Mighty Guides

Sponsored by

ANOMALI

7 Experts on Cyber Fusion

Collaborative Security to Defend the Modern Threat Landscape

Table of Contents

Introduction	3
Foreword	4
Chapter One: What Is Cyber Fusion?	7
Chapter Two: The Challenges of Modern Cybersecurity	12
Chapter Three: Where Cybersecurity Is Falling Short	15
Chapter Four: The Role of Threat Intelligence	19
Chapter Five: Best Practices in Achieving Cyber Fusion	24
Learn More About Our Experts	29

Introduction

The modern attack landscape of relentless, patient, well-funded threat actors illustrates the need to adapt our organizations accordingly. Few organizations would say that they have been resting on their laurels. Network operations centers have been monitoring uptime for decades—an essential task focused primarily on availability rather than security. Ad hoc computer emergency response teams or cybersecurity incident response teams combatting the emergency of the moment were another milestone. Still, they are reactive, with the collective wisdom lost as members disband and return to their representative departments. Information sharing and analysis centers (ISACs), industry groups, and other threat intelligence-sharing communities facilitate collaboration and information sharing but are external by their very nature.

The situation calls for a new approach that merges historically successful best practices from each security team into a cohesive new entity: a cyber fusion center. In a cyber fusion center, people, processes, and purpose act in unison to achieve a common goal, underpinned by threat intelligence at every touchpoint.

This ebook introduces cyber fusion as the inflection point for siloed cyber threat intelligence (CTI), security operations center (SOC), and incident response (IR) teams, fusing security operations under a single umbrella. It describes cyber fusion challenges and opportunities and, with special insight from industry experts, describes implementation best practices.

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

Global organizations must balance a rapidly evolving cyber security threat landscape against business requirements more than ever. Digital transformation has quickly expanded their attack surface. At the same time, security teams face talent shortages across the board, leaving them to do more with less, burdened with resource-intensive false positives and non-stop cyberattacks.

Enter cyber fusion.

Cyber fusion takes a proactive approach to cybersecurity that helps organizations break down barriers and open communications across their entire organization and helps them identify and address cyber risks before they become an issue.

By developing a cyber fusion framework, or a cyber fusion center, organizations can bridge the gap between critical functions to facilitate collaboration, communication, and operational effectiveness, reduce risks, and improve response to threats.

Cyber fusion empowers collaboration between key stakeholders and is a vehicle to provide input and constant communicate cross-functionally. This enables the security team to understand the makeup of their infrastructure, identify key vulnerabilities, and prioritize requirements.

Cyber fusion provides a more effective, holistic approach to cybersecurity by combining technology, intelligence, and human expertise to ensure organizational alignment with everyone‘s primary goal in mind – to stop attacks and respond to breaches before they disrupt normal business operations.

Regards,
Mark Alba
Chief Product Officer,
Anomali

ANOMALI

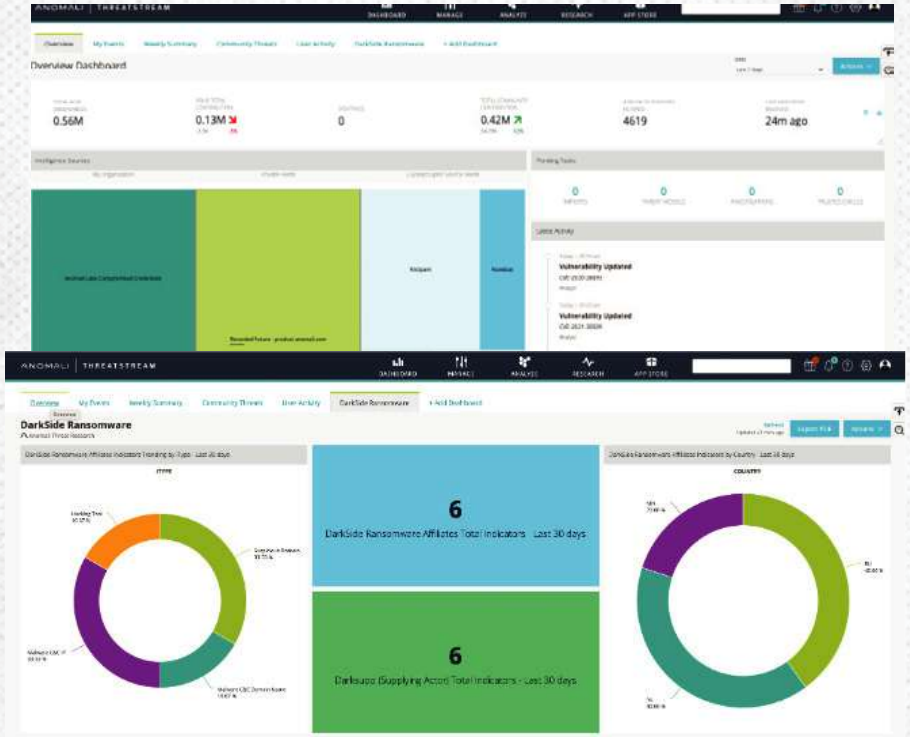
Anomali is the leader in intelligence-driven extended detection and response (XDR) cybersecurity solutions. Anchored by big data management and refined by artificial intelligence, the Anomali XDR platform delivers proprietary capabilities that correlate the largest repository of global intelligence with telemetry from customer-deployed security solutions, empowering security operations teams to detect threats with precision, optimize response, achieve resiliency, and stop attackers and breaches. Our SaaS-based solutions easily integrate into existing security tech stacks through native cloud, multi-cloud, on-premises, and hybrid deployments. Founded in 2013, Anomali serves public and private sector organizations, ISACs, MSSPs, and Global 1000 customers around the world in every major industry. Leading venture firms including General Catalyst, Google Ventures, and IVP back Anomali. Learn more at **www.anomali.com**.

