exabeam®

The Ultimate Guide to Threat Detection, Investigation, and Response (TDIR)

eBook

Table of Contents

What Is Threat Detection, Investigation, and Response?

Threat detection, investigation, and response (TDIR) is the prevailing workflow of security operations teams. TDIR combines a collection of cybersecurity practices dedicated to identifying, analyzing, and addressing security threats. It's not just about finding threats; it's also about understanding them and devising effective ways to mitigate their impact and defend against them in the future.

In a recent global study commissioned by Exabeam, IDC estimates that cybersecurity spending reached more than $92 billion in 2022, and is projected to rise to over $170 billion by 2027.[1] Despite substantial investments, 57 percent of respondents encountered significant security incidents in the past year that required additional resources to remediate.

Survey participants highlighted the key challenges in delivering TDIR, with common concerns including, in order:

1. Time-consuming investigation processes
2. Limited visibility into IT environment
3. Lack of knowledge on how to respond to incidents
4. Lack of automation across TDIR workflow
5. Insufficient threat intelligence
6. Complex tooling
7. Lack of skilled personnel
8. Ineffective, manual reporting for stakeholders

Clearly, there is room for improvement in TDIR to address these challenges now and to anticipate future needs.

For example, cybercriminals currently leverage artificial intelligence (AI) for various attacks. Forbes points out instances of malicious actors utilizing AI-powered deepfakes and adaptive malware.[2] AI-related attacks will continue to evolve; who knows what cybercriminals will conceive next? Whether using AI or not, the list of attacks goes on: password cracking, vulnerability scanning, intelligent system weakness detection and exploitation, email compromises, supply chain attacks, ransomware attacks, fraudulent transactions, payment gateway fraud, distributed denial of service (DDoS) attacks, and more. This is all happening today. It's a digital arms race.

TDIR's primary objective is to protect an organization's digital assets and personally identifiable information (PII) from potential adversaries. Achieving this requires deploying a combination of technologies and methodologies designed to detect, investigate, and neutralize threats. Some tools, such as XDR, EDR, and NDR, claim to provide support for TDIR. While they do provide some support, they are limited in their ability to see beyond a single point product or a suite of homogenous products, and often first generation offerings. Security information and event management (SIEM) solutions are the most comprehensive, best known, and most deployed solutions to support TDIR.

[1] Exabeam. (2024, January 30). 2023 Exabeam State of Threat Detection, Investigation, and Response Report. https://www.exabeam.com/tp/2023-tdir-global-report/

[2] Islam, R. (2023, June 23). AI and cybercrime unleash a new era of menacing threats. Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/06/23/ai-and-cybercrime-unleash-a-new-era-of-menacing-threats/

TDIR isn't a simple or one-time process. It demands a continuous cycle of detection, response, and improvement to adapt to constantly changing threats. This Exabeam Ultimate Guide is intended to help you better understand the TDIR workflow, address associated challenges, and deliver more effective outcomes for your organization.

The stages of the TDIR workflow are categorized as:

1. Detection of threats and anomalies
2. Threat investigation, prioritization, and analysis
3. Response, remediation, and lessons learned

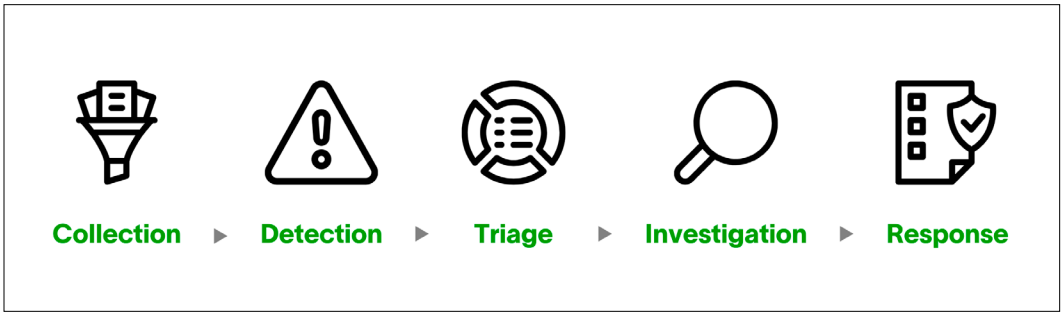


Figure 1. **The stages of the TDIR workflow**

Each stage is interconnected, creating an integrated approach. In modern TDIR, machine learning (ML) and AI play pivotal roles, automating the techniques used in proactive threat hunting and threat detection. In this guide, threat detection refers to the process preceding an alert generated by a SIEM system or other application supporting TDIR. This process includes data onboarding, preparation, and ingestion, rules and correlations, and, for some platforms, behavioral model development, deployment, and learning organizational behavior.

The investigation, prioritization, and analysis stages rely on information gathered during threat detection. Subsequently, the response, remediation, and lessons learned phases all arise from the first two stages of the process.

While each section of this Ultimate Guide is useful on its own, together they offer a more holistic perspective of TDIR today.

In the conclusion of this eBook, we discuss Exabeam and the Exabeam Security Operations Platform. Exabeam is the first company to inject AI and automation into the entire TDIR workflow.

Detecting Threats and Anomalies

Challenges

Security operations teams struggle with alert fatigue. Some alarms are false, others indicate threats to systems not critical to the organization's business model, and some represent serious threats that can pose a material risk to the organization. This problem is exacerbated by the overwhelming volume of alerts, a byproduct of monitoring all possible log streams — this isn't a human-solvable problem. One way an organization can contend with this is to identify and monitor only those log streams they can connect to critical business processes. Some use AI techniques that consume volumes of alerts to learn which are noisy, which are important and which are critical. Unfortunately, this is easier said than done.

Historically, threat detection relied heavily on signatures and correlation requiring the prediction of an attacker's strategy and the implementation of defensive logic accordingly. This was particularly useful, and 100% effective, at detecting explicit attack conditions ("known knowns"), but it falls short when these conditions change. However, while conditions are constantly changing, the underlying attack behaviors are virtually always the same.

The power of AI behind user and entity behavior analytics (UEBA) helps identify the attacks missed by signatures and correlation by learning what normal and abnormal are, and pinpointing the behaviors that might reveal a high risk incident.

Detection isn't just about identifying known threats; it also involves spotting anomalies indicative of previously unknown threats, including zero-day exploits. The incorporation of AI is instrumental in achieving a successful TDIR strategy. While traditional security tools utilize pattern matching and static signature-based detection, an AI-based security solution relies on massive data volumes to generate effective models and dynamic detection engines. This overcomes the obstacles posed by fingerprinting and over-fitted conditions, allowing for detections that would otherwise be impossible.

Threat detection today begins with log ingestion and enrichment, review, management, and analysis. Most organizations use a SIEM platform for this.

SIEM and TDIR

SIEM platforms often play a central role in TDIR by collecting log and event data from on premises and cloud security systems, networks and infrastructure, and turning it into actionable security insights. SIEM technology can help organizations detect threats across different network layers that individual security systems cannot see, investigate past security incidents, perform incident response, and prepare regulation and compliance reports. TDIR is also enabled using XDR products. These are typically limited to a single vendor ecosystem, and have gained limited traction on unseating a SIEM for TDIR.

SIEM comes with a lot of baggage, and for good reason. The product category has a reputation of being dated, expensive, and too complex. The legacy SIEM, still widely deployed in the market, has been upstaged by more modern, cloud-native, next-generation offerings that offer an integrated experience that includes UEBA, security orchestration, automation, and response (SOAR), and, more recently, generative AI capabilities.

