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.

In this ebook, we will explore a fictional company's journey (CloudCo) towards securing its multi-cloud environment and protecting its sensitive information from potential threats. We will delve into the proactive threat hunting process that the company's security team has implemented, the tools and techniques they use, and the benefits they have gained from this process. We will also discuss the challenges that CloudCo may face in maintaining the security of its multi-cloud environment, and the steps the company can take to overcome these challenges.

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.

Use Case: Proactive Threat Hunting in a Multi-cloud Environment

In the fast-paced world of technology and innovation, companies are increasingly relying on cloud computing to support their business operations and meet the demands of their growing customer base. One such company, CloudCo, is a financial technology (fintech) organization that provides innovative financial services to businesses and individuals worldwide.

CloudCo's has rapidly grown in recent years, and it now serves millions of customers across the world. CloudCo has embraced the power of the cloud to support its business operations and to ensure that it can meet the demands of its growing customer base.

CloudCo's multi-cloud environment is critical to its success. It uses a combination of public and private clouds to store and process sensitive customer data, such as financial transactions, personal information, and confidential business documents. The company also uses cloud-based applications and APIs to provide its customers with access to financial services, such as online banking, investments, and loans.

However, the sensitive data retained by CloudCo is at risk of being exfiltrated by malicious actors. The company is aware that its virtual machines (VMs) in the cloud can be vulnerable to attacks, and that an unauthorized user who gains access to a VM could potentially move laterally to access the sensitive data. This is a major concern for CloudCo, as a data breach could result in severe financial losses, damage to its reputation, and loss of customer trust.

To protect its sensitive data, CloudCo has implemented a proactive threat hunting process. The company's security team is responsible for continuously monitoring the multi-cloud environment and for identifying and responding to potential threats. The team uses threat intelligence, threat hunting tools, and hands-on investigations to validate potential threats and to determine their impact. The team also performs risk analysis, threat modeling, and mitigation to prevent potential threats from being realized.

CloudCo employed a market-leading security research organization to provide them with monthly threat intelligence reports. These reports were tailored to the company's specific industry and provided valuable information on potential threats, including the names of threat actor groups and their tactics, techniques, and procedures (TTPs).

One month, the company received a report that alerted them of a potential vulnerability that could lead to a breach. The report indicated that a specific threat actor group was targeting virtual machines (VMs) in multi-cloud environments, and that they had the capability to move laterally to exfiltrate sensitive information.

This report was a wake-up call for the company, and they immediately sprang into action. The company's security team assembled, and they began the proactive threat hunting process to identify and prevent any potential harm to the organization's storage, databases, key vaults, applications, and APIs.

Starting with the collection and analysis of data from various sources, including security logs, network traffic, and endpoint data, the team used threat intelligence to identify new and emerging threats and to determine which potential threats to focus on. They then used threat hunting tools, such as security analytics platforms, to identify potential threats and to conduct hands-on investigations to validate the threats and determine their impact.

The team performed a risk analysis to assess the impact of the potential threats, evaluate the likelihood of a threat being realized, and determine the potential consequences of a successful attack. They then performed threat modeling to create a representation of the virtual machines (VMs), storage, databases, key vaults, applications, and APIs, identify the assets, evaluate the threats, and determine the mitigation strategies.

Thanks to the proactive threat hunting process, the company's security team was able to identify and respond to the potential threat before it could cause any harm. They implemented the necessary mitigation strategies, continuously monitored their multi-cloud environment, and reviewed the results of their threat hunting process to identify areas for improvement.

With the help of their monthly threat intelligence reports and the proactive threat hunting process, the company was able to maintain the security of their multi-cloud environment and protect their sensitive information from potential threats.
determine their impact. The team also performs risk analysis, threat modeling, and mitigation to prevent potential threats from being realized.

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

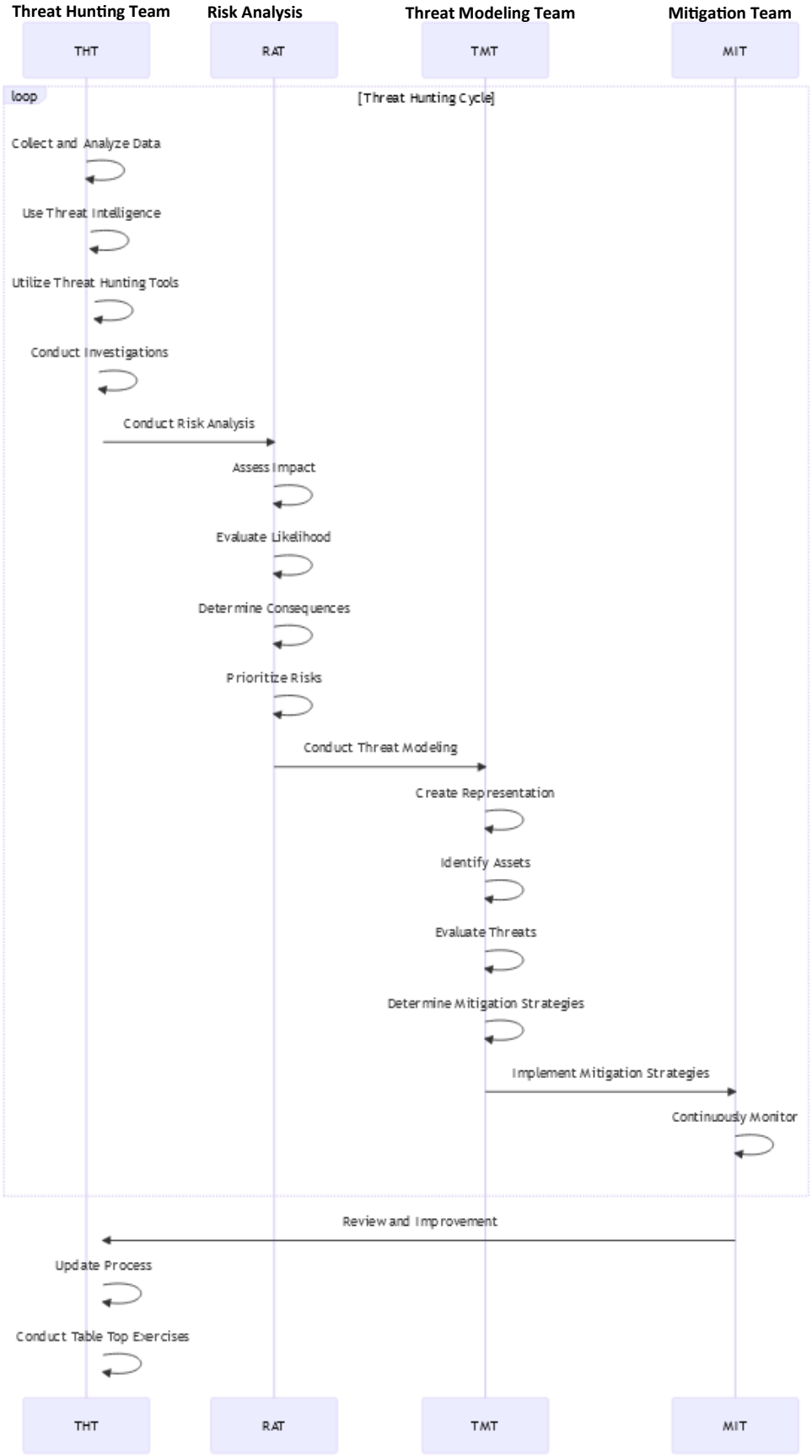
- Regularly review the threat hunting process to identify areas for improvement.
- Update the process as needed to reflect changes in the threat landscape and to incorporate new techniques and tools.

