The Need to Focus on the Adversary

Enhancing Your Security Defenses by Focusing on *Your* Adversaries

Mighty Guides

Sponsored by

ANOMALI

Table of Contents

Mighty Guides

Meet Our Experts

We interviewed information security experts on the frontlines of defending their companies from cyberattacks. Whether they work in higher education, technology, travel, or healthcare, these executives are united by the same goal—proactively detect attacks, predict an adversary's next steps, and shut them down.

We hope you enjoy their insights!

David Rogelberg
Publisher,
Mighty Guides Inc.
david@mightyguides.com
(516) 788-7886

Mighty Guides

Micah Czigan

CISO,
Georgetown University

Mark Eggleston

CISO,
CSC

Nick Jones

CISO,
TUI

Bradley J. Schaufenbuel

VP & CISO,
Paychex

Saeed Valian

CISO,
symplr

Aaron Weismann

CISO,
Main Line Health

Joe Ariganello

VP of Product Marketing,
Anomali

Introduction

The rapidly falling cost of processing power and storage has dramatically changed the face of information technology over the past decade, both for security teams and threat actors. Security information and event management (SIEM) technologies, which ingest log data from multiple sources, have long been our go-to means of correlating and alerting on events across applications. But SIEM solutions are limited to a reactive focus on a victim's devices, applications, or users.

Extended detection and response (XDR) moved us forward to actively match artifacts of threat intelligence against local security logs. Integrated with your security stack, XDR can automate actions—such as blocking an attacker's domain name in your Internet Provider Security tag or web content filter—and help to quickly determine how long a newly discovered attacker may have been in your network. Though, if computers can beat chess masters, it stands to reason that we can build systems to defeat the bad guys before checkmate.

Focusing on the adversary is a new approach to take with threat detection and response. Attackers favor specific tools and tactics, and, by casting a wide net, we can infer the avenues available to attackers depending on what is accessible to them and what kind of attack they are attempting. Next-generation platforms use advanced artificial intelligence and machine learning to not only proactively detect active attacks but also predict an adversary's next steps.

Foreword

By **Mark Alba**, Chief Product Officer, Anomali

Anomali is collaborating with MITRE Engenuity on the Attack Flow Project to better understand the adversary and help organizations get ahead of an attack. To help convey the importance of focusing on the adversary, I would like to share an analogy from the art world.

In a typical home burglary, often victims can tell you very little about what happened because the invasion happened in the dead of night. They may not have seen the burglar. They may not have even been home. Art thefts are a different story; much information is known about art thieves from closed-circuit TV security. In some cases, you can understand more about an art thief committing a successful art theft than you can from the ones that get caught in the act. For example, the clothing, tactics, and techniques of art thieves are hugely valuable to criminologists figuring out how to address and catch these criminals.

The first step for criminologists is to collect all known evidence—the intelligence from the specific burglary or publicly known information about the art theft and thief. Criminologists tokenize and normalize this evidence, removing extraneous information, and then tag and categorize it based on the type of threat. Next, they look for a modus operandi. Why did this thief do what they did? What were they attempting to do? What would they have done, had they been successful?

By identifying modi operandi for all the thefts they've investigated, criminologists can build a pattern of attack. The crime pattern can be used to both understand what happened in a particular attack and predict when the next attack will happen.

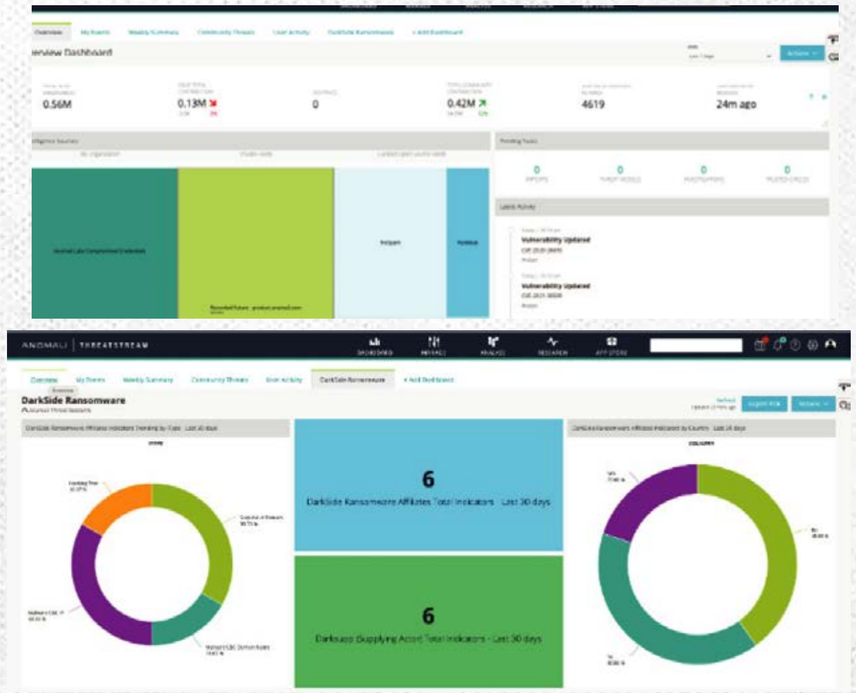
What we're doing is similar. In our case, we're using indicators of compromise (IOC) and behavioral detection as evidence to understand attackers and their patterns and behaviors and applying this understanding to anticipate subsequent attacks. Read on to learn more.