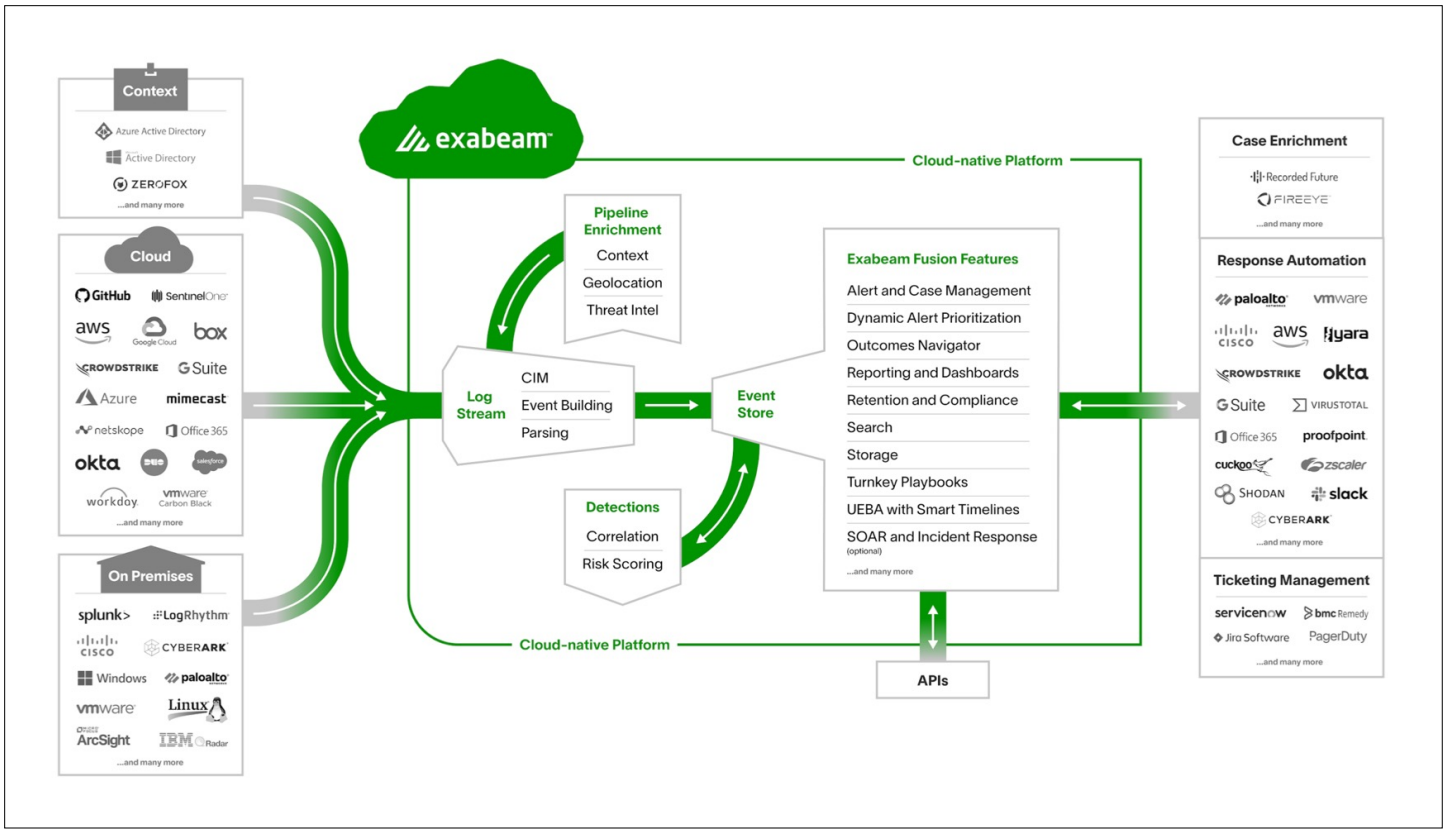


Figure 2. **SIEM logging process**

Data Is the Lifeblood of TDIR

A SIEM, fundamentally, is a log management platform with analytics, reporting, case management, and some automation. Log management involves collecting the data, managing it to enable analysis, and retaining historical data for compliance purposes and threat hunting.

Data Collection

TDIR requires log and event collection from hundreds of organizational systems. Each device generates an event with every occurrence, consolidating these events into a flat log file or database. SIEM tools use four methods to collect data:

1. **Agent installation (most common):** Using an agent installed on the device
2. **Direct device connection:** Establishing a direct connection to the device through network protocols, JSON, or other API calls
3. **Direct access to log files:** Accessing log files directly from storage, typically in Syslog format
4. **Event streaming protocols:** Employing event streaming protocols such as SNMP, Netflow, Kafka, Kinesis, Dataflow, or IPFIX

The SIEM system is tasked with collecting data from the devices, standardizing it, and saving it in a format conducive to thorough analysis. Some vendors incorporate a common information model (CIM) to organize data at ingestion to simplify the normalization, categorization, and transformation of raw log data into actionable events in support of security use cases.

Next-Gen SIEM

Historically, SIEM systems were expensive, monolithic enterprise infrastructures, built with proprietary software and custom hardware provisioned to handle its large data volumes. Along with the broader software industry in general, SIEM systems are evolving into becoming more agile, lightweight, and intelligent solutions.

Next-gen SIEM solutions use a modern architecture that is not only more affordable and easier to implement, but also significantly enhances the capabilities of security teams to discover security issues faster. These SIEM solutions come pre-integrated with common cloud systems and data sources, facilitating direct log data retrieval. Many managed cloud services and SaaS applications prevent installing traditional SIEM collectors, making direct integration between SIEM and cloud systems critical for visibility.

Key features include:

- **Modern data lake technology:** Offering big data storage with massive unlimited scalability, low cost, and improved performance.
- **New managed hosting and management options:** MSSPs are helping organizations implement SIEM by overseeing running parts of the infrastructure, whether on-premises or in the cloud, and by providing expertise to manage security processes.
- **Dynamic scalability and more predictable costs:** SIEM administrators no longer face the arduous task of meticulously calculating sizing calculations and making architectural changes when data volumes grow. SIEM storage can now grow dynamically and predictably expand with increasing volumes.
- **Data enriched with context:** This is essential to deliver more complete detections and helps filter out false alarms. The integration of context in the SIEM enables more precision resulting in more effective detection and response.
- **Pre-integrated with cloud application and cloud security sources:** More and more workloads and applications are moving to the cloud. Having a direct integration between a SIEM and cloud systems is critical for visibility.
- **New insights with UEBA:** Modern SIEM architectures include AI and advanced analytics components like generative AI, ML, and behavioral profiling. These go beyond traditional correlations to discover new relationships and anomalies across expansive huge data sets. Read more in our article on UEBA.
- **Powered incident response:** Modern SIEM solutions leverage SOAR capabilities to automatically respond to security incidents.

Data Management

SIEM systems, especially at large organizations, can store mind-boggling amounts of data. The data must be:

- **Stored:** On-premises, in the cloud, or a combination.
- **Optimized and indexed for purpose:** Enabling more efficient analysis and exploration.
- **Tiered:** Allocating high-performance storage for hot data used in live security monitoring and cost-effective storage for cold data which may be used in future investigations.
- **Enrichment:** This is a critical step for TDIR. Enrichment is the process of adding context to your log data, making it more valuable for detection, privacy, reporting and compliance. Examples of enrichment include threat intelligence, geolocation, and user-host-IP mapping.

Data Storage for TDIR

Next-gen SIEM solutions leverage modern data lake technology like Amazon S3, Hadoop, Google Cloud Storage, or ElasticSearch, providing practically unlimited data storage at low cost.

