exabeam

Guide

A SOC Manager's Guide to New Efficiencies: Automating the Full Threat Detection and Response Workflow

The two sides to automation

SOC teams manage and defend against security threats that have become increasingly complex and advanced everyday. With employees working remotely across a myriad of devices and networks – and accessing resources and services across public, private, and hybrid clouds – there is an ever-expanding attack surface for malicious actors to exploit. In order to defend against these attacks, SOC teams combine security and IT operations products – adding to the stack as new threats and types of attacks emerge.

In order to effectively use security tools and products, SOCs stitch them together with workflows and automation. Often, these integrations become more disjointed and unwieldy as the number of tools and processes needed to support them increases. And more security tools and solutions mean more security personnel to support them – leading to strained resourcing and budgets that SOC managers need to navigate around.

Too many alerts, too little time

Security analysts have the responsibility of helping an organization implement the tasks needed to run an effective threat detection, investigation, and response (TDIR) program. Figure 1 below outlines the relative percentage of time analysts spend performing in each of four major categories of work within the SOC workflow.

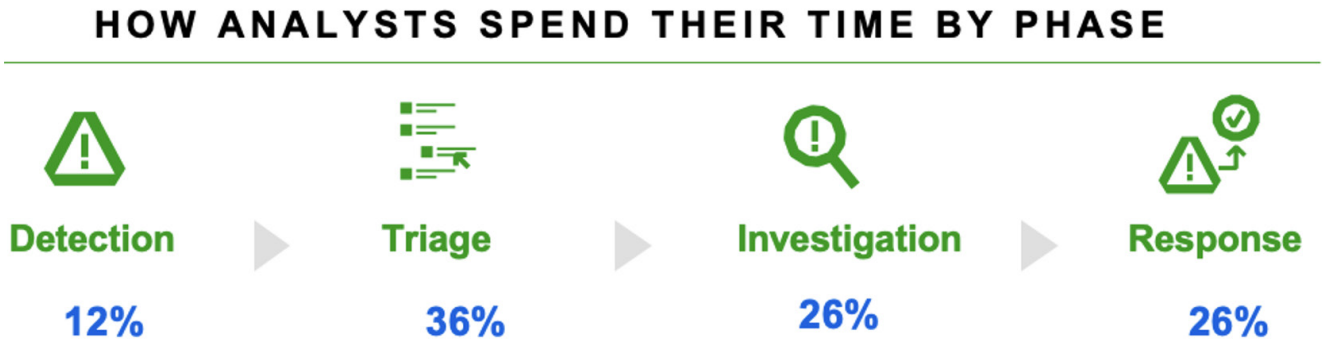

Figure 1 - How analysts spend their time according to a **Ponemon Institute report.**

Research by the Ponemon Institute, shows that roughly 76% of analyst time is spent triaging alerts from various security tools and performing incident investigation. While automation of SOC tasks and workflows can help with this problem, the most common approach to automating response in the SOC — deploying a SOAR tool — focuses too narrowly at incident response, which comprises only 38% of analyst time.

This guide will provide an overview of how automation can be applied to an organization's entire SOC threat detection and response workflow – including benefits, requirements, and best practices. This document is meant to help SOC teams as they choose the appropriate solutions that will best enable their organizations to defend against cyber threats in an efficient and scalable manner.

Prerequisites to deliver TDIR automation

Broad security portfolio

SOC teams will need a stack of mature security solutions to cover the necessary attack vectors to meet most organizations' automation requirements. Teams should look for security solutions that not only cover various attack vectors (like clouds, networking, endpoints, email, etc.), but also generate the necessary security telemetry that's used for analyses to address threats and are capable of taking corrective actions to remediate or defend. Without adequate security monitoring in place, the SOC will not have the visibility required to perform its duties.

Centralized security data

With the proper purpose-built security products in place, it is also necessary to ensure the security team has access to that data. This is often done by centralizing it in a SIEM, centralized log management (CLM) or cloud data lake. Centralization allows for more comprehensive analysis and correlation of events happening across an organization's employees and data.

