Mighty Guides

Sponsored by

ANOMALI

7 Experts on Threat Frameworks

Use Frameworks like MITRE ATT&CK to Visualize Threats and Take Action

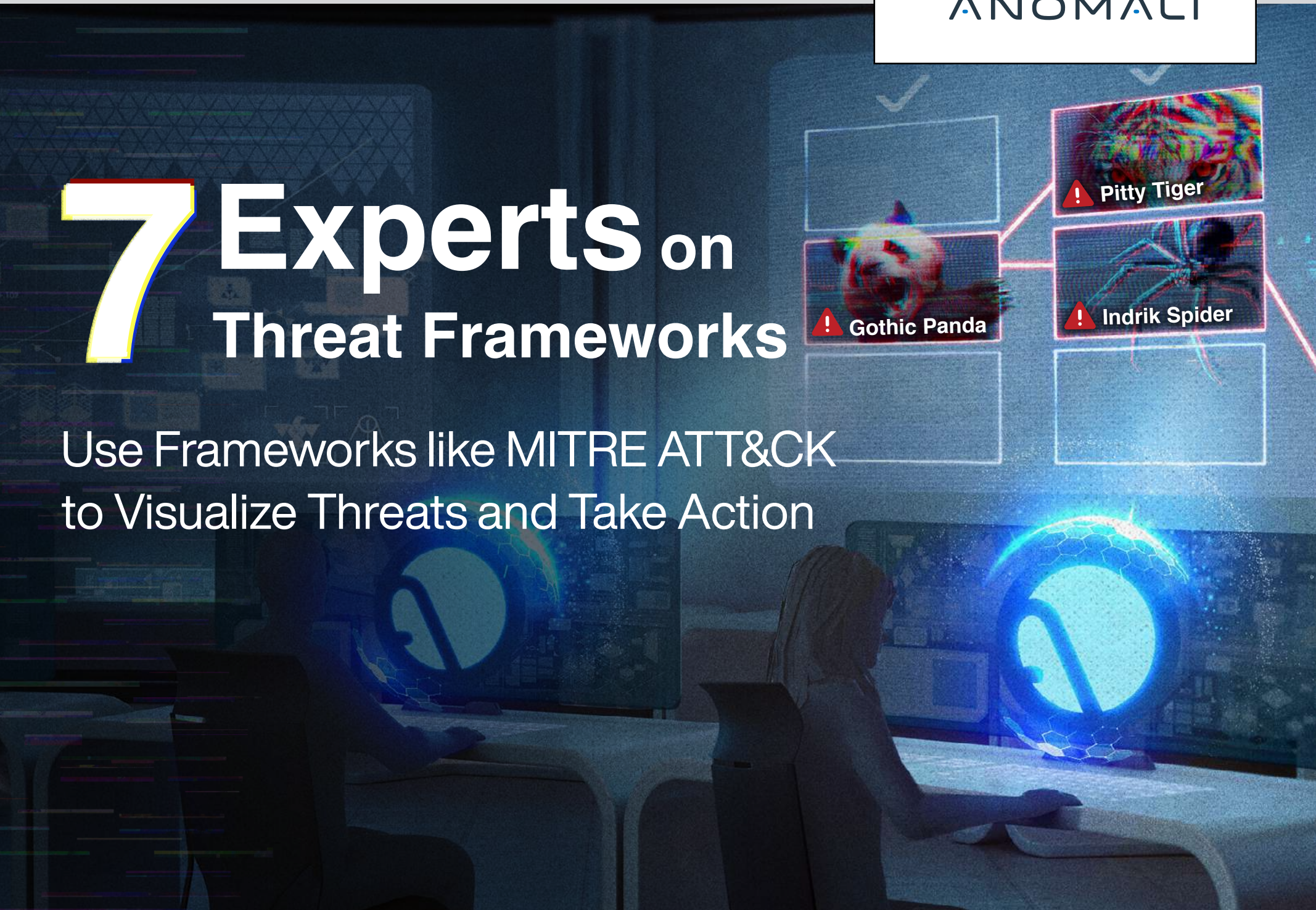


Table of Contents

Introduction

We may live in the golden age of information but, like too much of any good thing, information without context can be counterproductive.

Early attempts at instituting intelligence focused on identification and classification of discrete bits of data and making them actionable. IP addresses, domain names, file extensions, and file hashes all found their niches in defense in depth.

Threat intelligence feeds of indicators of compromise (IOCs) remain a vital component in this arsenal, but your adversaries have learned and adapted: They are keenly aware of how to defeat simple defenses. You have blocked an IP address? They rent a botnet. Blocked a domain name? They buy cheap, disposable names. Blocked a file extension or file hash? They pack and encrypt their files.

Hopeless? Hardly. Thankfully, countless hours have gone into devising ingenious frameworks that extend and expand our classification capabilities. MITRE ATT&CK, the newcomer threat intelligence framework, has fast become the most popular in large part because of its vast technical breadth and depth. Analysts can quickly gain a visual understanding of where they stand and what steps to take next.

This ebook describes the major threat frameworks, existing pain points, and opportunities, with steps to integrate and operationalize them into your security program so that you can grow the capability for more proactive, prescriptive, and predictive actions.

All the best,
David Rogelberg
Editor,
Mighty Guides Inc.

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

Foreword

Security frameworks give security teams a measure of where they are and where they need to go to protect their most valuable assets. They also enable analysts to understand and visualize attack patterns, which is one of the main reasons why cybersecurity has been a significant driver for framework adoption.

Many different kinds of frameworks are used worldwide, each serving a unique purpose. Three common cybersecurity frameworks used in the Security Operations Center (SOC) include the Cyber Kill Chain, MITRE ATT&CK, and the Diamond Model, all of which you'll learn more about in this ebook.

MITRE ATT&CK is quickly gaining traction in the threat intelligence community and is generating excitement among security professionals. You can use ATT&CK to map out your security defenses and understand where there might be gaps in protection. Attackers can be identified by using techniques and tactics they've been known to employ. This allows defenders to identify potential vulnerabilities in their systems and to develop countermeasures to protect themselves from these threats.

As organizations become increasingly vulnerable to rapidly multiplying and evolving threats, frameworks can help strengthen their defenses by anticipating how attacks might unfold so they can strategize their response and ensure a threat-informed defense.

