ANOMALI

GUIDE

AI-Powered TDIR

A Proactive Approach to Identifying and Mitigating Cyberattacks

AI-Powered TDIR

A Proactive Approach to Identifying and Mitigating Cyberattacks

What is TDIR?

Threat detection, investigation, and response (TDIR) is an end-to-end workflow process that helps organizations safeguard their IT environments. It is a risk-based approach to identifying and neutralizing threats by understanding the attack surface, network traffic, user behavior, and operating systems. The TDIR framework helps organizations manage incidents from initial detection to remediation.

There are three phases of the TDIR workflow:

- **Threat detection:** Identifying malicious activity across an organization's devices, network, software, and user identities
- **Threat investigation:** Analyzing detected threats by conducting forensic analysis, identifying the root cause, and understanding potential impacts
- **Response:** Containment actions to limit the impact of threats to minimize damage and prevent future attacks

The Evolution of TDIR

The cybersecurity landscape has reached an inflection point. As data volumes surge and expansive cloud architectures blur the boundaries of the typical enterprise network, organizations face five interconnected challenges that are reshaping how we approach security:

1. **Data is outpacing analysis capabilities.** Organizations today are generating and processing unprecedented amounts of security telemetry from on-premises systems, cloud applications, IoT devices, and remote endpoints. This influx of data isn't just rapid — it is increasingly diverse and unstructured, making it more challenging to organize, analyze, and extract meaningful insights. Security teams must somehow sift through this deluge to spot potential compromises, even as data volumes multiply exponentially.

2. **Cloud adoption is transforming the security perimeter.** As businesses embrace digital transformation, they are migrating to the cloud to leverage its scalability and operational agility. However, this shift introduces new cybersecurity challenges, requiring different processes and approaches, especially when working with multiple cloud providers. With data, applications, and workloads distributed across hybrid and multi-cloud systems, organizations must address new vulnerabilities and ensure consistent security controls.
3. **The cybersecurity talent shortage is reaching critical levels.** The demand for skilled cybersecurity professionals far outpaces supply, creating a talent gap that leaves many organizations struggling to staff their security operations centers (SOCs). The shortage of qualified candidates places additional pressure on already overworked security teams, making it difficult to monitor, investigate, and mitigate threats effectively, leaving organizations more vulnerable to attacks.
4. **Meanwhile, the attack surface continues to expand.** Remote workforces, connected devices, and third-party integrations create an ever-growing web of potential entry points for adversaries. As organizations innovate and adopt new technologies, they inadvertently expand their attack surface. This gives cybercriminals more opportunities to infiltrate systems and makes comprehensive vulnerability management increasingly challenging.
5. **Adversaries are weaponizing stealth and sophistication.** Threat actors constantly evolve their techniques to bypass traditional security measures, using advanced tactics such as fileless malware, living-off-the-land attacks, and AI-driven tools. These sophisticated methods allow malicious activity to blend seamlessly with legitimate behavior, making detection more challenging. Standard detection engines, relying on static rules and signature-based approaches, are no match for these stealthy, dynamic threats.

Manual processes can no longer keep up with the speed and complexity of modern cyber threats. Effective threat detection and response at scale requires AI.

AI enhances TDIR by automating routine tasks, analyzing massive data sets, and identifying anomalies in real time. AI-powered tools:

- Filter out noise and prioritize threats to help analysts focus on the most critical incidents.
- Enable predictive analysis, allowing organizations to anticipate potential attacks and proactively strengthen their defenses.
- Provide the scalability and efficiency needed to process vast amounts of data, correlate disparate signals, and generate actionable insights.

By augmenting human capabilities, AI allows organizations to detect threats faster, reduce response times, and minimize the impact of cyber incidents, ensuring a more resilient security posture.

Components of AI-Powered TDIR

Threat Detection

Threat detection begins with ingesting and normalizing logs across the entire IT infrastructure. This vast well of data provides the perfect fuel for machine learning (ML) models that can serve as the foundation of more advanced threat detection systems. AI algorithms eliminate the need for manual configuration of data from different log sources, normalizing and enriching data with context and making it easier to correlate security events within a security information and event management (SIEM) system.