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

Meet Our Experts

Mark Alba
Chief Product Officer,
Anomali

Brian Yau
Director of Cyber Fusion Center,
Crypto.com

Joe Corsi
Deputy CISO,
Excellus BCBS

Kevin McLaughlin
VP, Global Security, Risk &
Compliance, Stryker

Genady Vishnevetsky
CISO,
Stewart Title

Michael Tayo
Cloud Security Engineer,
Tempus Labs, Inc.

Michal Merta
Cyber Fusion Center Lead,
Accenture

Chapter One

What Is Cyber Fusion?

Cyber fusion is characterized by a unification of traditional security activities with common business functions—CTI, automation and orchestration, IR, threat hunting, and SOC monitoring—in addition to those departments typically affected by cyberattacks, such as human resources and finance. Cyber fusion enables organizations to function as a single agile, cohesive team with shared vision, tools, cultures, and processes so that they can proactively defend against the ever-changing landscape of modern cybersecurity.

In the cybersecurity organization, each group advises the next to collaboratively identify specific threats and threat actors, analyze them, and mitigate attacks in real-time. The organization anticipates future events and acts decisively by detecting not only simple indicators of compromise (IOCs) but indicators of attack as well as adversarial tactics, techniques, and procedures (TTPs). At each touchpoint in the chain, integrated feedback loops form a cycle of continuous improvement. Organizational stakeholders supply the critical function of top-down support and strategic intelligence, crucial for shared direction and informed tactical decision-making.

Connectivity through Technology

Cyber fusion lives comfortably at the cutting edge of cybersecurity, a system of technological integrations that use threat intelligence to coordinate all sources of intelligence. Extended detection and response is typically a core component of the concept, with data collected from across installed security telemetry and correlated with intelligence, speeding response times and freeing analysts to refocus their efforts on proactivity. Cyber fusion promotes technical integrations across vendors and solutions in a given security stack, supporting automated response actions or playbooks.

"Cyber fusion is an amalgamation of many core teams which may include Threat Intelligence, Security Operations Center, Security Engineering, Incident Response, Vulnerability Management, and others based on the dependencies and variables unique to each organization."

Brian Yau

Director of Cyber Fusion Center, Crypto.com

Initial raw data are translated into meaningful categories of actors, events, and attributes, shaping actionable insights from an array of external paid or open source feeds. A machine learning engine powers the analysis of local security telemetry and global threat intelligence to produce high-fidelity alerts anchored in adversarial TTPs and simpler matches against IOCs.

Cost Savings

Faster response times and more effective use of existing resources are a force multiplier in reducing security costs. With threat intelligence integrated across systems, enriching alerts and reports with additional context, analysts can more quickly draw conclusions and determine their next steps. Alerts are often visually mapped against one or more of the major threat frameworks, such as the MITRE ATT&CK Framework, to aid in deciphering and illustrating patterns among the many events and log sources. With teams working collaboratively, budgets and tooling can be pooled to simplify architecture, training requirements, and licensing economies of scale.

What Is a Cyber Fusion Center?

Cyber fusion centers are the evolutionary embodiment of traditional security specialties and processes, such as CTI, SOCs, and IR, operationalized to function as a single entity. CTI monitors the threat landscape and initiates research and analysis from observations as well as priority intelligence requirement requests, providing analysis of a specific topic in support of stakeholder decision-making. This intelligence may be tactical in nature, as with the unearthing or attributing of new TTPs; it may be operational, aimed at planning and conducting defensive operations; or it can be strategic, used to formulate high-level security planning and direction.

"Leveraging artificial intelligence and machine learning, teams can quickly analyze threat data from high quality alerts and distribute that relevant intelligence easily to all stakeholders."