Log Retention

Adhering to Industry standards (PCI DSS, HIPAA, SOX), requires the retention of logs for periods ranging from one to seven years. Given the substantial volume of logs required for TDIR and generated daily by large enterprises, SIEM systems must adopt intelligent approaches to manage logs for compliance and forensics. Several strategies are employed to reduce log volumes:

- **Syslog servers:** Syslog, a standard for log normalization, retains essential information in a standardized format. This approach enables the compression of logs, allowing for the retention of large volumes of historical data.
- **Deletion schedules:** SIEM tools implement automated deletion schedules to purge old logs no longer needed for compliance. This process involves direct access to log files directly stored typically in Syslog format.
- **Log filtering:** Recognizing that not all logs are essential for compliance or forensics, logs can be selectively filtered based on source system, timestamps, or other rules defined by the SIEM administrator.
- **Summarization:** To maintain only pertinent data elements, such as event counts and unique IPs, log data undergoes summarization, ensuring that crucial information is preserved while reducing overall log volume.

Capturing the Right Data for TDIR

Ideally a system should capture as much data as possible to address the specific use case objectives of an organization. Not all data is security relevant, it's imperative and critical for cost containment to capture the "right" data. Once the right data is confirmed, its journey begins as it flows down an ingestion pipeline, with hundreds of millions of log entries gradually distilled to a handful of actionable security alerts.

Effective TDIR depends on a SIEM tool that will filter out noise, index, and optimize pertinent data to facilitate analysis. Ultimately, only around 1% of data, deemed the most relevant for the organization's security posture, undergoes in-depth correlation and analysis. Those correlations that exceed security thresholds become actionable security alerts.

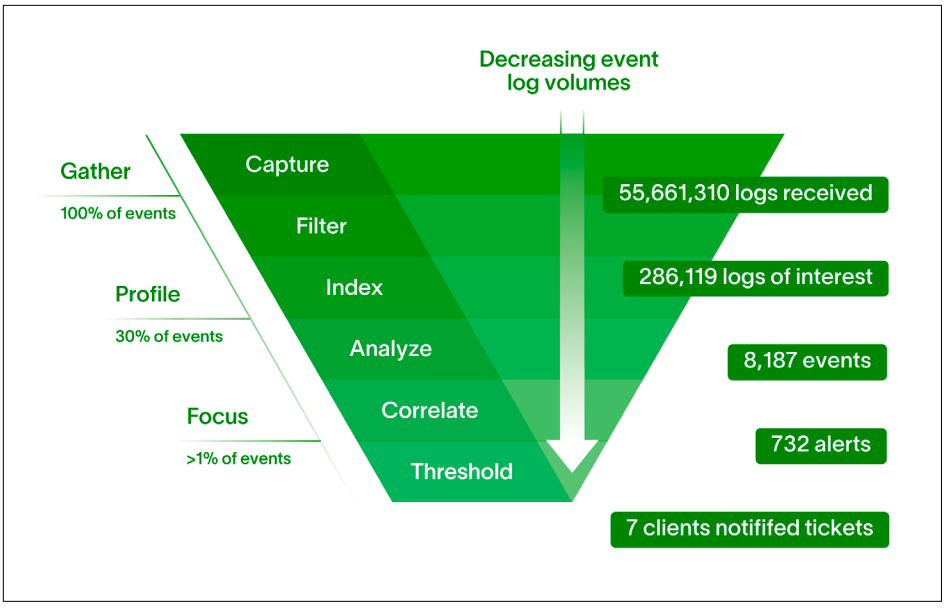


Figure 3. **Event log management and analysis process**

Four Log Management Best Practices to Support TDIR

Log management is a core function of a SOC, defining the depth and scope of the SOC's visibility. Effective log management is essential to threat detection and response, ensuring regulatory compliance, facilitating audits, and enabling forensic analysis of security incidents.

The volume and variety of logs can be overwhelming in a modern, fast-paced business environment. The SOC can quickly accumulate massive log volumes, but not all logs hold equal significance for cybersecurity. Log management helps define and prioritize logs and sources. It also helps maintain the log collection infrastructure.

Many organizations prefer SIEM platforms for TDIR versus standalone log management platforms. A SIEM provides the ability to detect sophisticated threats, provide greater visibility across distributed infrastructures, enable advanced data analytics, and align log coverage with frameworks such as PCI DSS, NIST, and MITRE ATT&CK®. SIEM tools also enable the automation of response actions.

Choose the Right Log Sources

SIEM engineers can collect log data from a myriad of sources, however not all logs are equal and some contain more valuable information than others. Choosing a vendor who focuses on security and business outcomes will ensure log collection is aligned to the needs of both the SOC and the organization.

Identify Requirements for TDIR and Log Management

A critical step in log management for TDIR is to know your needs. This means understanding your organization's business critical functions and researching the dynamic threat landscape to identify how adversaries might leverage new attack vectors and techniques to exploit security vulnerabilities.

First, define your organization's attack surface, security priorities, relevant threat types, and historical correlation requirements to enable threat detection. Next, list the privacy and security regulations applicable to the organization to ensure compliance. You can use preparation lists to inform decisions about the volume of logs you store and manage. You can use the ATT&CK framework to help plan your cybersecurity strategy. And finally, know what you want to report on; the amount of preparation you put into your data ingestion can greatly improve your detection, reporting compliance, and license utilization.

Optimize TDIR Through Your Log Sources

Effective and efficient TDIR requires you to make the most of your security log management effort. Start by integrating the log sources that match your risk register and profile to minimize future issues with log management.

Prioritize and integrate log sources based on the requirements established during integration testing. It is also important to define the rules for log failure alerts and establish the frequency of log collection for important sources. Blindly navigating your log management can result in delays, false negatives, and ineffective reporting. An important best practice is to make informed assessments of the log management platform and data-driven security implementation decisions. Continuously evaluate your log visibility using automated and manual red-team approaches to identify and mitigate new security gaps.

Continuously Improve Your TDIR Effort Using Threat Intelligence

Knowing the threat landscape is key to ensuring effective log visibility, but the modern cybersecurity landscape is constantly changing. Thus, it is important to have a continuous process for adding threat intelligence context into your data ingestion flow.

Infusing threat intelligence into your log collection is akin to equipping your security team with a crystal ball. By enriching logs with external data on attacker tactics, malware signatures, and emerging vulnerabilities, you enable better detections. This transforms raw log entries from mere noise into actionable insights. Imagine suspicious IP addresses instantly linked to known malicious actors, anomalous file accesses tied to specific attack types, and vulnerabilities flagged before they're exploited. This enriched context fuels faster investigations, prioritizes response efforts, and enables proactive threat hunting, ultimately transforming your logs from a historical record into a powerful, real-time shield against evolving threats.

Threat Investigation: Prioritization and Analysis of Threats

Once threats and anomalies have been detected, the next step is to prioritize and analyze them. No organization has unlimited time, money, or workforce to dedicate to cybersecurity. And not all threats pose the same level of risk in terms of effect or impact on the organization, so it's important to determine which ones need immediate attention.

Prioritization involves assessing the potential impact of the threat on the organization's critical operations and data. Analysis involves understanding the nature of the threat, its origin, its current reach and scope, and its potential trajectory. This step is crucial for devising an effective response strategy and ensuring the threat is really expunged from your systems. If your analysis is incomplete, your response will likely be incomplete.

Challenges

Unfortunately, manual threat analysis can be tedious, as much an art as a discipline, and too often undervalued as a skill set. Threat analysts tend to start their careers in security operations centers as Tier 1 analysts before moving upward, and many end up leaving before they find the passion and develop the skill sets and knowledge base — including the aggressive curiosity that helps a threat analyst succeed.

Lack of Standardized Processes for TDIR

Security operations teams have increasingly sophisticated tools that allow them to analyze and investigate security-related events. However, in many organizations, TDIR processes are not well-defined. As a result, different analysts have different ways of analyzing and detecting threats. This wastes time and causes gaps in detection (because some methods might be better than others). Two analysts given the same initial information can, and frequently will, arrive at different outcomes at the end of their analysis based on their different understanding of the network and protocols involved.

