Welcome to the Ultimate Guide to Threat Hunting!

Are you looking to enhance your threat detection efforts and stay ahead of potential cyber attacks? Look no further, as this guide will equip you with the essential knowledge and practical tips to get started with threat hunting.

What is Threat Hunting?

Threat hunting is a proactive, human-led process of searching through networks, endpoints, or datasets to detect malicious, suspicious, or risky activities that may have gone unnoticed by existing security tools. As a result of this iterative search, organizations can improve the speed and accuracy of their response to potential threats.

Why is Threat Hunting Important?

Threat hunting has become a critical aspect of modern enterprise Security Operation Centers (SOCs) in recent years. In fact, a recent survey conducted by the SANS institute showed that 91% of organizations reported improvements in response speed and accuracy after incorporating threat hunting into their overall detection practices.

Ready to Get Started with Threat Hunting? This guide will provide you with the necessary steps and techniques to effectively plan and carry out threat hunting activities. From clarifying what threat hunting is to debunking common myths, you will leave this guide with a solid understanding of how to integrate threat hunting into your overall security efforts.

Debunking Threat Hunting Myths Before diving into the practical tips for threat hunting, let's clear up some common myths about this critical practice.

Can be Fully Automated—No Really

Hunting is a **proactive activity** in the field of network security that requires the input of a human analyst. Unlike reactive methods that are solely focused on remedying incidents identified by automated tools, hunting involves hypothesis-based investigations aimed at uncovering threats that may have been missed by the automated systems. The goal of hunting is to expand on the context of incidents identified by automated tools, rather than simply resolving them.

Needs Lots Data—No Really

Hunting is often compared to the role of beat cops in law enforcement, as security analysts "patrol" through data to look for anomalies and signs of malicious activity. While it may seem like a relatively new concept, the practice of hunting has been used by security analysts for years. Basic hunting techniques, such as outlier analysis and stack counting, can be highly effective in uncovering threats, even with **simple data sets and tools.**

Only Elites can Do IT —No Really

The advent of purpose-built threat hunting platforms has made the process of hunting more efficient and effective. Tools like Sqrrl's or Sentinel Threat Hunting Platform simplify the process of fusing different data sets and leveraging advanced techniques. There are many different hunting techniques with varying levels of complexity, but even **basic techniques can be highly effective**. The key to getting started is to know what questions to ask and to begin exploring data sets related to those questions.

Crafting Your Threat Hunting Strategy

As a threat hunter, you play a vital role in ensuring the security of an organization's systems and data. A key part of this role is determining what to hunt for and how often to hunt, which requires a combination of knowledge about the organization's threat landscape and the use of data and tools. In this section we will walk through a fictional use case to demonstrate the steps involved in crafting a successful threat hunting strategy.

Imagine you are a threat hunter for a large financial institution. You are tasked with proactively identifying and mitigating potential security threats to the organization's systems and data. To begin, you familiarize yourself with the types of threats that the financial institution is likely to face. This includes researching recent cyber attacks and vulnerabilities, as well as understanding the organization's unique risk factors, such as its size and the sensitive nature of the information it handles. This research allows you to build a comprehensive understanding of the organization's threat landscape, which is essential for determining what to hunt for.

With this information in mind, you define your hunting objectives. In this case, you decide to focus on hunting for specific malware variants, attack tactics, and indicators of compromise (IOCs) that are relevant to the financial institution's threat landscape. This helps to prioritize your hunting efforts and ensure that you are focusing on the most pressing threats.

Next, you leverage existing data sources to inform your hunting strategy. You use network logs, endpoint data, and threat intelligence feeds to identify potential threats and prioritize your hunting efforts.

This data also provides insight into what types of threats the organization is most vulnerable to, allowing you to make informed decisions about what to hunt for and how often to hunt.

When it comes to determining how often to conduct hunts, it is important to strike a balance between staying ahead of potential threats and not overburdening your team. In this case, you decide to conduct hunts on a weekly basis, taking into consideration the organization's threat landscape and the resources available to you. This allows you to stay ahead of potential threats, while also ensuring that your team has the time and resources to conduct thorough and effective hunts.

It is also important to continuously evaluate and adjust your hunting strategy. This includes regularly reviewing the results of your hunts and using this information to refine your strategy. You update your hunting objectives as needed, adjust your hunting frequency as necessary, and incorporate new data sources and tools as they become available. This helps to keep your strategy relevant and effective, even as the threat landscape evolves.