Defined processes

When looking to automate threat detection, triage, investigation, and response it's mandatory that your SOC has a well-defined idea of steps that will be taken at each stage of the workflow, for each type of threat encountered. In the absence of well-defined processes SOCs will need to rely on their security vendors to supply strong packaged content that can guide their automation efforts.

This guide will delve into what strong, prescriptive content looks like and how it can accelerate your ability to successfully achieve threat detection and response outcomes. For now, the important takeaway is that you must be prepared to think through your processes in advance of automation, or work with an experienced vendor in this area.

Improve your results with more effective automation at each stage of the SOC workflow

Automating to improve threat detection

Did you know? According to Ponemon Institute, 33% of alerts in traditional SIEMs are false positives, increasing the workload of analysts downstream as they investigate incidents.

Automating detection means moving from beyond static rules and IOCs to more dynamic mechanisms like user and entity behavior analytics (UEBA). UEBA analyzes all activity for every user and machine in an environment to learn their normal operating behavior, and then to automatically identify risky, anomalous deviations from established baselines. This approach improves threat detection accuracy as it can use data from all available security and contextual data sources, takes into account the roles and activities of the machines and users involved, and can find unknown and zero day threats based on abnormality, making it future proof. Why this approach counts as automation is that the system self-learns and self-tunes based on behavior so it not only detects things in an automated fashion, it also does not require the maintenance of more static approaches. Correlation isn't enough to solve these sophisticated types of challenges.

Benefits of implementing automated threat detection:

- Reduced complexity and costs as teams don't need to manually create and maintain correlation rules
- Reduced false positives that take up resources downstream in investigation and incident resolution stages
- Automatic adaptation to changes, like a surge in remote work due to COVID or acquisition of another business unit
- Automatic improvement over time as UEBA tunes using techniques like Bayesian scoring

Automating detection is essentially a matter of letting machines do the heavy lifting; it helps free up your staff, can provide more accurate detection, and reduce downstream work.

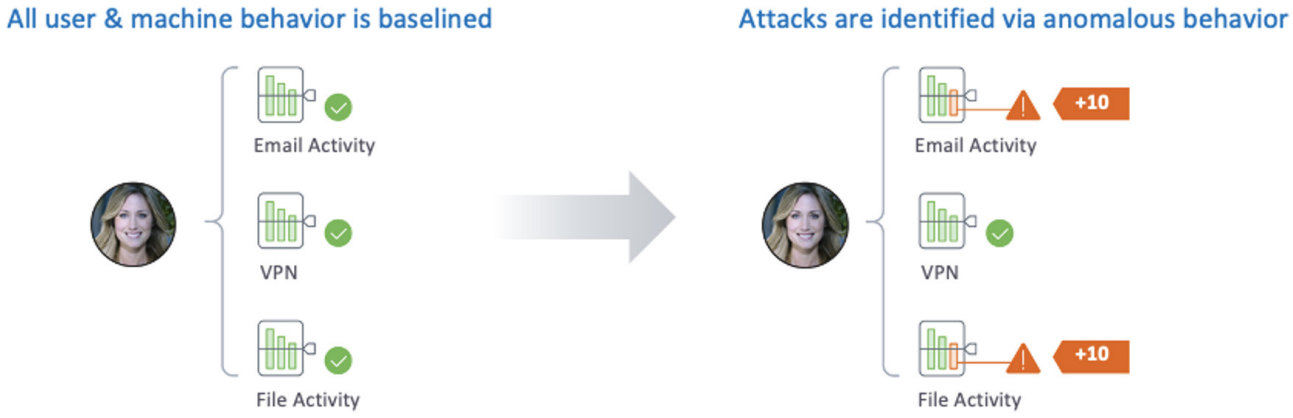

Figure 2 - UEBA learns behavior across many data sources and finds deviations from normal.

Automating away the pains of alert triage

Did you know? It takes an analysts an average of 207 minutes to triage a single alert.

Alert triage is a painful task. Analysts must answer many basic questions about an alert before they can make an informed decision on what to do with it. Each question typically involves querying a SIEM or security point product for information and context and each query can take several minutes to return results. The result is a process that tends to be manual, time consuming, and error-prone. See figure 3 below to learn some of the typical questions an analyst might want to answer about a **single alert**.