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

Let's delve into the fiction use-case of CloudCo, a rapidly growing financial technology company. CloudCo uses a multi-cloud environment to store and process sensitive customer data, but this puts the data at risk of being exfiltrated by malicious actors.

To protect its sensitive data, CloudCo has implemented a proactive threat hunting process, managed by its security team.
The team uses threat intelligence, tools, and hands-on investigations to validate potential threats and prevent them from being realized.
The company's proactive threat hunting process, combined with monthly threat intelligence reports, has enabled CloudCo to maintain the security of its multi-cloud environment and protect its sensitive information from

For any type of investigation, reactive and proactive you'll need data. For the our CloudCo scenario, the following types of data would typically be used:

- **Security logs**: Security logs contain information about the activity on the virtual machines (VMs), storage, databases, key vaults, applications, and APIs. The logs can provide valuable information about potential threats, such as attempts to access sensitive information, unusual login activity, or attempts to exploit vulnerabilities.
- **Network traffic**: Network traffic data provides information about the communication between devices in the network, including the virtual machines (VMs), storage, databases, key vaults, applications, and APIs. The data can be used to identify potential threats, such as network scans or data exfiltration attempts.
- **Endpoint data**: Endpoint data, such as data from servers, can provide valuable information about potential threats, such as malware infections, unauthorized access, or attempts to exploit vulnerabilities.
- **Threat intelligence**: Threat intelligence is information about current and emerging threats, including information about new malware, exploits, and attack tactics. Threat intelligence can be used to prioritize the potential threats to focus on during the threat hunting process.

These data sources, along with the use of threat hunting tools and hands-on investigations, would provide the information needed to identify and respond to potential threats in a proactive threat hunting scenario.

HYPOTHESIS

In a proactive threat hunting scenario, the starting point is often based on threat intelligence and data analysis. The security team will use the following types of hypotheses as a starting point for their threat hunting process:

Hypothesis: Unauthorized Access to Sensitive Information through Lateral Movement

Our security logs have identified unusual login activity on one of our virtual machines (VMs) in the multi-cloud environment. Additionally, our threat intelligence has indicated that there is an emerging threat related to unauthorized access to sensitive information. Based on this information, we hypothesize that an unauthorized user may have gained access to sensitive information stored on a cloud storage or database by breaching a virtual machine (VM) and moving laterally to exfiltrate data.

To validate this hypothesis, we will collect and analyze security logs, network traffic data, storage and database logs, and endpoint data. We will also conduct hands-on investigations to determine if an unauthorized user has gained access to sensitive information through lateral movement. If our hypothesis is correct, we will implement mitigation strategies to prevent further unauthorized access and to secure sensitive information.

As the principal threat hunter team leader, I would instruct the team to gather the following data to validate Hypothesis 1 "Unauthorized Access to Sensitive Information through Lateral Movement":

1. Security Logs: The security logs from virtual machines (VMs), cloud storage, and databases will be collected to identify unusual login activity and access sensitive information.
2. Network Traffic Data: The network traffic data from the virtual machines (VMs), cloud storage, and databases will be collected to identify any unusual or suspicious network activity.
3. Storage and Database Logs: The logs from the cloud storage and databases will be collected to identify any unusual or suspicious access to sensitive information.
4. Endpoint Data: The endpoint data from the virtual machines (VMs) will be collected to identify any unusual or suspicious activity related to the breach of a virtual machine (VM).

These data sources will be used to validate the hypothesis and to determine if an unauthorized user has gained access to sensitive information through lateral movement. The data will be analyzed to identify any patterns or anomalies that could indicate unauthorized access. The results of the data analysis will be used to determine the next steps in the threat hunting process.

nextsteps

The **next step** in the threat hunting process, after collecting the data, would be to analyze the data and identify potential threats.

This step would involve using various tools and techniques to identify patterns, anomalies, and correlations in the data that could indicate unauthorized access to sensitive information.

Here's a detailed description of the next step:

1. **Data Analysis**: The security logs, network traffic data, storage and database logs, and endpoint data collected in the previous step will be analyzed to identify any patterns, anomalies, or correlations that could indicate unauthorized access to sensitive information through lateral movement. The data will be analyzed using various tools and techniques, including statistical analysis, data visualization, and machine learning algorithms.
2. **Threat Identific**ation: Based on the results of the data analysis, potential threats will be identified and prioritized. The team will focus on the most significant threats that have the greatest potential impact on the organization's security posture.

Here's a more detailed description of step 1 (Data Analysis) and step 2 (Threat Identification) in the threat hunting process:

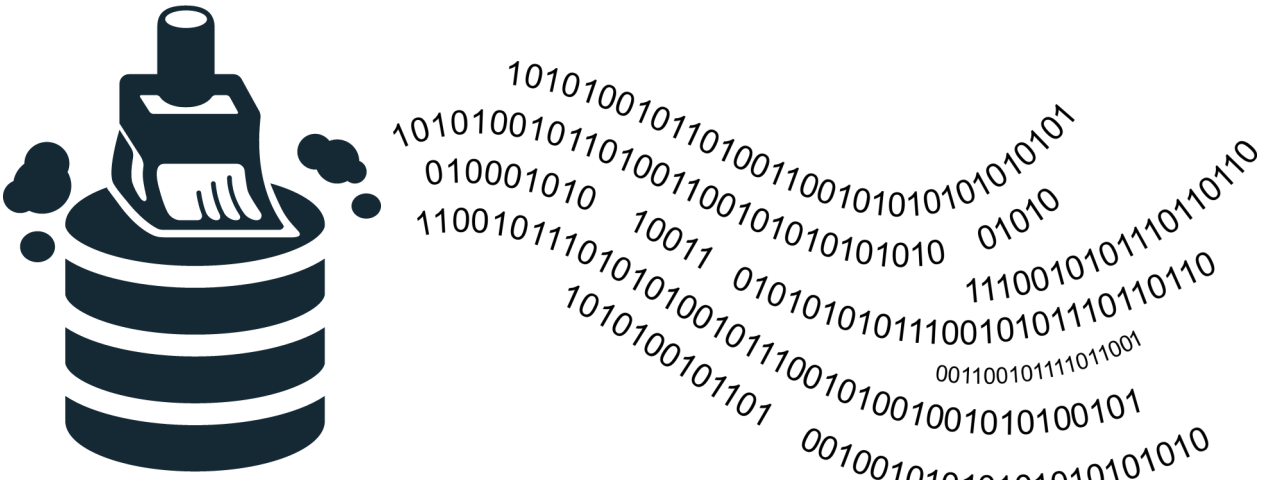
Step 1: Data Analysis

1. Data Collection: The data collected in the previous step will be loaded into a Threat Hunting Platform for analysis – if data is already in a SIEM, it can also be used.
2. Data Cleaning: The data will be cleaned to remove any duplicate or irrelevant information.
3. Data Transformation: The data will be transformed into a format that can be easily analyzed and visualized.
4. Data Correlation: The data will be correlated to identify any patterns, anomalies, or correlations that could indicate unauthorized access to sensitive information through lateral movement. The data will be correlated using various tools and techniques, including statistical analysis, data visualization, and machine learning algorithms.
5. Data Visualization: The results of the data correlation will be visualized using various tools and techniques, including graphs, charts, and heat maps. The visualizations will provide insights into the data and help the team identify any patterns, anomalies, or correlations that could indicate unauthorized access to sensitive information through lateral movement.

Step 2: Threat Identification

1. Threat Prioritization: Based on the results of the data analysis, potential threats will be identified and prioritized. The team will focus on the most significant threats that have the greatest potential impact on the organization's security posture.
2. Threat Validation: The team will validate the potential threats to determine if they are real or false positives. The team will use additional data sources, such as threat intelligence, to validate the threats.
3. Threat Characterization: The validated threats will be characterized to determine their type, origin, and impact. This information will be used to determine the next steps in the threat hunting process, including risk analysis and threat modeling.

By analyzing the data and identifying potential threats, the team can validate the hypothesis and determine if an unauthorized user has gained access to sensitive information through lateral movement. The results of this step will be used to determine the next steps in the threat hunting process, including risk analysis and threat modeling.



Let's expand on the details of "**Data Cleaning**" and "**Data Transformation**" in the context of the fiction use case and in correlation to Hypothesis 1: Unauthorized Access to Sensitive Information through Lateral Movement.

Data Cleaning:
Data cleaning is an important step in the data analysis process as it helps to ensure that the data being analyzed is accurate and relevant. During the data cleaning step, the team will perform the following tasks:

1. Duplicate Data Removal: The data will be scanned for any duplicate records and the duplicates will be removed. This helps to ensure that the data being analyzed is accurate and reduces the risk of false positives.
2. Irrelevant Data Removal: The data will be scanned for any irrelevant information and the irrelevant information will be removed. This helps to ensure that the data being analyzed is relevant to the hypothesis and reduces the risk of false negatives.

Example: For the fiction use case, the security logs collected from the virtual machines (VMs), cloud storage, and databases will be cleaned to remove any duplicate or irrelevant records. For example, the logs related to routine system maintenance or software updates will be removed as they are not relevant to the hypothesis.

Data Transformation:
Data transformation is an important step in the data analysis process as it helps to prepare the data for analysis and visualization. During the data transformation step, the team will perform the following tasks:

1. Data Formatting: The data will be formatted into a standard format that can be easily analyzed and visualized. This helps to ensure that the data can be easily manipulated and compared.
2. Data Normalization: The data will be normalized to remove any discrepancies or inconsistencies in the data. This helps to ensure that the data being analyzed is accurate and consistent.

Example: For the fiction use case, the security logs collected from the virtual machines (VMs), cloud storage, and databases will be transformed into a format that can be easily analyzed and visualized. For example, the logs will be transformed into a standard format that can be easily analyzed and visu-

Let's consider the following examples:

Duplicate Data Removal

Consider a security log from a virtual machine (VM) that contains the following records:

```
Timestamp, User, Action
01/01/2023 10:00, John Doe, Login
01/01/2023 10:01, John Doe, Login
01/01/2023 10:02, John Doe, Logout
```

In this example, the first record is a duplicate of the second record. During the data cleaning step, the duplicate record will be removed to ensure that the data being analyzed is accurate.

Irrelevant Data Removal

Consider a security log from a virtual machine (VM) that contains the following records:

```
Timestamp, User, Action
01/01/2023 10:00, John Doe, Login
01/01/2023 10:01, John Doe, Update Software
01/01/2023 10:02, John Doe, Logout
```

In this example, the second record is irrelevant to the hypothesis as it is related to a routine software update. During the data cleaning step, the irrelevant record will be removed to ensure that the data being analyzed is relevant to the hypothesis.

Data Formatting

Consider a security log from a virtual machine (VM) that contains the following records:

```
Timestamp, User, Action
Jan 1 10:00:00, John Doe, Login
Jan 1 10:01:00, John Doe, Logout
```

In this example, the data is not in a standard format that can be easily analyzed and visualized. During the data transformation step, the data will be formatted into a standard format, such as ISO 8601, that can be easily analyzed and visualized.

Data Normalization

Consider a security log from a virtual machine (VM) that contains the following records:

```
Timestamp, User, Action
01/01/2023 10:00, John Doe, LOGIN
01/01/2023 10:01, John Doe, LOGOUT
```

In this example, the data contains discrepancies or inconsistencies in the format of the "Action" field. During the data transformation step, the data will be normalized to remove any discrepancies or inconsistencies in the data. For example, the "Action" field could be normalized to a standard format, such as all lowercase, to ensure that the data is consistent and reliable.