Crafting a successful threat hunting strategy requires a combination of knowledge about the organization's threat landscape and the use of data and tools. By following these steps, you can prioritize your hunting efforts, stay ahead of potential threats, and ensure the security of the organization's systems and data. Remember, threat hunting is a continuous process, and it is important to regularly evaluate and adjust your strategy to ensure maximum effectiveness.

The Art of Threat Hunting

Understanding the Steps Involved

Threat hunting is a proactive approach to security that involves continuously searching for and mitigating potential security threats before they can cause harm. To be effective, threat hunting requires a well-defined process that brings together the knowledge and expertise of security experts, including threat hunters, risk analysts, and threat modelers.

The threat hunting process is designed to provide a structured approach, ensuring that the organization's security experts are working together effectively and efficiently to identify and mitigate potential threats. It includes steps for collecting and analyzing data, conducting risk analysis and threat modeling, and implementing mitigation strategies.

One of the key components of the threat hunting process is the collection and analysis of data from various sources, such as security logs, network traffic, and endpoint data. This data is used to identify potential threats and prioritize the organization's threat hunting efforts. Threat intelligence is also used to identify new and emerging threats, and threat hunting tools, such as security analytics platforms, are used to identify potential threats.

The threat hunting process also includes a risk analysis component, where the team assesses the impact of the potential threats identified during the threat hunting process. They evaluate the likelihood of a threat being realized, determine the potential consequences of a successful attack, and prioritize the risks based on the results of the analysis.

The threat modeling component of the threat hunting process is focused on creating a representation of the systems, applications, and networks that are being analyzed, identifying the assets and data that are critical to the organization, and evaluating the potential threats to these assets and data. The team then determines the most effective mitigation strategies to minimize the risks.

Finally, the threat hunting process includes steps for implementing the mitigation strategies identified during the threat modeling process and continuously monitoring the systems, applications, and networks to ensure that the mitigation strategies are effective. The process also includes regular review and improvement, and table top exercises to test the effectiveness of the threat hunting process and the preparedness of the security team.

By following a well-defined threat hunting process, organizations can prioritize their threat hunting efforts, minimize the risks to their systems and data, and stay ahead of potential threats. The process provides structure and guidance to the threat hunting effort, ensuring that the organization's security experts are working together effectively and efficiently to identify and mitigate potential threats.

High-level overview of the process

Preparation

- Define the scope of the threat hunting process, including the systems, applications, and networks that will be analyzed.
- Assemble a team of security experts, including threat hunters, risk analysts, and threat modelers.
- Establish clear objectives and goals for the threat hunting process.
- Identify and prioritize the risks that the threat hunting process will focus on.

Threat Hunting

- Collect and analyze data from various sources, such as security logs, network traffic, and endpoint data.
- Use threat intelligence to identify new and emerging threats.
- Utilize threat hunting tools, such as security analytics platforms, to identify potential threats.
- Conduct hands-on investigations to validate potential threats and determine their impact.

Risk Analysis

- Assess the impact of the potential threats identified during the threat hunting process.
- Evaluate the likelihood of a threat being realized.
- Determine the potential consequences of a successful attack.
- Prioritize the risks based on the results of the analysis.

Threat Modeling

- Create a representation of the systems, applications, and networks that are being analyzed.
- Identify the assets and data that are critical to the organization.
- Evaluate the potential threats to the assets and data.
- Determine the most effective mitigation strategies to minimize the risks.

Mitigation

- Implement the mitigation strategies identified during the threat modeling process.
- Continuously monitor the systems, applications, and networks to ensure that the mitigation strategies are effective.