Roughly 36% of the average analyst's time is spent on performing triage because these mini-investigations need to be conducted for every alert to understand whether it should be escalated. The amount of time invested in this stage of the SOC workflow makes 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 these 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 judgement call—escalate or dismiss the alert—all from within a single UI. 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 highlighting the relevant data learned in this stage.

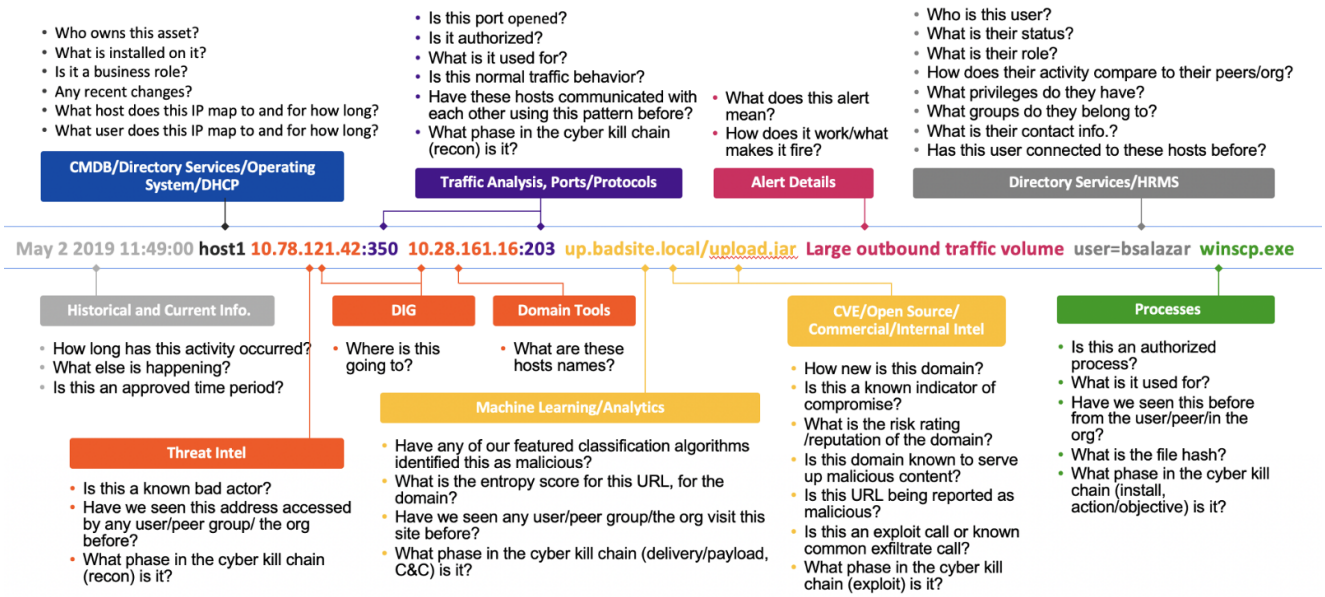

Figure 3 - This figure shows some of the questions a tier 1 analyst may ask while triaging an alert.