Regards,
Mark Alba
Chief Product Officer,
Anomali

Meet Our Experts

Mark Alba
Chief Product Officer,
Anomali

Alex Attumalil
Deputy CISO,
Leading Sportswear Manufacturer

Christopher Russell
CISO,
tZERO Group

Troy Rydman
CISO and VP
of Cybersecurity,
Fast.co

Chris Thompson
CISO,
Leading Home
Remodeling Company

Genady Vishnevetsky
CISO,
Stewart Title

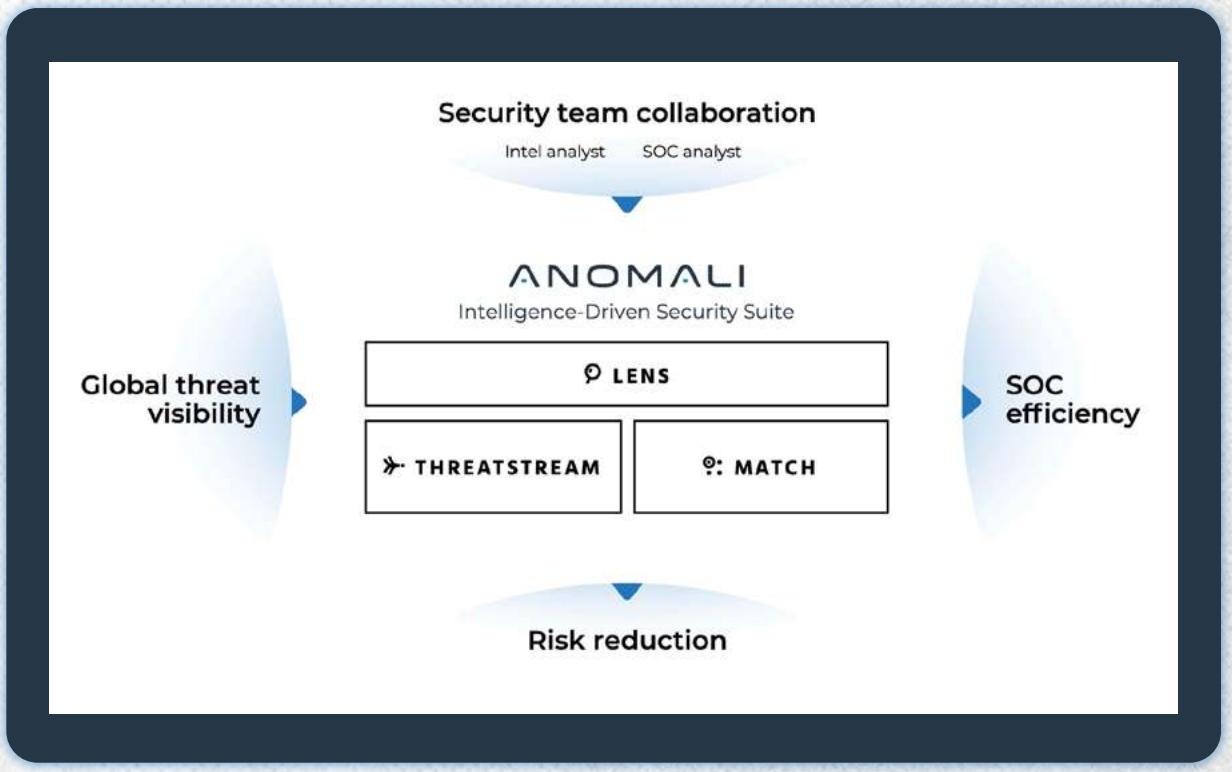
Bob Fabien “BZ” Zinga
Head of Information Security,
Directly

ANOMALI

The Anomali® Platform

The Anomali Platform is a cloud-native extended detection and response solution or XDR that integrates with your existing security telemetry to enhance your investments and deliver detection and response capabilities that stop breaches and attackers.

The Anomali Platform is fueled by big data, machine learning, and the world's largest intelligence repository, to automate the collection of threat data and drive detection, prioritization, and analysis. Anomali surfaces relevant threats and improves organizational efficiencies to provide security teams with the leverage needed to make informed decisions and defend against today's sophisticated threats.



LEARN MORE | DISCOVER | WHAT IS CYBER RESILIENCE? | REQUEST A DEMO

Chapter One

An Overview of Threat Frameworks

Threat frameworks help defenders see order in the chaos of seemingly never-ending streams of security logs and intelligence feeds. They provide a visual taxonomy of a threat actor, illustrate how an attack has progressed, indicate which steps a given attacker may take, and list defensive steps to take. In this way, security teams can take decisive action.

Chief Information Security Officer Perspective

Threat frameworks relate to the needs of and pain points common to security professionals, from boardroom to analyst. A chief information security officer must understand the big picture: What is the organization doing today? How is our coverage? Are we affected?

Mapping existing defensive and detection capabilities against frameworks, especially MITRE ATT&CK, can help security pros assess capability and visibility gaps . . . or overlaps. This perspective can help justify existing expenditures, streamline or eliminate duplicate tools, and prioritize new investments.

Given the popularity of cloud computing and software-as-a-service products, especially gauged against the recent pandemic-driven tectonic shift to remote work, moving workloads to the cloud is largely a matter of when, not if. Threat models of relevant tactics, techniques, and procedures (TTPs) can help security teams visualize demarcations between the organization and a given cloud service provider's shared responsibility model. This analysis can aid in determining how much risk the organization can shift to the cloud without leaving money on the table or the business exposed.

As the latest breach makes its way across the blogosphere, the question the organization asks first is, "Are we affected?" A simple question but one that requires time-consuming analysis to answer clearly and completely.

"Frameworks help establish a true defense-in-depth strategy where threat responses can amount to simple monitoring updates or notifying management that we're protected against a new zero-day. Cybersecurity is about being proactive and ready for the unknown."

Troy Rydman
CISO and VP of Cybersecurity,
Fast

Security teams that have already institutionalized threat frameworks can provide timely reporting about business risk. If the news is about a threat actor known to be partial to attacking financial institutions using Microsoft exploits but you are a Linux-based retail shop, there is probably no need to buy pizzas and fire up the war room to run a midnight patch frenzy.

Analyst Perspective

All teams can benefit from integrating threat frameworks into operations from day one. Frameworks are designed to scale from a small, single-analyst shop to a global enterprise with dedicated cyber threat intelligence (CTI), a security operations center (SOC), incident response (IR), and red teams.

No team can defend against all threats, especially if hampered by resource constraints, but your adversary has to be right only once. Understanding threats can reduce the scope of your analysis to what is relevant for your organization, your architecture, and your vulnerabilities and reduce your overall mean time to detection (MTTD) or response accordingly.

> **Threat frameworks help visualize a threat actor's motives to understand the phases of an attack to see how it can progress, what steps a given threat actor is going to take, and what mitigation steps are necessary.**
>
> 
>
> **Mark Alba**
> Chief Product Officer, Anomali

Mapping events to threat frameworks and quickly revealing threats or threat actors by matching IOCs and TTPs can visually portray an attack landscape in real time. It introduces the capability for predictive analysis based on historical data and trends, even attribution to a specific threat actor by that actor's characteristic TTP footprint. Understanding an attacker's objective enables you to predict next steps and interrupt the threat, ideally before the attacker reaches their end game.

"If a security team truly understands the threat actors they face, they can put controls in place at each phase of an attack to increase the odds of intercepting and preventing a worst case scenario for their organization."

Chris Thompson
CISO,
Leading Home Remodeling Company

Threat Framework Models: An Overview

Threat framework models are constructs built to contextualize and organize threat information during an investigation as an attack evolves and provide a common language among teams. These models enrich operational intelligence, helping analysts understand more than the sum of the parts, and pivot investigations to otherwise-hidden depths.

There is a multitude of threat framework models in use today by organizations as diverse as small single-digit security teams to the largest enterprises and government entities. Most share some general commonalities but each is uniquely specialized to suit specific security use cases, providing choices as to which model(s) to select and operationalize.

MITRE ATT&CK

MITRE ATT&CK is by far the most comprehensive and popular of all current threat framework models. It consists of a detailed chart of potential threats, categorized by the associated attack phase, along with descriptions of attacks and their subtypes. It also includes a list of known threat actors, their known targets (e.g., Retail, Financial, etc.), and preferred TTPs. MITRE ATT&CK is actively maintained with updates based on current real-world attacks.

Cyber Kill Chain Model

Lockheed Martin's Cyber Kill Chain Model focuses on the linear flow of common cyber attacks, from initial reconnaissance to exploitation and actions on objectives. This model helps to shine the light on possible future steps based on current evidence, allowing you the opportunity to get one step ahead of the attacker before the worst happens.