Review and Improvement

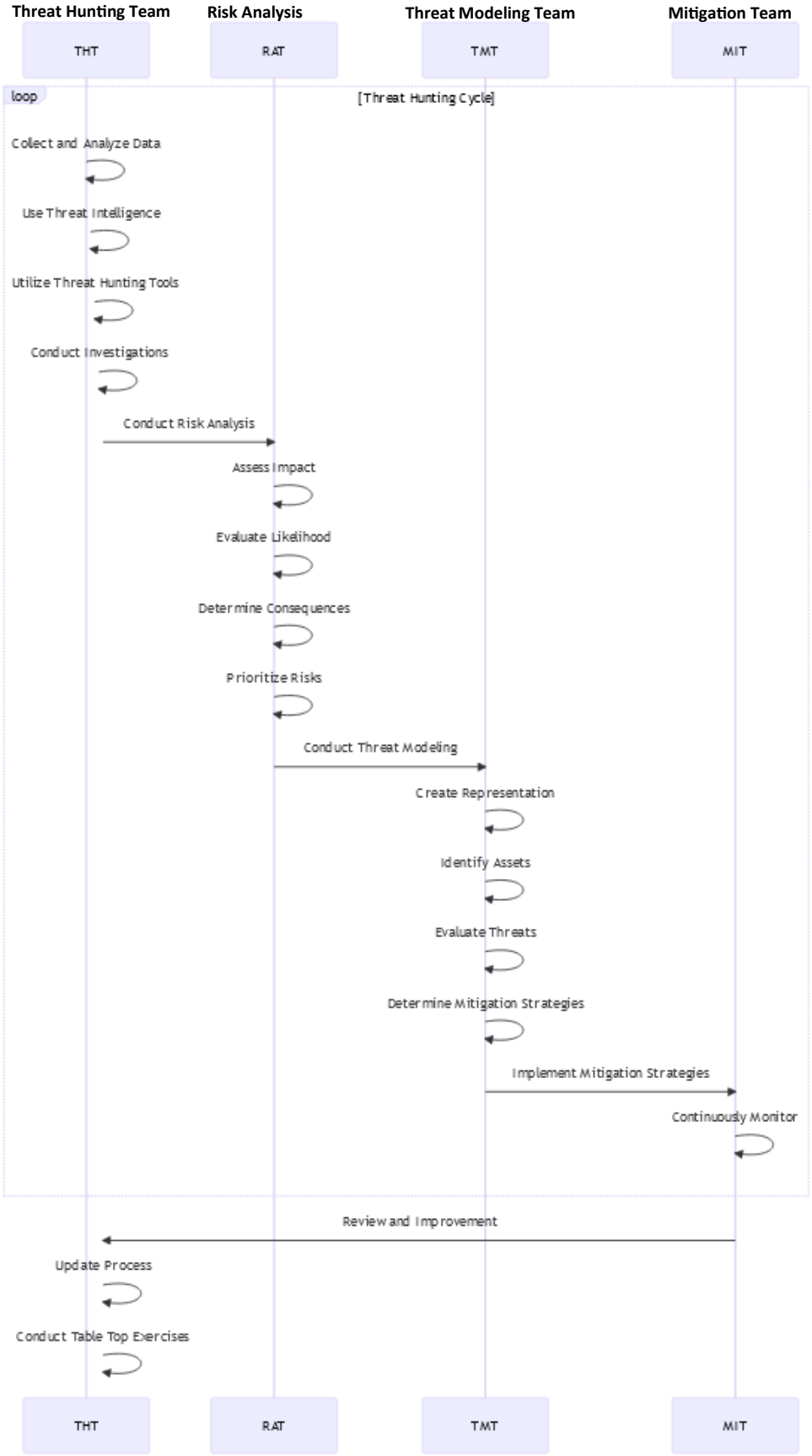
- Regularly review the threat hunting process to identify areas for improvement.
- Update the process as needed to reflect changes in the threat landscape and to incorporate new techniques and tools.

Table Top Exercises

- Conduct regular table top exercises to test the effectiveness of the threat hunting process and the preparedness of the security team.
- Evaluate the results of the exercises and make improvements to the process as needed.

This end-to-end process including the steps for risk analysis and threat modeling. The process is intended to be a cycled process, meaning it should be repeated on a regular basis. The frequency of the cycles can vary depending on the organization's risk tolerance, the threat landscape, and the resources available for threat hunting. For example, an organization with a high risk tolerance and a rapidly changing threat landscape may choose to conduct threat hunting cycles on a weekly or even daily basis, while an organization with a lower risk tolerance may choose to conduct the cycles on a monthly or quarterly basis. Regardless of the frequency, the idea is to continuously repeat the process, updating and improving it as needed, to ensure that the organization remains proactive in its approach to threat hunting and remains protected against potential threats.

In this diagram, the different teams involved in the threat hunting process are represented as **swimlanes**, with each step of the process represented by a sequence of arrows. The flowchart visually demonstrates the interdependencies between the different steps and teams, making it easier to understand and manage the threat hunting process.



