CyberProof®

ATTACK USE CASES

# SECURITY ORCHESTRATION AND AUTOMATION

# TABLE OF CONTENTS

# INTRODUCTION

It's no secret that cyber attacks are on the rise, becoming more complex to detect and mitigate. As security teams grapple with more tools to manage and alerts to process, they can quickly become overwhelmed. As a result, they don't have time to proactively hunt for threats and test for vulnerabilities. With each new threat, it becomes harder to collate and correlate intelligence and collaborate with stakeholders to solve complex problems. This in turn means that the most urgent incidents get missed and the capacity to respond rapidly and effectively is limited.

CyberProof can help. The CyberProof Defense Center (CDC) is a cloud-based Security Orchestration, Automation, and Response (SOAR) platform used by our security operations team to deliver Managed Detectoin and Response services. The following sections provide greater detail about how we utilize orchestration and automation to detect and overcome attacks.

# BRUTE FORCE ATTACK

## THE PROBLEM

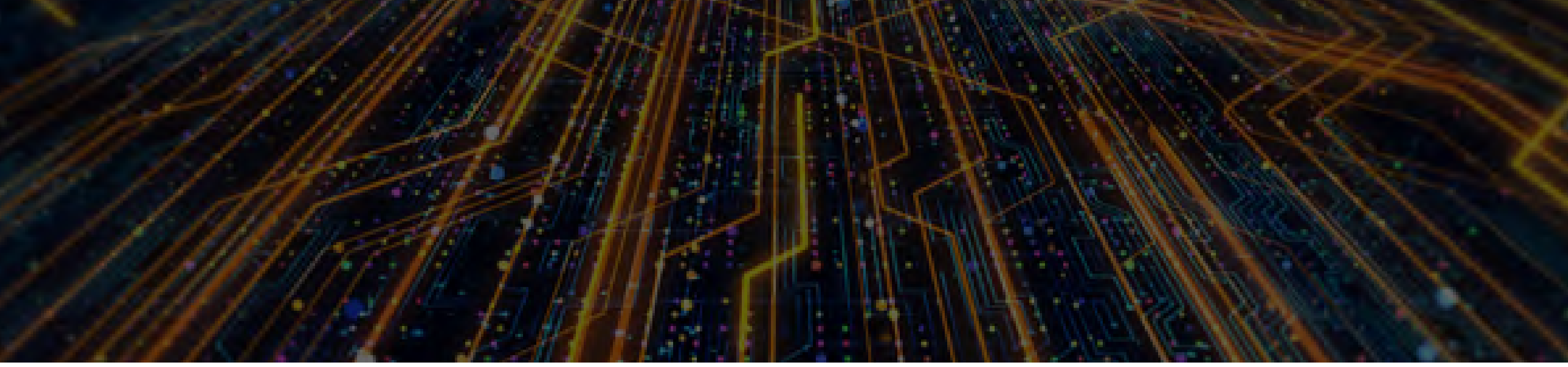
The number and intensity of brute force attacks increased dramatically in recent years – and stronger brute force attacks have become the norm.

## BACKGROUND

Brute-forcing passwords can allow attackers entrance to target infrastructure. For example, a hacker can compromise an organization's server first by a brute-force attack on passwords for the RDP protocol, then by conducting reconnaissance of the internal network. Factors that contribute to the success of this kind of attack include the use of dictionary passwords, the lack of two-factor authentication, and insufficient protection of resources. The attack is even more likely to be effective if the password for the OS administrator is weak, and if computer and server RDP ports are open to Internet connections.

Brute force attacks can involve any of the following scenarios:

1. **Internal brute force attack,** where someone on the inside of the organization attacks.
2. **External brute force attack,** which is remote – i.e., an attack on a service provided by the organization that is used by its employees.
3. **Application attack,** i.e., an attack on external and mobile applications that are used by employees or customers.
4. **Offline brute force attack,** in which an attacker succeeds in obtaining a database of encrypted passwords and continues to attack it offline.

