objective phases where the adversary is often exposed because of the operational requirements of performing lateral movement, outbound communications, and data exfiltration.

Intrusion lifecycle models are useful for thinking through how an organization's defensive measures map to how the adversaries actually operate. When used properly these models can help to identify gaps and weaknesses that should be filled. Here is an example of mapping defensive controls to Cyber Kill Chain using the CNO objectives from JP 3-13[5] (table adapted from[6]):

	Recon	Delivery	Exploitation	Installation	C2	Actions on Objectives
Detect	NIDS Router Logs Web Logs	NIDS HIDS Vigilant User Anti-virus	NIDS HIDS Anti-virus	HIDS Application Logs Anti-virus	NIDS HIDS Anti-virus	NIDS HIDS Anti-virus DEP Application Logs
Deny	Firewall ACL	Mail Filter Web Filter	HIPS Antivirus Hardened System	App Whitelisting Blocked Execution	Egress Filter Firewall ACL Sinkhole	Egress Filter Firewall ACL Network Segmentation
Disrupt	Active Defenses	Mail Filter Web Filter	HIPS Antivirus Hardened System	Antivirus HIPS	DEP Sinkhole	Network Segmentation DEP HIPS
Degrade	Honeypot Redirect Loops Active Defenses	Sinkhole Combination of Deny/ Disrupt	HIPS Antivirus	Combination of Deny/ Disrupt	Sinkhole	Network Segmentation
Deceive	Honeypot Redirect Loops Active Defenses	Honeypot	Honeypot	Honeypot	Honeypot Sinkhole	Honeypot

Table 1: Mapping Defensive Controls to the Cyber Kill Chain

Attributional Models

Attributional Models are analytic models with a goal of relating intrusion/attack activity with other activity, infrastructure, tools, victims, and ideally known adversaries. Attributional models seem simple in concept but are often very difficult in practice.

The Diamond Model

The Diamond model is one of the most popular attributional models guiding threat researchers through expanding the known malicious indicators used by adversaries. The Diamond Model aims to guide analysts' collection and analysis activities toward enumerating salient details related to the four core elements of the Diamond model: 1) Adversary, 2) Infrastructure, 3) Capability, and 4) Victim, as well as the two meta-features 1) Social-Political, and 2) Technology[7].