A **RACI** chart (***Responsible, Accountable, Consulted, and Informed***) can be a useful tool for managing task assignment, ownership, and responsibilities in a threat hunting process. A RACI chart is a matrix that defines the roles and responsibilities of individuals or teams for specific tasks or activities.

In the context of the threat hunting process, the RACI chart can specify who is responsible for conducting the threat hunting activities, who is accountable for ensuring the success of the process, who should be consulted for input and guidance, and who should be informed of the results.

RACI

The RACI chart below provides clarity on the roles and responsibilities of the different teams involved in the threat hunting process, helping to ensure that tasks are assigned appropriately and that accountability is clear. It also helps to ensure that all stakeholders are informed and consulted as needed, promoting collaboration and effective decision-making.

Activity	Responsible	Accountable	Consulted	Informed
Threat Hunting	Threat Hunting Team	Threat Hunting Team	Risk Analysis Team, Threat Modeling Team	Mitigation Team, Management
Risk Analysis	Risk Analysis Team	Risk Analysis Team	Threat Hunting Team, Threat Modeling Team	Mitigation Team, Management
Threat Modeling	Threat Modeling Team	Threat Modeling Team	Threat Hunting Team, Risk Analysis Team	Mitigation Team, Management
Mitigation	Mitigation Team	Mitigation Team	Threat Hunting Team, Risk Analysis Team, Threat Modeling Team	Management

"Preparation" phase

Define the scope of the threat hunting process:

The first step in preparing for a threat hunting process is to define its scope. This involves determining the systems, applications, and networks that will be analyzed, as well as any specific areas of focus. For example, the scope of the threat hunting process may be limited to the organization's critical assets and data, or it may include all systems and devices connected to the network.

Assemble a team of security experts:

The next step is to assemble a team of security experts who will be responsible for conducting the threat hunting process. This team should include threat hunters, risk analysts, and threat modelers with the necessary expertise and experience to effectively detect and respond to potential threats. The team should also include individuals with a broad understanding of the organization's security posture and the threat landscape.

Establish clear objectives and goals:

Before starting the threat hunting process, it is important to establish clear objectives and goals. This will help to ensure that the process is focused and efficient, and that all stakeholders understand what is expected. Objectives and goals should be specific, measurable, and aligned with the organization's overall security strategy.

Identify and prioritize the risks:

The next step is to identify and prioritize the risks that the threat hunting process will focus on. This will help to ensure that the process is focused on the areas of highest risk and that resources are used effectively. Risks can be identified through a variety of means, such as a risk assessment, threat intelligence, or historical data on security incidents.

Activity	Responsible	Accountable	Consulted	Informed
Define the scope of the threat hunting process	Threat Hunting Team	Threat Hunting Team	Management	N/A
Assemble a team of security experts	Management	Management	Threat Hunting Team	N/A
Establish clear objectives and goals	Threat Hunting Team	Threat Hunting Team	Management	N/A
Identify and prioritize the risks	Threat Hunting Team	Threat Hunting Team	Risk Analysis Team, Management	N/A

"Threat Hunting" phase

Collect and analyze data from various sources:

The first step in the threat hunting process is to collect and analyze data from various sources, such as security logs, network traffic, and endpoint data. This data can be used to identify potential threats and to gain a better understanding of the organization's security posture. To ensure that the data is comprehensive and up-to-date, it is important to regularly collect data from all relevant sources.

Use threat intelligence to identify new and emerging threats:

The next step is to use threat intelligence to identify new and emerging threats. Threat intelligence can be obtained from a variety of sources, such as industry reports, open source intelligence, and commercial threat intelligence providers. Threat intelligence can provide valuable insights into the latest threats and vulnerabilities, helping to ensure that the threat hunting process is proactive and effective.

Utilize threat hunting tools to identify potential threats:

Threat hunting tools, such as security analytics platforms, can be used to identify potential threats. These tools can automate many of the manual tasks involved in threat hunting, such as data collection and analysis, and can help to identify potential threats more quickly and efficiently.