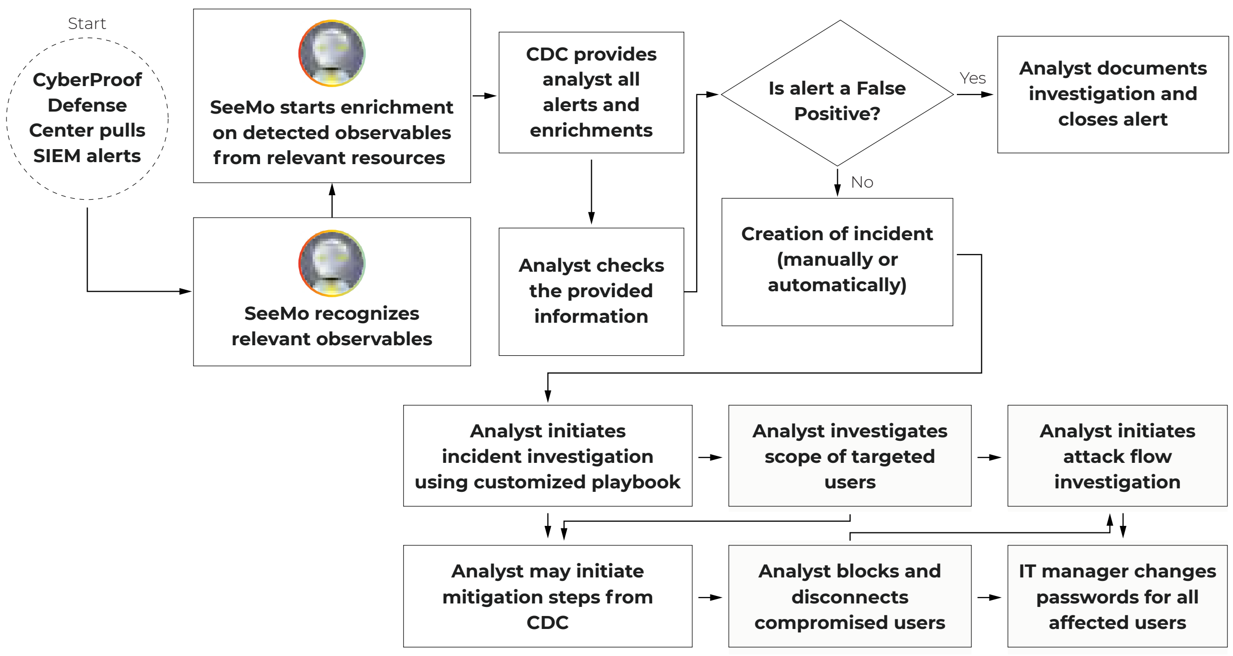


# HOW IT WORKS

In this use case, we're focusing on an internal brute force attack.

An attacker obtains access to high-privilege users, which gives the attacker the ability to harm the organization.

The attacker tries to uncover the password for a particular user, leveraging the many automation tools available that allow testing thousands of options per minute.


Start
CyberProof Defense Center pulls SIEM alerts
SeeMo recognizes relevant observables
SeeMo starts enrichment on detected observables from relevant resources
CDC provides analyst all alerts and enrichments
Analyst checks the provided information
Is alert a False Positive?
Yes
Analyst documents investigation and closes alert
No
Creation of incident (manually or automatically)
Analyst initiates incident investigation using customized playbook
Analyst investigates scope of targeted users
Analyst initiates attack flow investigation
Analyst may initiate mitigation steps from CDC
Analyst blocks and disconnects compromised users
IT manager changes passwords for all affected users

