Mighty Guides

Sponsored by

ANOMALI

7 Experts on XDR

Using Extended Detection and Response to Improve Defense Capabilities

Table of Contents

Introduction

Cybersecurity has reached an inflection point. A diverse selection of individually effective security tools and an abundance of available threat intelligence data exist, yet the majority of recent breaches were discovered and reported externally through ransomware actors, business partners, and customers.

If incidents like SolarWinds are any indication, our adversaries possess increasing levels of funding, sophistication, and patience. Despite increased regulatory attention and pressure from leadership, as well as mandates from the president's office, cybersecurity is coming up painfully short, with the mean time to detection (MTTD) measured in weeks, months, or even years.

Extended detection and response (XDR) represents a compelling solution to this problem. Teams can quickly determine the scope of an attack and respond based on historical security telemetry and global intelligence about threat actor tactics, techniques, and procedures (TTP). XDR can tip the needle from reactive to proactive, reducing both the cost of incident management and the potential damage of a cyberattack.

This ebook explores core XDR concepts and differentiators. It covers the security challenges facing organizations today and where so many fall short. It describes the critical role of threat intelligence to XDR. Finally, it provides an insight into the key factors to consider when evaluating a prospective XDR platform.

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

Cybersecurity industry professionals have been hearing a lot about extended detection and response (XDR) lately, an emerging innovation that widens visibility over your digital surface to better detect and respond to threats relevant to your organization.

Although XDR is still in a semi-nascent stage, even those who are finding it confusing know that it can't be dismissed as a passing fad, as industry analysts, pundits, and enterprises have started identifying it as a category.

It's become increasingly clear that even highly robust detection solutions continually miss damaging incidents. Detection is often myopic, focused on the immediate attack and not the future actions of an attacker campaign. Security data is often tied up in silos, making it tough to pinpoint relevant threats and compromises, reach conclusions, and respond decisively.

XDR helps solve this problem. With the right components and framework in place, organizations can use XDR to pull together, correlate, and contextualize telemetry and data from endpoints, clouds, messaging, SIEMs, network traffic, and threat intelligence to detect, investigate, confirm, and act against a current or future attack or breach at the fastest speeds possible.

In the world of cybersecurity, there is no such thing as impregnable defenses. As an industry, we need to continue to transform to keep up with today's sophisticated attackers. XDR is a key and revolutionary advance that is driving reduced risk and heightened defense.

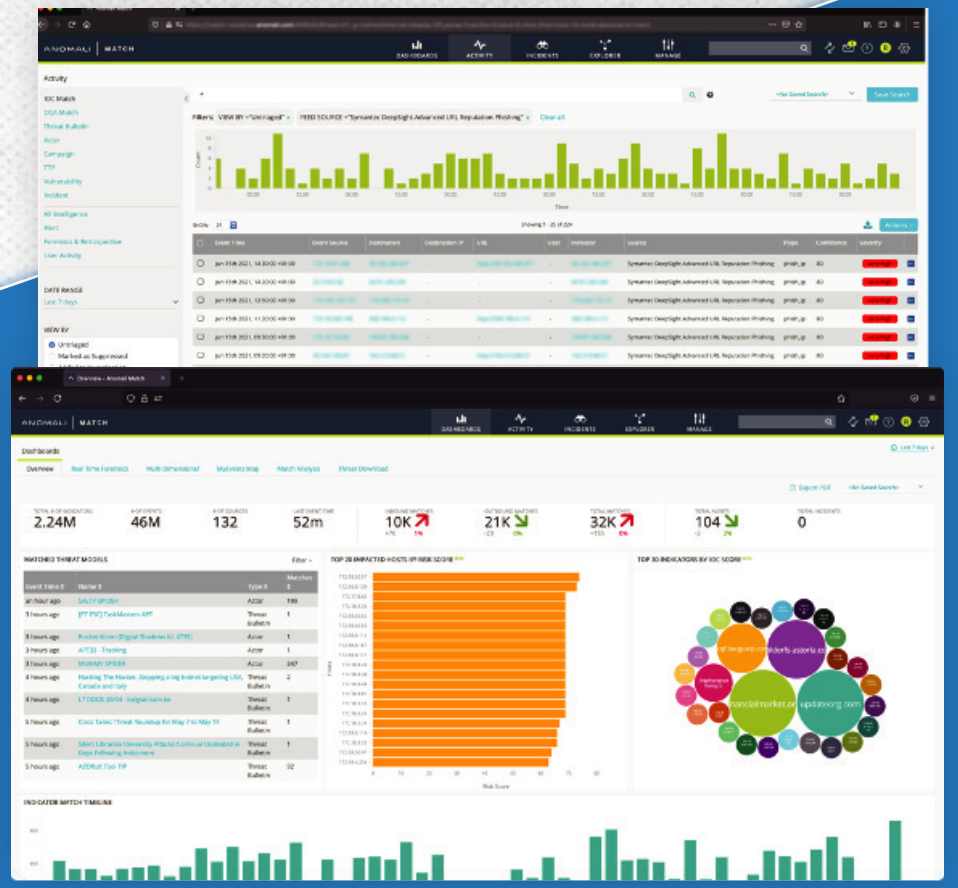
Regards,
Mark Alba
Chief Product Officer,
Anomali

ANOMALI

Match:

Intelligence-Driven Xtended Detection and Response

Anomali Match is an intelligence-driven detection engine that helps organizations quickly identify and respond to threats in real-time by automatically correlating ALL security telemetry against active threat intelligence to stop breaches and attackers.