In addition, alerts vary in importance, and different vendors use different systems to score risk. So, if an organization's system incorporates a number of vendors, analysts can have trouble prioritizing a number of different alerts because their risk is rated using different criteria. The result is inconsistent and often incomplete investigation processes for TDIR.

Lack of Insights

Another challenge is that many SIEM solutions do not provide insights security teams can immediately act on. They support complex customization, and teams invest major efforts in customizing the SIEM to their particular business needs. However, these installation and configuration delays can slow time to value in security initiatives, and even after the investment, many projects show limited increases in coverage against important threats.

SOCs need a platform that can quickly bring in new log sources and intelligently unify all relevant security data to reveal advanced attackers. As attackers use more sophisticated tactics, techniques, and procedures (TTPs) to exploit vulnerabilities and circumvent traditional security controls, organizations need to protect assets both inside and beyond the network perimeter.

Disjointed Security Stack

Security organizations need integrated, proactive security measures to protect technology assets across traditional endpoints, mobile, and cloud workloads. Adding more point solutions is not viable, because teams then need to learn and become certified on each tool, and more tools will create even more alerts to review and investigate.

Complexity of Security Investigations

Another pain point is the growing complexity of security investigations. Many security and risk managers are implementing threat hunting techniques, actively searching for bad actors such as malicious insiders, lone wolf attackers, cybercriminal syndicates, and state-sponsored attackers.

Working with vendor-provided, siloed security tools makes it difficult to explore data and discover threats. These tools also generate many false alarms and do not integrate well with analytics and incident response tools.

Modern Problems Require Modern SIEM solutions

These challenges gave rise to the development of modern integrated SIEM systems, which consolidate data from across the environment, making it easily accessible to security analysts in one central interface.

Modern SIEM solutions provide end-to-end workflows and analysis packages that make it possible to automate and standardize the TDIR process. This allows teams to derive value from the solution from day one without complex implementation and become more effective at detecting and triaging the most critical threats.

Prioritization

Analysts spend an enormous amount of time pivoting across tools and dashboards to get the relevant information needed to triage alerts and assemble a timeline. This process is not only tedious and time consuming, but is also manual and error prone, contributing to analyst burnout and turnover. The Exabeam 2020 State of the SOC Report revealed that a typical SOC dedicates over 50% of its time to the tasks of alert prioritization and triage.[3]

Automating Triage to Accelerate TDIR

The amount of time invested in this stage of the SOC workflow made it ripe for automation. Triage automation involves bringing the information needed to understand the nature of the alert to the analyst so they don't need to perform mini-investigations for each alert. A triage automation solution should centralize all alerts, aggregate duplicate alerts, categorize them by type, and enrich them with context such as information from a UEBA tool (normal behavior, anomalies, risk scoring) and machine-built timelines.

This provides the analyst all the information they need to make a rapid judgment call — escalate or dismiss the alert — from within a single user interface. From a workflow point of view, any decisions made while triaging must automatically propagate downstream to other systems, for example by creating a ticket in a case management system and prioritizing the relevant data learned in this stage.

[3] Exabeam. (2022, March 11). The Exabeam 2020 State of the SOC Report - Exabeam. https://www.exabeam.com/library/the-exabeam-2020-state-of-the-soc-report/

Automatically Created Threat Timelines Integrate Investigation With Detection

Most enterprise security analysts rely on correlation rules to detect potential threats. For the rules to work, analysts have to know in advance what they're looking for. For example, a rule for a virtual private network (VPN) log might raise an alert if the number of failed logins exceeds 20 times in five minutes. Or for an identity and access management (IAM) log, another rule might entail raising an alert if the same user account is created and deleted within a 24-hour period.

Automatically created threat timelines provide analysts with a better method of TDIR — one that doesn't require prior knowledge of attacker tactics and techniques. With these timeliness, a modern platform pre-processes all logs and combines them with other data sources to detail user and asset activities. This helps identify any anomalous behavior, and thus attacks.

Threat timelines remove the need to build and maintain long lists of correlation rules that need constant tweaking to keep up with network and personnel changes. But they still allow analysts to build rules to create alerts if desired — for example, if they are importing them from a legacy SIEM system.

Threat Timelines Let Analysts Quickly Detect and Respond to Complex Threats

Modern threats come in many forms and can be internal or external to an organization. Insider threats stem from the actions of someone within an organization who, whether unintentionally or with ill intent, exfiltrates data or causes an outage that adversely affects the business. Meanwhile, external threats have become more targeted: For example, malware can be installed inside an organization's network via a phishing attack, leading to a compromised user account.

Both insider and adversary-controlled activities can often be detected via anomalous deviations from users' and devices' historical patterns. By using a unique process to learn from all available log sources, timelines are assembled to help analysts discover such anomalous activities. With timeline automation, a pre-built incident timeline flags anomalies and displays details so analysts can fully scope an event and the severity of its risk.

Timelines enable analysts to detect insider and external threats quickly and accurately, and avoid investing valuable time combing through raw logs to investigate an incident. What used to take days or weeks to investigate using legacy SIEM can now be done in minutes or even seconds. Furthermore, effective timelines serve as an invaluable visualization tool, allowing an analyst to reframe an environment in the context of a single or multiple entities (such as users or devices) over a period of time. This viewpoint helps focus on anomalous actions, which is how humans are wired to interpret behavior. This is presented by an engine that is able to prioritize valuable detections across an entire environment and ignore the noise that represents common, benign behavior.

Automated timelines eliminate the need for analysts to build their own and reduce the need for analysts to "query and pivot" between IT and security applications to collect event details. When timelines are pre-built for all users and devices automatically, analysts can review the activities anytime, whether there is an identified incident or not. For threat hunting and analysis, the dots have already been connected.

Tracking Lateral Movement

A specific challenge in TDIR is identifying lateral movement. Lateral movement is difficult to track, because frequently, logs alone don't contain all of the data analysts need to recreate an attack. For example, consider a user who switches between two accounts while logged onto a single machine. Without timelines that associate events, the "two users" would likely appear completely unrelated and a lateral movement attack would likely be missed. And when the attacker is using valid credentials, as is so often the case, this is usually invisible to legacy tools.

Timelines can follow attacks as they move through organizations. They are able to positively attribute relevant behavior to the responsible user, even when lateral movement is involved. Such activity is then flagged as risky and displayed in a timeline for rapid investigation.

