SWIMLANE

TDIR:

A Security Guide to Threat Detection and Incident Response

Understanding TDIR: Threat Detection and Incident Response

The Current State of Security

The increasing dependence of businesses on online accessibility and the cloud to provide services has driven the rapid rise of threat actors and with it the number of security incidents. Business email compromise is the most damaging type of incident with complaints to the FBI accounting for nearly $2.4 billion in 2021. In addition, the past several years have seen an exponential rise in advanced persistent threats (APTs) distinguished by sophisticated attackers using complex and often tailor-made malware and exploit chains to achieve their objectives. There has been a corresponding and unsettling rise in ransomware incidents and supply chain compromises.

Compounding the problem, the telemetry security teams need to detect incidents comes from a multitude of heterogeneous sensor types that provide an overwhelming amount of data. Several vendors have developed solutions to make the flood of alerts and other event data more manageable. We'll look at two families of solutions that use enrichment and automation to achieve this: Threat Detection and Incident Response (TDIR) and Security Orchestration Automation and Response (SOAR). There is some overlap in the functionality of these two products, but they are both integral to a well-functioning incident response plan.

What is TDIR?

Threat Detection and Incident Response

Threat Detection and Incident Response (TDIR) is an outcomes-oriented methodology which combines capabilities that are traditionally associated with security operations center (SOC) products like security information and event management (SIEM), security orchestration automation and response (SOAR), user and entity behavior analytics (UEBA), and Threat Intelligence into a solution for improving detection and response KPI's for the modern enterprise. Extended detection and response (XDR), security analytics platforms, and next-generation SIEMs are typically associated with TDIR. They have a similar set of capabilities and are the direct descendents of older detection tools. They differ from older tools by presenting a more holistic view of an incident by correlating events from multiple sources and enriching incident data with threat intelligence and additional analytics. Automation of certain response actions is made more feasible by the more valuable contextual information available in the tool.

What is SOAR?

Security Orchestration, Automation, and Response

SOAR is a term that is often used to describe a variety of functions in several different solutions. Generally, a SOAR performs some activities related to security incident response, orchestration and automation, and threat intelligence. Much of the value of true SOAR products are that they are vendor agnostic and extremely flexible tools which focus on connecting integrated data from disparate security systems to incident response playbooks which can be fully or partially automated. By focusing on processes codified in playbooks, SOAR platforms enable security teams to:

- Automate common tasks saving valuable analyst time
- Standardize and ensure the implementation of best practices
- Collect and report on analyst generated telemetry to gain insights on the effectiveness of processes

Crucially, the same playbook logic and processes can be used regardless of the specific vendor used in a role. Documenting and reporting on investigations is particularly useful since this is a hugely important process and one that takes a great deal of analysts time. Integration of reporting and record-keeping allows analysts to focus on investigations rather than formatting reports. Well-organized records of investigations are crucial in root-cause analysis.

Low-code security automation solutions usher in the next generation of SOAR products, such as Swimlane Turbine, which use sensors at the edge of an active sensing fabric to drive alert enrichment, automated incident response, and reporting.

The flexibility of SOAR tools means they have even found applications outside of security and IT. However, if we just focus on security and specifically TDIR, it's important to look at the whole incident response process of which TDIR is a part. TDIR capabilities are an important piece of an incident response plan, but an incident response plan encompasses much more than detecting threats and creating alerts with correlated data or taking scripted actions in response to some predefined detections.

How do TDIR and SOAR fit into an Incident Response Plan?

In the context of an incident response plan, an incident is an adverse event that might result in unauthorized disclosure, modification, or destruction of resources and the aim of an incident response plan is to prevent or mitigate those events while also adhering to any compliance requirements. Governmental and industry bodies such as NIST, CREST, SANS, and ISC2 have developed several incident response models to help organizations implement effective incident response strategies. They differ in terminology and in how specific steps are grouped conceptually, but generally describe the same process. Getting into the details of these models could easily fill a book, so, for the sake of brevity, we'll loosely base further discussion on the model described in NIST 800-61.