Anomali Match enables organizations to:

- Pinpoint relevant threats
- Accelerate Threat Hunting
- Continuously Monitor Intel
- Elevate strategic intelligence
- Predict the next attack

LEARN MORE | WHAT IS XDR? | MATCH INTERACTIVE INFOGRAPHIC | REQUEST A DEMO

Meet Our Experts

Mark Alba
Chief Product Officer,
Anomali

Dmitriy Sokolovskiy
VP and CSO/CISO,
Avid

Lance Auman
Lead Security Engineer,
iHerb

Konrad Fellmann
VP and CISO,
Cubic Corporation

Genady Vishnevetsky
CISO,
Stewart Title

Dave Ruedger
CISO,
Invitae

Michael Marschean
CIO,
Subcom

Chapter One

What Is XDR?

XDR represents an evolution beyond traditional security information and event management (SIEM), security orchestration, automation, and response (SOAR), or endpoint detection and response (EDR). The cohesive software as a service (SaaS)-based threat detection and incident response platform natively integrates across an organization's security stack, providing a mechanism for simple or automated response actions.

XDR contextualizes threat intelligence and business risk across all platform facets, allowing deep insights into attacks and threat actors. Combined with mapping against threat frameworks such as MITRE's ATT&CK framework, analysts are presented with a visual palette to quickly pivot their investigations to uncover events that may have been missed otherwise. And with false positives virtually eliminated, teams can mount a swifter and more effective response to emerging threats.

How Does XDR Work?

An XDR solution collects data across all installed security telemetry, including SIEM logs, vulnerability scans, and other local telemetry integrations and stores it in a data lake—a massive repository of historical metadata. Organizations can choose to expand the efficacy of event correlations by ingesting logs from physical security, fraud detection, and similar security systems.

An artificial intelligence (AI) engine simultaneously analyzes the data lake, correlating disparate events with contextual clues such as indicators of compromise (IoCs) and threat actor TTPs. This newly enriched data is then leveraged to produce high-fidelity incident alerts or drive automated responses.

"While EDR has been instrumental in monitoring and containing intrusion, its visibility is limited to the endpoint. XDR bridges the gap by enriching telemetry data from other sources and allowing analysts to make faster and more reliable decisions."

Genady Vishnevetsky
CISO,
Stewart Title

How Is XDR Operationalized?

XDR insights into an organization's security posture enable a significantly more proactive threat management and mitigation approach. By visually mapping threats to internal playbooks or frameworks such as MITRE ATT&CK, XDR lends analysts a better understanding of attackers and attack patterns.

> **Security teams can no longer only rely on the same tools they've used for threat detection and response.**

Mark Alba
Chief Product Officer, Anomali

By mapping assets to business risk and criticality, XDR offers a high-level security-minded view of an organization's ecosystem.

As the platform detects new threats:

- XDR actively integrates relevant information into a comprehensive alert.
- Security operations centers (SOCs) and incident response (IR) teams can quickly gauge the impact of the alert.
- Analysts search historical data within the platform to rapidly determine the original source event and vector.
- Analysts leverage visual TTP threat framework mapping to identify threat actors and potentially predict their future actions.
- The organization responds directly from the platform via optimized integrations to its existing security stack.
- Armed with a solid understanding of scope and scale, the business decision-makers recover from the incident in confidence.
- Teams cross-pollinate feedback to inform and improve future threat hunting.

"Analysts have a tremendous amount of data coming in from many sources, which is time- and resource-intensive to analyze. XDR automatically correlates data from many disparate sources, which helps analysts prioritize their actions, improving detection and response time."

Konrad Fellmann
VP and CISO,
Cubic Corporation

How XDR Enhances Cyber Resilience

To ensure continuous production and optimal service levels amidst a constantly evolving threat landscape, security teams must practice more than cybersecurity—they need cyber *resilience*. An organization should rapidly detect, respond, and recover from threats. More importantly, it should learn from each incident, maturing from reactive to proactive in the process. XDR plays a pivotal role in enabling this level of resilience.

The recent Apache Log4j "Log4J Shell" vulnerability provides an interesting case study. As information regarding the vulnerability emerged, XDR's AI detected events by matching local security telemetry against global threat intelligence and alerted security personnel. Teams searched earlier threat activity, evaluating for indicators of attack (IOA) weeks, months, or even years, depending on capabilities before the incident and initiating response actions directly within the console.

In the days that followed, analysts could use XDR to iterate their migration efforts continually as new information became available. With XDR's reporting available to surface the breadth and depth of organizational impact, chief information security officers (CISOs) were able Tto confidently ensure an informed recovery and bolster processes and defenses against future threats.