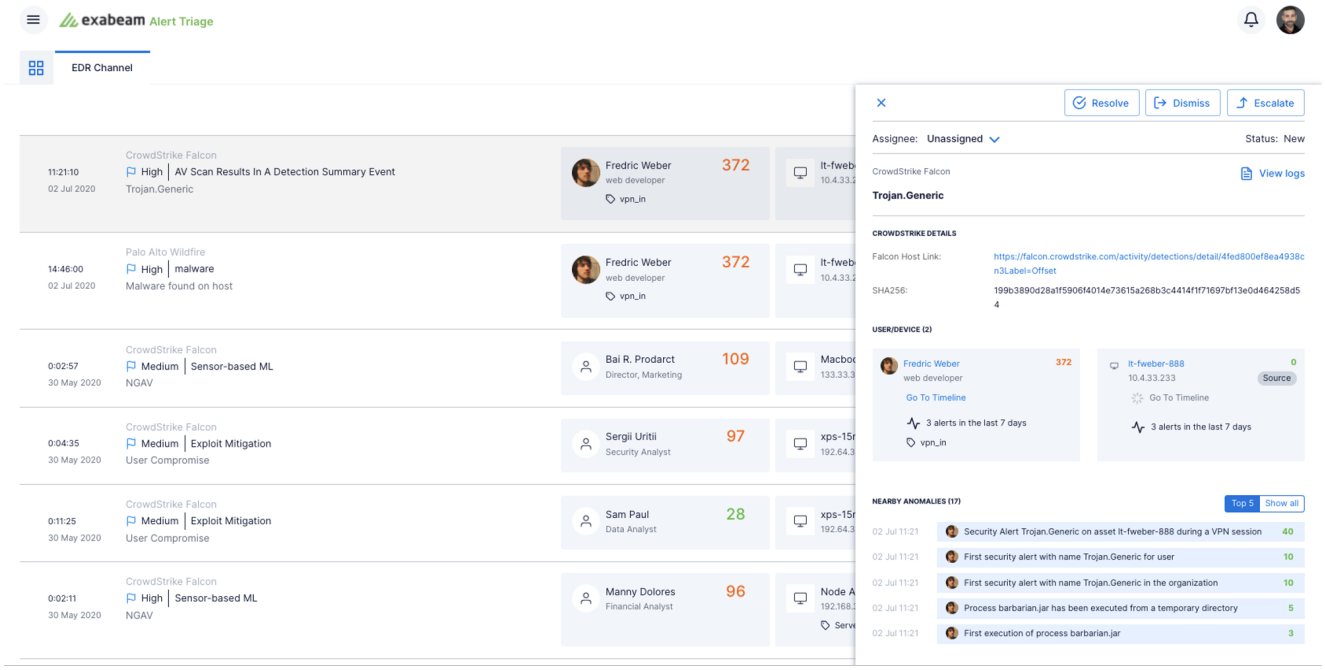

Figure 4 - The figure above shows an alert triage tool that automates triage by enriching alerts with behavioral context and machine-built timelines.

Benefits of implementing automated alert triage:

- Increased speed in triaging as all information is in one place for an analyst to determine next steps
- Increased accuracy as alerts are enriched with behavioral information and associated back to responsible users and machines
- Increased productivity due to streamlined workflows and integration with case management and incident response products
- Reduced alert fatigue for tier 1 analysts who get inundated with alerts across the myriad of security tools an organization may have
- Leave the office at quitting time ...

Automating investigations to reap huge dividends

Did you know? Each manual investigation takes roughly 20 hours and 700 queries.

Investigation is similar to triage in that it requires gathering data from a number of places and assembling it into a cohesive story, the difference between the two stages is the depth to which an analyst must dive. At the triage stage, it's necessary only to determine if the alert presents a real threat and whether or not a ticket should be opened. During the investigation stage it's necessary to understand what happened, what was the scope of the incident, what users and systems were impacted and more. The pain here, both in terms of resources and time, is so acute that oftentimes SOCs may go so far as to skip this step entirely; for example reimaging a machine infected with malware instead of completing a full investigation. While in no way a best practice, this is more common than it should be and it destroys evidence with no understanding of the full scope of an incident.

Automation presents the opportunity to ensure that investigations are performed without taxing SOC team resources. Automating this step means letting modern SIEM and XDR tools do the heavy lifting by gathering evidence and assembling it into a machine-built timeline that tells the story of the incident in a human consumable way. These timelines include all of the information an analyst needs to understand the scope of an incident, such as what happened in what order, what user and device activity was taken, was it normal, etc. These timelines even have the ability to follow lateral movement and reconstruct it back into a single chain of events. This information should be programmatically appended to the incident in the SOC's case management tool to ensure the relevant case has all the newly obtained information about the threat. Automating investigation pays dividends for SOC teams in the incident response phase as it ensures that parts of an attack aren't missed, and thus can be remediated.