Kevin McLaughlin

VP, Global Security, Risk & Compliance, Stryker

The CTI team analyzes collected and processed data; evaluates real and potential threats; and disseminates knowledge about adversaries and their motivations, intentions, and methods—but with latitude to pivot on findings and follow attack patterns where they lead. The result is disseminated as threat bulletins (sometimes called situational awareness reports) to internal stakeholders and shared with the ISAC, where appropriate.

SOC team members monitor systems and logs 24/7 for the tell-tale signs of malicious activity using IOCs and evidence of the many threat actor TTPs, sourced from CTI team threat bulletins or security solution providers. Findings are prioritized based on an understanding of attacker motives, targets, objectives, internal vulnerabilities, and business risk.

> **Effective cyber fusion coordinates efforts across security teams, including SOC, IT, physical security, fraud, etc., and integrates automation to collect and curate data from internal and external sources and provide actionable intelligence to stakeholders to make informed decisions.**

Mark Alba
Chief Product Officer, Anomali

With a warm hand-off from the SOC, the IR team contains and eradicates threats by using preplanned courses of action, often termed playbooks or runbooks. Time is of the essence, so there is a strong reliance on easily repeatable tasks and automation.

Throughout all facets of the operation, feedback loops exist for continuous process improvement. Each team informs the other about ways to increase efficacy, cast wider nets, or take deeper dives.

"Communication is key to help break down silos across an organization to ensure that everyone is aligned and contributing to the shared goal of keeping the organization safe."

Michael Tayo
Cloud Security Engineer,
Tempus Labs, Inc.

Cyber Fusion—Partners

The cyber fusion process often works with and incorporates other teams into the fold. Physical security badge access logs can determine whether an employee was legitimately on-site at a given time. Accounting and fraud can inform business risk, especially when combined with asset inventory and vulnerability management systems. A spike in application errors could just as easily point to an active attack as to publication of malicious code. Both are examples of how correlating otherwise-unrelated events can alter the risk to the organization.

Because of their ability to simulate real-world exploitable attacks, often colored through the lens of the CTI team, red teams can be especially valuable partners. If an attack was not detected, the SOC can coordinate to adjust alerting. If the attack was successful, security engineers or DevOps can layer on additional defenses.

Cyber Fusion—Management

All the while, senior management keeps business stakeholders informed with key metrics and reporting that drive future project and activity prioritization. They also document the growing team's collective knowledge.

"Threat intelligence management is a critical piece in streamlining processes and automation, enabling teams to proactively analyze and act upon relevant intelligence to defend their environment—especially in the changing geopolitical landscape."

Kevin McLaughlin

VP, Global Security, Risk & Compliance, Stryker

Key Takeaway

Cyber fusion functions as a single team with shared vision, tools, cultures, and processes to defend the changing landscape of cyber security.

"With the adoption of new technologies and as attacks have grown in sophistication, security teams and stakeholders should work together closely to adapt to the ever-changing threat landscape."

Brian Yau
Director of Cyber Fusion Center,
Crypto.com

Chapter Two

The Challenges of Modern Cybersecurity

The Modern Threat Environment

Today's threat environment is sophisticated and disruptive, as shown in the rising year-over-year trend of ransomware cybercrime as a service or the myriad attacks attributed to nation-state–sponsored threat actors. Not all attacks are hacks in the traditional sense of the word, though: Some require us to reconsider existing processes and overcome blind spots.

Your fraud team may be aware of sensitive information buried in dark web forums but lack a mechanism to trigger other teams to investigate the root cause of how those data were originally exfiltrated or compromised. Evidence of bot attacks might be buried in DevOps application logs as "valid" web traffic but can present a risk as costly or more than an internal breach.

Team Overload

Cyber fusion requires experience, knowledge, and tradecraft, which in turn require human decisions. The IT industry, however, faces a skills gap that can make it difficult to fill such specialized positions. Retention is important, yet with approximately 10,000 new software vulnerabilities discovered every year, analysts can begin to feel as though they are drowning in data with no clear insight into what is valuable and actionable and what should be prioritized. If everything is an emergency, then nothing is an emergency, as the saying goes. This confusion can cause good analysts simply to burn out.

An examination of the tools and services that drive many modern enterprises reveals several similarities. Great tools can improve productivity, but more disparate tools do not necessarily

"Traditional teams need to adapt to the latest techniques and trends with technology that minimizes the probability of human errors and helps identify potential cases for automation. These tools will improve detection capabilities and ensure teams have the intelligence they need at the right times."

Michal Merta
CISO,Cyber Fusion Center Lead,
Accenture

equate to increased efficiency. Rather, an increase in the number and variety of tools may force analysts to specialize in fewer tools, which naturally inhibits their ability to see the bigger picture and connect the dots across platforms. The number of deployed tools and platforms can make it difficult for analysts to use them all to their greatest potential, creating siloed environments or specialist roles where there is more need for generalists.