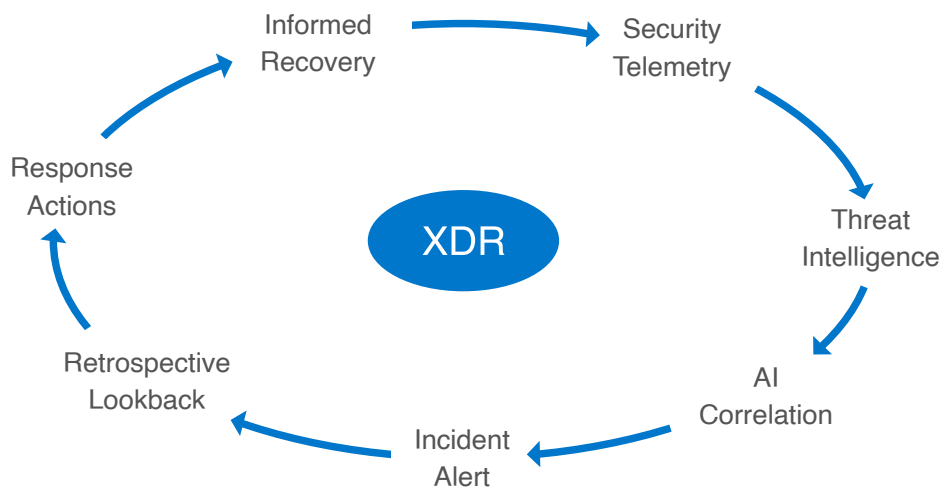


Figure 1: XDR Process Cycle

"The organizational attack surface continues to increase. For instance, cloud presence and API-connected applications are growing exponentially."

Genady Vishnevetsky
CISO,
Stewart Title

Key Takeaway

Extended Detection and Response (XDR) is an evolution beyond signature-based anti-malware, driven by a core of automation and threat intelligence.

"Your security stack represents countless hours of implementation, training, support, and documentation. XDR's product integrations speed initial platform adoption while maximizing the efficacy of your existing security investments."

Lance Auman
Lead Security Engineer,
iHerb

Chapter Two

The Challenges of Modern Cybersecurity

Even before the pandemic, modern organizations faced a broad range of roadblocks and pitfalls. As attackers grow more intelligent and more sophisticated, security teams struggle with limited resources, poor processes, and complex infrastructure. The global shift to distributed work has only exacerbated these issues.

Team Overload

The average organization employs dozens of unique security products to power comprehensive detection and prevention, and security personnel must train to proficiency to implement and utilize the tools. This learning curve makes matters more complicated, as you must account for integrations, system dependencies, business priorities, and an organization's unique risk profile.

Operationalizing the requisite mass of policies, rules, alerts, and architectures can be difficult for even the most experienced and talented personnel. Factor in a stream of never-ending emails and contextless late-night alerts, and you have a recipe for disaster. Harried and exhausted, analysts become increasingly likely to resort to shortcuts and make mistakes, while mounting alert fatigue may eventually lead to burnout.

Worse still, while contending with this deluge of alerts, analysts may overlook threats that urgently require their attention. Alternatively, they may simply over-tune their detection rules in an effort to reduce the barrage of false positives. Notably, this was one of the root causes of Target's infamous data breach.

"When threat intelligence is incorporated into the XDR framework, this reduces the need for extra labor in an area that has traditionally suffered from a shortage of highly skilled staff."

Dave Ruedger
CISO,
Invitae

Digital Transformation

Digital technologies hold great promise regardless of industry, with the potential to improve productivity, unlock new lines of business, and streamline workflows. Unfortunately, the hurried migrations necessitated by COVID-19 created considerable strain for security teams. More than 50% of projects were reportedly either unsteady or entirely untested prior to this shift.

Organizations must now contend with a drastically altered attack surface as employees working from home access internal resources and cloud systems from questionably secure systems and networks. And, all the while, businesses continue to rush new technologies to production in support of distributed work. Over-stressed teams were already struggling to keep pace. Now they're falling continually further behind.

Traditionally the security world has faced three major challenges in helping teams maximize operations.

- **Lack of visibility into relevant threats on both a global scale and within local context.**
- **Precision detection capabilities to cut through the noise and show whether a threat does or doesn't exist.**
- **Inability to connect all the siloed security data and disparate intel to respond effectively.**

Mark Alba
Chief Product Officer, Anomali

"Most companies have invested greatly in their current security stacks, both in the cost of the products and the level of effort to mature the deployment. But now, security perimeters have shifted and opened the doors to new threats that companies have to manage."

Konrad Fellmann
VP and CISO,
Cubic Corporation

Talent Shortage

There has been an ongoing skills shortage in the security sector for years. While opinions as to the cause vary—the mounting cost of formal education, overly strict certification prerequisites, competitive salaries, or simple burnout—the end result is the same. And though the gap has recently begun to narrow; there's still a long road before organizations have enough qualified, experienced personnel.

To compensate, as many as 60% of security shops have augmented threat management with in-house IT staff over dedicated and experienced analysts. Executive teams are likely to learn the hard way during the critical hours of a major incident that this is a mistake. There simply aren't enough hours in the day for IT personnel to balance their regular duties with threat hunting.

Cost Constraints

The pandemic caused IT budgets to explode with newly shifted priorities such as cloud migrations, borderless networking, and decentralized security. Unfortunately, these new projects did not erase existing mandates and priorities. As a result, businesses must contend with a multitude of difficult cost analysis decisions.

Even long-time security stalwarts such as SIEM platforms may receive the cut amidst growing licensing and storage expenses. Cost-cutting measures to that end may include reducing retention timelines, archiving log data to cheaper and slower storage, and eliminating logs deemed extraneous. None of these measures are ideal, and all of them reduce the platform's effectiveness.

A fast response to cyber-incidents is imperative. Teams simply can't afford to wait for log restoration out of warm or cold storage when time is critical.

"Home network environments don't have the same level of rigor and security a corporate environment would provide, so companies must deploy greater security controls on their corporate-managed endpoints."