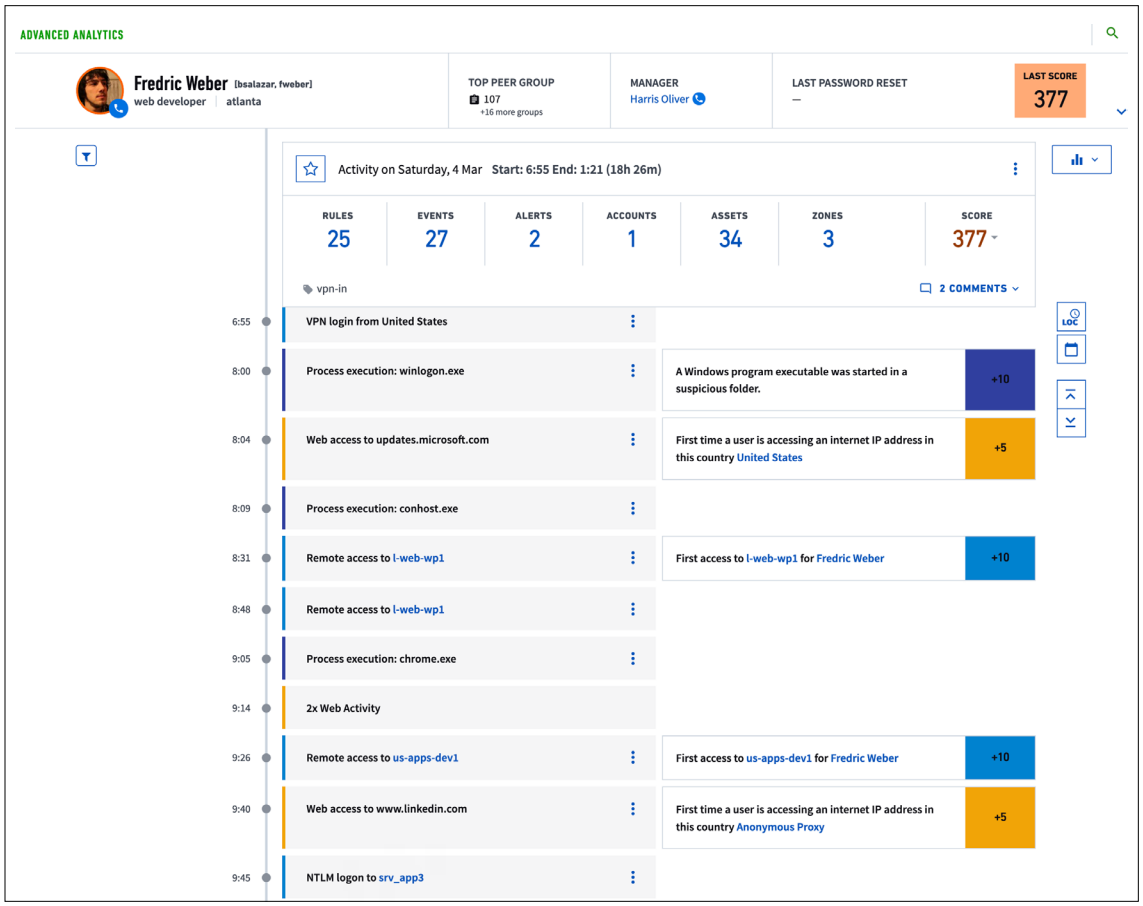


Figure 4. **An automatically created incident timeline for a device,** showing multiple lateral movements as the attacker switches between accounts — including a privileged or executive user account

Figure 5. **Steps to build an automatically created incident timeline**

Deconstructing an Incident Timeline

Collecting Logs

Security management improves as the amount of information available to analysts increases. Large companies and government agencies often log data sources that range from legacy on-premises systems to cloud applications and infrastructure. By enabling organizations to pull a large variety and volume of event data into a central repository, modern TDIR solutions help analysts get the clearest picture of user and device activity in their environment.

Parsing Logs Into Fields

Once collected, the log components must be parsed based on their relevance to security. These relevant components are then identified (tokenized) and broken into fields to permit more accurate and fast better searching, alerting, and reporting.

Creating Events by Combining Log Fields

The next step to build a timeline is to identify events — actions that occur at points in time — to normalize log information and make it easy for analysts to quickly understand what a user or device did. To create an event, the timeline should combine relevant parts of a log or multiple logs.

Adding Context While Creating Events

Often, data from log fields tells only part of the story. Adding missing information to the log source such as host or IP name, or a threat intelligence IoC, helps improve analysts' understanding of what took place. For example, most systems identify new users by their Active Directory (AD) account. Some systems use an email address to identify new users; others may use an organizational role to identify new users. A well-constructed timeline would map emails and user hierarchy to AD accounts, adding a new "user" field to augment the original log. Context data is equally important in its unique ability to correlate seemingly disparate events. As logs are far from universal in nature, the ability to connect an event together based on an entity attribute (for example a user's principal name [UPN] versus just the email address) can be the difference between a missed and identified detection.

Automatically created incident timelines frequently build data graphs that automatically fill in missing holes in log data in real time. Data graphs can be useful for identifying lateral movement, especially when enriched with context from UEBA.

Events might include:

- User creation
- Remote logins
- Data loss protection alerts
- Inbound/outbound emails of unusual size
- First-time processes on systems
- And more

Creating Sessions

These named events are then grouped into user sessions that form the timelines. Sessions can be opened and closed based on behavioral conditions (such as logging into a laptop), or by a configurable set of logical conditions. Sessions organize events in sequence; they also put time-based boundaries around behavior to establish a normal behavior baseline. A typical session might comprise a work day, during which a user's or device's activities are tracked through the network environment. Organizing events into sessions provides analysts with considerably more context for TDIR than if they were to look at a single event in isolation.

Modeling Behavior and Normal Activity

To develop a baseline of normal, ML models and rules are generated against raw events, which are then represented or displayed in a timeline. The models can automatically determine when they have sufficient relevant data to accurately classify a given behavior as anomalous. User and device norms can typically be set with only a few weeks of data.

Detecting Anomalies

A single anomalous model usually doesn't trigger an alert. Instead, various anomalous models in different dimensions, such as time, location, and activity level, are usually required to trigger an alert. This approach reduces the number of false alarms. Instead, each anomalous model the system applies adds to the overall risk score for a given session. If the total exceeds a predetermined value in a timeline, the system triggers an alert. For example, an alert could be triggered as a result of a user logging in at an unusual time, from an unusual place, or being active on an atypically large or small number of machines. Instead of static rules that must be maintained, timelines are heavily weighted toward models to improve analysts' ability to detect the threats commonly overlooked by other tools.

False Alarms

Mitigating and managing false alarms has become a priority for most security teams. Each false alarm consumes analysts' time and distracts them from investigating real security incidents. Timelines dramatically reduce the number of false alarms by requiring anomalies in multiple dimensions before triggering an alert.

The underlying timeline models also calibrate the score of anomalous events based on contextual factors — including an understanding of roles, groups, and normal behavior. For example, having learned from historical access patterns and other contextual information, the models can reduce false alarms when users access a resource for the first time. Yet system control remains flexible. For example, analysts can mute certain anomaly alerts, such as policy violations they don't consider to be security threats.

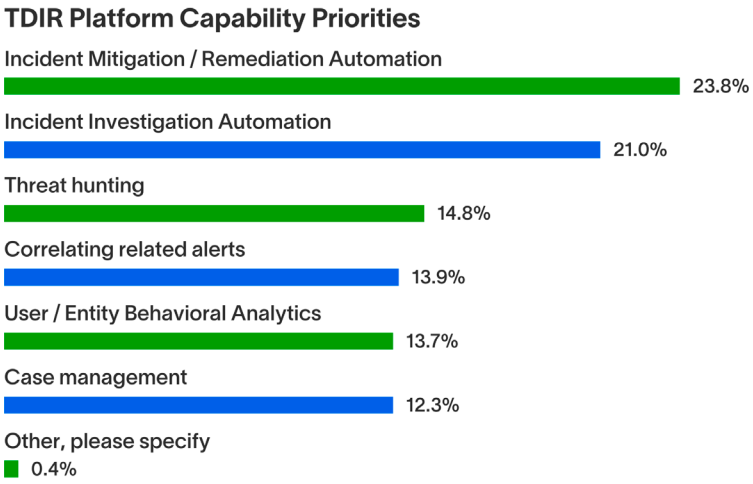
Scoring Risk Due to Anomalous Activity

With timelines, user-specific models assign risk scores for those whose observed event patterns sufficiently differ from their own past patterns. Cross-user comparisons are also made to normalize behavior. Not all event anomalies are given equal importance. (Anomalies due to changes in common events, such as a user logging into a device, are typically less interesting than rarer events, such as an account password change or a new user being added.) Thresholds are established for different types of events. For example, a higher risk score would likely be generated if a user logs into a device (such as a server) for the first time, coupled with a high volume of privileged activities (such as account switching or obtaining privileged access). In both examples, the risk score increases if these actions are performed on a critical server.

Using Timelines for Investigations and Response

Automatically created incident timelines accelerate TDIR and are designed with analysts in mind. They should have an intuitive user interface (UI) and not require knowledge of data science. This enables more junior analysts to perform investigations that might have otherwise required a senior analyst's attention. This is especially important in a time when skills are short and experience limited. To conduct an investigation, an analyst can review timelines for a user or device, clicking on specific events to glean additional information, all the while staying within the single user interface. An analyst of any level can simply enter a user name and a date to instantly see everything that user did that day.