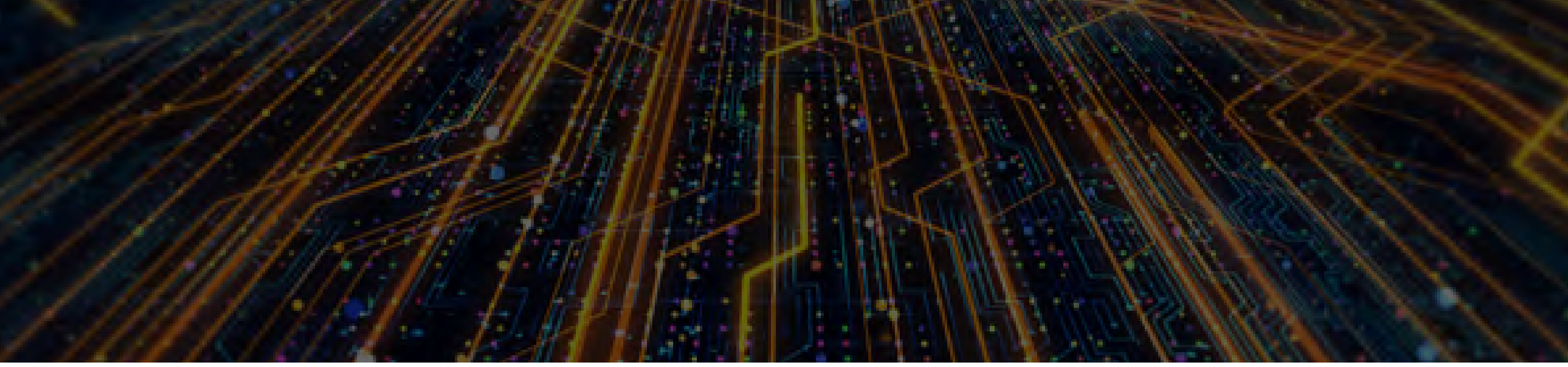
Workflow for Brute Force Attack

# THE SOLUTION

## STAGE 1: PREPARATION

Prior to the attack, cyber security protective mechanisms need to be put into place:

- Using the CDC, connect to the customer's authentication and authorization service.
- Create a customer-specific digital playbook for handling a brute force attack.



## STAGE 2: DETECTION & ANALYSIS

An indication of a brute force attempt is detected by the SIEM – which has been pre-configured with a set of rules developed and provided by CyberProof.

The SIEM identifies failed attempts to gain access, and the following process takes place:

1. The CDC provides enrichment information:
   - **User Information** – The CDC provides enriched information related to the user.
   - **Work Station Information** – The CDC provides enriched information about the user's work environment.
   - **Network Topology** – The CDC provides the analyst with details of the network topology and the architecture to better understand the layout of the attack.
   - **User Confirmation** – The CDC makes contact with users whose accounts indicate a brute force attempt, sending messages by cell phone that ask whether they attempted to log in. Each user responds, either indicating it was an error, or confirming the existence of a brute force attack. This eliminates the possibility of a False Positive.
2. CyberProof analysts follow a playbook that contains a set of manual and automated predefined actions, such as determining the number of users being attacked and checking for irregular network behavior – to eliminate the risk of an actual brute force attack, or to identify the source of an attack and mitigate it.

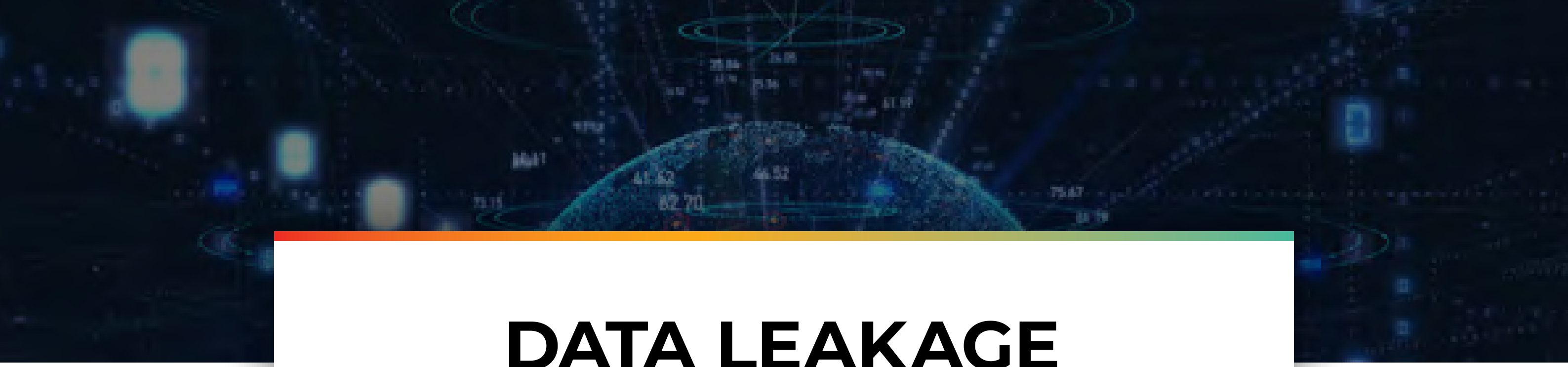
## STAGE 3: MITIGATION

The mitigation process involves the following process:

1. Block compromised users and accounts (manually or automatically).
2. Disconnect users whose accounts were compromised, who are already connected (manually or automatically).
3. Perform a controlled password renewal for all of the affected user accounts (manually or automatically).
4. Perform a manual process of root cause analysis, updating rules in accordance with new brute force methods.
5. The organization must assess if the attack caused legal or financial damage  and whether it had an impact on brand equity or at the level of public relations - and act accordingly.