ANOMALI

Anomali ThreatStream:

Actionable Intelligence Management

Anomali ThreatStream is a Threat Intelligence Management Solution that automates the collection and processing of raw data and transforms 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

Chapter 1

THE NEED TO FOCUS ON THE ADVERSARY

Security teams today are essentially at the whim and mercy of threat actors. Cyber threat intelligence (CTI), security operations center (SOC), and incident response teams run in endless circles searching relentlessly among terabytes of data for the fingerprints of attackers' tools, tactics, and procedures (TTPs). These TTPs surface as specific atomic IOC—file names, IP addresses, domain names, and the like—which offer a myopic view into an attack, akin to fingerprints left behind as evidence but none of which tell the whole story.

Investigating without full and proper context and missing the bigger picture, defenders end up operating in a purely reactionary mode. They can only hope for enough time to find and thwart real damage after an alert.

If only teams weren't spread so thin and could spend as much time focusing on the attacker as on the attack itself, then they might be able to change the paradigm—shifting from reactive response to proactive defense.

From Your Local Area to Your Local Area Network

Consider your local neighborhood watch. Neighborhood watch is effective because its members innately know their friends from their foes, draw upon a baseline of prior experience in their area, and can

> ***One of my favorite Sun Tzu quotes from the Art of War is: 'If you know the enemy and yourself, you need not fear the result of a hundred battles.' Having an understanding of the potential threats and threat actors that could target an organization can help security teams become more proactive."***

Joe Ariganello

VP of Product Marketing, Anomali

Sophisticated modern attacks tend to be relatively novel, involving components that XDR may not otherwise surface without relevant intelligence, especially with attacks that creatively leverage legitimate tools or social engineering."

Aaron Weismann

CISO, Main Line Health

quickly detect anything out of the ordinary. Together, they know enough to anticipate where bad guys are most likely to strike and stop them before they start—a best-case scenario we can all aim for.

Information security is a bit more complex, but the same concepts ring true. We know our system architecture and the vulnerable bits existing along its attack surface. Our logs diligently record activity, allowing us to search and detect the acronym soup of threat actor IOC and TTPs. We have systems capable of learning the baseline of "normal" traffic and activity, allowing us to spot anomalies. If we can next learn the predictable patterns followed during different types of attacks, then we can begin to determine what's likely to happen next and take appropriate action to stop the attack. The more we understand this full picture, and the more we understand our attackers, the more likely we will know how and where to shift left and stop the attack before it starts.

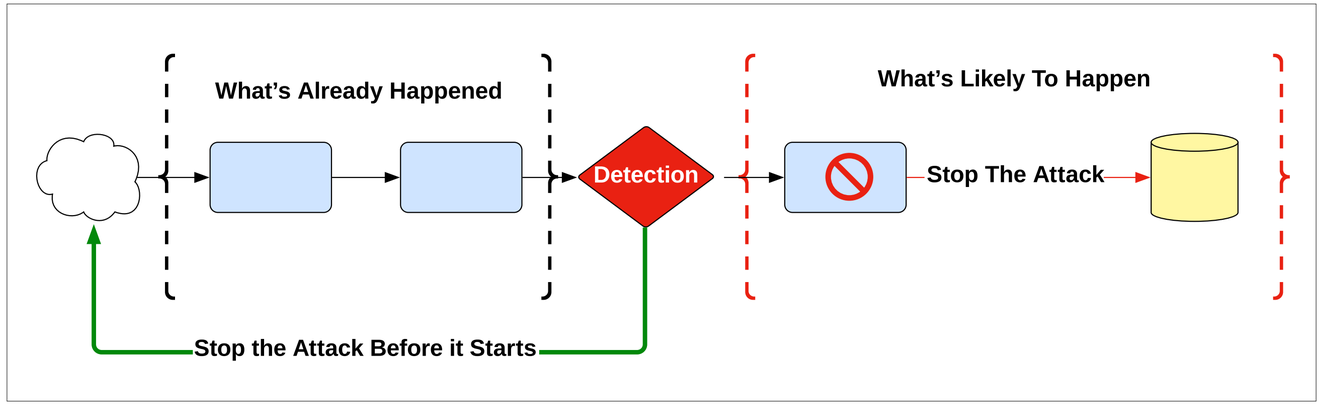


Figure 1: Using detection to stop the attacker or cut off the attack vector

Key Takeaway

The more we understand about our attackers—their preferred victims, tactics, techniques, and procedures—the more we can become proactive.

Chapter 2

TYPES OF ADVERSARIES

Threat actors today come in a variety of forms, from hacktivists, unscrupulous competitors, disgruntled insiders, and criminals to terrorists or entire nation states.

Researchers prescribe names like Fancy Bear or acronyms like APT28 as a means of cataloging the information maintained about each group of threat actors to help provide meaning and context. Attackers seldom focus solely on a single organization but rather shotgun their efforts across many locations and entities. As such, they often are identified by several names linking back to one group.