Using automation and moving away from manual investigations reduces analysis time from days to minutes, or even seconds. Without any additional effort, analysts can also look at timelines for adjacent days and related users or assets. In the 2023 Exabeam State of TDIR Report, respondents identified investigation and remediation automation capabilities as their foremost priorities for a TDIR platform[4].



Source: IDC's *Global TDIR Survey*, commissioned by Exabeam, August–September 2023, n = 1,155

Figure 6. **TDIR platform capability priorities**

[4] Exabeam. (2024, February 8). 2023 TDIR Global Report - Exabeam. https://www.exabeam.com/tp/2023-tdir-global-report/

Timelines Ease Hunting for Complex Threats

Analysts can use timelines to detect attackers' TTPs by hunting behavior anomalies mapped to the ATT&CK framework. And they can search for a specific TTP. They also don't have to write complex queries to look for indicators of compromise (IoCs). An example of this type of search criteria might be:

Lateral movement tactics:

- A possible pass-the-hash attack from the source
- The first account management activity from an asset
- The first account management activity from an asset for a specific user
- The first remote login to an asset
- A service account that has logged into more than 30 assets

Privilege escalation tactics:

- An account switch to a privileged or executive account
- A non-executive user login to an executive asset
- An abnormal addition to a privileged group by user

Automated Timelines Summary

Not all timelines are created equal. They are not just a collection of logs sorted by their timestamp. To be as effective as possible and fully support TDIR, an automated timeline requires several key attributes:

- It must be able to merge and normalize raw, often cryptic logs into easy-to-understand, human-readable events. This is particularly true for AD events.
- It must show user and machine events regardless of log sources. To do so, the underlying process must convert log fields into user activities. This is usually not a one-to-one translation of a log field into an event, but involves combining logs and adding context.
- It must be able to determine the beginning and end of user or entity activity, mapping it to sessions so as to normalize behavior.
- It must annotate each event with possible anomalies associated with it (relative to the user or entity history), and do so in a way that minimizes false positives.
- It must be able to identify and group all events belonging to a user regardless of whether the person moved laterally through various devices or switched identities.
- It must present and score events that exhibit anomalous user behaviors.

Response, Remediation, and Lessons Learned

The aim of incident response is to identify the scope of the events, contain the damage, and mitigate or eradicate the root cause of the incident — all essential to delivering TDIR. An incident represents a change in security posture potentially in breach of law or policy, or a threat to information assets, such as networks, computers, or smartphones — which may or may not be materially reportable.

Why Is Incident Response Important?

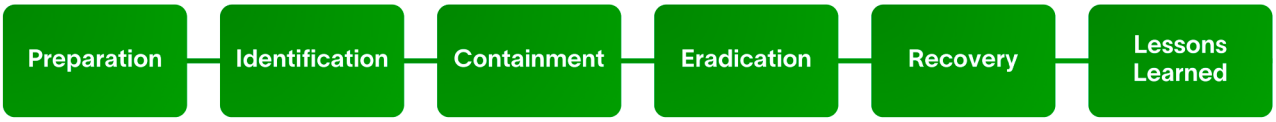
When your organization responds to an incident consistently and quickly, it can reduce losses, restore processes and services, reduce the scope or effects, and mitigate exploited vulnerabilities. An incident that is not effectively managed can lead to a data breach with potentially catastrophic consequences, such as data loss, system crashes, and expensive remediation — or even external financial penalties depending on the type of incident and the industry involved. Incident response provides this first line of defense against security incidents, and in the long term helps support a set of TDIR best practices to prevent breaches before they happen.

An incident response plan helps prepare your organization for both known and unknown risks. Consistent incident response procedures will allow you to manage security incidents when they occur and implement best practices to block further intrusion. Incident response is essential for maintaining business continuity and protecting your sensitive data.

Your response strategy should anticipate a broad range of incidents. Even simple incidents can impact your organization's operations and reputation long term. TDIR is a methodical process, and the time you invest upfront preparing for response will yield huge dividends when a threat turns into an incident.

The Six Steps of Incident Response

Following are the six steps we recommend for incident response:



1. Preparation

Here are steps your organization should take to prepare for cybersecurity incidents:

- Form an internal incident response team, define executive sponsors, and develop policies to implement during a cyberattack. Review the tools needed to defend against each incident type and centralize their management.
- Review security policies and conduct risk assessments modeled against external attacks, internal misuse/insider attacks, and situations where there are external reports of potential vulnerabilities and exploits. NIST provides a good framework.[5]
- Prioritize known security issues or vulnerabilities that cannot be immediately remediated — know your most valuable assets, so you can concentrate on critical security incidents against critical infrastructure and data. You likely have done this when building out your use cases.
- Develop a communication plan for internal, external, and (if necessary) public breach reporting. In the USA, for example, The Securities and Exchange Commission has imposed requirements for publicly-traded companies to disclose cyberattacks within four business days after determining they are material incidents.
- Outline the roles, responsibilities, and procedures of the immediate incident response team, and the extended organizational awareness, operational, or training needs.
- Recruit and train team members, and ensure they have access to relevant systems, technologies, and tools.
- Plan education for the extended organization and test that education and preparedness at least annually. Make sure security and awareness training is part of all onboarding activities at every level, and set up a mechanism through which anyone can report a suspected security event.
- Review your software supply chain and inform vendors and partner affiliates on how to report potential security incidents or information. This should be part of their negotiation and master services agreements.

[5] Initiative, J. T. F. T. (2012). Guide for conducting risk assessments. https://doi.org/10.6028/nist.sp.800-30r1

2. Identification

Decide what criteria call the incident response team into action, and create a triage or information gathering document for the focal point. If, for instance, all security incidents are reported to the security operations team, the analysts on duty will need to know how to ask the right questions to perform basic triage.

Modern SIEM solutions gather events from monitoring tools, log files, error messages, firewalls, and intrusion detection systems (IDSs). This data should be analyzed by automated tools and security analysts to decide if anomalous events represent security incidents. For example, just seeing someone hammering against a web server isn't a guarantee of compromise. Security analysts should look for multiple factors, changes in behavior, outbound traffic, and new event types being generated.

When an incident is isolated, the incident response team should be alerted. Team members coordinate the appropriate response to the incident:

- Identify and assess the incident and investigate to gather evidence.
- Decide on the severity and type of the incident and escalate, if necessary.
- Document all actions taken, including when all communication occurred, addressing "who, what, where, why, and how." This information will be used later as evidence, if the incident reaches a court of law.

Keep in mind that every step of awareness and investigation, from logs to emails, phone calls, and personnel involved, become part of the record of investigation. Make sure that your incident response teams and security analysts understand the importance of recording the name, dates, times, and communications to every person involved throughout this process.

3. Containment

Once your team isolates a security incident, the aim is to stop further damage. This includes:

- **Short-term containment:** An instant response, so the threat doesn't cause further damage. This can include taking down production servers that have been breached or isolating a network segment that is under attack.
- **Communication to anyone who could potentially be involved.** If there is an outbreak of ransomware, plugging into the system in the morning could prove dangerous and increase the scope, depending on the timing. Have a methodology of reaching all employees to inform them of safe practices for their work day during an incident.
- **System backup:** You should back up all affected systems before you wipe and reimage them to acquire a "current state" or forensic image. A forensic image is a bit-for-bit copy of a hard disk, or a specific disk partition. Disk images are created after an incident to maintain the state of a disk at a specific point in time and thus provide a static snapshot, which you can use as evidence of the security incident, and to investigate how the system was compromised.
- **Long-term containment:** While making temporary fixes to replace systems that have been taken down to image and restore, rebuild clean systems so you can bring them online in the recovery stage. Take measures to prevent the incident from recurring or escalating: install any security patches on affected and associated systems, remove accounts and backdoors created by attackers, alter firewall rules, and change the routes to null route the attacker addressed, etc.
- **Create scope documentation:** It is important to know precisely which credentials, service accounts, endpoints, servers, etc. were involved in the incident. It's also important to establish a place for storing disk images, lists, and reports for a clean chain of investigation and evidence preservation.