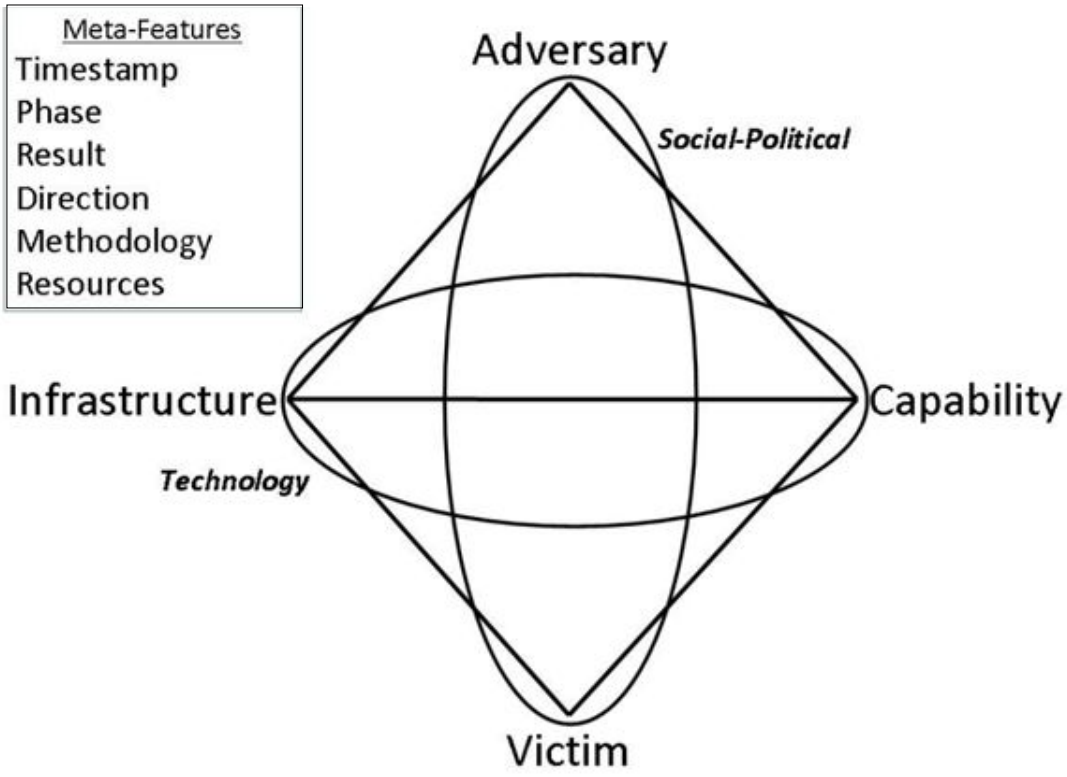


Figure 3: Diamond Model

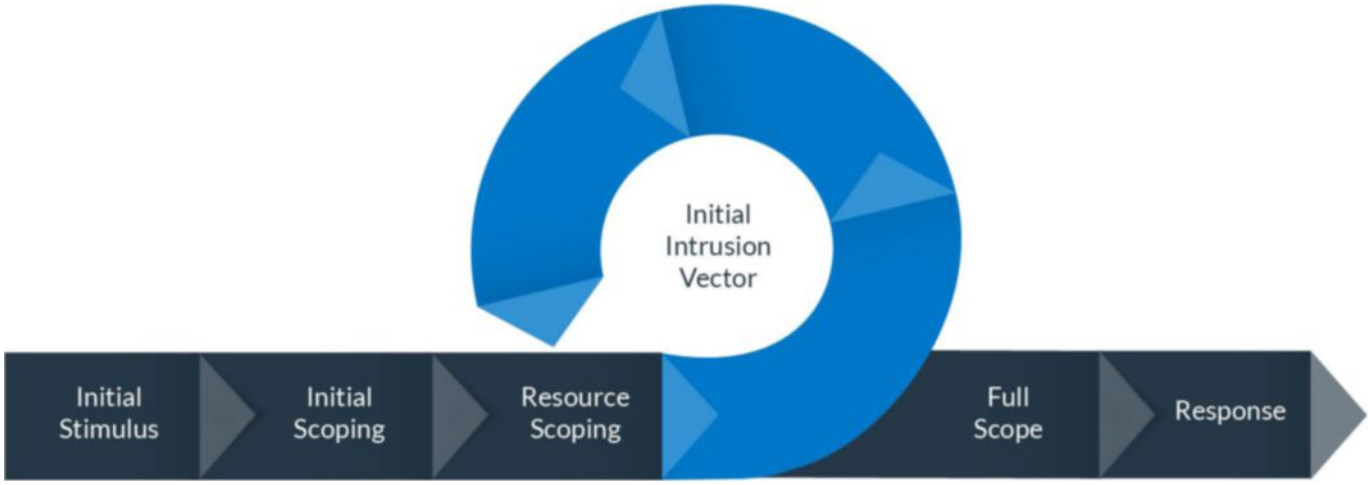
Attributional Models are useful for threat intelligence analysis, particularly for security organizations with visibility into campaigns spanning multiple victims or collections of organizations that share threat intelligence data with enough detail to create the strongly connected networks/ graphs of related attack activity. They provide both the guidance as to what data should be collected for enrichment and how those data points can be connected to enable inferences. They also offer a model for linking the data points to promote analysis and exploration.

Intrusion Response Models

Intrusion response models are analytic methodologies for conducting incident response and remediation activities.

Security Incident Response Matrix

Intrusion response models such as the Security Incident Response Matrix (SIRM) help guide responders through the analysis of security events. SIRM specifically aims to guide analysts as to which data they should gather during the iterative process of incident triage and incident response. It also lays the groundwork for automating much of this process, assuming the data required is available in the victim organization. Data collected during the use of SIRM is often useful for feeding back into both the Cyber Kill Chain and Diamond model.



Data Description Models

The five models of Structured Threat Information eXpression (STIX™)[8], Trusted Automated eXchange of Indicator Information (TAXII™)[9], Cyber Observable eXpression (CybOX™)[10], Malware Attribute Enumeration and Characterization (MAEC™)[11], and the OpenIOC Framework[12] provide a means for describing and transporting threat intelligence in an interoperable manner that machines can process.