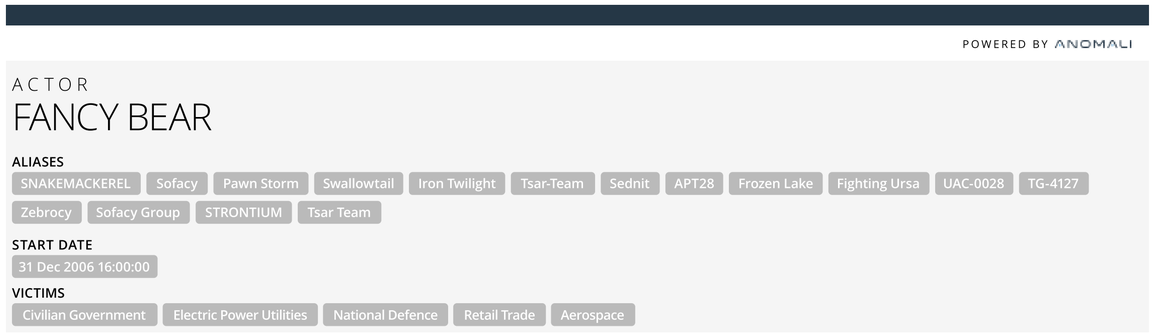


Figure 2: Fancy Bear Threat Actor Profile (Anomali ThreatStream)

> ***There are far too many threat actors and related TTPs to defend against every possible attack vector and scenario. By understanding their threat landscape, security teams can narrow down the likely set of threat actors to a more realistic and manageable list.”***

Micah Czigan

CISO, Georgetown University

> ***Many veterans in cybersecurity will acknowledge that 'new' attack types are not all that new, rather a variation or permutation of an earlier attack type."***

Mark Eggleston

CISO, CSC

Attacker Motivations

The differing motivations among threat actors are reflected in the victim verticals typically targeted by their various attack campaigns. Understanding these motivations can help narrow down the list of all potential attackers to only those who may be uniquely interested in your organization—a finite number that can help CTI and SOC teams focus their efforts. For example, a group interested in stealing financial data may target retail organizations or financial institutions.

Preferred TTPs

Inherently human, threat actors tend to reuse certain types of tactics and rely on specific tools over others. For instance, perhaps a threat actor leans toward PowerShell exploits and favors the Empire toolkit. Such preferences and their supporting details—the fingerprints of an attacker—are stored in comprehensive adversary profiles.

Specialist Threat Actors

These days, it's not uncommon for threat groups to collaborate, as many have become specialists, mostly focusing on certain attack phases or types. These attack-as-a-service offerings may include one group who specializes in Office 365 attacks and another who specializes in phishing exploits. Transactions to fill needs for an attack campaign can be found as services or purchases brokered in underground dark web marketplaces.

Adversary Intelligence

In years past, if you wanted to search for a specific threat actor in your network, then you would need to compile all of

> ***Cybersecurity professionals face various threats from multiple groups, including nation-states, organized crime, hacktivism, and human error. The threat landscape is evolving quickly, and security professionals must ensure they keep pace.”***

Joe Ariganello

VP of Product Marketing, Anomali

the known IPs, file hashes, and related information that the group has ever employed anywhere and build a complex and convoluted query to seek evidence. These queries are not only very difficult to construct and slow to run but also nearly impossible to maintain. Given the necessarily dynamic nature of the Internet, search parameters are virtually incomplete the moment they’re saved, as new data becomes associated with the actor.

With a modern threat intelligence platform or XDR solution, analysts can search for the same information but interface using human friendly names. For instance, a search for FIN7 returns the same atomic indicators but with additional context about the threat actor from all of their known names or acronyms. As these profiles are dynamically updated, searches and alerts don’t require continuous tuning and tweaking, accelerating investigation and mitigation.

Information about an attacker's history and preferences is invaluable in shining a light on what an actor may be expected to do—or has already done—in your network. As you refine the list of adversaries most likely to target your organization, you can use these details to help bolster defenses based on the realities of your unique threat landscape.

Generic attack detection becomes far more useful with attack attribution to a specific threat actor. The adversary profile informs where the group may pivot next, allowing incident responders to quickly stop the bleeding. The next important step is spotlighting where the attack may have been initiated or searching for other sections of your network that may have fallen prey along the way. Equipped with this knowledge, you can better understand where and how to mitigate future attacks.

> ***"Most cybersecurity measures have been reactions to existing threats with emphasis on known malicious threats and behaviors, allowing cyber criminals to stay one step ahead of cybersecurity professionals."***

Saeed Valian

CISO, symplr

Key Takeaway

Threat actors vary in their motivations, tools, and tactics. Learn which adversaries are most likely to threaten your organization and use that information to bolster defense and tune alerting.

Chapter 3

OVERCOMING SECURITY CHALLENGES

It would be nice to believe that we could associate a detection or alert as game over for adversaries, but often such association isn't possible—and not for lack of want.

Resource Constraints

Organizations routinely struggle with various resource constraints. A shortage of security talent has caused many SOCs and security teams to run lean and overburdened. The problem can be exacerbated by competing projects or priorities, as with the pandemic-driven boom in digital transformation and zero-trust solutions.

Tool Overload

Another critical factor for security teams is the avalanche of disparate tools that analysts must learn and maintain. Teams must sift through multiple data sources across dozens of distinct tools, often with little or no integration, chasing the data and weeding out false positives. Worse yet, each tool requires unique and specialized experience and training.

> ***"The security talent shortage makes it difficult for organizations to hire and retain experienced security professionals. A robust security technology stack is useless if an organization does not have trained professionals to maintain it and properly triage alerts."***

Bradley J. Schaufenbuel

VP & CISO, Paychex

Information Silos

Many of these tools produce such high volumes of data that they end up siloed with their own independent management interfaces for searches and reports. This isolation renders an elephant in the room: because most attacks leave a trail across multiple tools, analysts must manually correlate the data to reach conclusions and act.

Most importantly, by the time a detection rule triggers an analyst's understanding of the threat and actions that need to be taken, the damage may already be done.

> ***SOC or IR teams that aren't empowered, lack training, or can't easily find essential information because it's buried in disparate consoles, cannot be expected to react effectively."***

Aaron Weismann

CISO, Main Line Health

Key Takeaway

Organizations face a number of issues and constraints that can affect security posture and becoming more proactive.