Dave Ruedger
CISO,
Invitae

The Modern Threat Landscape

Attackers are becoming progressively better at circumventing defenses while remaining undetected. Attack frequency has grown more than a hundredfold, with a 600% increase in 2020 alone. Sophistication is similarly on the rise, as multiple segments of the criminal underworld continue to develop—from state-sponsored attacks to the burgeoning cybercrime-as-a-service market.

One of the most troubling reflections of this growth is evidenced by increased attacker dwell times.

The Flame super virus, for instance, was in the wild for roughly two years before detection. The Dragonfly malware was present in industrial systems for at least three years before analysts were aware of its existence. Project Sauron, meanwhile, managed to remain hidden for a staggering five years.

We can expect this trend to continue, exacerbated by pandemic-driven architecture and the explosive new growth of application programming interface (API)-based microservices.

"In recent years, there has been a rapid rise in highly sophisticated and tenacious threat actors and extortion-like ransomware attacks. It is more important than ever to quickly identify bad from good."

Lance Auman

Lead Security Engineer,

iHerb

Key Takeaway

Overloaded security teams must keep pace with the modern threat landscape against a backdrop of digital transformation, talent shortages, and cost constraints.

"The pandemic brought a massive expansion in which locations, devices, and people make up the new enterprise perimeter. Now malicious actors are utilizing new attack vectors to get inside."

Dmitriy Sokolovskiy
VP and CSO/CISO,
Avid

Chapter Three

Where Cybersecurity Is Falling Short

Team Overload

More than half of organizations are untested in the face of digital threats.

Traditional SOC teams largely rely on predefined alerts, akin to the early days of antivirus signatures. IR teams, meanwhile, are forced to play a game of digital whack-a-mole, reimaging infected machines without knowing the full impact of an incident or identifying the initial attack vector. The problem has grown exponentially with the new pandemic-driven norm of work from home, which is pushing the corporate perimeter into employees' homes. This blindness in the name of expediency is self-defeating, allowing the same threat actors to target one's business repeatedly.

> **There's an abundance of security data tied up in silos, making it impossible to pinpoint relevant threats and compromises, reach conclusions, and then respond decisively.**
>
> 
>
> **Mark Alba**
> Chief Product Officer, Anomali

Businesses must juggle a collection of disparate tools, each of which requires tuning, integrations, and ongoing maintenance, making the situation more complicated.

"XDR offers a synergistic platform for CTI, SOC, and IR teams to function as a single entity with shared goals, processes, and continuous improvement from lessons learned. Expanding to Red Team, Fraud, Physical Security, DevOps, SRE, and related teams is a further force multiplier in successful XDR implementations."

Lance Auman
Lead Security Engineer,
iHerb

Although single-vendor stack XDR customers have a slight edge in this respect, they carry the additional risk of vendor lock-in and must manage a single point of failure and detection. Nonetheless, that time could be better spent building out proactive security.

With all hands treading water, security teams fall into predictable silos of knowledge and action. Information is parceled out between teams with little communication, coordination, or feedback. These constraints, unfortunately, relegate an organization to inefficient and reactive incident response.

Cost Constraints

Funding is a common issue across business verticals. Many shops maintain incomplete tool sets, and 66% rely on internal scripts to fulfill their needs. And although SIEMS are still valuable for fulfilling compliance mandates, they're beginning to show their age—64% of teams consider them beneficial only for post-breach activity. Consequently, they've become a common target for cost-cutting measures, further reducing their effectiveness.

Modern Security and Threat Landscape

It's clear from the current prevalence of data breaches in the news that not enough organizations maintain a proactive security approach. The timelines of many recent breaches further demonstrate a frightening reality. An attacker may already dwell in your systems, and your outdated tools and overloaded teams have yet to detect them.

The metrics are even bleaker if you consider the number of organizations that hide from responsible disclosure.

Rather than assuming the existence of a breach at the outset and architecting around that standard, many teams fall prey to overconfidence. They think they understand the source, intent, and scope of the types of attacks targeting them. Current trends and metrics indicate that this assumption is unfounded—security personnel are wrong far too often for comfort, even if they're never in doubt.[1]

[1] P. W. Singer and Allan Friedman, "Why It Matters" in *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford Press, 2014), page 150.

"XDR allows your security team to stay focused, identify real threats, and take threat response to the next level."

Michael Marschean
CIO,
Subcom

Key Takeaway

Forced to focus on the attack and not the attacker, teams miss the bigger picture. Threat actors may already dwell in your network.

"Security perimeters were easier to define in the past when employees were behind firewalls in the office and most workloads were performed in physical data centers. Now, with remote workers and public SasS solutions, the perimeters are more complex and harder to manage."