> **While organizational processes are the basis for creating an effective cyber fusion center, automation tools are also essential. The risks of not automating can include missed threats, dormant threats, siloed threat intel, and unaligned intel.**

Mark Alba
Chief Product Officer, Anomali

Budgetary Effects

Given a shared stake in monitoring key performance indicators (KPIs), it is reasonable to believe that SOC, Network Operations Center, and DevOps teams may unknowingly have purchased monitoring platforms with substantially overlapping feature sets. Collaboration, information sharing, and IR are hindered if groups monitor their own fiefdoms, each with competing priorities, budgets, and redundant tools or processes. Less can be more when implemented well.

"Threat intelligence should enrich analyst views in existing tools. To be most effective, security teams must operate in a single pane of glass."

Genady Vishnevetsky
CISO,
Stewart Title

Key Takeaway

Overloaded security teams lack the time and resources to properly collaborate, both internally and between external departments, resulting in inefficiencies.

"Threat data collected from security incidents and enriched with threat intelligence helps analysts quickly understand the threat to not waste any time and take immediate action."

Brian Yau
Director of Cyber Fusion Center,
Crypto.com

Chapter Three

Where Cybersecurity Is Falling Short

Not maximizing resources effectively is a common denominator in poorly performing teams. Siloed teams function more or less independently, with separate and potentially competing management, priorities, and budgets. The problem can be exacerbated with teams external to security. Mark Twain said that "continuous improvement is better than delayed perfection," a prescient observation for teams that lack feedback loops or coordination.

Opportunity: Inefficient Operations

CTI teams may find themselves answering the wrong questions if information requirements are ill-defined, effectively burning hours tracking lower-risk or minimal-impact threats. In contrast, the same group can produce too much information, creating a virtual fog of more. Without feedback, the problem can repeat itself unabated, with threat bulletins shared with already-overloaded SOC and IR teams.

SOC teams can feel pummeled by alerts, reducing their availability to tune out white noise or false positives, which compounds and perpetuates the problem. Over time, these teams can end up simply spotting a problem and telling someone, with no committed follow-through to determine whether the root cause was remediated and alerts should be modified.

IR teams can find themselves fighting an endless cycle of recurrence, repeatedly battling the same ingress vectors, attack types, and threat actors. Missing the bigger issues, they might mitigate the requested incident but disregard the root cause in the name of expediency. A focus on the attack but not the attacker can leave the threat alive on the network, readily returning to cause more mayhem.

"Close cooperation between teams is crucial. Offensive security teams can provide technical details about ongoing campaigns, and blue teams can include newly developed techniques into their response plans. Intelligence Analysts should continuously issue targeted reports to all relevant stakeholders that inform and help guide to resolution."

Michal Merta
Cyber Fusion Center Lead,
Accenture

Opportunity: Team Workload

In the same vein, institutional muscle memory can develop over time for common attacks from known groups, but any threat actor can jump to a new vertical at any time. Deep Panda, a group that was well known for attacking defense and financial institutions, did just that while absconding with millions of health care records. Security teams staying abreast of changes to relevant threat intelligence may have alerted Anthem to the change in modus operandi and given the company time to update its alerting and defenses.

> **Having well-defined prioritized cybersecurity requirements that are shared throughout the organization is essential. You need to ensure that the entire organization understands the type of global threat intelligence that should be collected and prioritized, continuously.**

Mark Alba
Chief Product Officer, Anomali

Lack of automation and a reliance on manual response actions can also contribute to team overload. One contributor is through traditional security incident and event monitoring alerts, often employing canned queries and correlations instead of artificial intelligence–driven alerts from anomalies to baselines. The issue is akin to the industry migration away from antivirus signatures to endpoint detection and response (EDR).

Another clue is excessive time spent investigating atomic IOCs, such as malicious IP addresses or file hashes. Automation and integration with existing security platforms can make short work of such threats, which leaves more time for root cause analysis, moving toward treating the cause and not just the symptom.

Keep in mind that the trail of an attack may appear to be separate, unrelated alerts across multiple systems. Mapping alerts to a threat framework could help security analysts visualize the attack without having to write a specific query or alert.

"Alert fatigue is a plague to cyber defense. Every new system brings new logs and new alerts. Security teams need solutions that can help filter out the noise and surface relevant threats, so analysts can focus on aligning to cyber security frameworks and scaling analyst resources."

Michael Tayo
Cloud Security Engineer,
Tempus Labs, Inc

Opportunity: Risk Assessment

Manual risk evaluation in the face of relentless, 24/7 attacks is time poorly spent. Valuable daylight is burned, and an entry point for subjective bias is introduced. Analysts can spend time chasing the latest threat burning across the blogosphere, even if it poses little actual risk to their organization.