Chapter 4

BECOMING PROACTIVE: PREDICT AND PREVENT

Struggling to surface relevant threats from the massive amount of security data they collect, security teams require better detection methodologies.

SIEM—Where We Started

The long-time stalwart in the security arsenal, SIEM represented an early attempt at moving the needle from reactive to proactive. One of cybersecurity's first true big data platforms, SIEM can ingest gigabytes or more of logged data per day into a searchable format. Security teams determine which use cases are priorities and write queries to correlate and search for those specific events among mountains of logs.

SIEM queries are saved and run either at scheduled times or in real time and then are used as alerts. Though a step in the right direction, SIEM remains constrained to the original query logic, somewhat akin to the way older antivirus products were limited by their signature files.

> ***"Security teams must prioritize which vulnerabilities to address and which attackers—and their associated attack techniques—to defend against. Prioritization is impossible without an adequate understanding of system exposure, which threat actors are anticipated, and what techniques these attackers utilize."***

Bradley J. Schaufenbuel

VP & CISO, Paychex

> ***Attack vectors into a company's network can allow an intruder to pivot in on multiple vulnerabilities, turning a bad scenario into something exponentially worse."***

Mark Eggleston

CISO, CSC

XDR—Where We Are

The next critical building block on the road to proactivity, XDR solutions ingest data from local security telemetry and correlate those events with global threat intelligence. These automated matches remove the query logic dependencies that bogged down traditional SIEM platforms.

An effective XDR solution can expedite the investigation process by integrating threat frameworks like MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). By visually mapping attack information against the MITRE ATT&CK framework, analysts can gain additional perspective by viewing patterns, especially in multiphased or multipronged attacks. In turn, analysts can begin predicting future actions in the attack cycle based on currently detected events, especially if sufficient evidence exists to attribute an attack to a specific threat actor and their expected TTPs.

Ideally, XDR should be able to trigger against both recent and old attacks. The capability to perform this kind of retrospective search answers the "Have we ever been affected?" question in a way that few other platforms can.

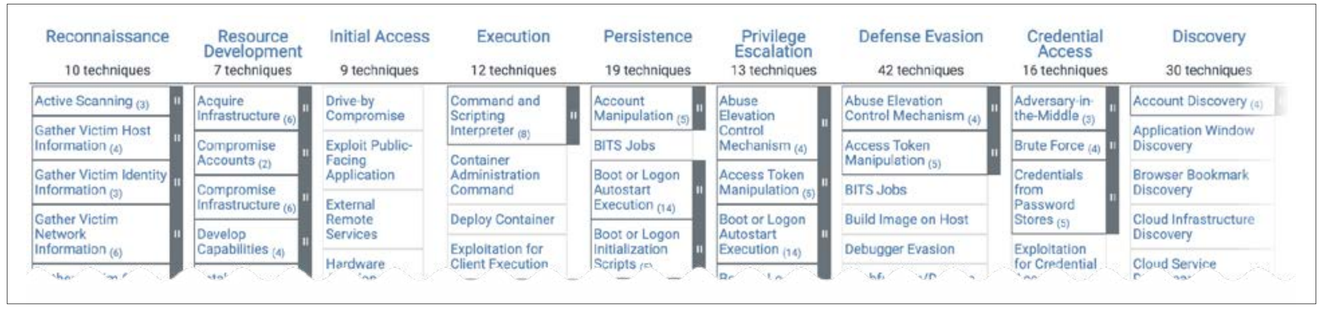


Figure 3: MITRE ATT&CK Framework (https://attack.mitre.org/matrices/enterprise)

This information is critical, as the latest threat or zero day makes waves through the media, with management kept actively informed about the risks (or lack thereof) to the organization.

Open-XDR can easily integrate with other tools in your security ecosystem to affect automatic actions. With this integration, analysts can react in real time, running automated courses of action such as sending commands to contain infected endpoints or block malicious domains at a web filter or firewall. It also enables you to uplevel your technology and your analysts to increase return on investment and efficiencies.

SIEM, SOAR, and XDR have all played a part in taking cybersecurity from reactive to proactive.

“Common impediments to security teams failing to respond quickly to detections: Multiple tools that do not integrate effectively into a SIEM or XDR, Talent Shortages of trained staff, and Team Overload as with one of the many digital transformation projects.”

Nick Jones

CISO, TUI

Today, threats evolve quickly. Organizations must shift from a reactive mode to a proactive mindset to keep pace."

Joe Ariganello

VP of Product Marketing, Anomali

> ***Security teams that architect for 'defense in depth' can employ a variety of controls, across all levels of system, architecture, or infrastructure to slow an attack or completely mitigate entire attack vectors."***

Mark Eggleston

CISO, CSC

Focus on the Adversary—Where We Need To Get To

We can use our full understanding of adversaries against them in a well-fed big data platform. Knowing which threat actors target your organization means you can prepare, prioritize, and improve your security posture before the advent of an attack. Knowledge about threat actor TTPs and IOC can allow us to quickly determine where an attack originated, predict where that attack can be expected to follow, and respond accordingly.

It's time to focus on the adversary and not just the acronyms!

Preparation: Bolster Defenses

After narrowing down the list of all threat actors to only those known to focus on your organization, you can begin to take some proactive steps. Browsing the list of preferred tactics for your threat actors provides clues about what infrastructure or services may be at risk within your network. The example threat actor tactics below rely on a Windows-centric infrastructure. Hardening PowerShell and the Windows command line could

Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	APT28 downloads and executes PowerShell scripts and performs PowerShell commands.[11][21][2]
		.003	Command and Scripting Interpreter: Windows Command Shell	An APT28 loader Trojan uses a cmd.exe and batch script to run its payload.[28] The group has also used macros to execute payloads.[18][30][17][21]

Figure 4: MITRE ATT&CK Tactic T1059 (https://attack.mitre.org/tactics/TA0002)

serve as a starting point for you to thwart these tactics, prioritizing your precious time.