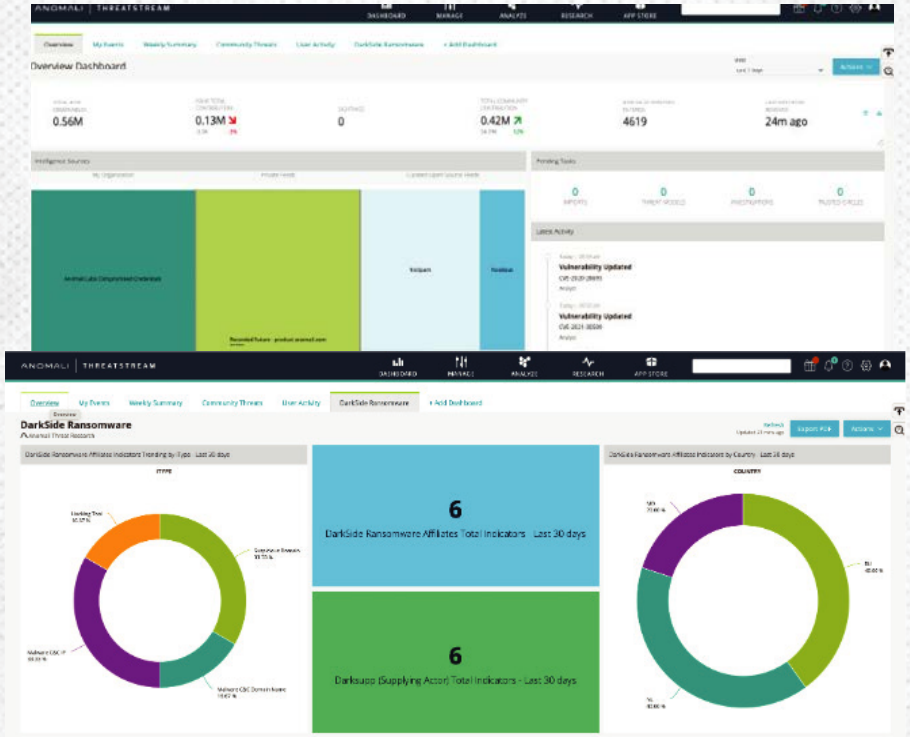
Konrad Fellmann
VP and CISO,
Cubic Corporation

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

Chapter Four

The Role of Threat Intelligence in Effective Security

Threat intelligence is the foundation of achieving effective cyber resilience, what Gartner describes as evidence-based knowledge, including context, mechanisms, indicators, implications, and details about existing and emerging threats. It exists at the intersection of critical data, analytics, and human agents. Moreover, it's the beating heart at the core of XDR, crucial for the analysis and delivery of timely, relevant, actionable information.

Data is not information, and information is not intelligence. Data is simply a collection of raw facts, and information is a logical grouping of contextual data.

Intelligence is how one applies that information to its security posture and defenses.

Tactics, Techniques, and Procedures

Typically, threat intelligence is characterized and organized by individual threat actors and their TTPs. This information may be applied to threat campaigns—a set of attacker activities or incidents carried out with a specific goal in mind. These campaigns are frequently vertical-specific, targeting healthcare and financial services industries. Nonetheless, defenders should be ready if and when an attacker jumps verticals and chooses a new target.

"When the community bands together, we can achieve better results with greater speed and accuracy. The same is true for threat intelligence."

Dave Ruedger
CISO,
Invitae

Threat intelligence in this arena often takes the form of IoC feeds—atomic-level data such as individual hashes, domain names, and IP addresses. The sources from which this data is drawn can vary wildly in quality, quantity, and accuracy, from highly curated paid feeds to simple open-source lists. They can span the full array of IoCs, or they can be specialized, like the dark web, social media, or brand monitoring.

Threat Framework Models

IoCs, such as file hashes or domain names, tend to be highly dynamic. TTPs, however, are remarkably similar among threat actors, many of whom prefer to stick with their time-tested methods. XDR contextualization provides an opportunity to identify, analyze, and locate these adversaries in their attack phases.

> **Automation and big data management are needed to collect data across all installed security telemetry, along with advanced intelligence to understand and correlate threats.**
>
> 
>
> **Mark Alba**
> Chief Product Officer, Anomali

One of the primary ways they accomplish this is through the use of threat framework modeling.

"XDR collects threat pointers and telemetry from multiple technologies and builds a threat intelligence ecosystem. Then it provides actionable steps to alert on or block the identified risks."

Genady Vishnevetsky
CISO,
Stewart Title

Constructed by experts over multiple years, these frameworks aid in visualizing and operationalizing threat information. The newest of these—the proverbial 800-pound gorilla of threat frameworks—is ATT&CK, compiled by The MITRE Corporation. This compendium of attacker tactics and techniques has quickly become the de-facto standard for most security teams today owing both to its ease of use and its exhaustive level of detail.

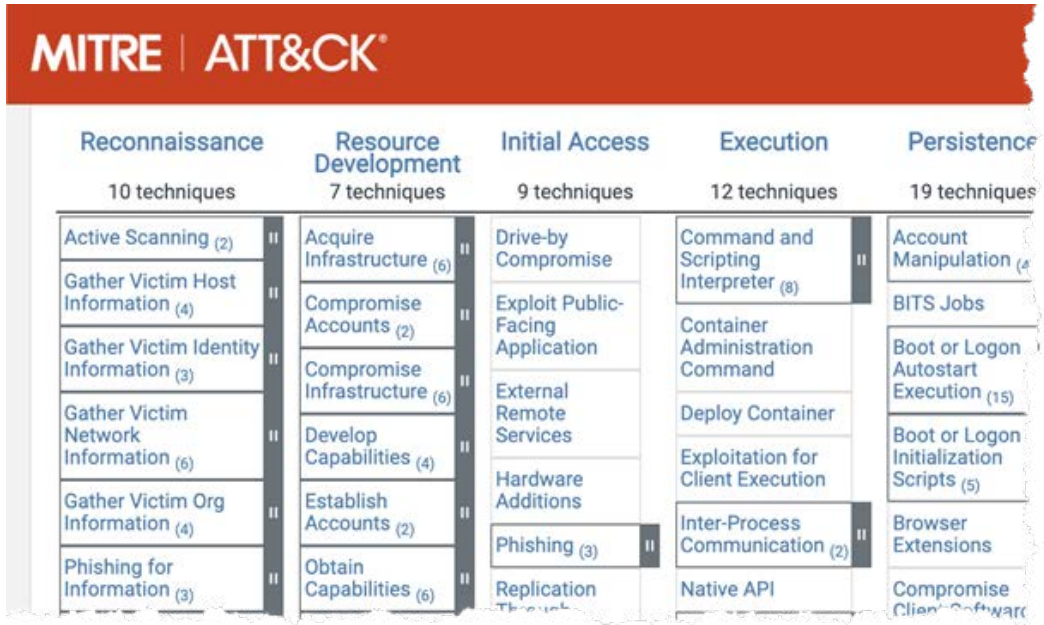


Figure 2. MITRE ATT&CK Framework. *(Source: https://attack.mitre.org/matrices/enterprise/)*