Correlating security events within a SIEM is the bedrock of efficient investigation and response to threats. Unlike traditional approaches that rely on predefined rules, an AI-powered detection engine leverages automation and advanced AI techniques to correlate diverse metadata. This approach enables real-time detection capabilities that can surface subtle behaviors or anomalies indicating potential security threats — even those that do not match predefined rule sets.

An example of this is user entity and behavior analysis (UEBA) capabilities. Using ML, UEBA builds a profile of normal user and entity behavior and then surfaces any behavior that deviates from the baseline. It detects incidents that rules-based detection engines may miss since it does not rely on predefined rules or attack patterns.

Threat Investigation

The ingestion pipeline of millions of logs gradually becomes security alerts. AI streamlines the investigation process, as the technology can differentiate between legitimate activity and actual threats in real time. AI can prioritize security alerts based on the severity and context, allowing security teams to focus on the most critical threats first. In addition, by learning from historical data, AI minimizes the number of false positives, increasing efficiency.

The AI-powered system can centralize and deduplicate alerts, categorizing them by type and enriching them with contextual insight. By highlighting the key indicators of compromise (IoCs), security teams can quickly pinpoint the source and scope of a threat with less human intervention.

A subfield of AI is natural language processing (NLP), defined as training computers to understand and process human language. Using plain language in searches reduces the need for specialized knowledge of specific query languages, enabling even non-technical users to query data and interpret results easily. NLP assists search engines in understanding and interpreting human language, such as acronyms, abbreviated forms of words, and tactics, techniques, and procedures (TTPs) of threats. It also helps automate the analysis of vast amounts of data, freeing security analysts to focus on high-priority investigations.

Threat hunting, a proactive approach to threat investigation, is when an analyst searches through an organization's network to identify potential malicious activity that automated detection systems may have missed. Threat hunting assumes that attackers have already gained access to a network. A threat hunter will search for evidence of that activity. Vast amounts of unstructured data can easily be searched and enable less experienced analysts the ability to threat hunt.

Most security organizations do not have the resources available to them to build a threat-hunting team. However, with NLP, even a novice analyst can perform sophisticated threat hunting quickly and inexpensively without learning an advanced query language.

Incident Response

The end goal of incident response is to limit the impact of a cyberattack by quickly taking necessary steps to contain the threat. An organization's response strategy should be continuously monitored and updated, including a wide range of incidents.

While many organizations conceptualize incident response through the lens of security orchestration and automated response (SOAR), this perspective is often narrowly defined. SOAR is typically described as an automation approach that helps organizations respond to security incidents more efficiently by reducing detection and response times.

However, the true essence of SOAR lies in security orchestration — a more nuanced concept. At its core, security orchestration is about strategically automating tasks to streamline incident response. It represents the critical ability to execute and coordinate actions across various people and tools within a unified platform, ultimately minimizing the time and complexity involved in addressing security incidents.

Advancements in AI eliminate and reduce tasks associated with security orchestration. With AI, analysts can immediately receive actionable insights to automate manual tasks by suggesting responses to specific threats. AI-powered summaries also help analysts categorize, remediate, and mitigate issues intuitively and easily.

Once a threat is mitigated, it is imperative that organizations document all the actions that were taken — including the "who, what, where, why, and how" — so that the organization can codify strategies for addressing similar threats in the future.

Benefits of AI-Powered TDIR

AI-powered TDIR delivers significant advantages for SOCs. By addressing key challenges, such as growing data volumes, complex threats, and limited resources, AI enables SOCs to operate with greater speed, accuracy, and efficiency.

- **Reduced risk:** AI-powered TDIR helps security teams identify potential threats before they can escalate into full-scale breaches. AI can detect anomalies and malicious activity at the earliest stages by analyzing vast amounts of data in real time and applying predictive algorithms. This proactive approach reduces the risk of significant damage by stopping attacks in their tracks, ensuring that systems remain secure and business operations can continue without disruption.
- **Improved detection fidelity:** Traditional detection methods often rely on static rules or signature-based tools that fail to identify dynamic and sophisticated threats. AI-powered TDIR enhances detection fidelity by incorporating behavioral analytics and contextual insights to distinguish genuine threats from false positives. This level of accuracy ensures that security teams can focus on investigating the most critical incidents, reducing alert fatigue and improving their overall effectiveness.
- **Faster response times:** Responding to cyber threats manually is time-consuming and prone to delays, which can give attackers a significant advantage. AI-powered TDIR streamlines response efforts by automating repetitive tasks, such as data correlation, threat enrichment, and incident prioritization. Additionally, AI provides actionable insights and step-by-step recommendations for containing and mitigating threats, enabling security teams to respond faster and more efficiently to minimize damage.
- **Increased security posture:** AI-powered TDIR strengthens an organization’s security posture by continuously monitoring systems and analyzing behavior across the entire IT environment. AI tools can identify vulnerabilities, assess risk, and enforce consistent security controls across on-premises, cloud, and hybrid infrastructures. This comprehensive approach ensures greater protection of sensitive data, reduces the likelihood of breaches, and enhances overall resilience against cyber threats.