Here are sample hunting queries in Microsoft Kusto query language, Splunk query language, and Elasticsearch query language that can be used to gather the relevant data

Microsoft Kusto query language

```
// Collect security logs
SecurityLogs
| where TimeGenerated >= startTime and TimeGenerated <= endTime
| where EventID == 4624 or EventID == 4625

// Collect network traffic data
NetworkTraffic
| where Time >= startTime and Time <= endTime
| where src_ip != "10.0.0.0/8" and dst_ip != "10.0.0.0/8"

// Collect endpoint data
EndpointData
| where Time >= startTime and Time <= endTime
| where EventType == "FileAccess" or EventType == "ProcessCreation"
```

Splunk query language

```
// Collect security logs
sourcetype="WinEventLog:Security"
starttime=startTime endtime=endTime
(EventCode=4624 OR EventCode=4625)

// Collect network traffic data
sourcetype="netflow"
starttime=startTime endtime=endTime
(src_ip!="10.0.0.0/8" AND dst_ip!="10.0.0.0/8")

// Collect endpoint data
sourcetype="endpoint_data"
starttime=startTime endtime=endTime
(EventType="FileAccess" OR EventType="ProcessCreation")
```

Elasticsearch query language

```
// Collect security logs
GET security_logs/_search
{
  "query": {
    "bool": {
      "must": [
        { "range": { "TimeGenerated": { "gte": startTime, "lte": endTime } } },
        { "terms": { "EventID": [4624, 4625] } }
      ]
    }
  }
}

// Collect network traffic data
GET network_traffic/_search
{
  "query": {
    "bool": {
      "must": [
        { "range": { "Time": { "gte": startTime, "lte": endTime } } },
        {
          "bool": {
            "must_not": [
              { "prefix": { "src_ip": "10.0.0.0/8" } },
              { "prefix": { "dst_ip": "10.0.0.0/8" } }
            ]
          }
        }
      ]
    }
  }
}

// Collect endpoint data
GET endpoint_data/_search
{
  "query": {
    "bool": {
      "must": [
        { "range": { "Time": { "gte": startTime, "lte": endTime } } },
        { "terms": { "EventType": ["FileAccess", "ProcessCreation"] } }
      ]
    }
  }
}
```

USING PYTHON TO CLEAN AND TRANSFORM DATA

Early we've discussed the importance of gathering data, but also ensuring that a proper cleaning and transformation is done. Here we take the data collected via queries, and we clean and transform it to remove any duplicate or irrelevant information and to make it easily analyzed and visualized. For this step we can use a variety of tools, but I prefer to use Python as it fits right into the objective.

Python is a great language for data cleaning and transformation because of its many advantages:

- It has a large number of libraries that make data analysis and manipulation more accessible and efficient, such as Pandas, NumPy, and Scikit-Learn.
- Python is easy-to-learn with a simple and intuitive syntax that makes it beginner-friendly for data scientists and developers.
- Python is interoperable with many other technologies and tools commonly used in data analysis and transformation, such as SQL databases, Hadoop, and Spark. This makes it easy to integrate Python into existing data processing workflows.
- Performance-wise, Python's performance can be significantly enhanced with libraries like Numpy and Pandas, which utilize optimized algorithms to perform mathematical operations and data manipulations efficiently.

Python is a general-purpose programming language, meaning it can be used for a wide range of tasks, which makes it flexible and an excellent choice for data cleaning and transformation, as well as other data science tasks like machine learning and data visualization.

Code:

```python
import pandas as pd

# Load the data into a pandas DataFrame
df = pd.read_csv("data.csv")

# Clean the data
df.drop_duplicates(inplace=True)
df.dropna(inplace=True)

# Transform the data
df["TimeGenerated"] = pd.to_datetime(df["TimeGenerated"])
df["EventType"] = df["EventType"].astype("category")
df["EventID"] = df["EventID"].astype("int")

# Normalize the data to remove discrepancies or inconsistencies
df["src_ip"] = df["src_ip"].str.lower()
df["dst_ip"] = df["dst_ip"].str.lower()
```

USING PYTHON FOR FURTHER DATA ANALYSIS

Finally, the cleaned and transformed data can be analyzed to identify potential threats and validate them. Here is a sample Python code to use algorithms to facilitate the analysis of the data.

Code:

```
import numpy as np
import matplotlib.pyplot as plt
from sklearn.cluster import KMeans

# Plot the data to identify patterns or anomalies
plt.scatter(df["src_ip"], df["dst_ip"])
plt.xlabel("Source IP")
plt.ylabel("Destination IP")
plt.show()

# Use KMeans clustering to group similar data points
kmeans = KMeans(n_clusters=3)
kmeans.fit(df[["src_ip", "dst_ip"]])

# Identify potential threats based on the cluster assignments
clusters = kmeans.predict(df[["src_ip", "dst_ip"]])
df["cluster"] = clusters

# Validate the potential threats using threat intelligence data
df["is_threat"] = np.where(df["cluster"] == 1, True, False)
```

This is just a sample code to demonstrate how algorithms can be used to facilitate the analysis of the data during the threat hunting process. The actual code used will depend on the specific requirements and goals of the threat hunting process.

Threat Prioritization -Validation - Characterization

Let's expand on the details of "**Threat Prioritization**", "**Threat Validation**", and "**Threat Characterization**" in the context of the fiction use case and ***Hypothesis: Unauthorized Access to Sensitive Information through Lateral Movement.***

Threat Prioritization

Threat prioritization is an important step in the threat hunting process as it helps to focus the team's efforts on the most significant threats—the team will perform the following tasks:

1. Threat Identification: The team will identify the potential threats based on the results of the data analysis.
2. Threat Ranking: The potential threats will be ranked based on their potential impact on the organization's security posture and the likelihood of a threat being realized. The team will focus on the most significant threats that have the greatest potential impact.

Example: The team will prioritize the potential threats based on their potential impact on the organization's sensitive information. The potential threat that involves an unauthorized user accessing and exfiltrating sensitive information from a cloud storage or database would be ranked as high priority, as it has a high potential impact on the organization's security posture.

Threat Validation

Threat validation is an important step in the threat hunting process as it helps to determine if a potential threat is real or a false positive—the team will perform the following tasks:

1. Additional Data Collection: The team will collect additional data from various sources, such as threat intelligence, to validate the potential threats.
2. Threat Analysis: The team will analyze the additional data to determine if the potential threat is real or a false positive.

Example: The team will validate the potential threats by collecting and analyzing additional data from various sources, such as threat intelligence and network traffic data. If the team identifies a potential threat involving an unauthorized user accessing and exfiltrating sensitive information from a cloud storage or database, the team will use threat intelligence and network traffic data to determine if the potential threat is real or a false positive.

Threat Characterization

Threat characterization is an important step in the threat hunting process as it helps to determine the type, origin, and impact of the validated threats—the team will perform the following tasks:

1. Threat Type: The team will determine the type of threat, such as a malware attack or unauthorized access.
2. Threat Origin: The team will determine the origin of the threat, such as an internal user or external attacker.
3. Threat Impact: The team will determine the impact of the threat on the organization's security posture, such as the potential loss of sensitive information.