Structured Threat Information eXpression (STIX™) is the core and leader in this space and it has objects for modeling all aspects of threat intelligence including: actors, campaigns, incidents, TTPs, indicators, and observables.

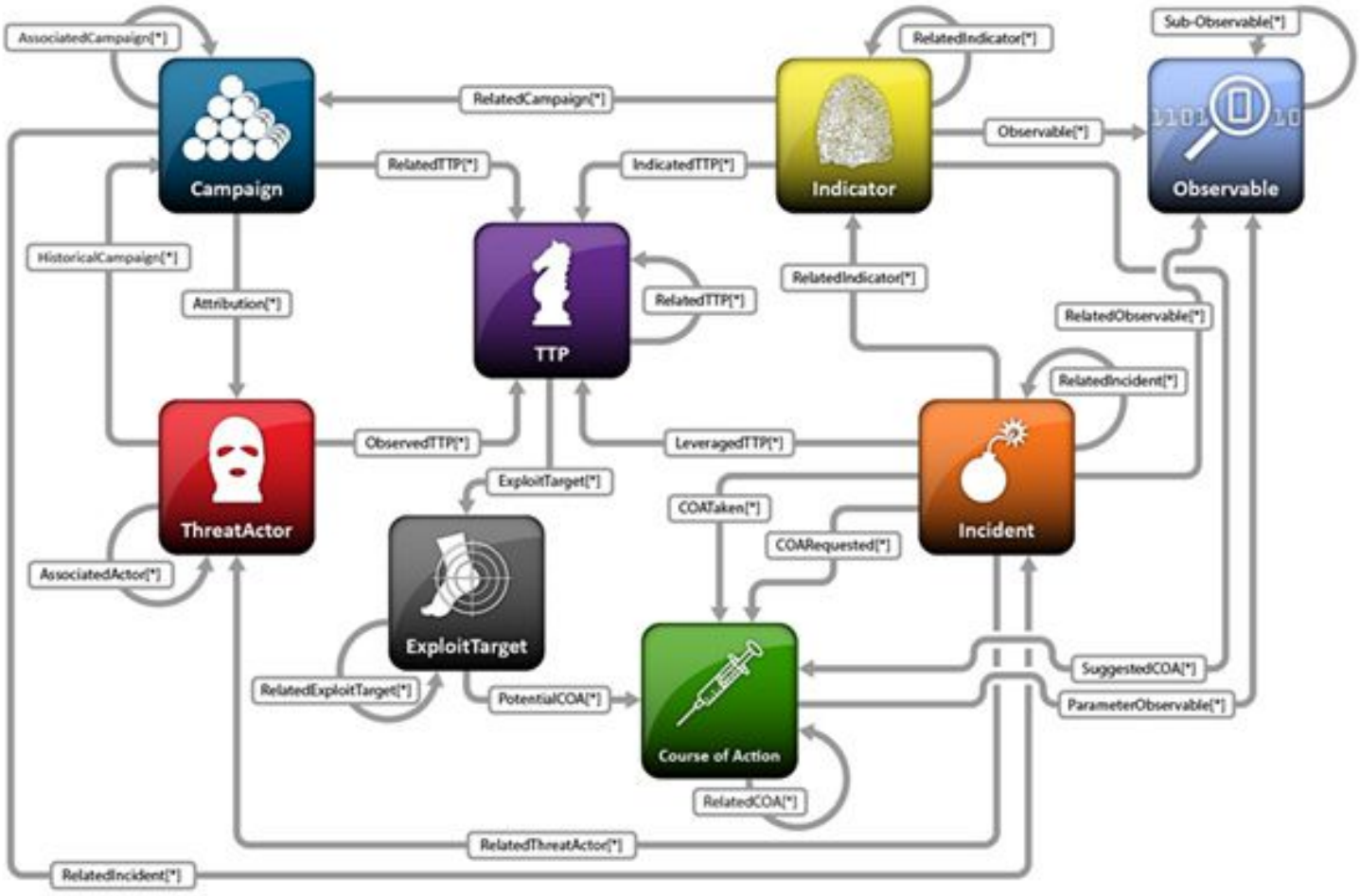


Figure 4: STIX Architecture

Related Work

None of these models are the first of their kind. Earlier adversary description models include Attack Trees from Bruce Schneier in 1996[13] and A Common Language for Computer Security Incidents[14] which described incidents with many links in a chain. Analytical models have included more generalized models such as theObserve, Orient, Decide, Act (OODA) loop by John Boyd. Previous machine language models for computer security include IDMEF[15], IODEF[16], CEF[17] and CIM[18]. AVOIDIT (Attack Vector, Operational Impact, Defense, Information Impact, and Target) is a A Cyber Attack Taxonomy designed to describe attacks, their impacts, and define mitigation strategies[19]. The Anomali Enterprise Model is designed to incorporate the most effective threat intelligence and breach analytics models and will continue to be extended as more models emerge.

The rest of this guide goes beyond the catchy titles and enumerates how organizations can effectively apply the Anomali Enterprise Model.

A New Unified Cyber-Security Framework: Anomali Enterprise Model

The Anomali Enterprise Model unifies and integrates the component models to provide a superior overarching model for organizational (enterprise, governmental and defense) cybersecurity. The aim of this model is to combine and integrate the best analytic threat models in order to operationalize them effectively.

The Anomali Enterprise Model integrates the following models: Security Incident Response Matrix (SIRM), the Diamond Model, and the Cyber Kill Chain. The Anomali Enterprise Model leverages the Structured Threat Information eXpression (STIX™) model for both organizing and relating all information exchanged.