## BENEFITS

By leveraging automation and the team's expertise, CyberProof allows you to reduce the time involved in identifying brute force attacks – thereby mitigating the damage, reducing dwell time from detection to remediation, and providing clear procedures that are understood inside the organization.



# DATA LEAKAGE

## THE PROBLEM

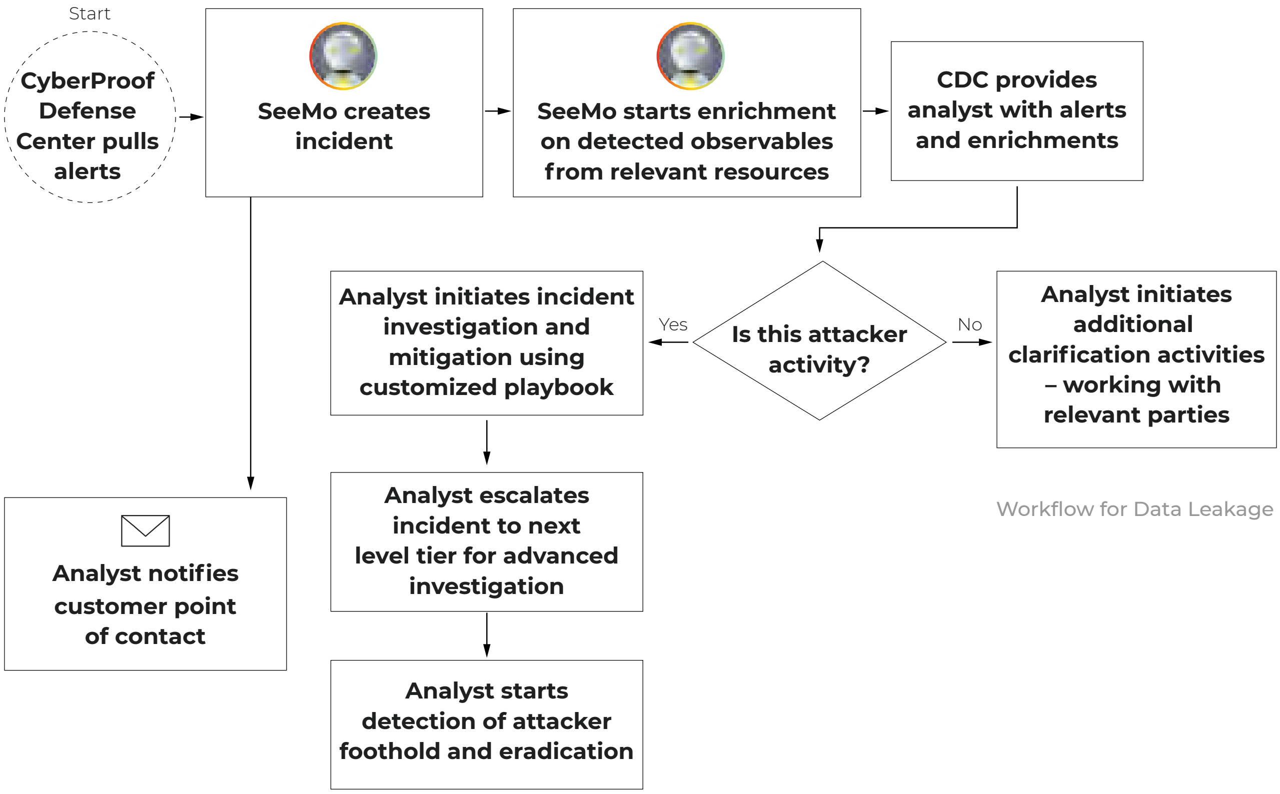
Data leakage is the unauthorized transmission of data from within an organization to an external destination or recipient. In some cases, data leakage is undetected for a long period of time, even when a Data Loss Prevention (DLP) system is in place.

## BACKGROUND

Data leakage includes several possible scenarios:

1. A hacker who penetrated into the organization is exfiltrating data through a compromise or breach.
2. An employee leaked sensitive information.
3. There was a human error in the configuration of security appliances and products.
4. The data was already exposed and it is being sold or offered online via darknet forums.

Data leakage can lead to direct costs (a fine that an organization has to pay, and the legal and brand-related costs of recovery) and indirect costs (the potential loss of customers and brand equity).