Example: The team will characterize the validated threats by determining their type, origin, and impact. If the team determines that a validated threat involves an unauthorized user accessing and exfiltrating sensitive information from a cloud storage or database, the team will characterize the threat as an unauthorized access threat, originating from an external attacker, with a high potential impact on the organization's security posture.

For the fiction use case, the team focused on the most significant threats that had the greatest potential impact on the organization's sensitive information.

The team validated the potential threats by collecting and analyzing additional data from various sources, such as threat intelligence and network traffic data. If the team determined that a validated threat involved an unauthorized user accessing and exfiltrating sensitive information from a cloud storage or database, the team characterized the threat as an unauthorized access threat originating from an external attacker with a high potential impact on the organization's security posture.

Thanks to the proactive threat hunting process, the organization's security team was able to quickly identify and respond to suspicious activity in its multi-cloud environment, preventing further harm and enhancing its overall security posture.


NEXT SET OF STEP
POST HUNT

After the threat hunting stage, the next step for the company security team is to perform a risk analysis and threat modeling.

Risk Analysis: In this stage, the team will assess the impact of the potential threats and evaluate the likelihood of a threat being realized. The team will use a framework, such as the FAIR (Factor Analysis of Information Risk) framework, to help structure their analysis. The FAIR framework provides a systematic way to evaluate the impact of a potential threat and prioritize the risks based on their impact and likelihood.
To support the risk analysis, the team may evaluate to implement tools such as Microsoft Defender for Cloud or AWS Security Hub, which provide a centralized view of the security posture across multiple cloud environments. These tools can help the team identify any misconfigurations or vulnerabilities in the environment and provide recommendations for remediation.

Threat Modeling: In this stage, the team will create a representation of the virtual machines (VMs), storage, databases, key vaults, applications, and APIs, identify the assets, evaluate the threats, and determine the mitigation strategies. The team can use a framework such as **STRIDE** (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of Privilege) to help structure their threat modeling analysis.
To support the threat modeling, the team may use tools such as **Microsoft Threat Modeling Tool or IriusRisk**, which help automate the threat modeling process and provide visual representations of the threat models. These tools can help the team identify the attack paths and potential vulnerabilities in their systems and provide recommendations for mitigation.

By performing a thorough risk analysis and threat modeling, the company security team can ensure that they have identified and addressed all potential threats to the multi-cloud environment, and that they have taken steps to mitigate the risks and protect the sensitive data stored in the environment.

Risk Analysis

Following the successful threat hunting process, the organization's security team now turns its attention to risk analysis. The goal of risk analysis is to assess the impact of the potential threats that were identified during the threat hunting process, to evaluate the likelihood of a threat being realized, and to determine the potential consequences of a successful attack.

To accomplish these objectives, the team will use a framework for risk analysis that includes the following steps:

1. Assess the impact: The team will assess the impact of the potential threats by determining the extent to which the threats could compromise the security of the multi-cloud environment, including the virtual machines (VMs), storage, databases, key vaults, applications, and APIs. The team will also assess the impact of the threats on the organization's sensitive information and its operations.
2. Evaluate the likelihood: The team will evaluate the likelihood of a threat being realized by considering the likelihood of a threat actor successfully executing the attack, the prevalence of the threat, and the organization's ability to detect and prevent the threat.
3. Determine the consequences: The team will determine the potential consequences of a successful attack by considering the impact of the attack on the organization's security posture, its sensitive information, and its operations.
4. Prioritize the risks: Based on the results of the analysis, the team will prioritize the risks by determining which threats have the greatest potential impact and likelihood of being realized. The team will focus its efforts on mitigating the highest-priority risks first.

The security team had identified several potential threats to the company's multi-cloud environment. These threats had the potential to result in a breach of sensitive information stored on the cloud. The next step was to perform a risk analysis to assess the impact of these potential threats and to prioritize the risks based on their impact and likelihood.

The team began by assessing the impact of each potential threat. They looked at the type of data that could be affected, the potential consequences if the data was accessed by an unauthorized user, and the impact on the business if this were to happen. The team also evaluated the likelihood of each threat being realized, considering the company's current security measures and the sophistication of the potential threat actor. Based on their analysis, the team determined that the most significant risk was the unauthorized access to sensitive information stored on cloud storage and databases. This information was critical to the operation of the business and its exposure could have severe consequences. The team also determined that there was a high likelihood of this threat being realized, given the sophistication of the threat actor and the vulnerabilities identified in the security logs and network traffic data.

The team then prioritized the risks based on their impact and likelihood. They decided to focus their efforts on mitigating the risk of unauthorized access to sensitive information, as it was the most significant risk and the one with the highest likelihood of being realized.

The team then developed a risk mitigation plan, including implementing additional security measures and conducting regular threat hunts to monitor for any potential threats. They also developed a plan to continuously monitor the security posture of the multi-cloud environment to ensure that the risk of unauthorized access to sensitive information was reduced.
Thanks to the proactive and thorough risk analysis, the security team at the large organization was able to prioritize the risks to its multi-cloud environment and implement effective mitigation strategies to prevent the unauthorized access to sensitive information. This helped to enhance the overall security posture of the organization and reduce the risk of a security incident.

To perform the risk analysis, the company's security team will use a risk assessment framework, such as the FAIR (Factor Analysis of Information Risk) framework. The framework will guide the team through the process of identifying the assets, evaluating the threats, and determining the risk level.
The team will assess the impact of the potential threats identified during the threat hunting process, considering the sensitive information stored in the multi-cloud environment, such as customer data and financial information. The team will evaluate the likelihood of a threat being realized, considering factors such as the sophistication of the threat actor, the vulnerabilities present in the environment, and the existing security controls.

Based on the results of the risk analysis, the team will determine the potential consequences of a successful attack. This could include unauthorized access to sensitive information, financial loss, reputation damage, and regulatory fines.

Finally, the team will prioritize the risks based on the results of the analysis, considering the impact and likelihood of each risk. This will help the team to focus on the most significant threats and to determine the next steps in the threat hunting process, including threat modeling and mitigation.
The security team at the large organization had just finished its threat hunting process and had identified several potential threats to the company's multi-cloud environment. These threats had the potential to result in a breach of sensitive information stored on the cloud. The next step was to perform a risk analysis to assess the impact of these potential threats and to prioritize the risks based on their impact and likelihood.
The team began by assessing the impact of each potential threat. They looked at the type of data that could be affected, the potential consequences if the data was accessed by an unauthorized user, and the impact on the business if this were to happen. The team also evaluated the likelihood of each threat being realized, considering the company's current security measures and the sophistication of the potential threat actor.