The **Lockheed Martin Cyber Kill Chain** is one of the earliest threat frameworks in the sector, and it still sees widespread use today. It provides an easy-to-understand model for visualizing the timeline and goals of a typical cyberattack. Mapping to these phases aids in understanding and predicting a threat actor's next moves.

Figure 3. Cyber Kill Chain Model. *(Source: Anomali)*

"By correlating the security data between systems to develop a holistic view of a potential threat, you can eliminate over 90% of the investigative analysis."

Michael Marschean
CIO,
Subcom

The **Diamond Model of Intrusion Analysis** identifies relationships between an attacker's behavior and motivation and 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, and email addresses.
- **Capabilities.** What the adversary can do, such as deploying malware or manipulating infrastructure.
- **Victim.** May include people, services, network assets, or information targeted by the adversary.

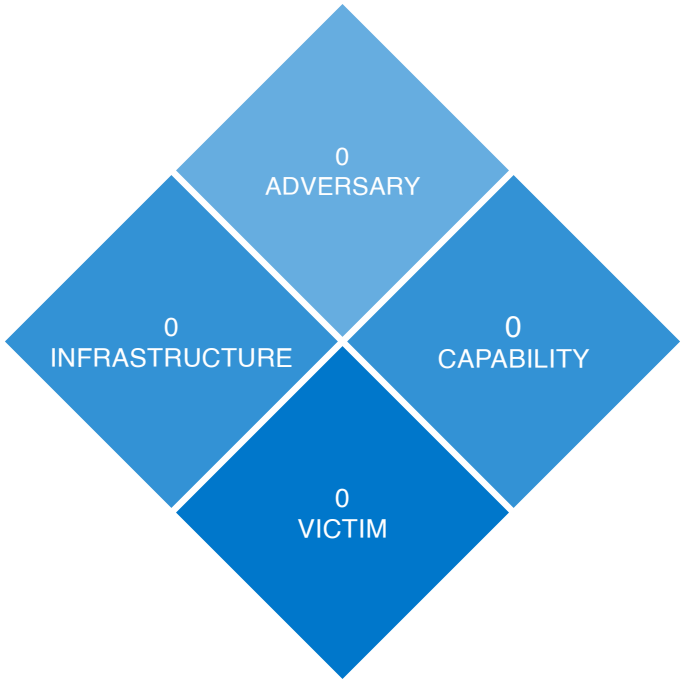


Figure 4. Diamond Model. (*Source: Anomali*)

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

"The key to successful information security is to deploy the limited resources toward the locations of the biggest threats."

Dmitriy Sokolovskiy
VP and CSO/CISO,
Avid

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 via STIX/TAXII.

These threat models greatly enrich operational intelligence, allowing an analyst to understand a great deal more about threats, pivoting investigations and potentially gleaning otherwise unforeseen insights. Decisions made without this expanded context may result in an incomplete picture—a myopic focus on the attack versus the attacker.

It's important to understand that threat intelligence alone is not a cure-all. If a team is already overwhelmed, it may be unable to prioritize the information. Threat intelligence may also become siloed to specific teams or limited to poorly disseminated reports, significantly educing its value.

"Integrating threat intelligence into the XDR lens is a shortcut to pinpointing these locations and saves our SOC and IR teams many very expensive hours."

Dmitriy Sokolovskiy
VP and CSO/CISO,
Avid

Key Takeaway

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

"Threat intelligence is a crowd-sourced model where information about active attacks is distributed at scale across the globe to mitigate risks before attacks happen."

Dave Ruedger
CISO,
Invitae

Chapter Five

What to Consider When Selecting an XDR Solution

XDR is still somewhat in its infancy and is being defined. As such, different solutions may vary considerably in both features and effectiveness. XDR should fundamentally provide a holistic intelligence-driven view of threats across the organizational landscape, leading to better, faster outcomes, though this may mean different things for different vendors. That said, some key factors should be considered during platform evaluation.

Cost Savings

A solid return on investment and a low total cost of ownership are critical to executives. To that end, look for predictable, user-based pricing, and avoid ingestion-based models such as events per second or gigabytes per day.

Because there is a degree of complementary overlap, you should also seek a product that can shoulder some of the load (and cost) from your SIEM solution. 66% of organizations maintain only six months or less of active log data in their SIEM. This is highly untenable, particularly in the face of increased attacker dwell times. The XDR platform should store actionable log metadata far outside the norm, extending even into years.

Integration with Security Investments

A vendor-agnostic solution capable of integrating with and augmenting your existing (and prospective) security investments is essential. Be aware, however, that not all XDR platforms are this capable. Some don't integrate or play well with other systems, functioning best as homogenous single-vendor greenfields or "rip-and-replace" style deployments.