Start
CyberProof Defense Center pulls alerts
SeeMo creates incident
SeeMo starts enrichment on detected observables from relevant resources
CDC provides analyst with alerts and enrichments
Is this attacker activity?
Yes
No
Analyst initiates incident investigation and mitigation using customized playbook
Analyst initiates additional clarification activities – working with relevant parties
Analyst escalates incident to next level tier for advanced investigation
Analyst starts detection of attacker foothold and eradication
Analyst notifies customer point of contact

Workflow for Data Leakage

## THE SOLUTION

Investigate and mitigate a data leakage incident as quickly as possible, to prevent additional loss. This is achieved in the CDC platform utilizing our automated AI-enhanced SeeMo bot and digital playbooks, which reduce risk of breach to a minimum.

## STAGE 1: PREPARATION

Prior to an attack, a definition of leakage should be agreed upon, to allow proper identification of incidents. Cyber security protective mechanisms must be put into place, including:

Setting up and integrating with the CDC: Vulnerability Scanning Tools, Cyber Threat Intelligence, Employee Awareness Programs, Data Leakage Monitoring, etc.

Receiving access to and integrating the customer's SIEM, security appliances, and connectors with the CDC for orchestration & automation of security alerts and incidents.

Customizing standard playbooks, and creating "customer-specific" playbooks for handling and investigating data leakage.

Creating a customized Incident Response Methodology (IRM) according to the customer environment.

## STAGE 2: DETECTION & ANALYSIS

The CyberProof team leverages the CyberProof platform and SeeMo, and obtains automatic enrichment of the data leakage. A combination of SeeMo automation and human expertise handles the following:

1. Continuously monitors all relevant security appliances and systems.
2. Checks for related security alerts that can provide additional context for this alert.
3. Provides enrichment for all involved hosts, users, URLs, and IPs (internal and external).
4. Researches the bad actors and tracks them; and conducts threat hunting to uncover additional suspicious activity and prevent additional hacks.
5. Investigates how and from where the data was exfiltrated.

## STAGE 3: MITIGATION

In the specific case where a hacker penetrated an organization and is trying to exfiltrate data, CyberProof follows automated mitigation steps in collaboration with the customer.

These include:

1. **Limit access** – For example, perform hardening of the Active Directory/Firewall by narrowing access for certain users or groups.
2. **Limit functionality** – Block the ability to exfiltrate additional data by disabling copy/paste functionalities or disabling/removing user accounts.
3. **Perform advanced investigation** – Understand circumstances and content, and gain a fuller picture.
4. **Eradicate the hacker's foothold** – Figure out how hackers compromised the organization and take steps to ensure they cannot cause further damage – for example, by understanding how they accessed sensitive information and identifying the server or station and credentials which they used.
5. **Perform threat intelligence** – Conduct tailored intelligence, actively monitoring multiple threat sources across the clear, dark and deep web; gain real-time visibility of organizations, data & people to track the leaked data.
6. **Assess the damage -** The organization must assess if the attack caused legal or financial damage and whether it had an impact on brand equity or at the level of public relations - and act accordingly.

## BENEFITS

By leveraging the power of automation and taking advantage of the team's expertise and proven processes, CyberProof allows you to reduce the time taken in identifying and handling data leakage – thereby minimizing the impact on your organization.

CyberProof's approach allow you to establish and maintain clear procedures that are understood inside the organization, and reduces the mean time to resolving incidents from detection to mitigation.