Diamond Model

The Diamond Model is unique in that it emphasizes four key aspects of an intrusion: the adversary (who), the infrastructure (what), the capabilities (how), and the victims (where). An intrusion event is defined as how the attacker demonstrates and utilizes certain capabilities and techniques over infrastructures against a target.

Mandiant's Targeted Attack Lifecycle

This model is very similar to Cyber Kill Chain Model but it acknowledges the reality that many attackers will branch out once they have a foothold. This model maintains an iterative loop to help track an attacker seeking to move laterally and maintain additional presence. Reconnaissance scans and footprinting, for example, may therefore be a subcomponent of a single attack where the Cyber Kill Chain would treat them separately.

STIX

Structured Threat Information eXpression (STIX) provides a predetermined schema for the sharing and interoperability of cyber threat intelligence. This model ensures that multiple threat feed subscriptions can ingest and coexist within one system with supporting metadata intact.

Cyber Kill Chain Model

Lockheed Martin adapted the military kill chain to cybersecurity, illustrating a linear flow of adversarial behavior as those attackers work to achieve final actions on their objectives (Figure 1). It is a high-level model that generally focuses on preventing single-attack processes. It is less capable at specifically identifying defenses but is exceptional at identifying ways to interrupt and undermine the path of an incursion. The model includes seven attack phases:

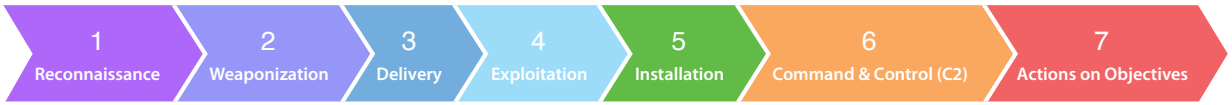


Figure 1. Lockheed Martin Cyber Kill Chain (*Source: Anomali Match Platform*)

1. **Reconnaissance.** The attacker gathers information about the target. This process generally begins passively, such as with Domain Name System information or gathering clues from LinkedIn or job listings, but progresses to active methods, such as port or vulnerability scans.
2. **Weaponization.** The attacker locates or creates an exploit based on the vulnerabilities found during reconnaissance.
3. **Delivery.** The attacker determines the delivery method for the exploit (such as phishing or SQL injection).
4. **Exploitation.** The attacker executes the delivered attack.
5. **Installation.** The attacker gains and maintains access.
6. **Command and control (C2).** The attacker establishes persistent access for remote manipulation and could act immediately or lurk in your system for months or even years.
7. **Actions on objectives.** This phase identifies the attacker's ultimate objective—data exfiltration, data destruction, or denial of service.

"There are many benefits to using threat intelligence, especially integrating threat data that focuses on protecting your infrastructure and providing advanced insights on threats targeting your business."

Alex Attumalil
Deputy CISO,
Leading Sportswear Manufacturer

Diamond Model

Complementary in many ways to the other models, the Diamond Model focuses more on threat actor attribution (Figure 3). It uniquely models and tracks attacks across multiple intrusions by analyzing the similarities, relationships, and characteristics of its four component categories. On its face, it may appear relatively simple, but it can be quite dynamic. By understanding your attacker, you gain a wealth of information about where to bolster defenses or improve alerting. The model's inherent weakness is that it must be updated routinely and maintained as the landscape changes.

It is broken into four quadrants:

- **Adversary.** The persona of the individual or group attacking you
- **Infrastructure.** IP addresses, domain names, or email addresses
- **Capabilities.** What the adversary can do, such as deploy malware, run exploits, or manipulate infrastructure
- **Victim.** May include people, services, network assets, or information

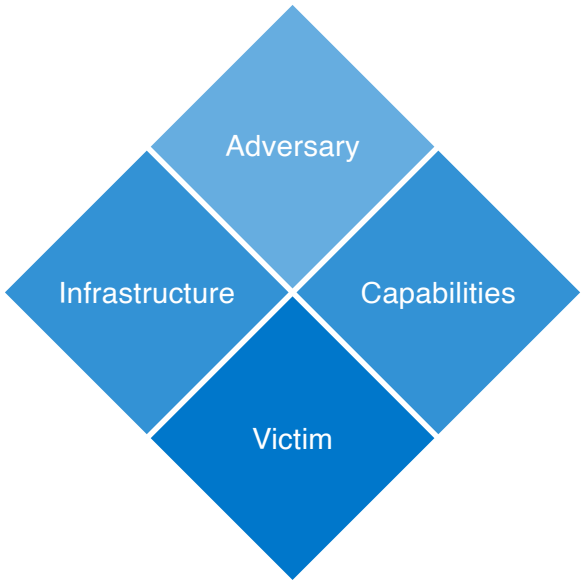


Figure 2. Diamond Model (*Source: Anomali Match Platform*)

Threat frameworks provide a structured approach to thinking about attack phases. Security teams can reference them while developing playbooks and response plans to ensure they are covering all the bases.

Chris Thompson
CISO,
Leading Home Remodeling Company

Mandiant's Targeted Attack Lifecycle

Expanding on the Cyber Kill Chain, Mandiant's targeted attack lifecycle model reflects the linear progression of an attack but includes a loop after privilege escalation to better reflect real-world post-compromise behavior (Figure 2). The added loop enables an analyst to level-set, rescope, and gain a stronger understanding of the depth and breadth of an attack. Port scanning at the perimeter may often be white noise—the cost of having a publicly exposed IP. A port scan within the network, however, is far less likely and could be indicative of an attacker conducting reconnaissance in an effort to expand and move laterally around the organization. Otherwise, the phases are similar to the Cyber Kill Chain:

- **Initial reconnaissance:** The attacker gathers information about the target.
- **Initial compromise.** The attacker gains an initial toe hold in the network, executing malicious code.
- **Establish foothold.** The attacker installs a persistent backdoor entry point to gain control of the target network's systems from outside the network.
- **Escalate privileges.** The attacker gains further access to systems and data in the target environment. Often, this phase begins in the context of a regular user, with the goal being to gain administrator privileges.
- **Internal reconnaissance.** The attacker explores the environment to better learn how and where to continue the attack.
- **Move laterally.** The attacker moves to additional systems in the environment.
- **Maintain presence.** The attacker establishes persistent remote access to the environment, typically to a remote C2 domain.
- **Complete mission.** The attacker completes the objective of the attack.

"Threat frameworks help analysts manage risk, understand the motivation and goals of threat actors, and anticipate TTPs that an adversary is likely to use to compromise a network."