"Automation tying IoCs directly into your security product suite ensures that all systems are consistently detecting and preventing attacks in real-time."

Joe Corsi
Deputy CISO,
Excellus BCBS

Key Takeaway

Asking the wrong questions without empowerment to follow trails and connect the dots leads to inefficient operations, amplified by a lack of automation.

"XDR solutions that incorporate threat intelligence provide enrichment that produces focused, targeted, contextual, prioritized data as the foundation for successful cyber fusion operations."

Genady Vishnevetsky
CISO,
Stewart Title

Chapter Four

The Role of Threat Intelligence

Threat intelligence, a pillar of cyber fusion, is what Gartner describes as “evidence-based knowledge, including context, mechanisms, indicators, implications.” In essence, it details existing and emerging threats. True intelligence lies at the intersection of critical data; an intelligence management platform; and humans analyzing and delivering information in a timely, relevant, and actionable manner. The key is to understand that data is not information, and information is not intelligence. Data is a collection of raw facts; information is a logical grouping of contextualized data.

Threat intelligence is information typically categorized or organized by threat actors and their known TTPs. Incidents that threat actors carry out using their TTPs for a given purpose are called a threat campaign. Threat bulletins describe threat campaigns, new TTPs, new vulnerabilities, and other information useful to the security community.

CTI teams spend most of their waking hours dealing directly with threat intelligence, expanding their knowledge of threats and threat actors that could negatively affect the organization. SOC teams monitor and raise alerts based on matches to threat intelligence, and IR teams use threat intelligence to determine the impact of a given alert, search for concurrent or prior events, and correlate all that information to contain and eradicate the threat.

Threat Intelligence Feeds

Threat intelligence feeds are lists of IOCs and atomic-level attack data, with sources varying in quality and accuracy from open source lists to highly curated paid commercial feeds. You can also find a variety of specialized feeds, such as those with dark web, social media, or brand monitoring.

“Intelligence-driven XDR solutions that collect internal security telemetry and correlate it with global threat intelligence provide analysts with the capabilities needed to defend against today’s attacks.”

Genady Vishnevetsky
CISO,
Stewart Title

Threat Framework Models

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.

MITRE ATT&CK

MITRE's well-known ATT&CK framework is the current 800-pound gorilla of the threat framework world. This compilation of attacker tactics and techniques has quickly become the standard for most security teams today because of its ease of use and its exhaustive detail (Figure 1).

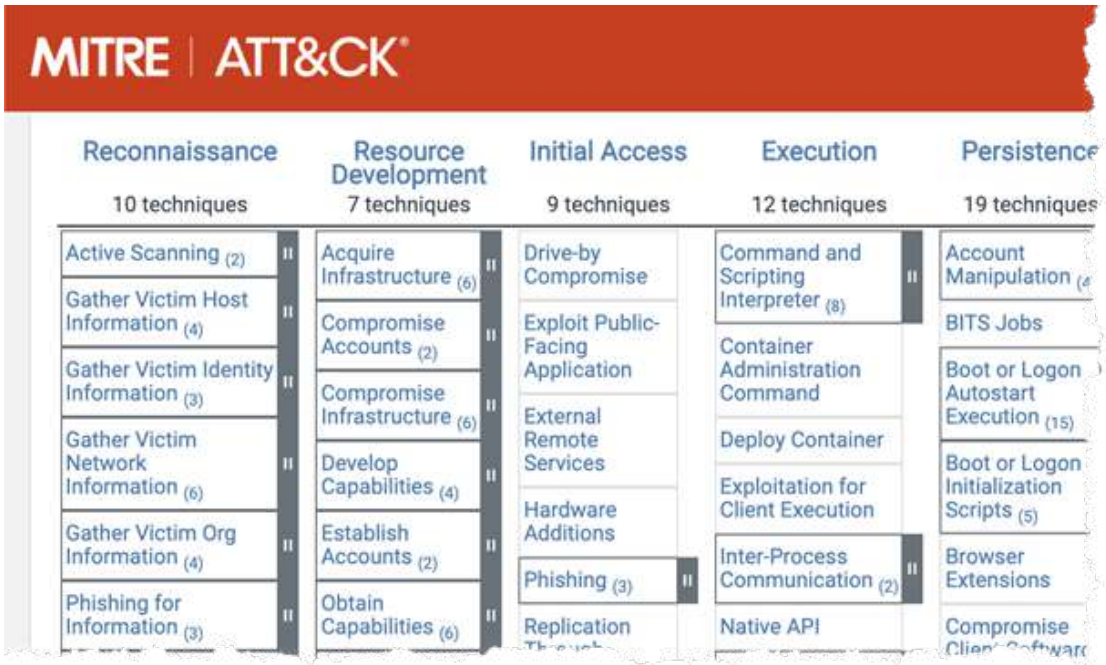


Figure 1. MITRE ATT&CK framework (*Source:* https://attack.mitre.org/matrices/enterprise/)

"Teams need to work closely with the business to be able to define priorities. A well planned and orchestrated security strategy combined with the right framework, such as MITRE ATT&CK, are critical to success."