Keep in mind that threat actors are constrained to the accessible attack surface of your unique threat landscape. Attacks are impossible without some form of access, such as a hole in the firewall or other backdoor entry point.

Threat Actor Tools

Associated attack tools are other critical bits of information that can be gleaned from an adversary profile. For many threat actors, this tool list may be pages long, but their descriptions can further inform how and where to prioritize your efforts. For example, the Koadic tool, associated with the threat actor Fancy Bear/ APT28, is a Windows-centric exploitation framework. The Koadic description shown below provides clues about where the tool may be used and associated IOC and data such as domain names, IP addresses, file names, and file hashes. These types of atomic indicators provide simple matches for detection by security systems.

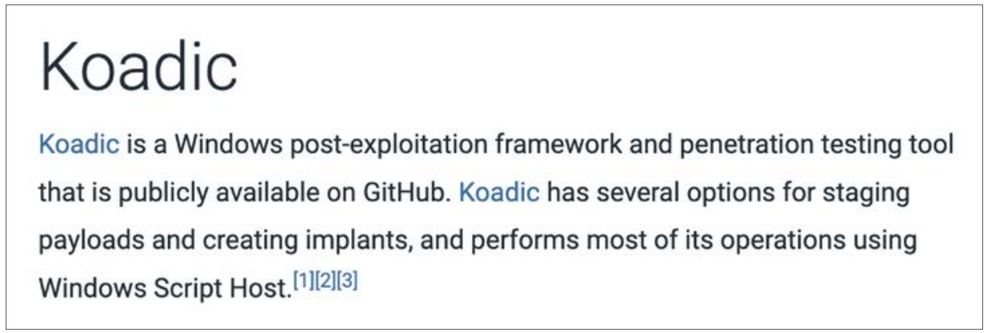


Figure 5: MITRE ATT&CK Tool Koadic (https://attack.mitre.org/software/S0250)

> ***Partnerships with security vendors and services providers that have a much broader view of the threat environment can help inform security teams about emerging threats.”***

Nick Jones

CISO, TUI

An organization with limited resources cannot do everything at once, so it must prioritize which vulnerabilities it addresses and which attackers and associated attack techniques it defends itself against."

Bradley J. Schaufenbuel

VP & CISO, Paychex

Introducing Attack Flows

The tactics threat actors employ occur in roughly repeatable sequences of actions—X happens before Y and Z—against certain types of assets that, in turn, require specific tools. For example, an attacker may need to run an exploit to elevate privileges before being able to exfiltrate data. Considering that the underlying environment defines which tools can be used, it's relatively simple to extrapolate how a library of many known attack flows could prove invaluable for analysts.

By truly understanding your adversary and threat landscape, you can not only detect an attack but also have enough information to predict next steps and hopefully force your adversary to pack up their toys and go play elsewhere.

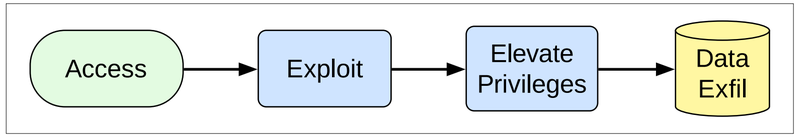


Figure 6: Basic Attack Flow Diagram

Key Takeaway

SIEM and XDR were steps in the right direction but truly understanding our adversaries is the key to responding quicker and stopping attacks before they can start.

Chapter 5

THE ROLE OF THREAT INTELLIGENCE

While it is the fundamental lifeblood of most modern security platforms, threat intelligence is only as good as the information that feeds it. This information can vary wildly, from highly curated paid feeds to open-source lists, with the latter questionably accurate at times. Feeds can be imported directly into security tools or, better still, moderated through a threat intelligence management platform.

Threat Intelligence Management

A good threat intelligence management platform automates the collection and processing of raw data into actionable threat intelligence for security teams. Such a platform integrates automation and machine learning to ingest multiple feeds from a variety of sources, deduplicate and normalize the data, and provide a searchable interface to present highly contextualized information. Reports for threat actors should include full adversary profiles with a description of their motivation; information about their historical campaigns; and their preferred targets, preferred tactics, and known tools—with an ability to drill down deeper for more granular details.

Threat intelligence enhances detection capabilities and informs security professionals of potential cyber risks

> ***"Active attacks can easily get buried in a sea of alerts, especially false positives. Security teams can easily get overwhelmed with data to the point where they miss 'the' relevant alert."***

Bradley J. Schaufenbuel

VP & CISO, Paychex

A strong, proactive approach using threat intelligence as the foundation will enable a cybersecurity team to focus on threats that matter most, gaining relevant context, implications, and remediation recommendations."

Joe Ariganello

VP of Product Marketing, Anomali

through real-time information to help them better answer several questions:

- Who are my adversaries, and how could they attack me?
- What are the attack vectors affecting the security of my business?
- What should my security teams be looking out for?
- How can I reduce my company's risk of a cyberattack?

Threat Intelligence Feeds

Special attention should be paid to which feeds to use in your systems. Free sources, such as IOC lists from a single tool or the known IP addresses of spammers, can be limited. Some specialty feeds, such as those monitoring for traces of your confidential data (e.g., personally identifiable information, credit card numbers), are available for sale in underground dark web forums.