"XDR is a must-have tool for every security team with a clear ROI to the business. It saves money while reducing risk, one of the few 'win-win' solutions out there when it comes to investing in security solutions."

Michael Marschean
CIO,
Subcom

AI-generated alerts from correlated global threat intelligence and local security telemetry should eliminate false positives and provide for automated response actions within your existing security investments, such as firewalls, web content filters, and EDR platforms.

Infused with Threat Intelligence

By curating, deduping, and prioritizing intelligence, XDR's intelligence-driven reporting should minimize the time spent on tedious analysis and mitigation, including unstructured data. Analysts should be able to view external threat analysis web pages or PDFs and match the page content, in real-time, against local systems to quickly determine relevance.

XDR should provide your cyber threat intelligence (CTI), SOC, and IR teams with valuable information and much-needed time.This frees analysts to focus their efforts on sources near the top of the cyber pyramid of pain.

After all, global intelligence is well documented, and most threat actors leverage the same set of tools and tactics across all their victims, seldom deviating.

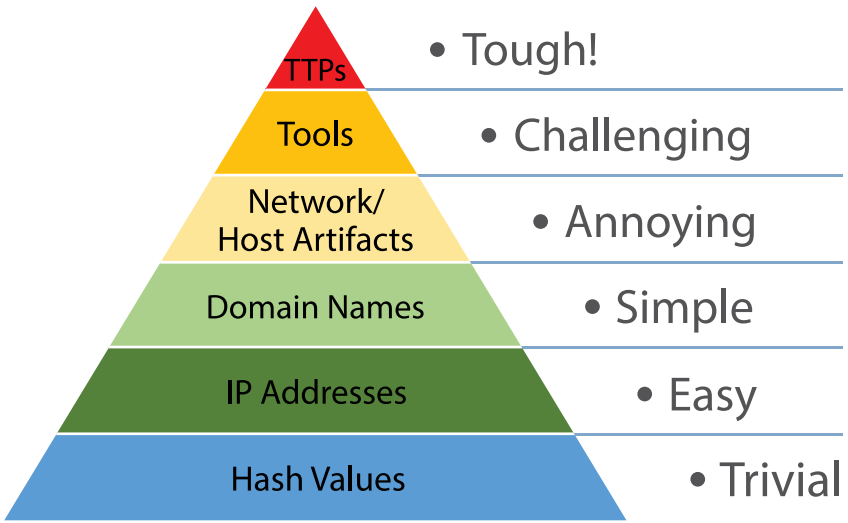


Figure 5. Cyber Pyramid of Pain *(Source: Emulating Attacker Activities and The Pyramid of Pain)*

"It's rare to find a company today that uses a single vendor for all its information and security needs, so being vendor-agnostic is one of the primary requirements of an XDR platform."

Dmitriy Sokolovskiy
VP and CSO/CISO,
Avid

Optimized Response

Every organization has a unique definition of value and a unique concept of what it has to lose.

An XDR solution should be able to point you to a threat immediately and demonstrate both how it impacted you and for how long. You should be able to perform an automated retrospective search directly charting a timeline back to the original intrusion without wasting time restoring old SIEM data. More importantly, the platform should prioritize the systems, people, and data most at risk during an incident.

> **With the right XDR components and framework in place, organizations can use XDR to pull together, correlate, and contextualize telemetry and data from endpoints, clouds, messaging, SIEMs, network traffic, and threat intelligence to detect, investigate, confirm, and act against an attack or breach at the fastest speeds possible.**

Mark Alba
Chief Product Officer, Anomali

Threat framework and risk mapping are also critical features, allowing your teams to promptly and visually pivot, expand, and explore.An XDR solution should guide you on where else to look and provide relevant intelligence while doing so.

XDR eliminates a lot of wasted effort.

Michael Marschean
CIO,
Subcom

Mitigation and Feedback Loops

XDR should help break down silos between SOC, IR, and CTI teams. By mapping threat intelligence throughout the platform and across your organization, a good XDR solution will help your business more thoroughly understand where security controls are the most crucial.

Put into practice, you might prioritize threat hunting and vulnerability mitigation efforts as more critical to your cybersecurity strategy.

Finally, an XDR platform should provide a means for feedback loops between CTI, SOC, and IR teams. The investigation pipeline should be a seamless transition from one team to the next yet still allow active communications to course-correct, determine lessons learned, and improve future threat hunting and response.

Anomali—Intelligence-Driven Extended Detection and Response

Anomali's intelligence-driven extended detection and response helps organizations quickly identify and respond to threats in real-time by automatically correlating all security telemetry against active threat intelligence to expose known and unknown threats.

Anomali's XDR combines global threat intelligence with extended detection capabilities to stop breaches and attackers, delivering all of the following:

- Unified threat detection utilizing installed security telemetry.
- Precision detection with timely alerts to stop threats earlier.
- Increased ROI with less administrative overhead.
- Higher fidelity alerts to reduce false positives and empower stretched IT teams.
- Retrospective search capabilities across 5+ years.

"It is imperative for an XDR platform to be vendor-agnostic and reuse existing investments."

Genady Vishnevetsky
CISO,
Stewart Title

Key Takeaway

Integrate and automate with your existing security investments. Augment your SIEM's capabilities with retrospective searches 5+ years prior to your incident.

"A vendor-agnostic platform provides the most value by allowing the customer to continue to utilize prior security investments and integrate the best tools going forward."

Michael Marschean
CIO,
Subcom

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.