Michal Merta
Cyber Fusion Center Lead,
Accenture

Cyber Kill Chain

The Lockheed Martin Cyber Kill Chain is one of the oldest threat frameworks in the sector and remains in widespread use (Figure 2). It provides an easy-to-understand model for visualizing the linear timeline and goals of a typical cyberattack. Mapping to these phases aids in understanding and predicting a threat actor's next moves.

Figure 2. Cyber Kill Chain Model. (Source: Anomali)

Most organizations are chasing after that last attack, not acting in a predictive or proactive way. They need to be able to look across their security posture, identify—using an attack chain model, like MITRE ATT&CK—areas of vulnerability, and then apply global threat intelligence against that model to understand how to better protect themselves.

Mark Alba
Chief Product Officer, Anomali

"Some organizations put too much emphasis on importing threat feeds and IOCs without contextualization. With enriched data, teams can work on writing more complex or specific detection rules—which leads to fewer false positives."

Brian Yau
Director of Cyber Fusion Center, Crypto.com

Diamond Model of Intrusion Analysis

The Diamond Model aids in attacker attribution by identifying relationships between behavior and motivation (Figure 3). It is broken into four quadrants:

- **Adversary.** The persona of the individual or group behind the attack.
- **Infrastructure.** The tangibles in a system, such as IP addresses, domain names, or email addresses.
- **Capabilities.** What the adversary can do, such as deploying malware or manipulating infrastructure.
- **Victim.** May include people, services, network assets, or information that the attacker targeted.

Figure 3. Diamond Model (Source: Anomali)

As information is gleaned from the attack, it is mapped to the quadrants for a more holistic analysis.

STIX/TAXII

Structured Threat Information eXpression (STIX) is a standardized language and serialization format used to exchange cyber threat intelligence. It commonly exists in conjunction with Trusted Automated eXchange of Intelligence Information (TAXII), the protocols used to share STIX information. Many threat feeds are published and ingested through STIX/TAXII.

"A defense-in-depth strategy enables threat intelligence experts to be hyper-focused on potential threats and risks to their organizations, safeguarding data and systems."

Kevin McLaughlin
VP, Global Security, Risk & Compliance, Stryker

Key Takeaway

Threat intelligence, aided by visualization in threat frameworks such as MITRE ATT&CK, contextualizes alerts to better inform decision-making.

"It's important to ensure that your team has a solution in place that can help automate the collection and processing of threat data to surface what's relevant and cut out the noise to reduce false positives."

Joe Corsi
Deputy CISO,
Excellus BCBS

Chapter Five

Best Practices in Achieving Cyber Fusion

Cyber Fusion Center Structure

Arguably the chief element of cyber fusion is a merger of traditional CTI, SOC, and IR silos under a singular organizational and managerial umbrella to maximize the flow of communication. Early starters may take an iterative approach and assign liaisons, tied to external teams, to ensure a proper bidirectional flow of information and feedback. Some organizations may even choose to take this approach literally and create a shared workspace for the team: a cyber fusion center. Regardless, define your success criteria early and measure your KPIs and other metrics frequently.

Cyber Fusion Platform Support

Certain security platforms and tools lend themselves to the cyber fusion model, with features and functionality to consider during evaluations. Remove the guesswork and manual processes, where feasible. Automate the ingestion, deduplication, and curation of feeds to produce high-fidelity threat intelligence. Consider open-source lists, premium feeds, local security telemetry, or specialty tools that can help parse, match, and import unstructured data, as found with PDF or web-based threat bulletins.

You want the platform to help produce prioritized alerts specific to the types of attacks your organizational vertical, architecture, risks, and vulnerabilities face. A macro view of all threats may be academically interesting but does not add value and could be counterproductive, consuming resources needlessly.

"In a constantly evolving threat landscape defenders are one step behind adversaries. The right technology can strengthen an organization's threat detection and protection capabilities while improving productivity and reducing costs."

Michael Tayo
Cloud Security Engineer,
Tempus Labs, Inc

Threat intelligence should be deeply integrated to enrich and contextualize alerts and reports. Teams should not waste time determining whether a given threat or vulnerability poses a true or current risk. Ideally, the information should be presented as visually mapped to threat frameworks to broaden the view of the attack stage and speed analysis.

Cyber fusion focuses on unified views, forcing analysts to use as few interfaces as possible. Copious readily available, vendor-agnostic integrations to your existing security stack should be paramount to this task. A well-developed software development kit can help fill gaps for unusual or one-off implementations.