Many organizations will choose to either subscribe to multiple feeds or purchase a complete and highly curated feed. Each feed is valuable for gathering information regarding adversaries and their capabilities and infrastructure. Finding the right feeds to defend your infrastructure and empower your analysts is important. At the end of the day, you need enough information to paint an accurate portrait of your adversaries.

Sharing Threat Intelligence

Adversaries seldom focus their efforts only on a single entity. Rather, they attack multiple organizations and may leverage a diverse set of tactics and tools, especially when they are confronted with specific systems or infrastructure. This holistic information can be collected and shared.

The better paid threat intelligence feeds include information from their own researchers and sanitized detection information from their global customer base, creating a sort of shared defender community. A good threat intelligence management platform should also be collecting data and surfacing relevant intel with the community.

As cyber threats become more sophisticated, the need to communicate and collaborate effectively has never been more critical. Sharing threat intelligence is an effective way to increase the breadth and depth of your threat intelligence and empower your security team.

Information Sharing and Analysis Centers

Information sharing and analysis centers are other good sources for threat intelligence. These entities collect and share cyber threat intelligence across groups of similar members: regional, governmental (e.g., critical infrastructure), or industry verticals (e.g., financial institutions, retail, and hospitality).

Encouraging and supporting information sharing within and across industries is a vital component for security programs worldwide. Making threat information discoverable and accessible using the appropriate medium within a timely and secure manner will help minimize the effectiveness and thus impact of cyberattacks for all organizations.

STIX/TAXII

Structured Threat Information eXpression (STIX) is the standardized language and serialization format used to exchange cyber threat intelligence, as through threat intelligence feeds. STIX provides a common schema/protocol for the automated sharing of threat intelligence between machine systems and is commonly found in conjunction with its communication protocol, Trusted Automated eXchange of Intelligence Information (TAXII).

Your Adversaries Share, Too

Adversaries are also known to share their “intelligence,” selling information gleaned about potential targets and from

> ***Information sharing is vital in order for security teams to keep pace with threat actors. Industry collaboration is vital to help protect similar organizations. Collaboration across verticals can help smaller or less advanced organizations protect themselves.”***

Nick Jones

CISO, TUI

> ***SOC analysts too often are missing the right telemetry to allow them to confirm that something suspicious may indeed be malicious.”***

Mark Eggleston

CISO, CSC

prior attacks or campaigns. Such sharing occurs most often on dark web forums, where specialist actors may sell their specialty data—say, an account checker selling lists of live accounts and usernames/passwords, or an actor selling sensitive personal identifiable information. This virtual ecosystem allows unrelated threat actors to purchase and use information as a virtual continuation of their original attack to complete account takeovers or commit fraud, for example.

Key Takeaway

Information is only as good as how it's actionable. Choose the right intelligence solutions to ensure threat data is operationalized to enable informed decision making.

Chapter 6

ATTACK FLOWS, IN DEPTH

We can utilize libraries of attack flow models to produce detections that reference patterns of attacks, visually mapping them to the current stage. Detections can further include the broader contextualization of threat severity, asset criticality, and attack surface vulnerability—bootstrapping security teams. To understand, let's build out an example attack flow.

Tactics, Assets, Properties

Tactics are what the attacker does, also known as the tried-and-true MITRE ATT&CK Tactics. *Assets* are the nouns in an attack sequence, from network edge to loot: servers, Kubernetes clusters, administrative credentials, your data, and so on. *Properties* describe what can be done with a given asset and can span from full-blown

"Visualizations can help teams to more quickly see where there are intersecting areas of the environment and focus their efforts on either remediation or forensic investigation."

Micah Czigan

CISO, Georgetown University

> ***Attack flow or process-based recognition can address the inherent drawbacks of strictly IOC-based detections.”***

Aaron Weismann

CISO, Main Line Health

code execution to simple read-only permissions. The latter may sound innocuous, but a seemingly low-risk property like a read-only permission may be all an attacker needs to exfiltrate your data.

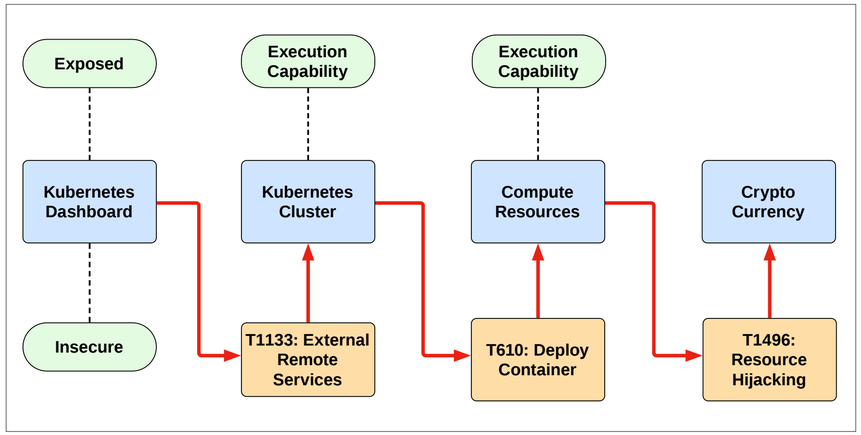


Figure 7: Attack Flow Relationships

Relationships

At the core of attack flows are the relationships between tactics, assets, and assets’ properties. In a successful attack, an adversary performs specific sequences of actions against your systems to reach their final action or objectives. The tactics in their toolbox are constrained by the properties of an asset; perhaps the asset allows execution capability, or maybe it is limited to read access. And many tactics are functional only against specific types or classes of assets. For example, some tactics may only execute on a Windows server or on a specific version of Apache. Further, some tactics may provide access to additional assets like an underlying console or administrative credentials.