Dmitriy Sokolovskiy, VP and CSO/CISO, Avid

Dmitriy is currently a CISO and CSO at Avid Technology. From 1999 to 2007, he consulted for defense contractors, public and private companies, and non-profits. Between 2007 and 2018, Dmitriy built and managed a cybersecurity PS team, personally participating in IR for some of the largest breaches in US history. Dmitriy advises infosec start-ups, VC, & PE firms. He is a SANS mentor and a member of the GIAC Advisory Board.

Lance Auman, Lead Security Engineer, iHerb

Lance has over twenty-five years of diverse experience in large enterprise security and infrastructure across multiple verticals. In his current role, he serves as the Lead Security Engineer for iHerb, a multi-billion-dollar global ecommerce platform. In prior roles, he served as Security Architect for Irvine USD, VP of Information Security for Penfed Credit Union, and Infrastructure Director for San Francisco USD.

Konrad Fellmann, VP and CISO, Cubic Corporation

Konrad Fellmann is VP and CISO of Cubic Corporation. He leads the cybersecurity program for the corporation. Prior to Cubic, Fellmann served in several security roles at companies such as IBM, Unisys, and WebMD where he provided security consulting, assessment, and regulatory compliance services. He holds several degrees and IT certifications and served as an officer in the United States Marine Corps.

Dave Ruedger, CISO, Invitae

Dave Ruedger is the CISO at Invitae, one of the fastest growing health tech companies whose mission is to bring genetics to mainstream medicine. With over 25 years of experience developing and managing security programs, Dave has guided and advised everything from pre-IPO startups to Fortune 500 enterprises, including roles as Chief Security Architect for Maxim Integrated and CTO & Co-Founder of a SaaS startup.

Michael Marschean, CIO, Subcom

Mike Marschean is a CIO with a passion for transforming technology organizations into business-focused teams. He delivers IT strategies and solutions to achieve the company's financial and strategic goals. Mike also develops teams that focus on deliverables and return on investment, using technology to achieve productivity, growth, and cost objectives to make the business more competitive.

Genady Vishnevetsky, CISO, Stewart Title

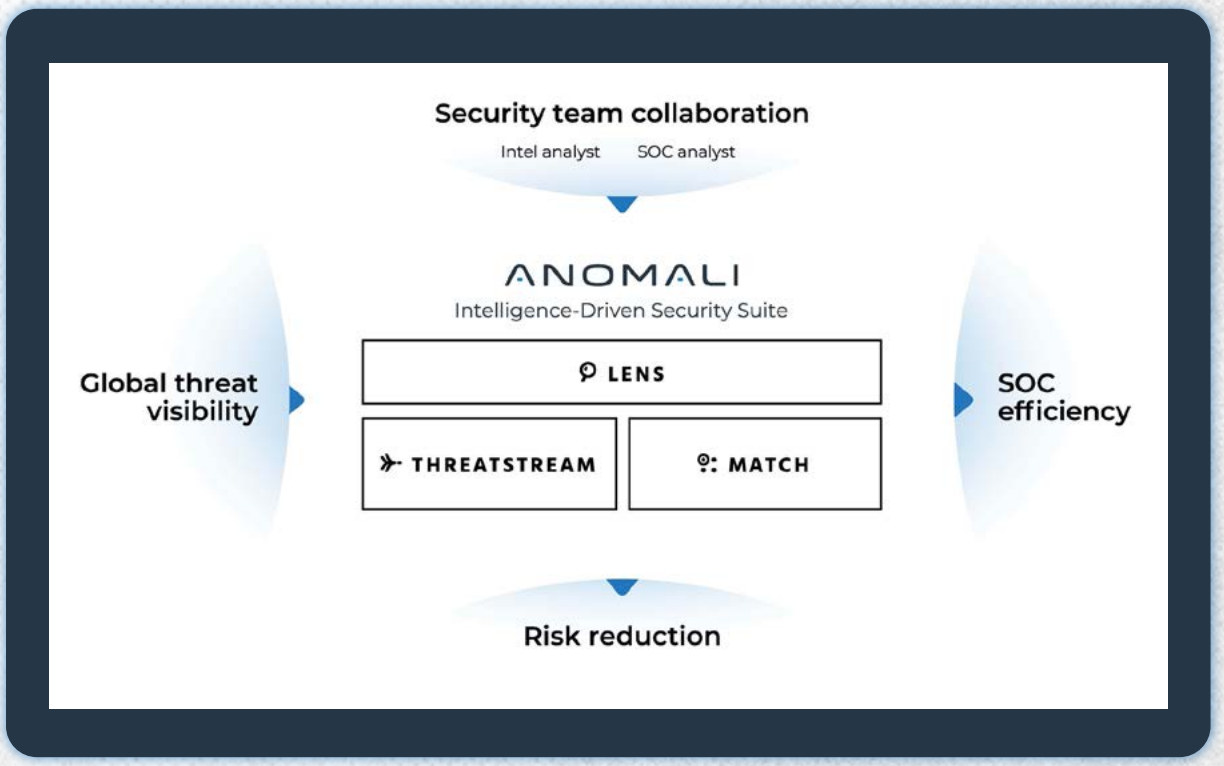
Genady Vishnevetsky serves as CISO for Stewart Information Services Corporation, a leading provider of real estate services. An established leader with experience in building successful security programs and developing the defense against emerging threats, Genady leads security, governance, and compliance 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.

ANOMALI

The Anomali® Platform

The Anomali Platform is a cloud-native extended detection and response (XDR) solution 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