Bob Fabien "BZ" Zinga
Head of Information Security, Directly

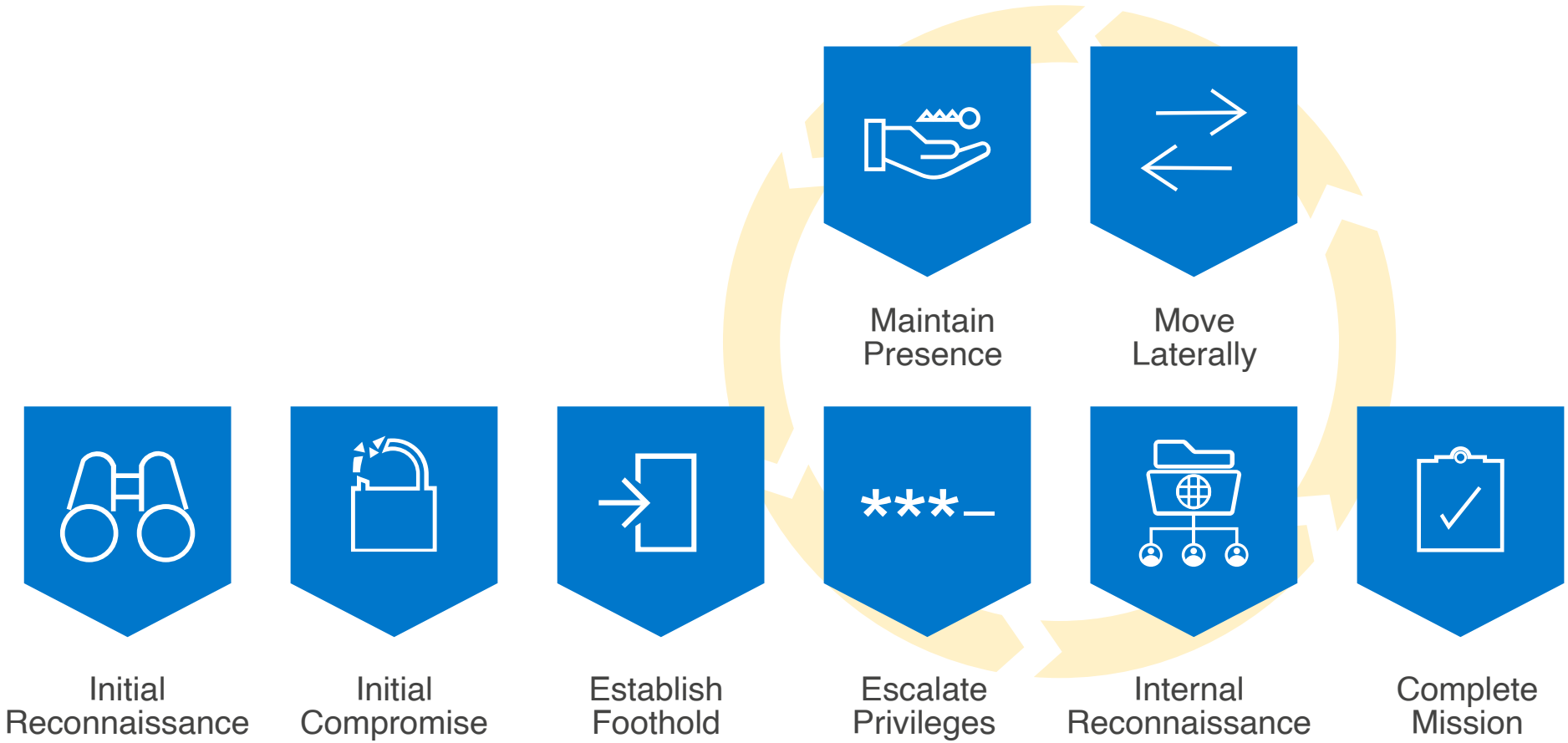


Figure 3. Mandiant Targeted Attack Lifecycle (*Source: Mandiant Red Teaming: Uncovering Modern Attack Paths Case Study)*

STIX/TAXII

Structured Threat Information eXpression (STIX) is a standardized language and serialization format used to exchange CTI. It commonly exists in conjunction with Trusted Automated eXchange of Intelligence Information (TAXII), the protocols used to share STIX information (Figure 4). An organization can subscribe to multiple threat feeds from multiple sources yet trust that the data remain normalized to ease integration.

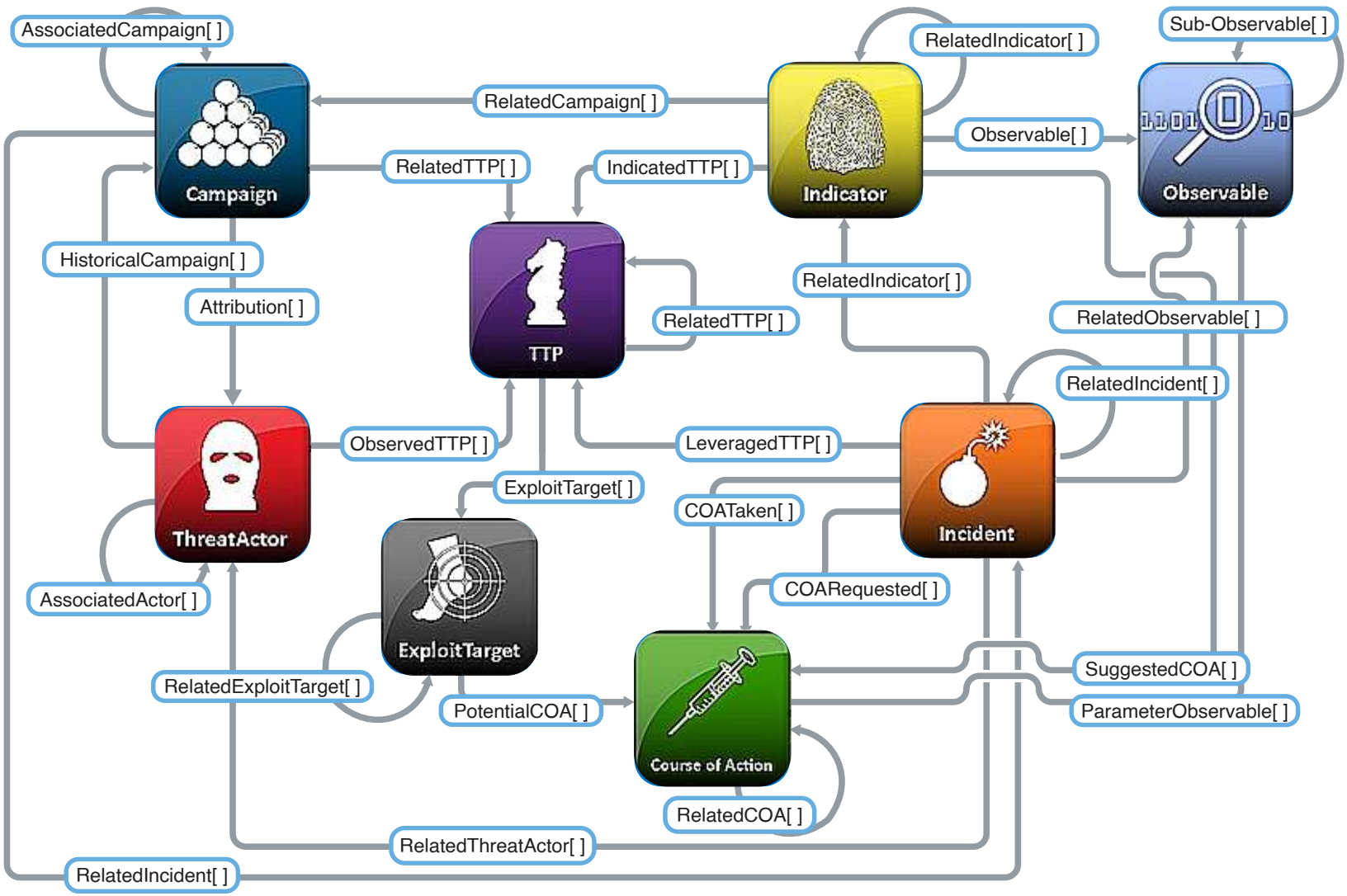


Figure 4. Diamond Model (*Source: About STIX*)

Key Takeaway

Threat frameworks bring order to the chaos of security logs and intelligence feeds, providing a visual map of an attack or attacker.

"Having multiple available frameworks that take a different approach to threat modeling ensures that you can integrate one that can be tailored to best suit your needs."

Chris Thompson
CISO,
Leading Home Remodeling Company

Chapter Two

MITRE ATT&CK

The new kid on the block, introduced in 2015, MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a highly organized, well-maintained, matrixed clearinghouse of attacker TTPs. These TTPs are matched by columns, representative of attacker phases, similar to the Cyber Kill Chain and Mandiant's targeted attack lifecycle.