Based on their analysis, the team determined that the most significant risk was the unauthorized access to sensitive information stored on cloud storage and databases. This information was critical to the operation of the business and its exposure could have severe consequences. The team also determined that there was a high likelihood of this threat being realized, given the sophistication of the threat actor and the vulnerabilities identified in the security logs and network traffic data.
The team then prioritized the risks based on their impact and likelihood. They decided to focus their efforts on mitigating the risk of unauthorized access to sensitive information, as it was the most significant risk and the one with the highest likelihood of being realized.

The team then developed a risk mitigation plan, including implementing additional security measures and conducting regular threat hunts to monitor for any potential threats. They also developed a plan to continuously monitor the security posture of the multi-cloud environment to ensure that the risk of unauthorized access to sensitive information was reduced. The decision was made to adopt solutions such as Microsoft Defender for Cloud or AWS Security Hub.

Thanks to the proactive and thorough risk analysis, the security team was able to prioritize the risks to its multi-cloud environment and implement effective mitigation strategies to prevent unauthorized access to sensitive information. This helped to enhance the overall security posture of the organization and reduce the risk of a security incident.

The security team had just completed its risk analysis and had identified several mitigation strategies to reduce the risk of unauthorized access to sensitive information stored on the cloud. The next step was to perform threat modeling to determine the most effective mitigation strategies and to ensure that the organization's critical assets and data were protected.
The team began by creating a representation of the systems, applications, and networks that were being analyzed. This included virtual machines (VMs), storage, databases, key vaults, applications, and APIs. The team then identified the assets and data that were critical to the organization, such as sensitive information stored in cloud storage and databases.

The team decided to use Microsoft Threat Modeling Tool and IriusRisk. These tools help automate the threat modeling process and provide visual representations of the threat models, making it easier for the team to identify and evaluate the potential threats to the organization's assets and data.
Using Microsoft Threat Modeling Tool, the team was able to create a visual representation of their multi-cloud environment, including the virtual machines (VMs), storage, databases, key vaults, applications, and APIs. This representation helped the team to understand the relationships between the different components of their environment and to identify the assets and data that were critical to the organization.
IriusRisk was also used to evaluate the potential threats to these assets and data. IriusRisk helped the team to identify the threat scenarios that could result in the unauthorized access to sensitive information stored on cloud storage and databases. The tool also helped the team to evaluate the likelihood of these threats being realized and to determine the impact on the organization if a breach were to occur.

Next, the team evaluated the potential threats to these assets and data. To structure their analysis, they used the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of Privilege) framework. This framework helped the team to systematically analyze each potential threat and understand the impact that it could have on the assets and data.

The team identified that the most significant risk to the sensitive information stored in cloud storage and databases was unauthorized access. Using the STRIDE framework, the team evaluated this threat in terms of Spoofing (the potential for an unauthorized user to masquerade as a legitimate user), Tampering (the potential for an unauthorized user to alter the data), Repudiation (the potential for an unauthorized user to deny that they accessed the data), Information disclosure (the potential for an unauthorized user to access and exfiltrate the data), Denial of Service (the potential for an unauthorized user to render the data unavailable), and Elevation of Privilege (the potential for an unauthorized user to gain administrative access to the data).

Based on their analysis, the team determined that the most effective mitigation strategies were to implement additional security measures, such as two-factor authentication and encryption of sensitive information, and to conduct regular threat hunts to monitor for any potential threats. The team also decided to continuously monitor the security posture of the multi-cloud environment to ensure that the risk of unauthorized access to sensitive information was reduced.

Thanks to the thorough threat modeling process, the security team at the large organization was able to determine the most effective mitigation strategies to reduce the risk of unauthorized access to sensitive information. This helped to enhance the overall security posture of the organization and reduce the risk of a security incident.

MITIGATION PHASE

The mitigation stage of the threat hunting process is critical to ensuring the security of CloudCo's multi-cloud environment. After performing a thorough risk analysis and threat modeling, the security team at CloudCo had identified several mitigation strategies to minimize the risks to the sensitive information stored on their cloud storage and databases.

One of the mitigation strategies was to implement multi-factor authentication (MFA) for all cloud-based applications and APIs that accessed sensitive information. This would prevent unauthorized access to the sensitive information, even if an attacker was able to gain access to a VM. The security team also implemented encryption for all sensitive data stored on the cloud, further reducing the risk of unauthorized access.

Another mitigation strategy was to regularly review and update the company's security policies and procedures. The security team conducted a comprehensive review of their security measures, identifying any gaps and areas for improvement. They then updated their policies and procedures to better protect their sensitive information and to ensure that their security posture was maintained.

To continuously monitor the security posture of their multi-cloud environment, the security team at CloudCo implemented a continuous monitoring program. This program monitored the security logs, network traffic, and endpoint data, and provided real-time alerts for the security team to investigate. The continuous monitoring program also provided the security team with valuable insight into the effectiveness of their mitigation strategies, and it helped them to identify any potential threats in a timely manner.

Finally, the security team at CloudCo conducted regular table top exercises to simulate potential threats and to enhance the company's preparedness and response capabilities. These exercises helped the security team to identify any weaknesses in their security measures and to improve their overall security posture.

A fictional example of a mitigation report

Mitigation Report: Protecting Sensitive Information in CloudCo's Multi-cloud Environment

Introduction

This report outlines the mitigation strategies that have been identified to protect sensitive information stored in CloudCo's multi-cloud environment. The report includes a detailed action plan and timeline to implement the strategies, as well as information on who should be responsible, accountable, and informed throughout the deployment.

Background

CloudCo is a financial technology (fintech) company that provides innovative financial services to businesses and individuals. The company has rapidly grown in recent years, and it now serves millions of customers across the world. CloudCo has embraced the power of the cloud to support its business operations and to ensure that it can meet the demands of its growing customer base.

CloudCo's multi-cloud environment is critical to its success. It uses a combination of public and private clouds to store and process sensitive customer data, such as financial transactions, personal information, and confidential business documents. The company also uses cloud-based applications and APIs to provide its customers with access to financial services, such as online banking, investments, and loans.

However, the sensitive data retained by CloudCo is at risk of being exfiltrated by malicious actors. The company is aware that its virtual machines (VMs) in the cloud can be vulnerable to attacks, and that an unauthorized user who gains access to a VM could potentially move laterally to access the sensitive data. This is a major concern for CloudCo, as a data breach could result in severe financial losses, damage to its reputation, and loss of customer trust.

Mitigation Strategies

The following mitigation strategies have been identified to protect sensitive information stored in CloudCo's multi-cloud environment:

- Implement Multi-factor Authentication (MFA)

  To protect sensitive information stored in the cloud, CloudCo will implement multi-factor authentication (MFA) for all users accessing the cloud environment. MFA will require users to provide two or more forms of authentication, such as a password and a security token, to access the cloud. This will reduce the risk of unauthorized access to sensitive information, even if an attacker gains access to a user's password.