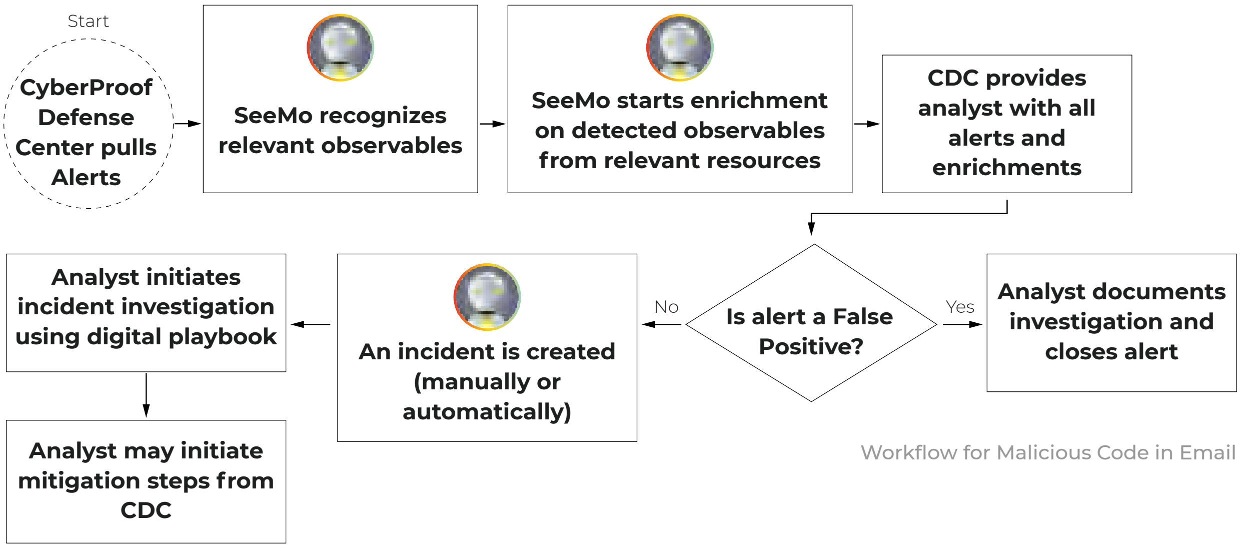
# MALICIOUS CODE IN EMAIL

## THE PROBLEM

While malicious code may present itself in many forms, lately the most common infection method starts by sending a malicious email to an employee. Existence or execution of malicious code within the organization perimeter presents a high risk and has the potential to “take down” multiple company activities. This use case describes a scenario in which an email was delivered; and the host was likely infected.

## BACKGROUND

Bad actors use malicious code to enter into an organization through email. Here’s one example of how it works: A victim clicks an attachment and starts the “process” suggested by the email; then, a downloaded document convinces the victim to disable security protection - enabling ActiveX or macros.


Start
CyberProof Defense Center pulls Alerts
SeeMo recognizes relevant observables
SeeMo starts enrichment on detected observables from relevant resources
CDC provides analyst with all alerts and enrichments
Is alert a False Positive?
Yes
Analyst documents investigation and closes alert
No
An incident is created (manually or automatically)
Analyst initiates incident investigation using digital playbook
Analyst may initiate mitigation steps from CDC

Workflow for Malicious Code in Email

# THE SOLUTION

Detect, investigate and mitigate a malicious code incident as quickly as possible to prevent additional loss. This is achieved using the CDC platform utilizing SeeMo bot and digital playbooks to reduce risk of breach to a minimum.

## STAGE 1: PREPARATION

Deploy Antivirus (AV) and Endpoint Detection & Response (EDR) updates, employee awareness, monitoring, etc. (This must be done as a precautionary measure prior to the attack.)

Receive access and connect the customer's mail box, SIEM, Mail Relay, and ticketing system to the CDC for orchestration & automation of alerts and incidents.

Create customer-specific playbooks for handling malicious code that penetrates into the network.

Create IRMs that are customized to the customer environment.

## STAGE 2: DETECTION & ANALYSIS

The CyberProof team leverages the CyberProof platform and SeeMo, and obtains automatic enrichment of the malicious code that penetrated into the network – investigating the alert as follows:

1. SeeMo collects all relevant information from the alert and obtains more details regarding the infected host, user, or department.
2. SeeMo then searches for all possible information about the malware: search by name, file name, hashing, etc.
3. The analyst collects all of the necessary information and makes an informed decision about how to mitigate the incident.

## STAGE 3: MITIGATION

SeeMo searches for all possible information about the malware: search by name, file name, hashing, etc.

The analyst then takes the following steps:

1. **Define action items** – The CDC enables the analysts to start handling the incident by providing action items to the on-premises security team and initiating mitigation actions.
2. **Deepen the analysis** – For incidents where additional analysis is required, CyberProof's tier 3 & 4 analysts do the following:
    - Analyze and classify the malware.
    - Investigate how it works.
    - Conduct forensics on the infected station.
    - Generate new Indicators of Compromise (IoCs).
3. **Work with the customer** – The analysts work with the customer in the following ways:
    - Block the network connection from the infected station.
    - Check the network & communication logs for attempts to the IoCs provided.
    - Block connection to remote Command and Control (C&C).
4. **Use the anti-virus** – To prevent future attempts, the analysts work with the organization to:
    - Verify that the anti-virus identifies the files; if not, upload and update the anti-virus provider.
    - Rescan the entire organization network for traces of the malicious code.
5. **Assess the damage** – The organization must assess if the attack caused legal or financial damage and whether it had an impact on brand equity or at the level of public relations - and act accordingly.