ATT&CK acknowledges that many attacks may not follow a strictly linear progression, especially after an attacker has gained an initial foothold. The model effectively assumes breach and moves past perimeter security to detection and response across all layers of security architecture, including post-compromise detection, an element noticeably lacking in other models (Figure 5).

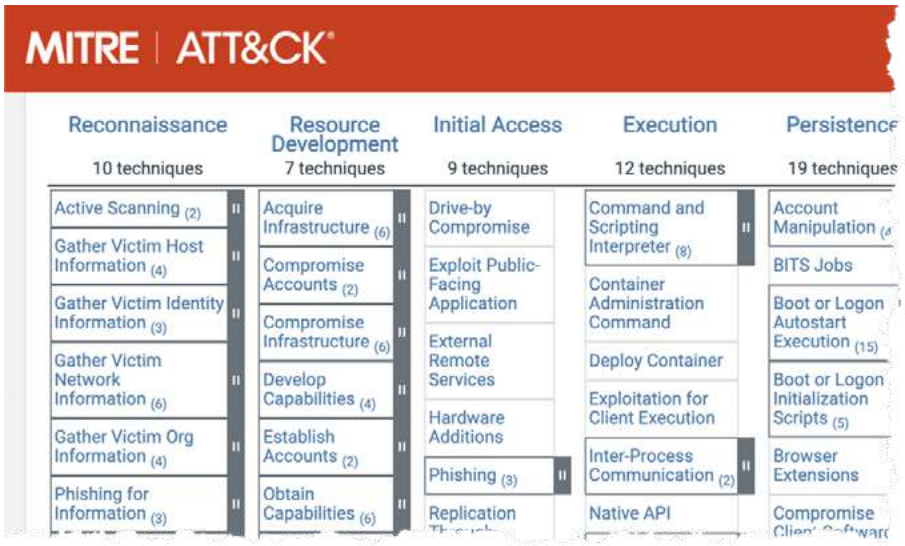


Figure 5. MITRE ATT&CK framework (*Source: The MITRE Corporation*)

"The MITRE ATT&CK framework has quickly become the de facto threat framework for many organizations because it is useful, practical, comprehensive, and quite effective."

Bob Fabien "BZ" Zinga
Head of Information Security,
Directly

MITRE ATT&CK is well supported and iteratively improved over time through an analysis of real-world information sourced from cutting-edge security research, blogs, and threat intelligence communities. It functions as a living document, maintaining parity with the latest attacks and tactics.

Notably, ATT&CK has never purported to be prescriptive guidance for compliance, as one might find with the Payment Card Industry Data Security Standard or National Institute of Standards and Technology 800-53. Avoid the temptation to treat it as such, and question any vendors that claim to be "ATT&CK compliant."

Proactively Prepare for Threats

To use ATT&CK to prepare for a threat, begin with a comprehensive analysis of your environment and its vulnerabilities. Know specifically which clouds, systems, libraries, and versions make up the components of your architecture and any of their published vulnerabilities—especially those with known exploits.

> **The MITRE ATT&CK Framework enables security practitioners to analyze threats and technical indicators to translate the attack into impact.**
>
> 
>
> **Mark Alba**
> Chief Product Officer, Anomali

Next, use ATT&CK's comprehensive list of known threat actors to narrow your scope to those attackers focused either on your industry vertical or your technology stack. Use that threat profile to understand your quarry's historical TTPs, a more durable metric than IOCs because attackers can easily change a source IP address but are far less likely to drop tried and true tactics. This focus has a side benefit of helping overcome human bias from your own red team, which is comfortable with its own arsenal of tools, to produce more realistic attack simulations.

"By understanding the most likely threats targeting them and how they will likely play out, security teams can build in redundant protection, alerting, and recovery controls to ensure they are protected or ready to react."

Christopher Russell
CISO,
tZERO

Finally, inventory your security controls and log sources against those required to detect your attackers' TTPs. The resultant overlap of known exploits, threats, and unmitigated vulnerabilities is your threat landscape and should become your short-term priority (Figure 6). Patch vulnerabilities, learn to detect these specific threats, or introduce compensating controls to act proactively.

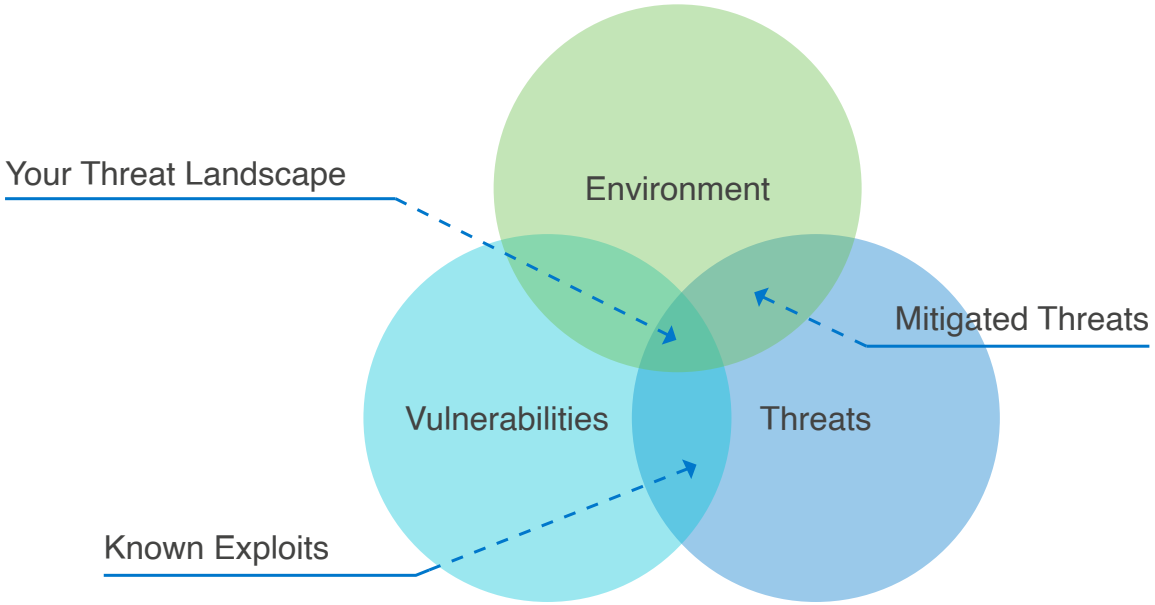


Figure 6. Threat Landscape

Speed Investigations

Combining global threat intelligence, especially when mapped to local security events and telemetry, ATT&CK can produce a map of your attack and your attacker to focus on what deserves attention straight away.

Visually identify which steps an attacker has already used. Use that view as actionable insight into where the attacker may progress next. With ATT&CK's leg up on attribution, you can review tactics and techniques that you may not yet have discovered. Use that knowledge to pivot to other logs and security tools.

"MITRE ATT&CK allows threat researchers, analysts, defenders, and technologies to understand the threat and work collectively to respond to it. Adoption of the framework increases overall agility for security teams and reduces incident response times."

Genady Vishnevetsky
VP and CISO,
Stewart Title

Holistic View of Security

ATT&CK provides a common vernacular of defensive and adversarial capabilities to better facilitate communication between teams or external entities. Specific techniques correlate to descriptions and IDs that all teams can agree on. T1091, “Replication Through Removable Media,” will mean the same thing to your teams as it does to your service providers or penetration testers—a cyber lexicon to help all parties speak the same language with clarity.