- Encrypt Sensitive Data

  CloudCo will encrypt all sensitive data stored in the cloud. This will ensure that the data is protected, even if it is accessed by an unauthorized user. CloudCo will use encryption algorithms that are widely accepted as secure, such as AES or RSA, and will use encryption keys that are stored securely and only accessible by authorized personnel.

- Implement Access Controls

  CloudCo will implement access controls to limit access to sensitive information stored in the cloud. Access controls will be based on the principle of least privilege, which means that users will only have access to the information that they need to perform their job. Access controls will be implemented using role-based access controls, which assign different levels of access to different roles within the organization.

- Regularly Monitor the Cloud Environment

CloudCo will regularly monitor the cloud environment to detect any unusual or suspicious activity. The security team will use security analytics platforms, such as Microsoft Kusto, Splunk, and Elasticsearch, to analyze logs and network traffic for signs of potential threats. The security team will also continuously monitor the cloud environment to ensure that the mitigation strategies are effective and to identify areas for improvement.

Action Plan and Timeline

The following action plan and timeline have been developed to implement the mitigation strategies:

- Implement Multi-factor Authentication (MFA)
  - Week 1: Evaluate MFA solutions and select a vendor.
    - Responsible: Security team
    - Accountable: CTO
    - Consulted: Procurement department, Legal department
    - Informed: Employees
  - Week 2-4: Work with the vendor to implement MFA for all virtual machines (VMs) in the multi-cloud environment. This includes testing and verifying the MFA solution to ensure it meets the company's security requirements.
    - Responsible: Security team, Vendor
    - Accountable: CTO
    - Consulted: Network architects, Procurement department
    - Informed: Employees
  - Week 5: Conduct user training sessions to educate employees on the use of MFA and the importance of using it to secure their VMs.
    - Responsible: Security team
    - Accountable: HR department
    - Consulted: Vendor
    - Informed: Employees
  - Week 6: Roll out MFA to all employees
    - Responsible: Security team
    - Accountable: CTO
    - Consulted: Vendor
    - Informed: Employees
- Implement Network Segmentation
  - Week 1-2: Work with network architects to evaluate the current network infrastructure and determine the best approach for implementing network segmentation.
    - Responsible: Network architects, Security team
    - Accountable: CTO
    - Consulted: Vendor
    - Informed: Employee
  - Week 3-5: Implement network segmentation by creating separate subnets for different types of VMs, such as storage, databases, and applications.
    - Responsible: Network architects, Security team
    - Accountable: CTO
    - Consulted: Vendor
    - Informed: Employees

Week 6: Test the network segmentation to ensure it is functioning correctly and meeting the company's security requirements.
Responsible: Network architects, Security team
Accountable: CTO
Consulted: Vendor
Informed: Employees

- Regular Penetration Testing
  Week 1: Evaluate penetration testing solutions and select a vendor.
  Responsible: Security team
  Accountable: CTO
  Consulted: Procurement department, Legal department
  Informed: Employees
  Week 2-4: Work with the vendor to schedule regular penetration testing for the multi-cloud environment. This includes testing for vulnerabilities and ensuring that the company's security measures are effective.
  Responsible: Security team, Vendor
  Accountable: CTO
  Consulted: Network architects
  Informed: Employees
  Week 5: Review the results of the penetration testing and make any necessary updates to the company's security measures.
  Responsible: Security team
  Accountable: CTO
  Consulted: Vendor
  Informed: Employees
  Week 6: Repeat the penetration testing process on a regular basis to ensure the company's security posture remains strong.
  Responsible: Security team
  Accountable: CTO
  Consulted: Vendor
  Informed: Employee
- Continuous Monitoring
  Week 1: Evaluate continuous monitoring solutions and select a vendor.
  Responsible: Security team
  Accountable: CTO
  Consulted: Procurement department, Legal department
  Informed: IT Department
  Week 2-4: Work with the vendor to implement continuous monitoring for the multi-cloud environment. This includes setting up alerts and notifications for potential threats and conducting regular analysis of the security logs, network traffic, and endpoint data.
  Responsible: Security team, Vendor
  Accountable: CTO
  Consulted: Security and IT architects, Procurement department
  Informed: IT Department

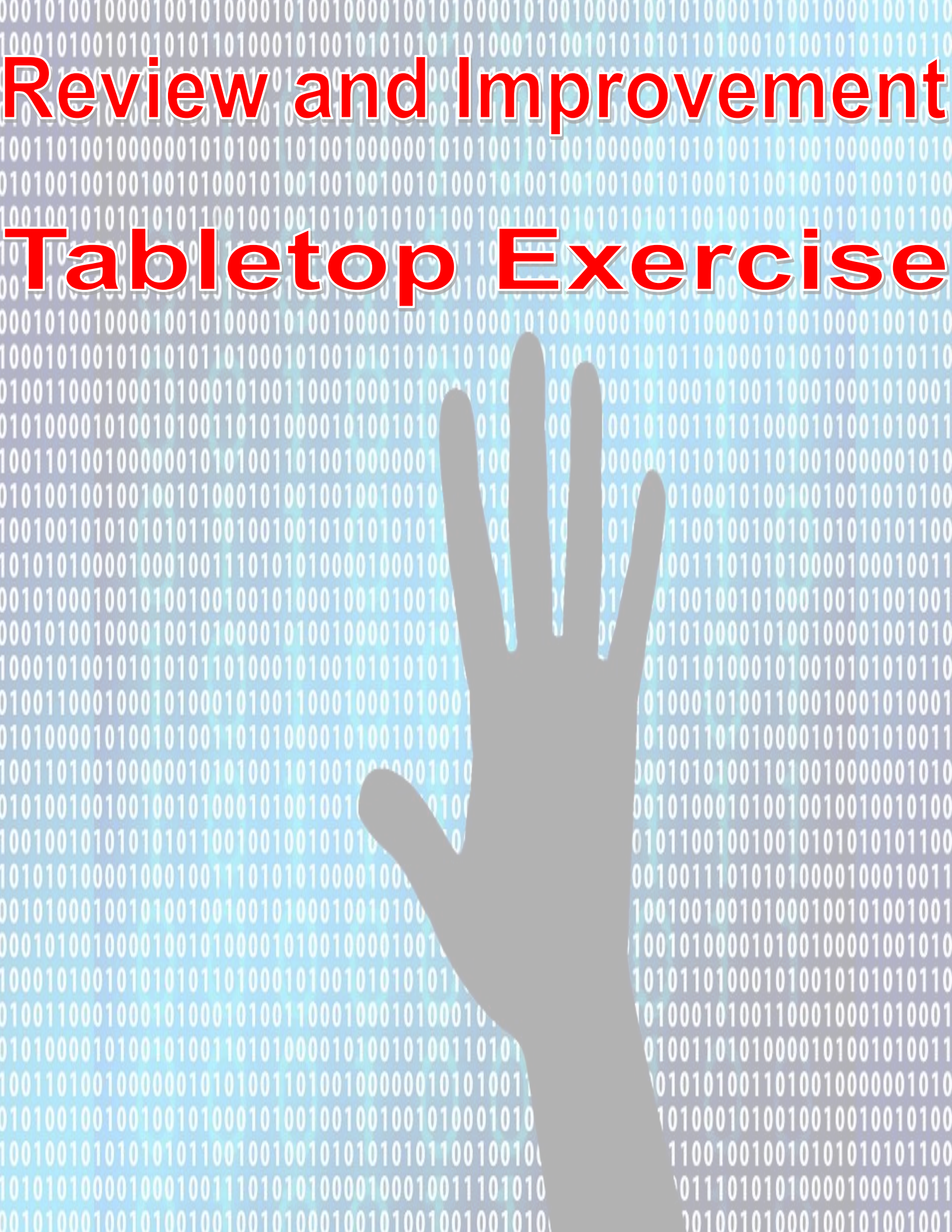
Week 5: Test the continuous monitoring solution to ensure it is functioning correctly and meeting the company's security requirements.
Responsible: Security team, Vendor
Accountable: CTO
Consulted: Security and IT architects, Procurement department
Informed: IT Department