## BENEFITS

By leveraging the powers of automation and taking advantage of our expertise and proven processes, CyberProof allows you to reduce the time taken in identifying and handling malicious code – thereby minimizing the impact on your organization.

CyberProof allows you to establish and maintain clear procedures that are understood inside the organization, and reduces the Mean Time to Response (MTTR) - resolving incidents from detection to mitigation.

# SUSPICIOUS EMAIL

## THE PROBLEM

Organizations are increasingly concerned about suspicious emails. The damage caused by suspicious emails can be significant: for midsize companies, the average cost of a phishing attack is $1.6 million.

This use case describes a scenario in which a suspicious email penetrated the network and reached an employee – bypassing all protective mechanisms. Since the suspicious email reached the employee, from the perspective of network security, the attack was successful – whether or not the employee actually sent money, handed over sensitive information, or downloaded malware.

## BACKGROUND

Suspicious emails are a high priority for any organization to identify and eliminate. Suspicious emails are categorized in the following ways:

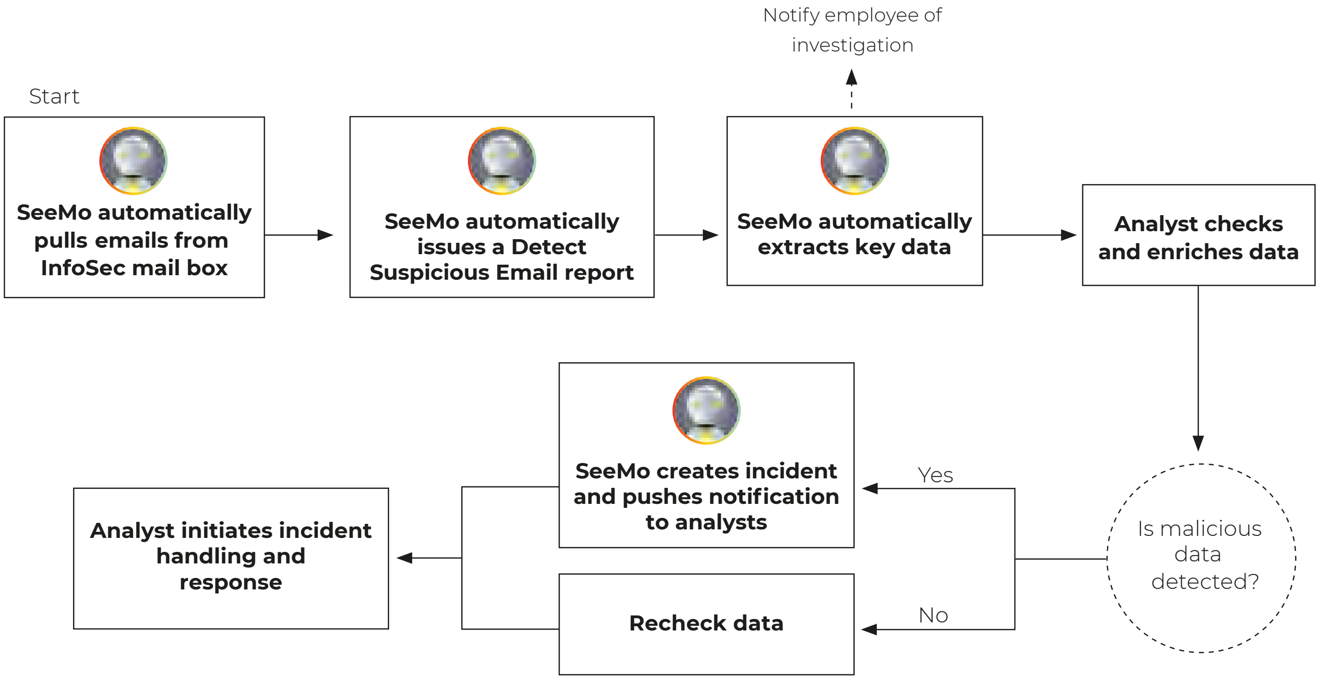
1 **Phishing –** designed to steal money or sensitive information, or to persuade the employee to download malware.