With ATT&CK, you also have a great opportunity to democratize cybersecurity. Visually educate developers, system administrators, and DevOps teams about where and how their work influences organizational security. Security awareness can halt vulnerabilities before they appear.

Realistic Threat Simulation

When you have a clear picture of your threat landscape, emulate your likely attacker’s TTPs. In other words, allow offense to inform defense. If the attempt is undetected, the SOC/IR teams should tune alerting until it is. If the attempt is successful, security engineers can enact measures to mitigate the attack.

Start with a single technique, announced to the teams. Broaden the scope as teams improve their capabilities. Move to spontaneous tests to validate real-world alerting. If your red team is still in its infancy, look into open source attack simulation collections, such as MITRE Caldera, Red Canary Atomic Red Team, or Uber Metta, as stepping stones to program maturity.

“More than any other framework, MITRE ATT&CK visualizes attack patterns by mapping adversary behavior against recommended courses of action. This is important because it increases overall effectiveness by saving time and prioritizing the use of security resources to address potential threats.”

Bob Fabien “BZ” Zinga
Head of Information Security,
Directly

Key Takeaway

MITRE ATT&CK moves beyond perimeter security to provide an accurate map of the tools and tactics of modern threat actors, even post-compromise.

"The MITRE ATT&CK framework allows analysts to map the behaviors of a known threat actor. This enables security teams to understand the most likely attack path for your organization and where to focus your investigation and resources."

Chris Thompson
CISO,
Leading Home Remodeling Company

Chapter Three

Role of Integrated Threat Intelligence

Threat Intelligence is the final distillation of a lifecycle during which data at the atomic level are collected, processed, analyzed, and disseminated to inform tactical, strategic, and operational planning and direction. A collection of raw facts, data alone lack the contextualization and logical grouping of information to be readily actionable. Threat intelligence platforms typically support ingestion of IOCs through STIX/TAXII feeds for automated processing into more actionable information.

> **Threat intelligence is the key to ensuring you understand what's happening to operationalize the frameworks effectively.**
>
> 
>
> **Mark Alba**
> Chief Product Officer, Anomali

True intelligence lies at the intersection of data, an automated analysis platform, and manual analysis/interpretation in a timely and relevant manner. Mapping information against threat frameworks is an effective way to translate data into intelligence.

Collect data, process the data into information, and then analyze the information to produce actionable intelligence that is disseminated to inform tactical, strategic, and operational planning (Figure 7).

"Curated threat intelligence feeds help analysts prioritize threats by allowing them to model and map otherwise generic TTPs to a specific organizational threat profile."

Genady Vishnevetsky
VP and CISO,
Stewart Title

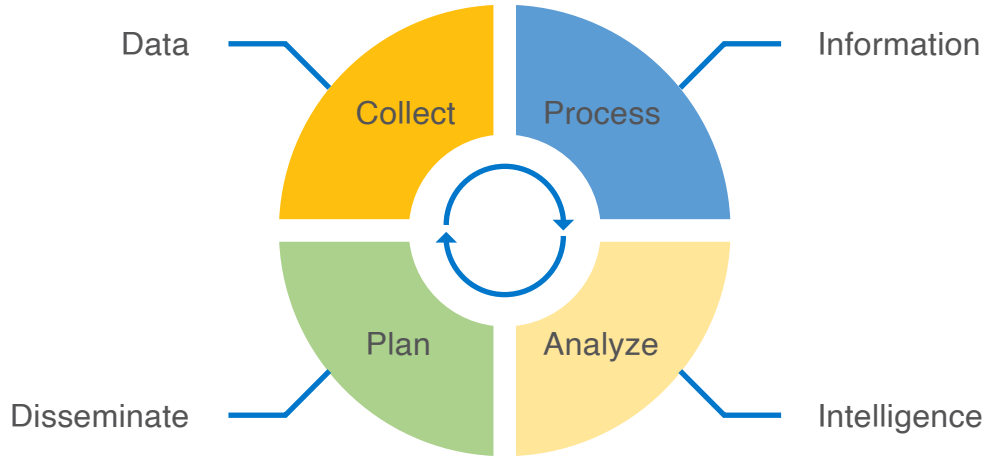


Figure 7. Threat Intelligence Lifecycle

Threat Intelligence Feeds

Low-level collections of individual IOCs, threat intelligence feeds can vary wildly in quality and accuracy, from highly curated paid sources to simple open source lists, such as known phishing email addresses. Some specialize in subsets of data, such as with dark web, social media, or brand monitoring.

Threat intelligence bulletins are reports, often categorized or organized by threat actors and their TTPs. Threat bulletins describe new tools, attacks, vulnerabilities, or threat campaigns—dedicated attacks against specific targets, such as an industry vertical or a new exploit.

Threat Intelligence to Threat Framework Mapping

Threat intelligence information can quickly come alive when mapped against threat frameworks. The visual structure of logged events matched against incoming threat intelligence can provide ready clues as to what phase an attacker is currently in and where they are likely to move next. That striking combination empowers security teams to mitigate future threats before they occur.

"CTI, SOC, and IR teams don't have the resources to solve for every potential attack vector. Having well mapped, relevant threat intelligence is critical to ensure all teams understand the threat and are focusing on the correct areas."

Troy Rydman
CISO and VP of Cybersecurity, Fast

Key Takeaway

Data is collected, processed into information, analyzed into actionable intelligence, and finally disseminated to inform tactical, strategic, and operational planning.

"There are many variables in regards to how the adversaries might perform the various TTPs. Curated threat intelligence feeds provide current values for those variables, above and beyond just simple IOC matches."

Christopher Russell
CISO,
tZERO

Chapter Four

Opportunities

The modern threat landscape changes rapidly, with the flavor of the day in constant flux. We've become almost numb from the breach-of-the-week plague of recent years. It seems only yesterday that SolarWinds stole the headlines, but then was quickly dwarfed by Log4Shell. The next great permutation of attacker and vulnerability can drop at any time.

Threat Inventory

With so many potential attacks from so many threat actors, it is virtually impossible to defend against everything. Deciding where to start and how to prioritize can be difficult, but keeping a finger on the pulse of emerging threats is vital to proactive security.

> **When new intelligence comes in, utilizing frameworks like MITRE ATT&CK to map that new information against your security defenses can give you a very easy to understand visual of what an attacker is going to do to address your security coverage to defend against it.**

Mark Alba
Chief Product Officer, Anomali

Threat Detection

Threat investigation between teams and across multiple security tools is difficult at best. Analysts can lose the proverbial forest for the trees, overloaded by alerts presented in different interfaces. Costly resources are wasted fighting fires rather than strategizing or automating.

"Threat frameworks enable organizations to measure the efficacy of their security investments, to understand where their strengths and weaknesses are. Risk grouping within the frameworks helps organizations prioritize investments and allows analysts to focus on what's most critical."

Genady Vishnevetsky
VP and CISO,
Stewart Title

Threat frameworks provide a missing structure to correlate events and aid in prioritization.

Start to rely on automation and integration to shift focus from signatures and low-level atomic indicators that are generally too dynamic to be relied on for any length of time. Layer your security to remove pieces from the chess board and make it increasingly difficult for your adversaries, edging up the cyber pyramid of pain (Figure 8). Blocking IP addresses is quick and easy, but it is also easily defeated. Shutting down the ability to use an entire tool or tactic may force your attacker simply to move on to the next victim.

In the haste to clear alerts or tickets, security teams can also go through the motions with insufficient information, coordination, or feedback. Such siloed teams make their individual decisions without a shared understanding of threats, threat actors, risks, vulnerabilities, or defenses.