Conduct hands-on investigations to validate potential threats and determine their impact:

Once potential threats have been identified, the next step is to conduct hands-on investigations to validate the threats and determine their impact. This may involve conducting additional analysis, reviewing logs and other data, or conducting interviews with relevant stakeholders. The results of the investigations can then be used to prioritize the risks and determine the most appropriate re-

Activity	Responsible	Accountable	Consulted	Informed
Collect and analyze data from various sources	Threat Hunting Team	Threat Hunting Team	N/A	Risk Analysis Team
Use threat intelligence to identify new and emerging threats	Threat Hunting Team	Threat Hunting Team	N/A	Risk Analysis Team
Utilize threat hunting tools to identify potential threats	Threat Hunting Team	Threat Hunting Team	N/A	Risk Analysis Team
Conduct hands-on investigations to validate potential threats and determine their impact	Threat Hunting Team	Threat Hunting Team	Risk Analysis Team	Management

"Risk Analysis" phase

Assess the impact of the potential threats:

The first step in the risk analysis process is to assess the impact of the potential threats that have been identified during the threat hunting phase. This can involve evaluating the potential consequences of a successful attack, such as data loss, system downtime, or reputational damage. The impact of the threats should be assessed in terms of their severity and likelihood.

Evaluate the likelihood of a threat being realized:

The next step is to evaluate the likelihood of a threat being realized. This involves assessing the likelihood that the threat will actually occur, taking into account factors such as the organization's security posture, the threat landscape, and the effectiveness of current security controls.

Determine the potential consequences of a successful attack:

The next step is to determine the potential consequences of a successful attack. This can involve evaluating the potential impact on the organization's critical assets and data, as well as the potential impact on the organization's operations and reputation.

Prioritize the risks:

The final step in the risk analysis process is to prioritize the risks based on the results of the analysis. Risks should be prioritized based on their impact and likelihood, taking into account the organization's risk tolerance and available resources. The prioritized risks can then be used to inform the threat modeling and mitigation phases of the threat hunting process.

Activity	Responsible	Accountable	Consulted	Informed
Assess the impact of the potential threats	Risk Analysis Team	Risk Analysis Team	Threat Hunting Team	Management
Evaluate the likelihood of a threat being realized	Risk Analysis Team	Risk Analysis Team	Threat Hunting Team	Management
Determine the potential consequences of a successful attack	Risk Analysis Team	Risk Analysis Team	Threat Hunting Team	Management
Prioritize the risks	Risk Analysis Team	Risk Analysis Team	Threat Hunting Team, Management	N/A

"Threat Modeling" phase

Create a representation of the system, network, or application:

The first step in the threat modeling process is to create a representation of the system, network, or application being analyzed. This can involve creating a diagram or model that accurately depicts the components, data flows, and other relevant aspects of the system. The representation should be detailed enough to accurately reflect the system's architecture and design, but simple enough to be easily understood by all stakeholders.

Identify the assets:

The next step is to identify the assets that are present within the system, network, or application. Assets can include data, systems, and other components that have value to the organization. The assets should be prioritized based on their importance and potential impact if compromised.

Evaluate the threats:

The next step is to evaluate the threats to the assets identified in the previous step. This can involve conducting a thorough analysis of the potential threats, taking into account factors such as the organization's security posture, the threat landscape, and the effectiveness of current security controls. The results of the threat analysis should be used to identify the most significant threats to the assets.

Determine the mitigation strategies:

The final step in the threat modeling process is to determine the mitigation strategies that should be implemented to protect the assets from the identified threats. This can involve selecting and implementing appropriate security controls, such as firewalls, intrusion detection systems, or data encryption. The mitigation strategies should be prioritized based on their impact and cost, taking into account the organization's risk tolerance and available resources.

Activity	Responsible	Accountable	Consulted	Informed
Create a representation of the system, network, or application	Threat Modeling Team	Threat Modeling Team	Risk Analysis Team	Management
Identify the assets	Threat Modeling Team	Threat Modeling Team	Risk Analysis Team	Management
Evaluate the threats	Threat Modeling Team	Threat Modeling Team	Risk Analysis Team	Management
Determine the mitigation strategies	Threat Modeling Team	Threat Modeling Team	Risk Analysis Team, Management	N/A

"Mitigation" phase

Implement the mitigation strategies:

The first step in the mitigation process is to implement the mitigation strategies that have been identified during the threat modeling phase. This may involve implementing new security controls, modifying existing controls, or updating the organization's security policies and procedures. The mitigation strategies should be implemented in accordance with best practices and industry standards.

Test the effectiveness of the mitigation strategies:

The next step is to test the effectiveness of the mitigation strategies that have been implemented. This can involve conducting penetration testing, vulnerability assessments, or other security tests to ensure that the mitigation strategies are working as intended. The results of the tests should be used to validate the effectiveness of the mitigation strategies and to identify any areas for improvement.