Best Practices for Implementing AI-Powered TDIR

Successfully implementing AI-powered TDIR requires a combination of the right technologies, processes, and strategies to effectively detect, investigate, and respond to threats. Organizations must align their security goals with advanced tools and methodologies to build a robust, AI-driven TDIR framework. By following best practices — including performing security assessments, deploying integrated tools, creating a solid incident response plan, and continuously monitoring for improvement — organizations can maximize the benefits of AI and stay ahead of evolving cyber threats.

Security Assessment

Evaluate your current systems and network to identify vulnerabilities and gaps in security controls. Ensure controls are effective and systems are protected as intended, using tools such as:

- Risk assessments
- Penetration testing
- Network scanning
- Vulnerability assessments
- Threat modeling
- Application security assessments

Deploy Easily Integrated Layered AI-Driven Security Tools

AI-driven tools streamline manual tasks, boost analyst efficiency, and enable proactive TDIR. Choose solutions that integrate seamlessly to strengthen defenses and reduce risk, such as:

- **SIEM:** Automatically collects and analyzes log data across your IT environment to proactively detect, monitor, and respond to threats.
- **UEBA:** Uses ML to establish baseline behavior, identifying anomalies to uncover unknown threats and advanced persistent threats (APTs) while reducing false positives.
- **SOAR:** Automates repetitive tasks and simplifies incident response workflows.
- **Threat Intelligence Platform (TIP):** Provides actionable threat intelligence to enhance detection and response to adversary TTPs.

Develop an Incident Response Plan

Create a clear plan that outlines how the SOC should detect, contain, and recover from cyberattacks. The plan should include roles, responsibilities, escalation steps, and communication protocols for various attack scenarios. This type of planning ensures a swift, coordinated response to minimize damage and restore operations.

Monitor and Improve

Document attack scenarios and keep them updated as new threats emerge. Regularly ensure processes and procedures stay current across the organization.

AI-Powered TDIR with Anomali

Anomali's Security and IT Operations Platform transforms how organizations implement TDIR. The platform, which consolidates ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP in one tech stack, ensures unparalleled efficiency that provides unified data collection, AI-Powered analytics, automated investigations, and streamlined workflows. What sets it apart is its seamless integration of native threat intelligence across every stage of the TDIR process, empowering teams to detect and mitigate threats faster and more effectively than ever before (in multiple languages).

The platform proactively pinpoints IoCs, threat actors, and campaigns within the TDIR process by leveraging native threat intelligence to link adversaries' indicators with their TTPs, driving automated actions for faster and smarter response.

In addition, underlying the Anomali platform is an integrated Data Lake that is not dependent on an external big data provider. In a world of ever-expanding threats of growing sophistication, Anomali's Data Lake provides the ability to ingest terabytes and search seven-plus years of petabytes of structured and unstructured data in seconds, not hours or days.

Reduce the attack surface with Anomali's first-to-market agentless implementation. Your security platform should find the threat, as opposed to being the threat.

Innovative, Effective Technology

An AI-Powered intelligence-driven platform for a more secure world. That's Anomali.

Discover how Anomali can help you implement AI-Powered threat detection, investigation, and response within your organization — schedule a demo.

Security and IT Operations Done Differently.

Anomali delivers the leading AI-Powered Security and IT Operations Platform. Only Anomali integrates ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one powerful platform. At the center is the Anomali Copilot that navigates a proprietary cloud-native security and IT data lake to drive first-in-market speed, scale, and performance at a fraction of the cost. Modernize security and IT operations to protect and accelerate your organization with better analytics, visibility, productivity, and talent retention.

Be Different. Be the Anomali. **Request a demo** to learn more.

ANOMALI