Benefits of implementing automated incident investigation:

- Automating investigation helps ensure that it happens
- Less time spent on incident investigation means more time can be spent on higher value tasks like threat hunting
- Machine-built timelines track lateral movement and reduce the chances of false negatives being missed in the response phase

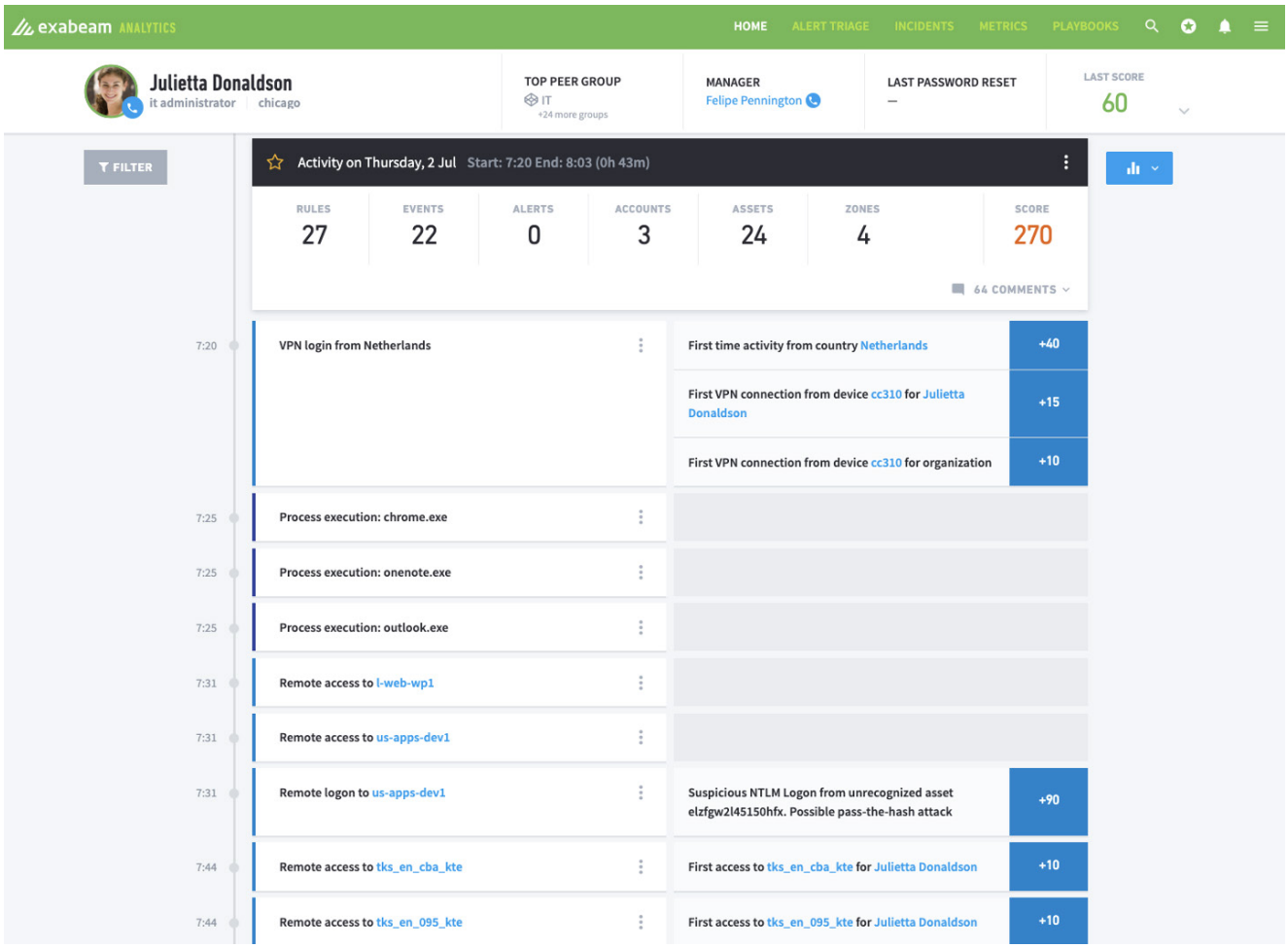

Figure 5 - This screenshot shows a machine-built timeline that automatically assembles evidence into an easy to read story.

Automating response to achieve greater productivity

Did you know? With proper response automation, response times for remediating incidents can drop by 47%.