Monitor the environment:

The final step in the mitigation process is to monitor the environment to ensure that the mitigation strategies are working effectively and that new threats are detected and responded to in a timely manner. This may involve regularly reviewing security logs and alerts, conducting security audits, or utilizing security analytics tools.

Activity	Responsible	Accountable	Consulted	Informed
Implement the mitigation strategies	Mitigation Team	Mitigation Team	Threat Hunting Team, Threat Modeling Team, Risk Analysis Team	Management
Test the effectiveness of the mitigation strategies	Mitigation Team	Mitigation Team	Threat Hunting Team, Threat Modeling Team, Risk Analysis Team	Management
Monitor the environment	Mitigation Team	Mitigation Team	Threat Hunting Team, Threat Modeling Team, Risk Analysis Team	Management

"Review and Improvement" phase

Review the results of the threat hunting process:

The first step in the review and improvement process is to review the results of the threat hunting process. This can involve evaluating the effectiveness of the process, the results of the risk analysis and threat modeling, and the effectiveness of the mitigation strategies. The review should also identify any areas for improvement and opportunities for enhancing the organization's security posture.

Evaluate the threats and risks:

The next step is to evaluate the threats and risks that have been identified during the threat hunting process. This can involve conducting a post-incident review, reviewing the results of the risk analysis, or assessing the effectiveness of the mitigation strategies. The results of the evaluation should be used to identify areas for improvement and to enhance the organization's understanding of the threat landscape.

Develop an improvement plan:

The next step is to develop an improvement plan based on the results of the review and evaluation. The improvement plan should include specific actions to address any identified areas for improvement, such as updating security policies, improving security controls, or enhancing the threat hunting process. The improvement plan should also include timelines, resources, and accountability for each action.

Implement the improvement plan:

The final step in the review and improvement process is to implement the improvement plan. This may involve updating security policies, modifying security controls, or enhancing the threat hunting process. The implementation of the improvement plan should be closely monitored to ensure that the desired outcomes are achieved and that the organization's security posture is improved.

Activity	Responsible	Accountable	Consulted	Informed
Review the results of the threat hunting process	Review and Improvement Team	Review and Improvement Team	Threat Hunting Team, Threat Modeling Team, Risk Analysis Team, Mitigation Team	Management
Evaluate the threats and risks	Review and Improvement Team	Review and Improvement Team	Threat Hunting Team, Threat Modeling Team, Risk Analysis Team, Mitigation Team	Management
Develop an improvement plan	Review and Improvement Team	Review and Improvement Team	Threat Hunting Team, Threat Modeling Team, Risk Analysis Team, Mitigation Team, Management	N/A
Implement the improvement plan	Review and Improvement Team	Review and Improvement Team	Threat Hunting Team, Threat Modeling Team, Risk Analysis Team, Mitigation Team, Management	N/A

"Table Top Exercises" phase

Define the scenario:

The first step in the table top exercise process is to define the scenario that will be used to simulate a potential threat. The scenario should be based on real-world threats and should reflect the organization's risk profile and the types of threats it is most likely to face.

Assemble the team:

The next step is to assemble the team that will participate in the table top exercise. The team should include members from various departments, such as security, IT, and business operations, to ensure that a comprehensive and coordinated response can be developed.

Conduct the exercise:

The next step is to conduct the table top exercise. The exercise should involve the team working through the scenario, discussing the potential threats and developing a coordinated response. The exercise should be timed to ensure that the team is able to develop a comprehensive response in a realistic timeframe.

Evaluate the results:

The final step in the table top exercise process is to evaluate the results of the exercise. This can involve conducting a debrief, reviewing the results of the exercise, and identifying areas for improvement. The results of the evaluation should be used to enhance the organization's security posture and to inform the development of future table top exercises.

Activity	Responsible	Accountable	Consulted	Informed
Define the scenario	Table Top Exercise Team	Table Top Exercise Team	Management	N/A
Assemble the team	Table Top Exercise Team	Table Top Exercise Team	Management	N/A
Conduct the exercise	Table Top Exercise Team	Table Top Exercise Team	Threat Hunting Team, Threat Modeling Team, Risk Analysis Team, Mitigation Team	Management
Evaluate the results	Table Top Exercise Team	Table Top Exercise Team	Threat Hunting Team, Threat Modeling Team, Risk Analysis Team, Mitigation Team, Management	N/A