> **To achieve cyber fusion, you need to align relevant stakeholders (CISO, SOC, analysts, etc.), automate routine tasks (collection, curation, and simple investigations), and operationalize threat intelligence to maximize your security position and lay the foundation.**

Mark Alba
Chief Product Officer, Anomali

Technical integrations can improve investigation effectiveness by streamlining available responses. Automation can send high-confidence threat IOCs for immediate blocks at your firewall, web content filter, or EDR platform. Analysts can quickly view relationships between lists of otherwise-separate lists of data; safely upload questionable files to an air-gapped sandbox; or click to retrieve additional information about suspect data, such as “whois” records or geo information.

Breaking down communications barriers and building feedback loops between teammates is far more than a simple value add. Look for features such as integrated chat, tags, notes, or seamless task reassignments.

“Matching IOCs to security telemetry has long been a security holy grail. It’s important to ensure you’re utilizing high-quality threat feeds that are analyzed and enriched with relevant information tailored to your environment. Each new feed should be analyzed and enriched to determine relevance to the environment.”

Brian Yau
Director of Cyber Fusion Center, Crypto.com

Best Practices: CTI, SOC, IR, Management

CTI analysts can serialize and tag bulletin information to help relate investigations across all teams. By keeping these analysts informed of architectural changes that affect the organization's attack surface, you can guide the very people who analyze global threat intelligence. Similarly, vulnerability management and asset management platforms can help the CTI team prioritize risk based on owned assets, systems, applications, or patch levels.

The SOC creates and monitors alerts based on CTI threat bulletins and all other relevant information. SOC security tooling should provide a degree of latitude to support analysts as they pull at an event thread and chase it wherever it may lead. A unified view can help maintain their train of thought rather than swiveling from monitor to monitor, tool to tool.

The IR team needs enough contextualized information to quickly discover, contain, and mitigate all instances of a threat. Team members can work with external departments, such as fraud, to understand the impact of a given alert or DevOps to learn about compensating controls. They should follow through and recommend updates to intelligence requirements based on their newly discovered threats or trends.

Finally, management should function from the top down, with support for security awareness ingrained into the fabric of the organization. Successful cyber fusion should honor and acknowledge potentially differing team cultures while streamlining operations in keeping with your unique business environment.

"Well-written playbooks minimize the probability of human errors and help to identify potential cases for automation wherever they make sense."

Michal Merta
Cyber Fusion Center Lead,
Accenture

Key Takeaway

Guided by threat intelligence, break down silos between teams to defend your specific organizational vertical, architecture, risks, and vulnerabilities.

"To defend your organization, you need to ensure that you have a solution in place that continuously monitors and detects threats 24/7, and one that, when a threat is detected, serves up the relevant intelligence security teams need to quickly act upon and mitigate the threat."

Kevin McLaughlin
VP, Global Security, Risk & Compliance,
Stryker

How Anomali Helps You Achieve Cyber Fusion

The Anomali Platform automates collection of threat data and drives detection, prioritization, and analysis, taking security from intelligence to detection in seconds.

Fueled by big data management, machine learning, and the world's largest intelligence repository, the Anomali Platform automatically correlates all installed security telemetry against active threat intelligence to stop breaches and attackers. Anomali's team of seasoned cyber threat intelligence analysts; partnerships that provide access to feeds, enrichments, and integrations; and support of some of the largest ISACs enable curation of the world's most complete threat intelligence collection.

The Anomali Platform automates routine tasks (collection, curation, and simple investigations) and identifies dormant threats. Anomali also features integrations with key frameworks, including the MITRE ATT&CK framework.

With The Anomali Platform, your security team will be able to operationalize threat intelligence across your entire organization, inform relevant stakeholders across the organization, and work together to contribute and maximize your security position.

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 degree in Economics from the University of Pennsylvania.

Michael Tayo, Cloud Security Engineer, Tempus Labs, Inc.

Michael Tayo is a curious and innovative cybersecurity practitioner with a passion for information security operations and automation development within on-premise and hybrid cloud environments. Michael has more than five years of experience within production environments where he supports rapid detection, triage, analysis, and response to potential security risks and threats. His goal is to support enterprise security practices with methods that utilize secure infrastructure services and software to improve overall security posture.

Joe Corsi, Deputy CISO, Excellus BCBS

Joe Corsi currently serves as the Deputy CISO at Excellus BCBS, a non-profit health insurance company supporting areas of Upstate NY. Joe has experience managing all areas of Enterprise Security including Security Architecture, Identity Management, Security Operations Center (SOC), Security Incident Response, Cyber Intelligence, Threat/Hunt, Insider Threat, Data Loss Prevention, and Governance, Risk, and Compliance. Prior to joining the private workforce, Joe served in the US Army.