In this stage, automation is commonly achieved with the use of SOAR solutions but can also be achieved with other solutions such as XDR. If using a SOAR or XDR product, it must interact with other security and IT tools, typically via API, to not only gather security data, but also take action and resolve an incident. SOAR tools perform automation based on the use of custom or prepackaged playbooks that codify SOC processes into a programmatic script which includes triggers and logic (see figure below). While many vendors provide prepackaged playbooks, not all stock content is created equal, as a result SOAR tools often require a significant amount of customization to work with your environment. Look for vendors which have comprehensive, prescriptive content for the threat types you're looking to automate resolution to. This will greatly accelerate your time to value.

Another key to effective integration is integration within your threat detection and investigation tool itself. For effective response automation, SOARs will need to integrate with a UEBA-based detection product to ensure that things aren't missed in the detection and investigation phase. It is also important that your SOAR tool integrates directly into your case management or ticketing system, which will allow for the system of record to be updated as new information comes up or actions are taken.

Benefits of implementing automated incident response:

- More complete response when paired with an effective UEBA solution
- Faster incident response times with automated actions and playbooks
- Higher analyst productivity due to automation

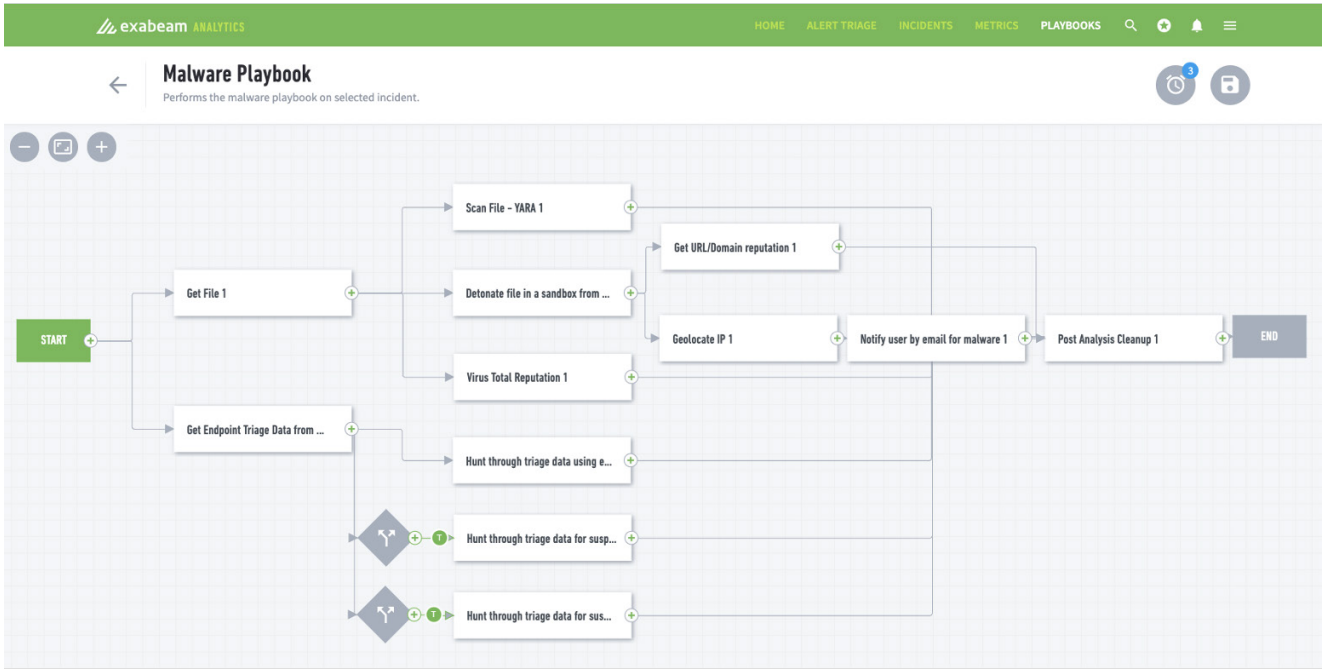

Figure 6 - This image shows the workflow in an automated response playbook for malware.