Week 6: Begin continuous monitoring of the multi-cloud environment to detect and respond to potential threats in real-time.

Responsible: Security Team
Accountable: CTO
Consulted: Continuous Monitoring Vendor
Informed: IT Department

Review and Improvement

Tabletop Exercise



The last parts of the full process are the **Review and Improvement, and the tabletop exercise**.

CloudCo understands the importance of regularly reviewing and improving their threat hunting process to stay ahead of evolving threats in the cyber landscape. To ensure that the process remains effective, the company has established a review and improvement phase. This phase involves regularly evaluating the threat hunting process and making updates as needed to incorporate new techniques, tools, and changes in the threat landscape.

To support the review and improvement phase, the company also conducts regular tabletop exercises. A tabletop exercise is a simulated scenario that is used to test the readiness and response of an organization's security team in the event of a potential threat. These exercises are designed to test the effectiveness of the threat hunting process and the preparedness of the security team. During these exercises, the team simulates a real-world threat scenario and responds to it as if it were a real incident. This allows the team to evaluate their response capabilities and identify areas for improvement in the threat hunting process.

Tabletop exercises are an important component of their proactive threat hunting process, as they allow the company to evaluate the effectiveness of their security measures and to identify areas for improvement. The following is an example of a tabletop exercise that could be conducted by CloudCo:
Scenario: A threat actor group has targeted virtual machines (VMs) in multi-cloud environments and has the capability to move laterally to exfiltrate sensitive information.
Objective: To test the company's readiness and response in the event of a potential breach.
Steps:

1. Assemble the security team and inform them of the scenario.
2. Review the proactive threat hunting process and the mitigation strategies that have been implemented.
3. Simulate a potential breach, with the security team responding as if it were a real-life event.
4. Evaluate the response of the security team and assess their ability to identify and respond to the potential threat.
5. Identify areas for improvement in the proactive threat hunting process and the mitigation strategies.
   Review the results of the tabletop exercise with senior management and implement any necessary changes to the proactive threat hunting process and the mitigation strategies.

The tabletop exercise should be conducted regularly, with different scenarios and objectives, to ensure that the security team remains prepared and to continually improve the company's threat hunting process.
The results of the tabletop exercises are used to make improvements to the threat hunting process, such as updating the mitigation strategies, refining the risk analysis process, and incorporating new threat hunting tools. These improvements help to ensure that the company remains well-prepared to respond to potential threats in their multi-cloud environment.
To ensure that the review and improvement phase and tabletop exercises are effective, the security team is responsible for leading the effort, with support from other departments such as IT, Legal, and Compliance. The security team will also keep key stakeholders informed of the results of the exercises and any changes made to the threat hunting process.
The review and improvement phase and table top exercises play a critical role in ensuring that CloudCo's threat hunting process remains effective and well-prepared to respond to potential threats in their multi-cloud environment. By regularly reviewing and improving the process, the company is able to maintain the security of their sensitive data and protect their customers from potential breaches.


conclusion

In conclusion, CloudCo has successfully implemented a proactive threat hunting process to protect its sensitive customer data in its multi-cloud environment. This process starts with the collection and analysis of data from various sources, including security logs, network traffic, and endpoint data. The security team uses threat intelligence to identify new and emerging threats and to determine which potential threats to focus on. They then use threat hunting tools, such as security analytics platforms, to validate the threats and determine their impact.

The team then performs a risk analysis to assess the impact of the potential threats, evaluate the likelihood of a threat being realized, and determine the potential consequences of a successful attack. They then perform threat modeling to create a representation of the virtual machines (VMs), storage, databases, key vaults, applications, and APIs, identify the assets, evaluate the threats, and determine the mitigation strategies.

Thanks to the proactive threat hunting process, CloudCo was able to identify and respond to the potential threat before it could cause any harm. The company implemented the necessary mitigation strategies, such as multi-factor authentication (MFA), network segmentation, regular penetration testing, and continuous monitoring. These mitigation strategies helped to protect sensitive customer data and maintain the security of the multi-cloud environment.

The company also conducted regular tabletop exercises to test the effectiveness of the threat hunting process and the preparedness of the security team. This helped to identify areas for improvement and ensure the process remains effective in protecting sensitive customer data.
The proactive threat hunting process has provided several benefits for CloudCo. It has helped to maintain the security of the multi-cloud environment and protect the sensitive customer data from potential threats. It has also helped to build trust with customers by demonstrating a commitment to security and protecting their data.

However, the company may face some challenges as it continues to implement the proactive threat hunting process. These challenges may include the cost and resource requirements for implementing the mitigation strategies, the need for regular updates to the process to reflect changes in the threat landscape, and the need for continuous monitoring and improvement to ensure the process remains effective.
Despite these challenges, the proactive threat hunting process is a critical component of CloudCo's overall security strategy and is essential for protecting sensitive customer data in its multi-cloud environment. The company will continue to invest in the process and incorporate new techniques and tools to ensure it remains effective in protecting its sensitive information from potential threats.