Genady Vishnevetsky, CISO, Stewart Title

Genady Vishnevetsky serves as CISO for Stewart Information Services Corporation, a leading provider of real estate services. An established leader with experience in building successful security programs and developing the defense against emerging threats, Vishnevetsky leads security, governance, and compliance programs for the global enterprise. He is an active, contributing member to the cybersecurity community, a frequent speaker at security events and conferences, security advocate, blogger, and influencer.

Brian Yau, Director of Cyber Fusion Center, Crypto.com

Brian Yao is the Director of Cyber Fusion Center at Crypto.com. He has experience in many areas, including security operations, incident response, threat hunting, SIEM architecture, and use-cases development. Brian previously worked as a security analyst at SWIFT and has numerous certifications, including CDP, OSCP, CRTE, CISSP, GCIA, GREM, GIAC AB, and eCMAP.

Michal Merta, Cyber Fusion Center Lead, Accenture

Michal Merta has worked for Accenture since 2006 and leads its cyber fusion center in Prague. His professional background includes infrastructure security, security assessments, and penetration testing. He is also interested in data privacy topics. He has a Master's Degree in information security and many additional certifications in information security fields including CISSP, CISA, CRISC, ISO27001 Lead Auditor, and SABSA. Michal is also a board member of (ISC)² Czech Chapter.

Kevin McLaughlin, VP, Global Security, Risk & Compliance, Stryker

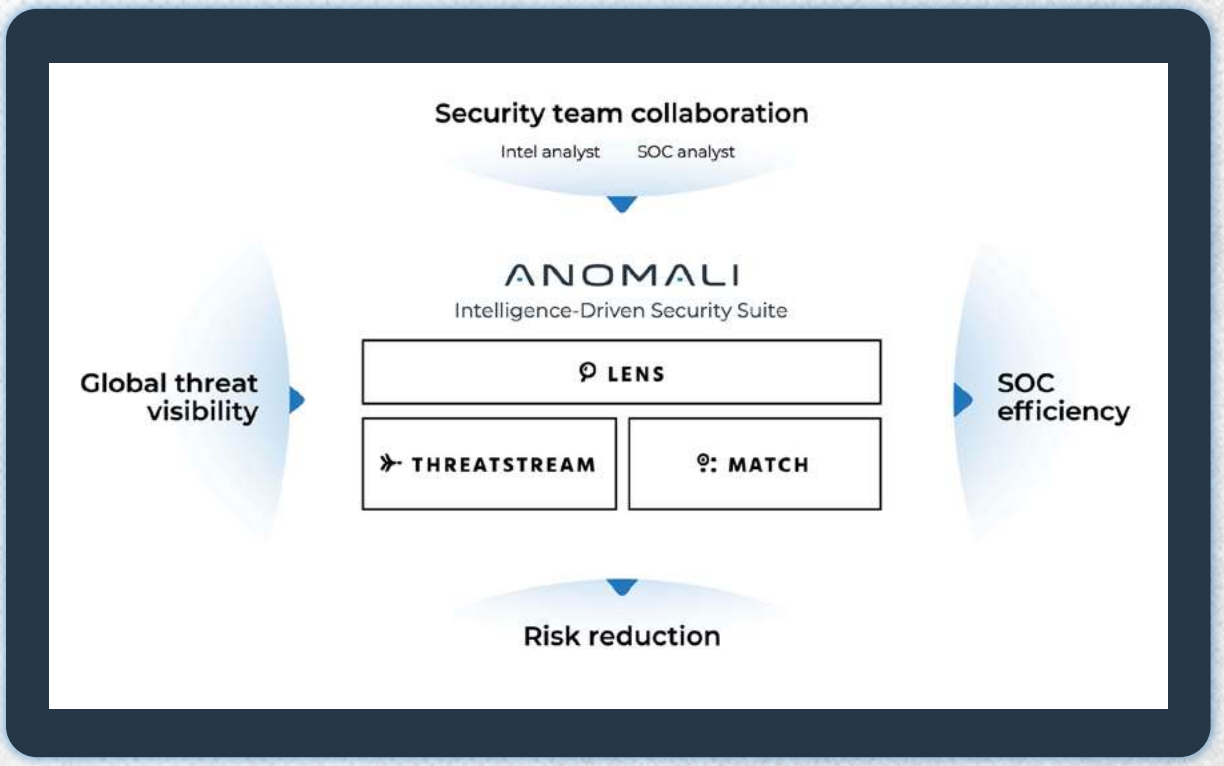
A U.S. Army veteran who proudly served and a prior U.S. Special Agent, Dr. Kevin L. McLaughlin has compiled over 39 years of law enforcement, corporate, and cybersecurity experiences. During his career, Kevin has been involved with creating three global cyber security programs, global security operations centers, and designing and implementing global cyber security architecture for three Fortune 300 companies. He is a certified CISO, CISM, CISSP, PMP, ITIL Master, GIAC-GSLC, and CRISC.

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