Introduce next-level automation using pre-packaged, threat-centric use cases

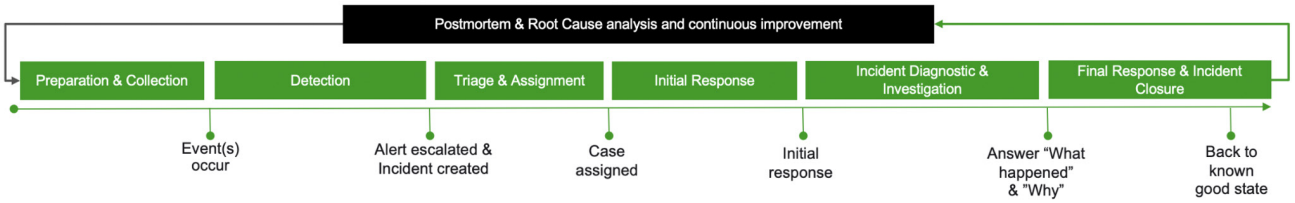

Figure 7 - Common phases of TDIR for SOC teams.

Traditionally, as SOC teams try to mature their operations through the use of automation, they often do so phase by phase starting on the left of the diagram in figure 7 and moving toward the right — from data collection to threat detection, triage, investigation and finally response. For example, SOC teams will bring in all the data they think they need into a SIEM, then try to automate detection for all of the threats they think they will face, and then try to automate response to all of those threats. They are essentially boiling the ocean at each phase by attempting all threat-centric use cases at the same time. This approach is very inefficient and often does not produce the desired results.

A different approach is to address a single threat-centric use case at a time. For example, if you want to tackle phishing, you'd bring in only the data sources that are relevant to that use case, automate the detection of phishing, and so on until you've automated all the way through to response. This lets your SOC team operationalize around one problem at a time such that they become a well-oiled machine for that specific threat type. Once your team is able to successfully achieve outcomes from end-to-end, then it's time to tackle the next threat.

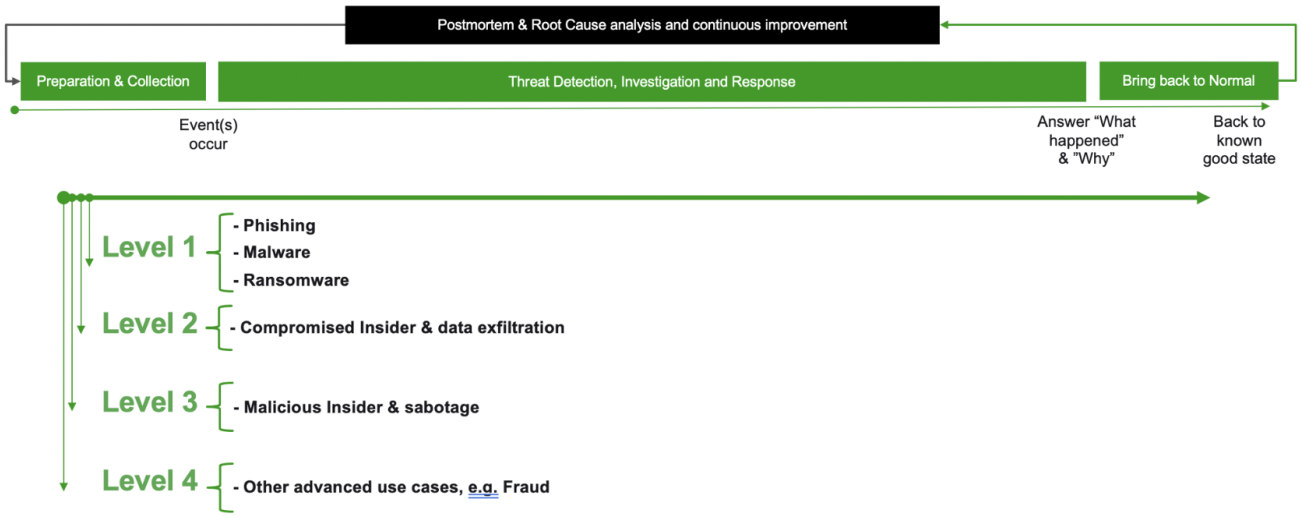

Figure 8 - Top-to-bottom use case approach to tackling threat types.