Preparation

- Write documentation and ensure up-to-date contact lists
- Complete and record user training
- Conduct regular incident response drills
- Implement hardening checklists
- Asset management
- Perform risk assessments regularly

Detection & Analysis

- Identification of the incident
- Discover indicators of potential compromise using security telemetry from sensors
- Analyze the incident and determine scope, impact, and source
- Document all findings
- Notify relevant parties

Containment, Eradication, & Recovery

- Prevent any further attacker activity
- Collect evidence
- Return systems to normal operation
- Patch and harden system against the recent attack

Post-incident Activity

- Generate incident response report from documented findings (who, what, where, when, why, and how)
- Hold a lessons learned meeting to discuss the incident and any discovered deficiencies in the process

Incident Response in More Detail

Preparation:

Preparation is key to an effective security process. Planning and implementing a successful strategy requires adequate understanding of the attack surface, anticipation of the threats the organization is likely to face, and visibility. In order to develop the understanding of threats needed to effectively direct and prioritize threats, many security teams use risk assessments, inventories of physical and software assets, and threat modeling sessions. Other tools that are helpful at this time include IT asset management(ITAM) and vulnerability scanners. SOAR technologies are useful in this stage by integrating with ITAM, CMDB, vulnerability management, and other tools along with any manual reports, audits, or risk assessments. For example, a SOC could create a playbook to test security controls, implement human-in-the loop automation for security hardening guidelines, or enrich asset management reports with associated user information from IAM solutions.

Detection & Analysis:

Many security solutions have been developed to facilitate the detection and analysis of threats. Traditional SIEMs have given security teams a way to manage the deluge of events coming from a diversity of network-based and host-based sensors. The sophistication and prevalence of firewall logs, EDRs, authentication, OS, and application logs have given security teams greater context and enabled more intelligent analysis. Given their ancestry, it is unsurprising that the XDR and security analytics platforms share a focus on detection and analysis.

Detection is most often achieved using detection rules in security sensors to identify potential security incidents, but can also include proactive threat hunting through security logs as well. XDR solutions give analysts much more power to search and create intelligent detections by virtue of the common data model used by the vendor-specific sensors. This also allows the tools to become much more accurate in identifying true positive incidents. Security analytics platforms and next-generation SIEMs can also find salient features in an event stream with greater accuracy and can take some remedial steps based on the category of incident detected.

Legacy SOAR solutions don't attempt to detect security incidents directly, and instead focus on enriching detected incidents with threat intelligence, previously conducted analyses, and by querying other sources. Unlike traditional SOAR tools, Turbine uses remote agents to receive high throughput event streams which could be used to create novel detections as well. Additionally, by incorporating case management, Turbine easily fills the need to document findings and notify stakeholders of developments.

Containment & Eradication:

Once an incident is detected and verified as a true positive, actions must be taken to limit further damage and to prevent the threat from spreading. The primary concern of preventing further damage must be balanced with the requirement to collect forensic evidence related to the incident. Due to the sensitive and often qualitative nature of many of the judgments, recovery processes will involve a human in-the-loop of automation. A security-focused system of record is helpful for coordinating activity between infrastructure, security, and management personnel to ensure that any forensic evidence is collected and assets are only put back into service when appropriate.

XDR and next-generation SIEM products have made inroads into automating these actions, however they tend to have closed-ecosystems limiting the utility of their automation capabilities. In contrast, next-generation SOAR solutions tend to be vendor agnostic,modular and much more flexible; very seldom do enterprises use security solutions from only one vendor. Flexibility is practically tantamount to usability in this case because the diversity of enterprise environments, processes, and procedures often requires some playbook customization and integration with tools from at least a handful of vendors.

Post-Event Activity:

Incident reporting is integral to the entire incident response process. During the final incident response stage, security leaders rely on documentation describing what was detected, the analysis done, corroborating evidence for any conclusions, and any decisions made to provide insights into the incident. Reporting is also important as leaders need to be able to easily communicate the results of the incident investigation with stakeholders and other organizations in order to meet relevant regulatory requirements. Metrics collected during the incident response process can help find weaknesses in the existing process. Here again, next-gen SOAR or security automation solutions such as Turbine which act as a system of record and as a source of telemetry can be extraordinarily useful.

Finally, the insights gained must be reviewed and used to improve the overall security of the organization. Organizations should hold a meeting to identify lessons learned and to identify potential improvements to security controls or practices. Deficiencies in the incident handling or response process should be identified and steps taken to correct them.

What's Next for TDIR & SOAR

Ultimately, the addition of TDIR to the already confusing menagerie of security acronyms will not make an immediately useful distinction. However, the holistic approach to incident response that the term attempts to capture does represent a significant shift in how security teams will need to operate in the future. XDR, security analytics platforms, and next-gen SIEM solutions can enhance analysts' capacity to quickly respond to alerts and are capable of more expansive roles in the incident response lifecycle than the more limited roles filled by the previous generation of security solutions. Meanwhile, low-code security automation solutions will usher in the next generation of SOAR products, such as Swimlane Turbine that uses sensors at the edge of an active sensing fabric to drive alert enrichment, automated incident response, and reporting. These technologies share some functionality driven by the need for automation and more intelligent correlation of the vast quantities of available data, but remain distinct and pivotal players in the security industry.

SWIMLANE