4. Eradication

Contain the threat and restore initial systems to their initial state, or close to it. The team should isolate the root cause of the attack, remove threats and malware, and identify and mitigate vulnerabilities that were exploited to stop future attacks. These steps may change the configuration of the organization. The aim is to make changes while minimizing the effect on the operations of the organization. You can achieve this by stopping the bleeding and limiting the amount of data that is exposed.

This is done as follows:

- Identify and fix all affected hosts, including hosts inside and outside your organization
- Isolate the root of the attack to remove all instances of the software or update to the latest patch levels
- Conduct malware analysis to determine the extent of the damage
- See if the attacker has reacted to your actions. Check for any new credentials created or permission escalations going back to the publication of any public exploits or POCs
- Make sure no secondary infections have occurred, and if so, remove them
- Allow time to make sure the network is secure and that there is no further activity from the attacker(s)

Ensure your team has removed malicious content and checked that the affected systems are clean. For example, if the attacker used a vulnerability, it should be patched. Or if an attacker exploited a weak authentication mechanism, it should be replaced with strong authentication. This may require heavy cooperation among architecture, operations, and engineering teams, so make sure they are all included in your communication plan.

5. Recovery

The purpose of this phase is to bring affected systems back into the production environment carefully to ensure they will not fall prey to another attack. Always restore systems from clean backups, replacing compromised files or containers with clean versions, rebuilding systems from scratch, installing patches, changing passwords, and reinforcing network perimeter security, (for example, boundary router access control lists and firewall rulesets).

Decide how long you need to monitor the affected network and endpoint systems, and how to verify that the affected systems are functioning normally. Calculate the cost of the breach and associated damages in productivity lost, and human hours to troubleshoot and take steps to restore, and recover fully.

6. Lessons Learned

Recovery involves restoring business operations to normal and addressing any residual effects of the threat. Learning, on the other hand, involves conducting a post-incident analysis to understand what went wrong and how to prevent similar incidents in the future through process, technology, tools, and improved procedures.

After any incident, it's important to hold a debriefing or lessons-learned meeting to capture what happened, explore what went well (or poorly — you need to be honest with your own teams and sponsors), and evaluate the potential for improving the organization's defenses and response processes. This can also involve bringing in new security and system logs to get a wider view of the use case, or improving coverage in visibility or rule sets and anomaly detection to prevent similar incidents in the future. Review what actions were taken to recover the attacked system, the areas where the response team needs improvement, and the areas where they were effective.

Reports on lessons learned provide a clear review of the entire incident and can be used in meetings, as benchmarks for comparison, and as training information for new incident response team members. Once a lessons-learned report has been completed, it can be used to facilitate communication between the incident response team and stakeholders to improve future processes.

The Computer Security Incident Response Team (CSIRT)

To prepare for and attend to incidents, it may be helpful to form a centralized incident response team, responsible for identifying security breaches and taking responsive actions. In a large organization, this is a dedicated team known as a CSIRT. The CSIRT includes full-time security staff — including any specialized insider threat teams. These individuals analyze information about an incident and respond.

In a smaller organization, the incident response team can consist of IT staff with some security training, augmented by in-house or outsourced security experts.

The incident response team also communicates with stakeholders within the organization, and is involved with offering preliminary written communication with external groups such as press, legal counsel, affected customers, and law enforcement.

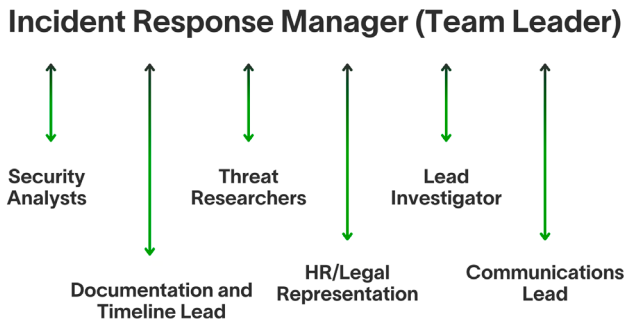


Figure 7. **The CSIRT**

The team should include some of the following (depending on size and needs):

- **Incident response manager (team leader):** Coordinates all team actions and ensures the team focuses on minimizing damages and recovering quickly. Prioritizes actions during the isolation, analysis, and containment of an incident. Oversees all actions and guides the team during high severity incidents.
- **Security analysts:** The manager is assisted by a team of security analysts who work across departments to isolate and rectify flaws in the organization's security systems, solutions, and applications. They recommend specific measures to improve the overall security posture.
- **Lead investigator:** Isolates root cause, analyzes all evidence, manages other security analysts, and conducts rapid system and service recovery.
- **Threat researchers:** Provide the context of an incident and threat intelligence. They use this information and records of previous incidents to create a database of internal intelligence.
- **Communications lead:** Communicates with all audiences inside and outside the company, including management, internal stakeholders, executives and/or board members, legal, press, and customers.
- **Documentation and timeline lead:** Documents team investigation, discovery, and recovery efforts. And, creates a timeline for each stage of the incident. Next-gen SIEM systems are able to generate documentation and incident timelines (see timelines above) automatically.
- **HR/legal representation:** There is the possibility that an incident could eventually involve criminal charges. (This is also why it is critical to maintain a clean chain of evidence and record of investigation.) Thus, you should have HR and legal guidance, especially if you engage secondary or external incident response professional services. There are limits to what an investigator can do. For instance, reading private emails on a person's computer is generally not allowed due to privacy concerns.

Incident Response Tools and Technologies

SIEM

As discussed above, SIEM solutions collect and aggregate log data generated by applications, servers, and network devices in an organization's IT environment. This data is then analyzed and correlated to identify patterns that could indicate a security incident.

SIEM tools not only help detect potential threats but also aid in incident response by providing actionable intelligence. They generate alerts based on predefined rules and severity levels, enabling security teams to prioritize and respond to incidents more effectively. Moreover, SIEM solutions support compliance reporting by providing evidence of security measures.

SOAR

SOAR capabilities allow an organization to collect data about security threats from multiple sources and respond to security events with little to no human assistance.

SOAR tools can automate common response actions, reducing the number of manual tasks that security teams need to perform. They can also streamline incident response workflows, making it easier for teams to track, manage, and resolve incidents. Additionally, SOAR tools can integrate with a wide range of security tools, providing a centralized platform for managing incident response. Because most organizations don't need a standalone solution, over the years SOAR capabilities have been absorbed into many SIEM platforms.

Playbooks

SOAR-powered playbooks can facilitate rapid responses that can disrupt ransomware kill chains and other attack types. These playbooks string together complex workflows, such as detonating a file in a sandbox and, based on the results, quarantine affected endpoints or block access to command and control servers. Security analysts can define triggers to automatically activate a playbook as soon as ransomware is detected, disrupting the kill chain and containing infections within minutes.

UEBA

UEBA learns the normal user, device, and peer group behavior, and detects deviations. These tools use machine learning AI, algorithms, and statistical analyses to detect meaningful anomalies within an IT environment.

In incident response, UEBA tools can help security teams identify unusual or suspicious behavior that may indicate a security incident. For instance, if a user suddenly starts accessing sensitive data they don't normally interact with, this could be a sign of an insider threat or a compromised account. By detecting such anomalies, UEBA tools can help teams respond to incidents before they result in significant damage.

