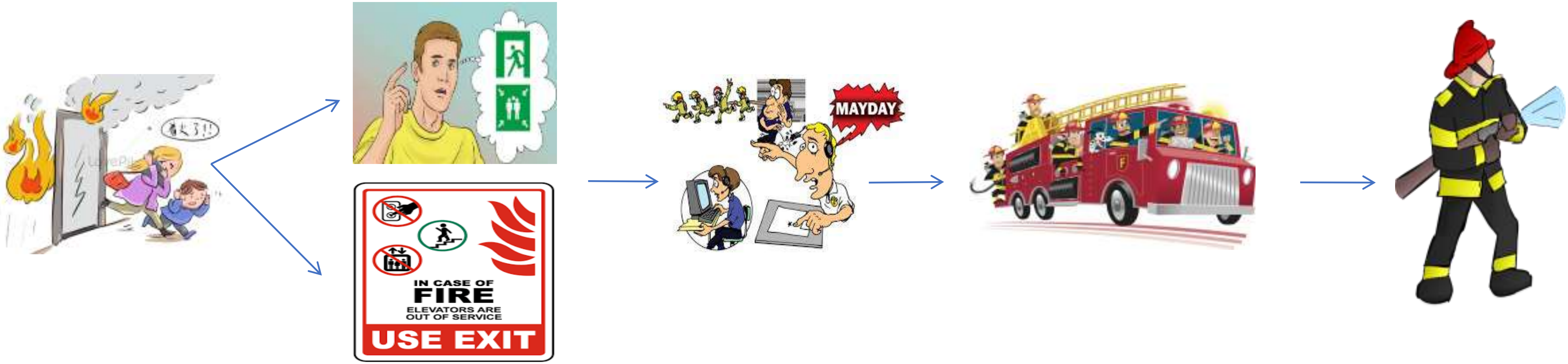
What is a playbook ?

A playbook is typically associated with responding to a cyber incident and gives the actions, procedures and communications associated with responding to a certain incident.

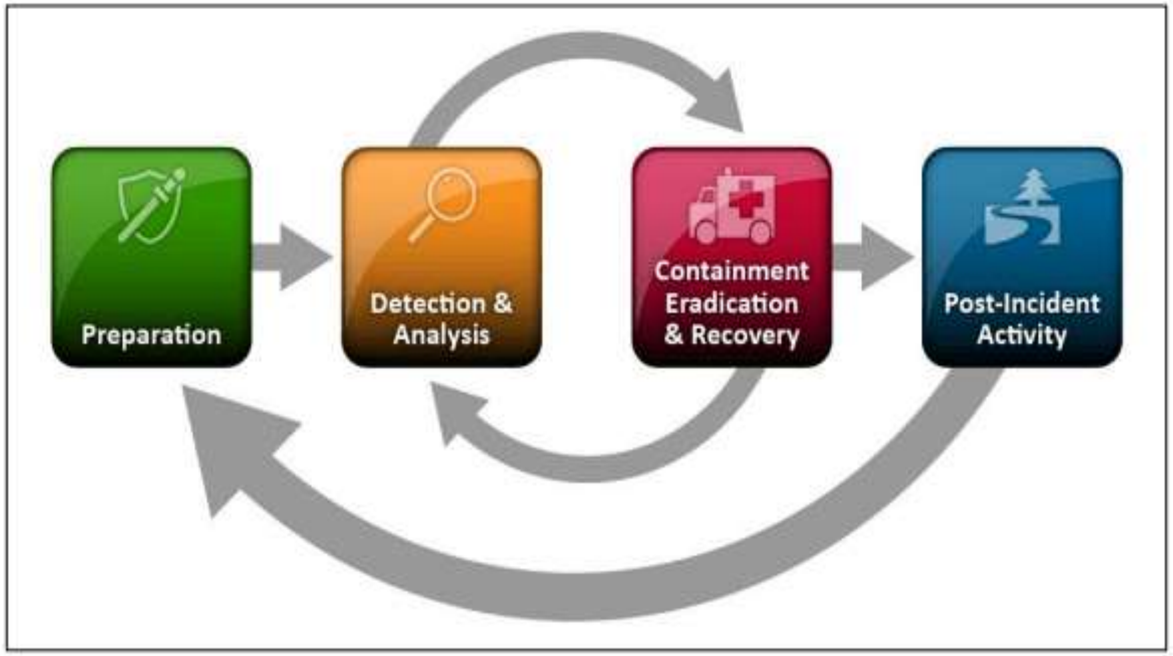
The purpose of a Cyber Security Playbook, or Security Playbook is a document that provides all members of an organization with a clear understanding of their roles and responsibilities - before, during and after a security incident.

Example: Fire fighting SOP is a document which defines the step by step procedures need to be followed at the time of Fire Emergency