Properties

Each phase of the attack pattern illustrated above is available due to the properties of assets. An *exposed* and *insecure* Kubernetes dashboard is available on the Internet. The dashboard leaves a Kubernetes cluster with *execution capability* vulnerable to MITRE ATT&CK Technique 1133: External Remote Services. Once in the cluster, the adversary deploys

a malicious cryptojacking container to hijack compute resources, ultimately cashing out on your dime.

Break the Flow, Predict the Flow

If we alerted at a specific point in the attack, we can then easily predict what may happen next. In detecting unusual events at the Kubernetes dashboard shown below, the path leads to the cluster, so we know where to investigate to stop the attack or, better yet, automate some mitigation action.

We can become proactive by using the same information in advance to shore up defenses and take entire attacks off the table. Moving the Kubernetes dashboard to a firewalled network removes it from the Internet and stops most of the attack above before it can start. Introducing proper role-based access control on the Kubernetes cluster restricts execution capability and can head off the container deployment.

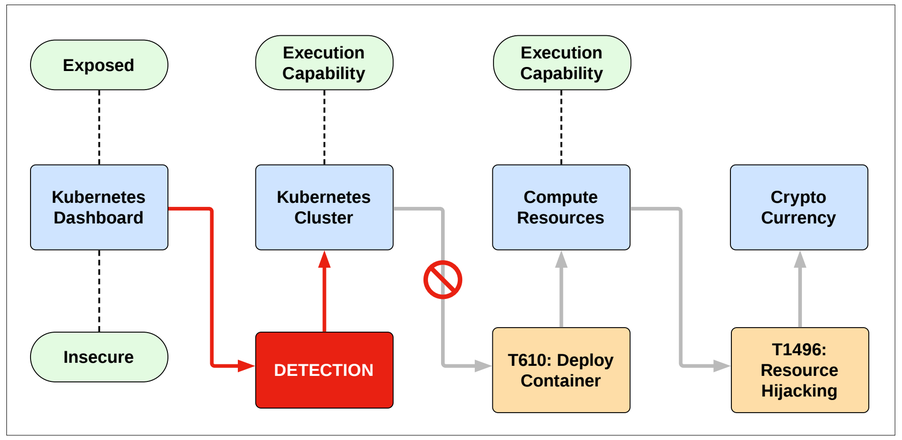


Figure 8: Using Attack Flow to stop an attack after detection

> ***A key to effective security is through continuous correlation with a balanced multi-layered approach constructed of different pillars including threat intelligence, contextualized data visibility, and human-led Artificial Intelligence/Machine Learning controls and automation.”***

Saeed Valian

CISO, symplr

> ***It's important to understand the full scope of your threat landscape so that teams can apply consistent policies to all parts of the enterprise. Leaving a single hole unprotected can prove an easy target for threat actors—and one that might go unnoticed."***

Micah Czigan

CISO, Georgetown University

Keep in mind that attack flows are not limited to a single potential conclusion. Discerning all available objectives can better inform your defense. Perhaps a path to coin mining presents a potential loss of thousands of dollars, whereas another path to data exfiltration could bankrupt an organization. By understanding all possible scenarios, decision makers can decide where best to utilize precious resources.

Adversary Detection and Response

Adversary detection and response is the final evolution in our path to proactivity breaking away from detections solely based on the IOC from TTPs. A sophisticated artificial intelligence engine takes in the full scope of adversary intelligence—which threat actors are targeting your organization and what their preferred tools and tactics are. Such an engine can detect active attacks and spiked deviations from baseline norms. We can ultimately predict future events based on attack flows and contextualize alerts with threat severity, asset criticality, and attack surface vulnerability.

Billions of potential threats are distilled into prioritized incidents and their component risk.

Break the spiral of threat hunting, alert creation, monitoring, and incident response. Stay a step ahead of your adversaries, pushing the limits of what we consider the state of the art, the state of the practice.

Key Takeaway

Use the new concept of Attack Flow Diagrams to empower security teams. Predict where attacks are most likely to occur and expedite mitigation during incident response.

Focusing on the Adversary with Anomali

In 2021, Anomali joined MITRE Engenuity's Center for Threat-Informed Defense to collaborate on the Attack Flow Project to better understand adversary behavior and improve defensive capabilities. This partnership culminated with the public release of the project in March 2022.

The Attack Flow Project will provide context around adversary behavior and help security teams expertly profile the adversary. The project will also enable teams to more effectively protect their organization before an attack, detect attacks in real time, and respond post-attack.

At the foundation of Anomali's detection and response capabilities is intelligence. We have the largest global repository of intelligence, which includes tactical indicators that we leverage as part of our detection and strategic intelligence.

This strategic intelligence enables us to provide context and visualization around adversary behavior to automate processes for cyber threat intelligence and SOC analysts. These processes include moving from a series of indicators toward indicators enriched with intelligence to identify the attacker, attack, and attack pattern.

This visualization not only gives an executive a view into what this means to an organization but also provides the practitioner with a simple way to see the progression of an attack. Analysts can move from a progression of an attack to "I need to dig into this specific asset and determine its criticality."

By partnering with MITRE Engenuity on projects like Attack Flow, Anomali seeks to shift toward predictive intelligence—leveraging cyber threat intelligence from successfully modeling and describing the attacks we've seen to understanding the attacks we're likely to see next.

This predictive capability allows defenders to become more proactive in their actions and more effective in allocating their budgets and determining where to spend their time working to improve security capabilities in their organizations.