2 **Malware –** involves malicious software taking over a device to spread to other devices and profiles, or infecting a device and turning it into a botnet.

3 **Spam –** persuades the employee to provide credit card or account details in order to get questionable products, offers, or pseudolegal services.

4 **Scam –** offers a bargain for nothing, for example, asking for business or inviting the employee to a website with a detailed pitch.

These kinds of attacks are on the rise because they can be extremely profitable for the perpetrator and as a consequence, the attacks are becoming increasingly more sophisticated. Another reason why they are popular with threat actors is that they provide direct access to end users, who are the most vulnerable part of the network.



Start
SeeMo automatically pulls emails from InfoSec mail box
SeeMo automatically issues a Detect Suspicious Email report
Notify employee of investigation
SeeMo automatically extracts key data
Analyst checks and enriches data
Is malicious data detected?
Yes
No
SeeMo creates incident and pushes notification to analysts
Recheck data
Analyst initiates incident handling and response

Workflow for Suspicious Emails

# THE SOLUTION

Reduce the time involved in identifying and handling the suspicious email.

## STAGE 1: PREPARATION

Prior to the attack, cyber security protective mechanisms need to be put into place, including:

- Setting up the CDC and receiving access to the customer's mail box, SIEM, Mail Relay, and ticketing system.
- Creating a customer-specific playbook for handling suspicious emails that penetrate the network.

## STAGE 2: DETECTION & ANALYSIS

The CyberProof team leverages the CDC, and obtains automatic enrichment of the email that penetrated the network, including:

**Links**

SeeMo checks if there is a link in the email and if it points to a malicious site.

**Attachments**

SeeMo checks if there is an attachment and determines whether it is malicious. If there is a zip file, SeeMo checks the status of what's zipped. Any attachments are tested in a sandbox environment using both a dynamic and static approach.

**Sender**

SeeMo determines whether the email sender's server IP matches the sender domain name and address, and looks for misalignment between the different fields.

**Recipient**

SeeMo sees if there is anything unusual about how the recipient is addressed.

**Body**

SeeMo evaluates if the body of the email is fraudulent: Does it include well-known phishing words or text? Common strategies employed include:

- Blackmail, such as threatening to publicize information or to lock you out of your computer

- The Nigerian Sting, such as "You won money, to receive it send us your bank details" or "I'm a helpless girl stranded in a difficult situation, I need some money, please send me your details"

**Header**

SeeMo evaluates whether the header is from a malicious player. Perhaps it comes from someone who is connected to the client – from a legitimate sender – and there is no threat?

**Based on this research, a decision is made to categorize the email as a regular email or as a phishing, malicious, spam, or scam email.**

## STAGE 3: MITIGATION

To mitigate a malicious code attack, CyberProof follows mitigation steps in collaboration with the customer.

These include::

1. **Automatically block the sender, by sender ID -** In some cases, this cannot be done automatically. Your organization may need to provide CyberProof with approval from the appropriate personnel before any email senders can be blocked.
2. **Disconnect relevant users -** Users should be disconnected if their accounts were compromised, and they are already connected (manually or automatically).
3. **Send automated response to the employee -** The employee should receive an update regarding which actions were performed.
4. **Assess the damage -** The organization must assess if the attack caused legal or financial damage  and whether it had an impact on brand equity or at the level of public relations - and act accordingly.

## BENEFITS

By leveraging the powers of automation and taking advantage of our team’s expertise, CyberProof allows you to reduce the time involved in identifying and handling suspicious emails – thereby mitigating the damage to your system.

## ABOUT CYBERPROOF

CyberProof is a security services company that intelligently manages your incident detection and response. Our advanced cyber defense platform enables operational efficiency with complete transparency to dramatically reduce the cost and time needed to respond to security threats and minimize business impact. SeeMo, our virtual analyst, together with our experts and your team automates and accelerates cyber operations by learning and adapting from endless sources of data and responds to requests by providing context and actionable information. This allows our nation-state cyber experts to prioritize the most urgent incidents and proactively identify and respond to potential threats. We collaborate with our global clients, academia and the tech ecosystem to continuously advance the art of cyber defense.

CyberProof is part of the UST Global family. Some of the world's largest enterprises trust us to create and maintain secure digital ecosystems using our comprehensive cyber security platform and mitigation services.

For more information, see: www.cyberproof.com

### LOCATIONS

Aliso Viejo | Barcelona | London | Singapore | Tel Aviv | Trivandrum