Operational Anomali Enterprise

The Anomali Enterprise Model is organized as follows:

Inputs

1. Threat Intelligence from open source, vendors, trusted sharing groups as well as an organization's sensors are also fed into the system. These items can be formatted as STIX documents.
2. Alerts and events are fed into the system. These can originate from many sources, but they typically come from an organization's security and infrastructure logs.

Analytic Models and Feedback

1. Alerts are triaged. Any event deemed to be a true positive (i.e. worth investigation) is triaged using the Security Incident Response Matrix (SIRM). During SIRM's iterative process of determining the full scope of the incident, intelligence is gathered and used both for gauging the scope of the incident as well as being fed into the attributional models such as the Diamond Model.
2. The Diamond Model should be used to organize all intelligence gathered as well as perform indicator expand and enrichment. All identified IOCs, Signatures, and TTPs should be gathered and used in the Cyber Kill Chain.
3. The Cyber Kill Chain should be used to map all appropriate detections (IOCs, Signatures, and TTPs) to specific controls within Detection and Mitigation Devices. All gaps in detection should be identified for future prioritization.
4. All detections (IOCs, Signatures, and TTPs) should be represented as STIX to enable the automated distribution to security products.
5. Once all detections are loaded into the various security products new alerts and notifications will get generated and these feed back into the system for alert triage.

In the next section we will review how the Anomali Enterprise Model can be applied across several examples.