Reach out to learn more.

Learn More About Our Experts

Micah Czigan

CISO,
Georgetown University

Micah Czigan has been Chief Information Security Officer at Georgetown University since 2020, where he focuses on ensuring the security and privacy of the Georgetown community and protecting the University's critical data as a Certified Information Systems Security Professional. Prior to this role, Micah worked for several private companies and federal agencies, including Symantec, the U.S. Department of Energy, and Washington Headquarters Services.

Mark Eggleston

CISO,
CSC

Mark Eggleston is responsible for CSC's global security and privacy program design, operations, and continual maturation. As a senior executive specializing in security and privacy program development and management, Mark's unique background and expertise in information technology, program, and people management have positioned him as a thought leader and frequent industry speaker. Mark holds CHPS, CHPS, and CISSP certifications.

Nick Jones

CISO,
TUI

Nick Jones is the Chief Information Security Officer at TUI, where he builds core security capability pillars and implements programs to reduce the likelihood of a major security breach. He was recognized as one of the top 100 global CISOs in 2022 and is a regular speaker at industry events. Nick is passionate about protecting global organizations and their staff and customers from cyberattacks.

Bradley J. Schaufenbuel

VP & CISO, Paychex

Bradley J. Schaufenbuel is Vice President and Chief Information Security Officer at Paychex. He has held security leadership positions at Paylocity, Midland States Bank, Midwest Bank, Zurich Financial Services, Experian, and Arthur Andersen LLP. Bradley holds twenty-five professional designations in many areas of information security and technology and was recognized as the North America Information Security Leader of the Year by GDS in 2021.

Learn More About Our Experts

Saeed Valian

CISO,
symplr

Saeed Valian is an award-winning information security and technology leader who proactively confronts and resolves technology, risk, and business challenges. Recognized as one of “10 Best CISOs of 2021” by Industry Era, as well as one of “The 10 Most Influential CISOs to Watch in 2021,” Saeed’s strategic and technical experiences have made him a thought leader in the security industry.

Aaron Weismann

CISO,
Main Line Health

Aaron Weismann is an experienced leader and technologist with more than a decade of strategic management, technology, and information security experience. He currently serves as the CISO of Main Line Health, where he implements programs and strategies to advance security operations and put patient safety first. Aaron is especially adept at translating highly technical security, technology, and governance concepts into communications for all organizational levels.

Joe Ariganello

VP of Product
Marketing, Anomali

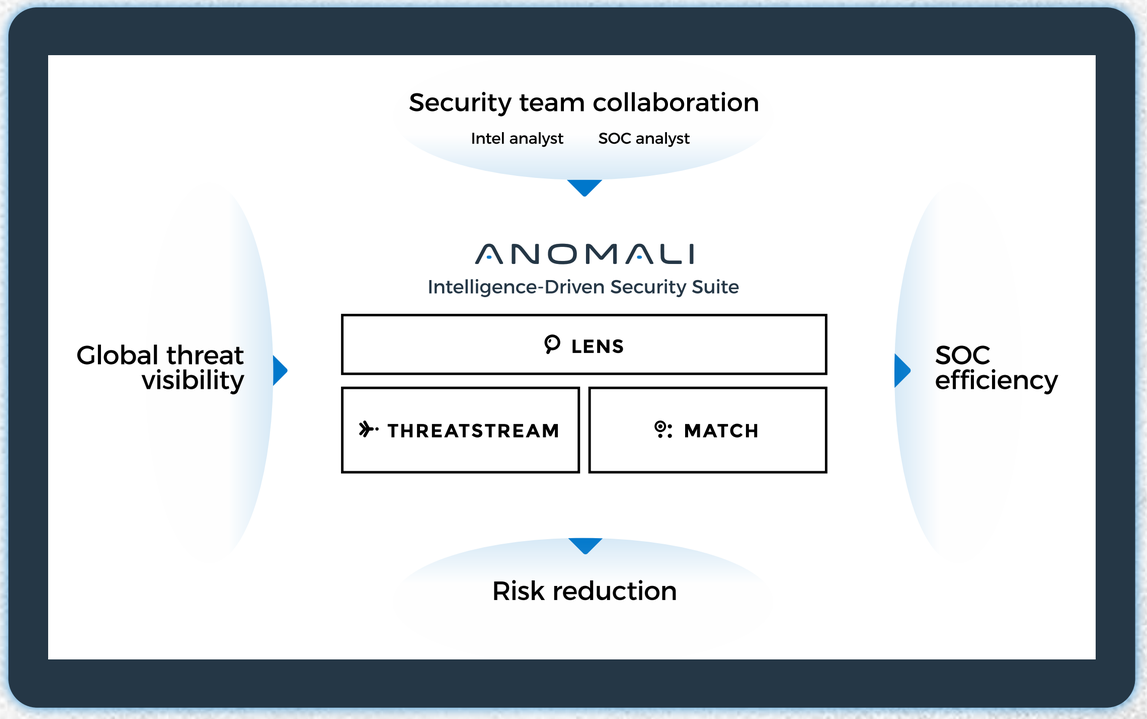
Joe Ariganello is the VP of Product Marketing at Anomali, with over 20 years of experience in global security, wireless, telecom, mobile applications, and the cable industry. Joe has helped Anomali transform from a threat intelligence platform provider into the XDR space, developing a new messaging framework and key content mapped to the buyer’s journey to inform prospects and customers and position Anomali as a leader.

ANOMALI

The Anomali® Platform

The Anomali Platform is a cloud native adversary detection and response platform that integrates with your 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