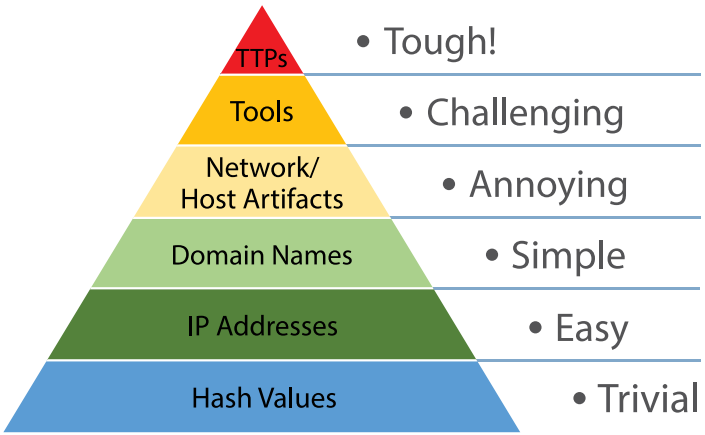


Figure 8. Cyber Pyramid of Pain (*Source: Attack IQ*)

Automation

With a relentless, 24/7 pounding across all endpoints, you cannot rely solely on manual processes. Automation is no longer a convenient time-saver: It's a necessity. Reading and analyzing threat bulletins, web posts, search results, or other unstructured data to locate, key in, and then correlate IOCs is feasible but hopelessly slow—and time is of the essence.

"We have seen success by focusing our threat intelligence on areas such as external security exposure, continuous monitoring, social media activity, doppelganger domain registrations, and dark web activity such as the sale of network access, sensitive data, or fraud methods. This helps us identify potential threats to ensure we're prepared to address them."

Alex Attumalil
Deputy CISO,
Leading Sportswear Manufacturer

Key Takeaway

Automate blocking indicators of compromise to refocus efforts on reducing your adversary's arsenal of tools and tactics. The attacker can move elsewhere.

"In a perfect world, security teams would have the resources to monitor and track for every means of attack, but that's not reality. Preparing for threats that you are not likely to face wastes security resources that could be spent combatting more relevant threats to your organization. "

Christopher Russell
CISO,
tZERO

Chapter Five

Intelligence-Driven Security Using Frameworks

Fortunately, commercially available threat intelligence management solutions and security tools can take full advantage of threat intelligence and threat frameworks to reduce your time from evaluation to implementation and operation.

Picture information security as a cycle of threat identification, defense and protection, attack detection, incident response, and recovery against the backdrop of threat intelligence (Figure 9). Break down these phases, and create a list of technical features to keep in mind while evaluating the purchase or integration of new security platforms.

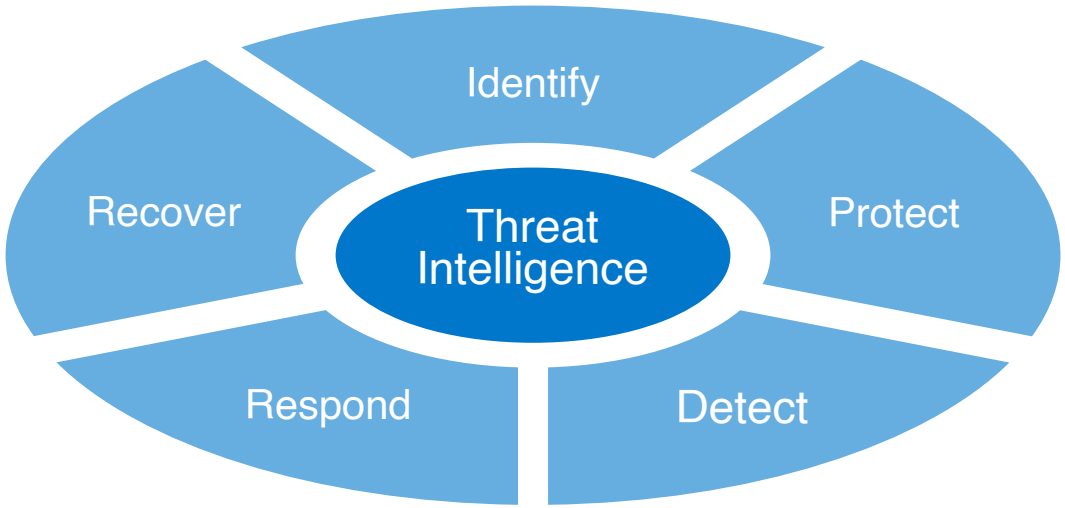


Figure 9. Information Security Cycle

"It's important to utilize threat frameworks to map your security posture against threat intelligence, potential attack vectors, and the experience from peers in your vertical. This enables you to close holes and mitigate the threats with the highest impact and probability first, and therefore, those having the largest impact on your overall security posture."

Troy Rydman
CISO and VP of Cybersecurity,
Fast

Identify

You must be able to sift through all the possible threat actors to narrow your scope to those attackers focused on your vertical or technology stack. Identify the threats before they actually hit you, like putting your fingers on the wire outside your enclave to feel the noise and chatter and to point at what is coming your way (as well as what is likely to bypass you entirely). Automate parsing IOCs from Cybersecurity and Infrastructure Security Agency bulletins or security blog posts to determine whether an attacker is already in your network, and then map the actions to ATT&CK for broader analysis.

> **We've integrated MITRE ATT&CK and other frameworks into our platform to deliver threat detection capabilities and relevant intelligence throughout the attack lifecycle to make it easier for Threat Intelligence and SOC Analysts to leverage during their investigation process.**

Mark Alba
Chief Product Officer, Anomali

Protect

To create a gap analysis of your defensive, alerting, and logging capabilities, reference ATT&CK to describe the log source requirements needed to detect specific tactics and their tell-tale signs. Overlay the TTPs of your most likely threat actors against an ATT&CK mapping of your defensive capabilities. Analyze the results to determine chinks in your armor, but also be on the lookout for overlaps: Consolidate where possible to simplify and trim your budget.

Detect

Reduce your MTTD by correlating global threat intelligence against local security telemetry. Solutions with artificial intelligence engines excel at producing high-fidelity alerts on anomalies

"Threat frameworks help security analysts understand a potential adversary and how they operate. They also help improve organizational efficiencies by fast-track training junior security analysts or engineers about how to mitigate attacks."

Bob Fabien "BZ" Zinga
Head of Information Security,
Directly

from your organizational baselines. Map the tracks of threat actors across frameworks to visualize patterns. Build custom rules and alerts to detect those patterns, where necessary.

Intelligence-Driven Response

Visualize active threats against an ATT&CK map as a means of predictive analysis from historical threat data. If you can attribute your attacker by their signature TTPs using either ATT&CK or the Diamond Model, then you gain information about where the attacker may hit next—or where you are not looking.

Prioritize and make intelligence-driven decisions based on your adversary's processes or patterns. An internal port scan alone is worrisome, but tying that scan to a subsequent data exfiltration alert informs the relative priority of what you are seeing and how to react.

Look for platforms that you can integrate with your existing security stack to automate response actions, such as blocking known malicious IOCs at your perimeter. Prepare runbooks or playbooks focused on expected attack types that include integrated automated response actions with your security tooling, such as endpoint containment.

Recover

Positive attacker attribution can go a long way in allaying fears about whether remediation efforts were sufficient or complete. With a degree of reliability, threat actors tend to stay within the lanes of their well-known tools and tactics. Security teams can search for forensic signatures, ascertained from ATT&CK, the Diamond Model, or threat bulletins, to clear the threat. Executive reports can create confident summaries of whom or what was ultimately affected and the measures you should take to avoid a recurrence.