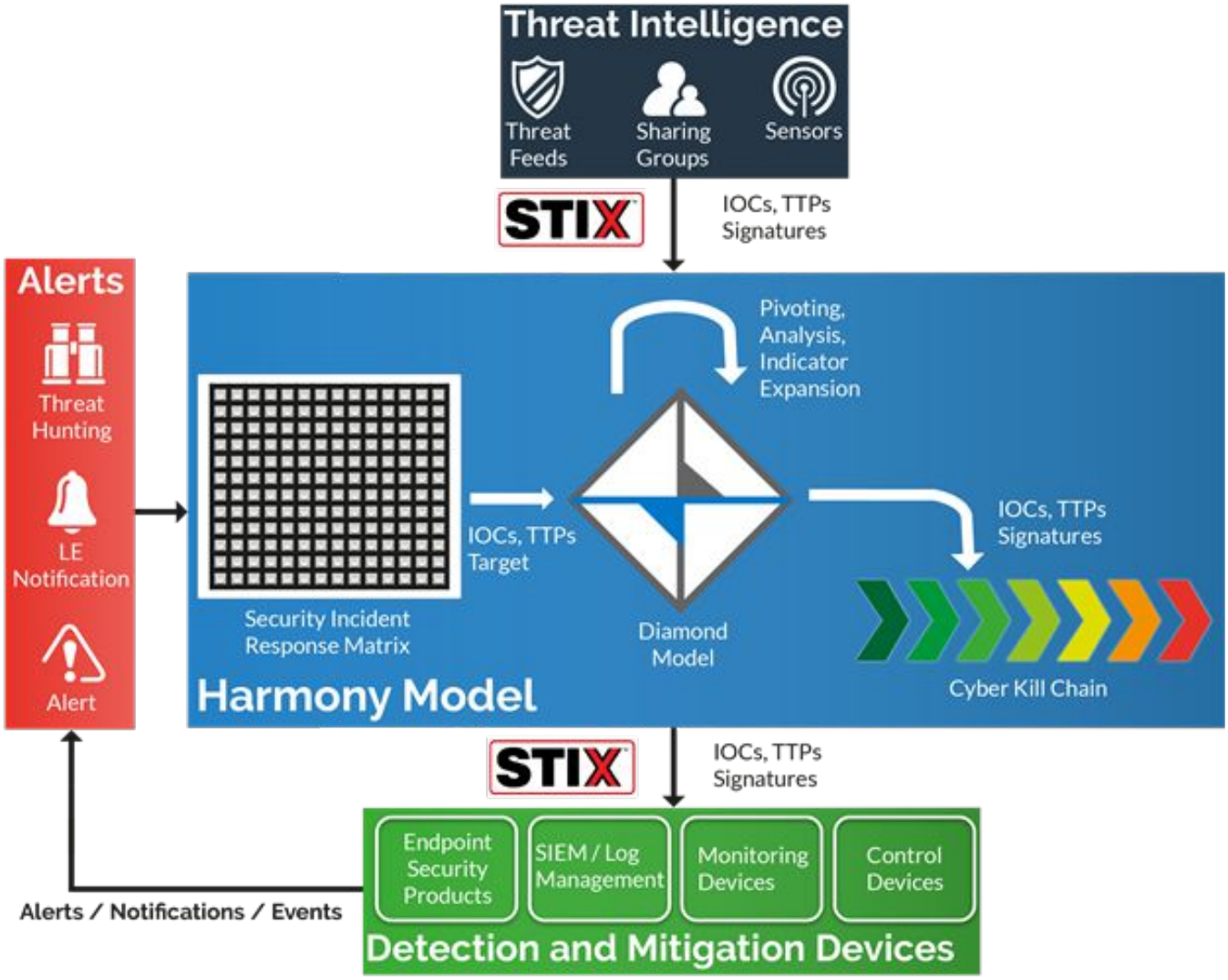


Figure 5: Anomali Enterprise Model

Anomali Enterprise Model Examples

Security Alert

This is a frequently encountered scenario where security operations staff is reviewing alerts from monitoring systems such as Intrusion Detection Systems (IDS), IOC correlation systems, or log analysis platforms. The staff evaluates an alert as a likely true positive. In this case the security staff investigates the alert using the SIRM model by performing initial scoping then iterating through resource scoping towards a full understanding of the compromise. Throughout this practice the staff will investigate any discovered indicators of compromise in an attempt to link the current activity to previously known activity via the Diamond Model. If the activity is not part of a known set of activity, a new actor can be created with additional infrastructure and tools via indicator expansion. By describing the techniques, tactics and procedures (TTP) the adversary used the staff can better detail these activities, aiding to increase confidence in the attribution as well as improving defenses against the TTPs. .

While the indicators + TTPs are being described, the staff will perform Kill Chain analysis of the activity. This supports the security staff in mapping:

- Any existing detections and protections to the activity
- Places where new detections can be put into place
- Places where detection is not possible

During this process the indicators used for protection are transmitted to devices through STIX over TAXII to security devices. More complex detection criteria and the information from monitoring systems is transmitted in Cybox and MAEC forms also over TAXII to the appropriate security devices.

Latest Threat Report Release

Security staff frequently receives reports of ongoing adversary activity via open reports and trusted intelligence vendors. After receiving these reports the staff should take the indicators and TTPs from the report, and describe them via STIX, Cybox and MAEC, which are then transported via TAXII to the detection / protection systems. Staff can also map the indicator and TTP information to their detection/protection controls via the Cyber Kill Chain. In addition to detections that are specific to this actor, staff will want to focus on generic detections that can detect entire classes of TTPs. During this activity the staff will want to use the Diamond Model to organize and link the indicators as well as perform indicator expansion and enrichment in order to identify additional indicators to add to the detection and protection systems.