Many modern SIEM platforms incorporate UEBA, but leading solutions provide an integrated experience, connecting UEBA capabilities into the SIEM within a single interface.

IPS and IDS

Intrusion prevention systems (IPSs) and IDSs are tools designed to detect and prevent security incidents. IDS monitors network traffic packets for signs of potential incidents, such as malicious payloads or suspicious behavior. If an incident is detected, IDS will send an alert to the security team.

On the other hand, IPS goes a step further by actively preventing incidents. For example, if an IPS detects an attempted security breach, it can take action to block the attack, such as by closing network connections or changing firewall rules.

Five Tips for Successful Incident Response

1. Isolate Exceptions

Technology alone cannot successfully detect security breaches. You should also rely on human insight. Following are a few conditions to watch for daily:

- **Traffic anomalies** — Sensitive connections and servers used internally will typically have a stable traffic volume. If you notice a sudden increase or decrease in monitored traffic — and either can be suspicious — take notice.
- **Accessing accounts without permission** — Privileged or administrator accounts have access to more information and systems than normal employees. However, employees tend to be the easiest entry point for cybercrime. Closely monitor privileged accounts and watch for privilege escalation on normal user accounts. Privilege escalation is a common malware trait, and should be identified quickly via rules or anomalies.
- **Excessive consumption and suspicious files** — If you see an increase in the performance of the memory or hard drives of your company, it could be that someone is illegally accessing them or leaking data.

Modern security tools such as UEBA automate these processes and can identify anomalies in user behavior or file access automatically. This provides much better coverage of possible security incidents and saves security teams' time.

2. Use a Centralized Approach

Gather information from security tools and IT systems and keep it in a central location, such as a SIEM solution. Use this information to create an incident timeline, and conduct an investigation of the incident with all relevant data points in one place.

You can also use a centralized approach to allow for a quick automated response. Use data from security tools, apply advanced analytics, and orchestrate automated responses on systems like firewalls and email servers, using technology like SOAR.

3. Assert, Don't Assume

Don't conduct an investigation based on the assumption that an event or incident exists. Instead of making assumptions, make assertions based on a question that you can evaluate and verify. For example "If I've noted alert X on system Y, I should also see event Z occur in close proximity."

Create your assertions based on your experience administering systems, writing software, configuring networks, building systems, and so forth. Imagine your systems and processes from the attacker's eyes.

4. Eliminate Impossible Events

You may not know exactly what you are looking for. On these occasions, eliminate occurrences that can be logically explained. You will then be left with the events that have no clear explanation. These are often represented at the start of incident triage calls, when people report symptoms without knowing what has caused them.

For example:

- Unexplained inconsistencies or redundancies in your code
- Issues with accessing management functions or administrative logins
- Unexplained changes in volume of traffic (like drastic drop)
- Unexplained changes in the content, layout, or design of your site
- Performance problems affecting the accessibility and availability of your website or resources

5. Take Post-Incident Measures

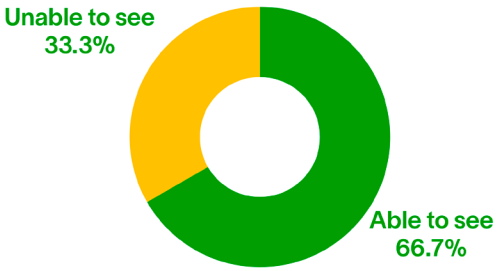
Continue monitoring your systems for any unusual behavior to ensure the intruder has not returned. Watch for new incidents and conduct a post-incident review to isolate any problems experienced during the execution of the incident response plan.

Achieving Security Operations Excellence

Throughout this guide, we have emphasized the essential role that TDIR plays in cybersecurity. It forms the foundation of security operations, and our insights from the 2023 Exabeam State of TDIR Report show that progress has been made, yet significant challenges remain.

One primary area needing improvement is automation. More than half of organizations have automated only half of their TDIR workflows, highlighting the need for greater efficiency and streamlined processes.

Visibility is another critical concern. Organizations can only see 66% of their IT environment, leaving gaps in security operations. Improved monitoring and surveillance capabilities are necessary.



Source: IDC's *Global TDIR Survey*, commissioned by Exabeam, August–September 2023, n = 1,155

Figure 9. **IT environment visibility**

Figure 8. **TDIR workflow automation**

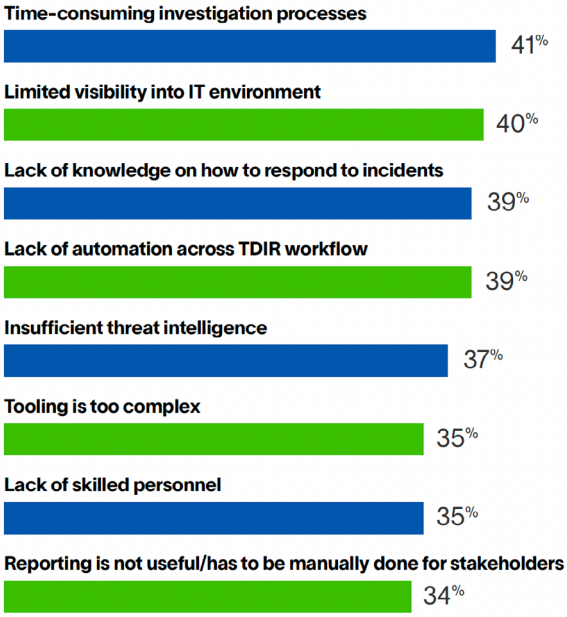
Source: IDC's *Global TDIR Survey*, commissioned by Exabeam, August–September 2023, n = 1,155

Advanced analytics also pose a challenge. Around 35% of organizations require assistance in understanding normal user, entity, and peer group behavior, reflecting the increasing complexity of cyberthreats.

Perhaps the most urgent issue is the need to improve investigation skills. A concerning 41% of respondents report time-consuming investigation processes, with all respondents stating that over half of their security teams' time is spent on TDIR. Investigation automation was reported as a top priority in TDIR platforms.

Clearly, there are ample opportunities for improvement in TDIR, which is critical for addressing these challenges and preparing for future demands.

We trust that this guide has effectively highlighted the importance of TDIR and provided actionable steps for your organization to confidently strengthen its security posture.



Source: IDC's *Global TDIR Survey*, commissioned by Exabeam, August–September 2023, n = 1,155

Figure 10. **Areas needing most assistance in TDIR**

Source: IDC's *Global TDIR Survey*, commissioned by Exabeam, August–September 2023, n = 1,155

Figure 4. **Top TDIR delivery challenges**

The AI-Driven Security Operations Platform

The Exabeam Security Operations Platform applies AI and automation to security operations workflows for a holistic approach to combat cyberthreats, delivering the most effective threat detection, investigation, and response (TDIR). AI-driven detections pinpoint high-risk threats by learning normal behavior of users and entities and prioritizing threats with context-aware risk scoring. Automated investigations simplify security operations, correlating disparate data to create threat timelines. Playbooks document workflows and standardize activity to speed investigation and response. Visualizations map coverage against the most strategic outcomes and frameworks to close data and detection gaps. Exabeam empowers security operations teams to achieve faster, more accurate, and consistent TDIR.

Whether you replace a legacy product with a SIEM, or complement an ineffective SIEM solution by adding the industry's most powerful UEBA and automation to it, the Exabeam Security Operations Platform can help you achieve security operations success.

About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. The company was the first to put AI and machine learning in its products to deliver behavioral analytics on top of security information and event management (SIEM). Today, the Exabeam Security Operations Platform includes cloud-scale security log management and SIEM, powerful behavioral analytics, and automated threat detection, investigation, and response (TDIR). Its cloud-native product portfolio helps organizations detect threats, defend against cyberattacks, and defeat adversaries. Exabeam learns normal behavior and automatically detects risky or suspicious activity so security teams can take action for faster, more complete response and repeatable security outcomes.