Vendors can help make this process easier by providing prescriptive workflows, and prepackaged content that helps provide all of the tools needed to successfully automate that specific threat. Think about how much easier it would be to cook a meal if someone handed you both the recipe and all of the ingredients, prepped and ready to go!

Starting with simple, yet prevalent use cases and automating with pre-defined playbooks and workflows will lead to more success. Additional, more complex use cases will build on the successes of the first ones — making use of prescriptive guidance and automated workflows from TDIR vendors. In this way, SOC teams won't be mired down trying to configure SIEMs and other security tools to address all threats all at once, with complex rules and a myriad of customization.

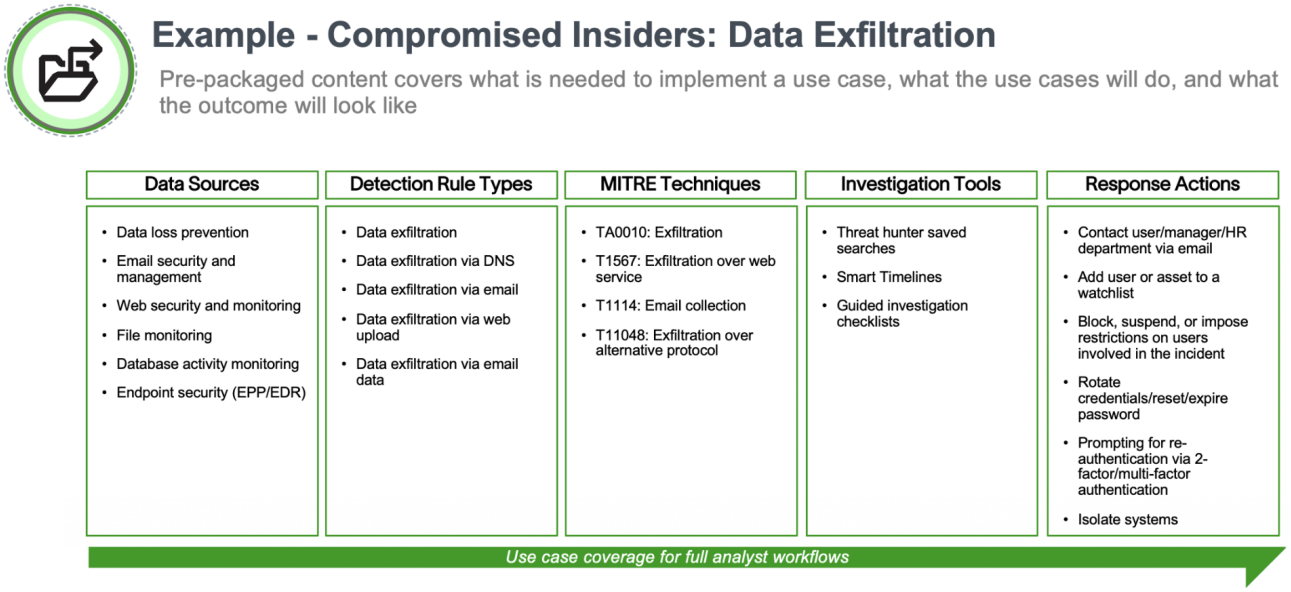

Figure 9 - The image above shows the contents of a prescriptive threat-centric use case package.

Conclusion

As more of an organization's SOC becomes automated, security teams can focus on higher value activities and more strategic projects like training and education. The more tedious and manual tasks that have been eliminated free up time for teams to consider other future avenues of risk that an organization should prepare for. Examples of these include: hunting for advanced, persistent threats, and even training and development of people and processes to keep up with the constantly evolving security stack in the SOC.

For in-depth analyst reports, guides, and tips on modernizing your SOC, visit our **SOC Modernization Resource Center**.

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. We are reinventing the way security teams use analytics and automation to solve threat detection, investigation, and response (TDIR), from common security threats to the most critical that are difficult to identify. The Exabeam Security Operations Platform is a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. It is designed and built to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives, and make security success the norm. For more information, visit www.exabeam.com.

exabeam

To learn more about how Exabeam can help you visit exabeam.com today.