Victim Notification via Law Enforcement

Once in a while organizations are notified of a breach by an external 3rd party such as a law enforcement (LE) agency. The 3rd party will deliver a range of dates, possibly some indicators of compromise (IOCs), and possibly one or more compromised IPs addresses from the victim organization. If that IP address is the public facing IP address of the web proxy or the public IP of a NAT gateway then the compromised host could be any device in their network.

At this point the security staff only have one option, to begin hunting. The IOC(s) and compromised IP(s) provided are the best place to start the search. After digging into the information available, the staff finally detects a tangible item and has a thread to work. Starting with that IOC the staff would use the Diamond Model to perform indicator expansion and determine if the indicator can be linked to any other know activity. All IOCs found should be loaded into detection and control devices for monitoring. The security staff should also concurrently investigate the identified compromised host and related internal activity via the SIRM. The details that are discovered via these parallel investigation paths are then fed back into the Kill Chain to insure that further detections are implemented. All of the technical data discovered through this activity is sent to the technical controls via TAXII/STIX/Cybox.

Threat Hunting

Threat Hunting (A.K.A. “Hunt Teaming” or just “Hunting”) is the process of attempting to identify previously unknown adversaries already operating in your environment. This process is often manual in nature, but depends on data processing and analysis tools. This process should be performed periodically and it often results in starting the investigation phase in a similar manner as if a Security Alert was generated.

Summary

Threat Intelligence platform vendors are already beginning to catch up to this multi-model approach to unify threat hunting and security operations for the benefit of improved security posture. It is clear that no one threat analysis model provides that right approach given the continued increase in the number and voracity of attacks. As pent up demand grows, and the multi-model approach is adopted, opportunities for automation will and should be a welcome byproduct.

References

[1] 2015 M-Trends Report, https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf

[2] Verizon 2015 Data Breach Investigations Report (DBIR). http://www.verizonenterprise.com/DBIR/2015/

[3] Hutchins, Eric, Michael Cloppert, and Rohan Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns, and Intrusion Kill Chains", Lockheed Martin Corporation, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

[4] Mandiant APT 1 Report. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

[5] Joint Publication 3-13, Information Operations. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

[6] Making the Mandiant APT1 Report Actionable. http://www.appliednsm.com/making-mandiant-apt1-report-actionable/

[7] Caltagirone, Sergio, Andrew Pendergast, and Christopher Betz, "The Diamond Model of Intrusion Analysis", http://www.dtic.mil/docs/citations/ADA586960

[8] Structured Threat Information eXpression (STIX™). https://stixproject.github.io/

[9] Trusted Automated eXchange of Indicator Information (TAXII™). https://taxiiproject.github.io/

[10] Cyber Observable eXpression (CybOX™). https://cyboxproject.github.io/

[11] Malware Attribute Enumeration and Characterization (MAEC™). https://maecproject.github.io/

[12] The OpenIOC Framework. http://www.openioc.org/

[13] Schneier Presentation at SANS Network Security 1999: https://www.schneier.com/attacktrees.pdf

[14] A Common Language for Computer Security Incidents. John D. Howard, Thomas A. Longstaff. http://prod.sandia.gov/techlib/access-control.cgi/1998/988667.pdf

[15] RFC 4765: The Intrusion Detection Message Exchange Format (IDMEF). https://www.ietf.org/rfc/rfc4765.txt

[16] RFC 5070: The Incident Object Description Exchange Format. https://www.ietf.org/rfc/rfc5070.txt

[17] Common Event Format. https://saas.hpe.com/marketplace/arcsight/common-event-format-guide

[18] Common Information Model. http://docs.splunk.com/Documentation/CIM/latest/User/Overview

[19] AVOIDIT: A Cyber Attack Taxonomy http://ais.cs.memphis.edu/files/papers/CyberAttackTaxonomy_IEEE_Mag.pdf

About Anomali

Anomali delivers earlier detection and identification of adversaries in your organizations network by making it possible to correlate tens of millions of threat indicators against your real time network activity logs and up to a year or more of forensic log data. Anomali's approach enables detection at every point along the kill chain, making it possible to mitigate threats before material damage to your organization has occurred.

To learn more, visit www.anomali.com, follow us on Twitter @anomalidetect, contact sales@anomali.com or call 1-844-4-THREATS.