When all is said and done, invest adequate time to dive deeply into the who, what, where, how, when, and why of an intrusion. Understand your successes and failures across alerts and defenses to inform future proactivity. Share lessons learned across teams to open the door for holistic process improvement across the organization.

"Security teams can prioritize threats by identifying the TTPs commonly in use by threat actors that typically target your vertical, allowing blue teams or those responsible to write better detections."

Christopher Russell
CISO,
tZERO

Key Takeaway

Utilize threat frameworks to aid the cycle of identifying threats, protecting the organization, detecting attacks, responding, and recovering with confidence.

"Threat vectors are a variable in the CISO's risk equation - how will they impact and how often? Applying frameworks can help ensure that threats are a well understood aspect of your risk assessment to ensure you have the appropriate defensive measures in place to improve upon your security posture."

Chris Thompson
CISO,
Leading Home Remodeling Company

How Anomali Helps

Anomali's commitment to empowering security professionals to better identify and disrupt malicious activity has led to us integrating key frameworks into our platform, including MITRE ATT&CK, mapping techniques to actual events to get ahead of the adversarial lifecycle.

The Anomali Platform works with ATT&CK to unite research, analysis, and publishing tools, speeding threat detection and delivering operationalized threat intelligence directly to analysts or into security controls. This automation improves productivity for security analysts and enables proactive defense measures.

Using relevant threat information to understand adversarial techniques and how they are used against a specific environment is another advantage of Anomali's integration of ATT&CK. For example, if a bank sees that another financial institution has been attacked by a particular threat actor or malware family and the security team identifies the attack techniques, it will improve the bank's ability to emulate an adversary with red and blue team scenarios.

Another way the Anomali Platform uses ATT&CK is to build visual representations of the attack techniques. Being able to visualize threat actors and their malware and map that information to the appropriate techniques is powerful. Effective visuals can communicate up the chain of command to those with less technical skill the threats that the team has encountered or tracked so that the organization can respond more effectively and efficiently.

Learn More About Our Experts

Mark Alba, Chief Product Officer, Anomali

Mark Alba is Chief Product Officer at Anomali, joining the company in April 2020. Mark has over 20 years of experience building, managing, and marketing disruptive products and services. Throughout his career, Mark has been on the front lines of innovation, leading product efforts in both start-up and large enterprise organizations. Mark holds a bachelor's degree in economics from the University of Pennsylvania.

Alex Attumalil, Deputy CISO, Leading Sportswear Manufacturer

Alex Attumalil is Deputy Chief Information Security Officer at a global apparel brand. He manages the strategic risk-based deployment of global security controls while enabling frictionless business operations. Alex has over twenty years of experience developing, managing, and maintaining information security programs and has taught as an adjunct professor, presented at cyber conferences, and serves as a technical consultant on various customer advisory boards.

Christopher Russell, CISO, tZERO Group

Christopher Russell is the Chief Information Security Officer for tZERO Group, a leader in blockchain technologies. He has a master's degree in cybersecurity and is the founder of h0neyb0t, a blockchain security research company. He is also a combat veteran of the US Army, where he was a human intelligence (HUMINT) collector and is a graduate of the Defense Language Institute, where he studied Arabic.

Troy Rydman, CISO and VP of Cybersecurity, Fast.co

Troy Rydman is a cybersecurity leader with demonstrated success in creating enterprise cyber programs in both the financial and fintech space and is a security advisor to the Utah food bank. He has created cybersecurity programs for Silicon Valley Bank, the largest bank in Silicon Valley, and Fast.co, a B2B leader in headless eCommerce checkout.

Chris Thompson, CISO, Leading Home Remodeling Company

Chris Thompson is a dynamic information security leader with more than 17 years of experience building security programs for global organizations. He has been responsible for the conception, design, implementation and operation of security strategies and has led IT governance initiatives, operational incident response teams, vulnerability management programs, risk assessments, and employee awareness programs.

Genady Vishnevetsky, CISO, Stewart Title

Genady Vishnevetsky is the Chief Information Security Officer for Stewart Title, a leading provider of real estate services, where he directs security, governance, and compliance programs for the global enterprise. An established leader with a track record in building successful security programs, he is an active member of the cybersecurity community, a security advocate, influencer, blogger, and frequent speaker at security conferences.

Bob Fabien "BZ" Zinga, Head of Information Security, Directly

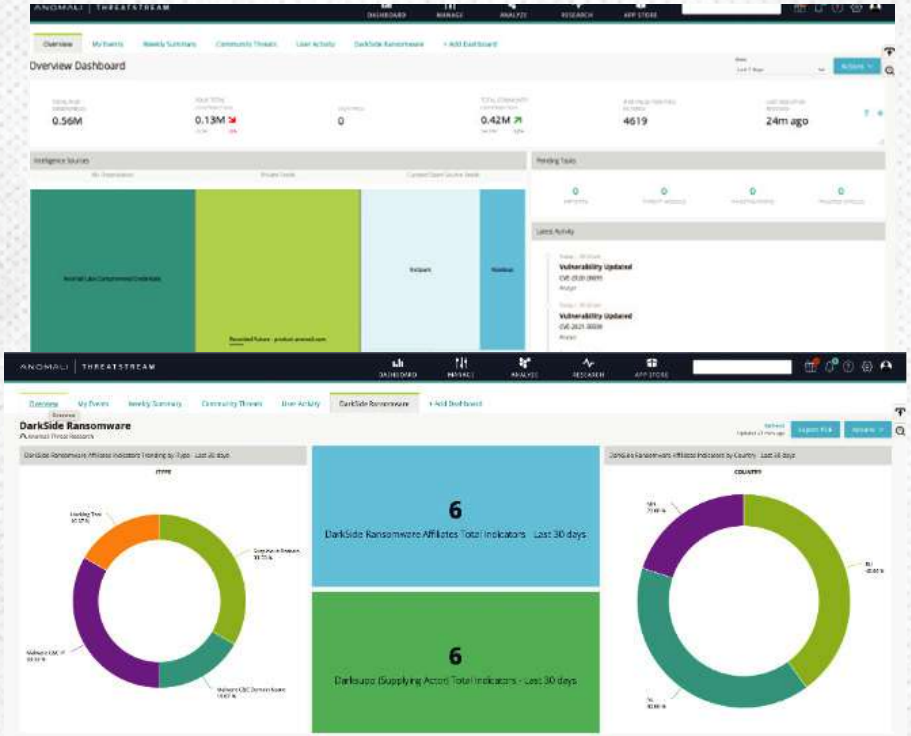
For over two decades, Bob Fabien "BZ" Zinga has worked in complex environments at the intersection of people, processes, and technology, successfully establishing globally recognized risk management and cybersecurity programs. BZ is the Head of Information Security at Directly, leading and managing a cross-functional annually audited Information Security Program. He is also an Information Warfare Commander and Commanding Officer in the US Navy Reserve.

ANOMALI

Anomali ThreatStream:

Actionable Intelligence Management

Anomali ThreatStream is a Threat Intelligence Management Solution that automates the collection and processing of raw data transforming it into actionable threat intelligence for security teams.



- Automate intel collection, curation, and enrichment
- Research, pivot on and investigate threats, TTPs, and actors
- 3rd party threat intel evaluation and procurement
- Automate distribution of intel to your security controls
- Secure threat sharing across trusted communities

LEARN MORE | WHAT IS THREAT INTEL? | THREATSTREAM INTERACTIVE TOUR | REQUEST A DEMO