NIST Incident Response Steps

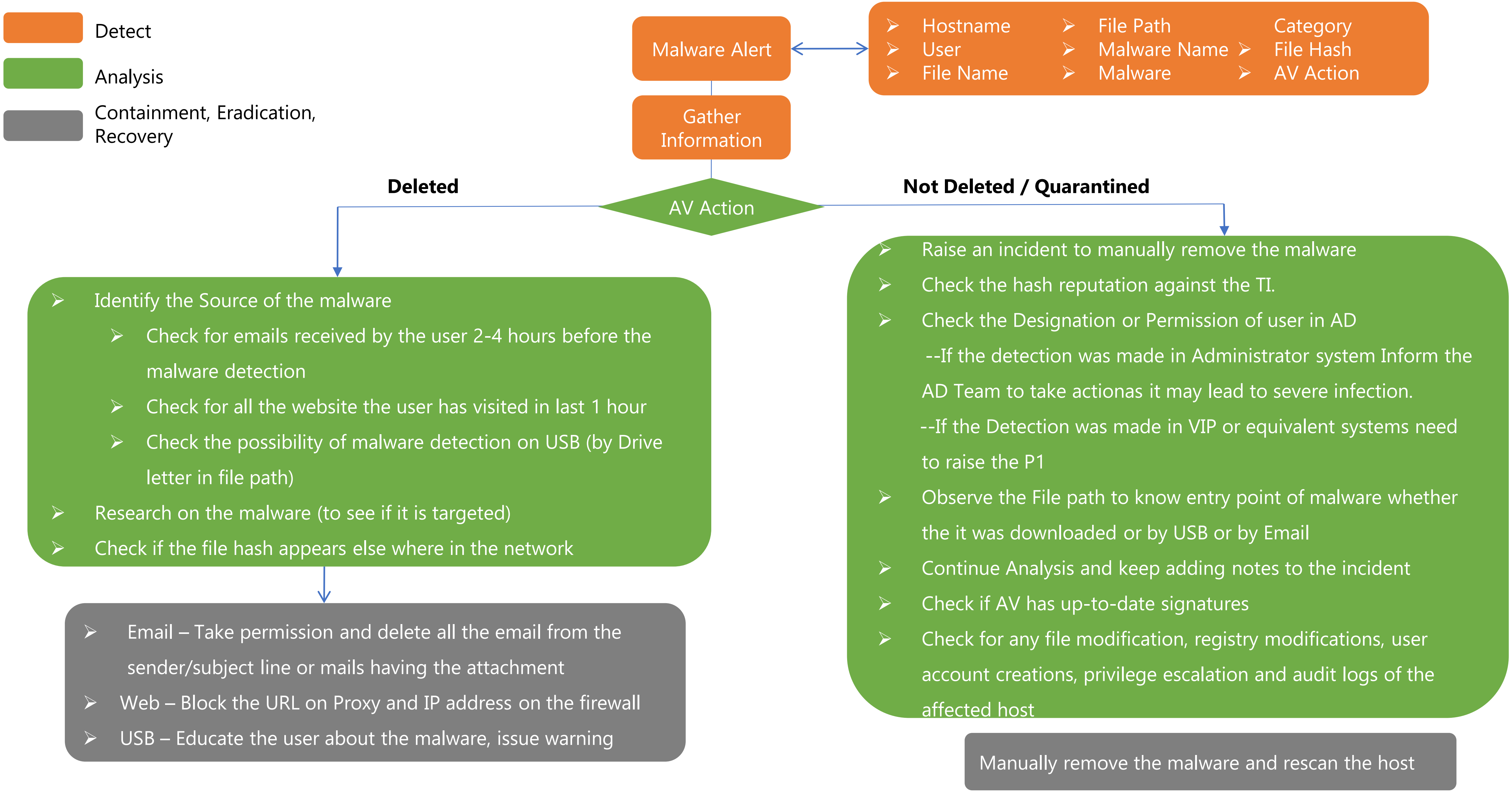
- NIST defines a four-step process for incident response, illustrated in the diagram.
- Incident response is a term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach.
- The goal is to effectively manage the incident so that the damage is limited and both recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum.



NIST Incident Response Steps

- **Preparation:** The Preparation phase covers the work an organization does to get ready for incident response, including establishing the right tools and resources and training the team. This phase includes work done to prevent incidents from happening.
- **Detection and Analysis:** At this point in the process, a security incident has been identified. This is where you go into research mode. Gather everything you can on the the incident. Then analyze it. Determine the entry point and the breadth of the breach.
- **Containment, Eradication and Recovery:** The primary purpose of containment phase is to limit the damage and prevent any further damage from happening. It aims to stop the bleeding. Eradication is the elimination of the components of an incident. It includes things like removing malware, eliminating malicious user accounts and identifying vulnerabilities that were exploited as part of the security incident and patching them. Recovery aims to get the system operational if it went down or simply back to business as usual if it didn't.
- **Post Incident Activity:** Post-incident activity centers on lessons learned to accomplish two things: Improve the incident response capability, and prevent the incident from recurring. The types of questions asked during the post-incident phase include the following:
  1. Whether the SLA was maintained?
  2. Whether the Analyst followed the SOP or not?
  3. Whether the tool triggered the alert as expected or not?
  4. Whether the analyst was capable enough to handle the Issue or not?
  5. Is there any downtime observed in any of the tools?
  6. Was there a proper escalation followed?
  7. Is remediation properly followed or not?

How do you handle a Malware alert?



🟧 Detect

🟩 Analysis

⬛ Containment, Eradication, Recovery

Malware Alert

- Hostname
- User
- File Name
- File Path
- Malware Name
- Malware
- Category
- File Hash
- AV Action

Gather Information

AV Action

Deleted

- Identify the Source of the malware
  - Check for emails received by the user 2-4 hours before the malware detection
  - Check for all the website the user has visited in last 1 hour
  - Check the possibility of malware detection on USB (by Drive letter in file path)
- Research on the malware (to see if it is targeted)
- Check if the file hash appears else where in the network

- Email – Take permission and delete all the email from the sender/subject line or mails having the attachment
- Web – Block the URL on Proxy and IP address on the firewall
- USB – Educate the user about the malware, issue warning

Not Deleted / Quarantined

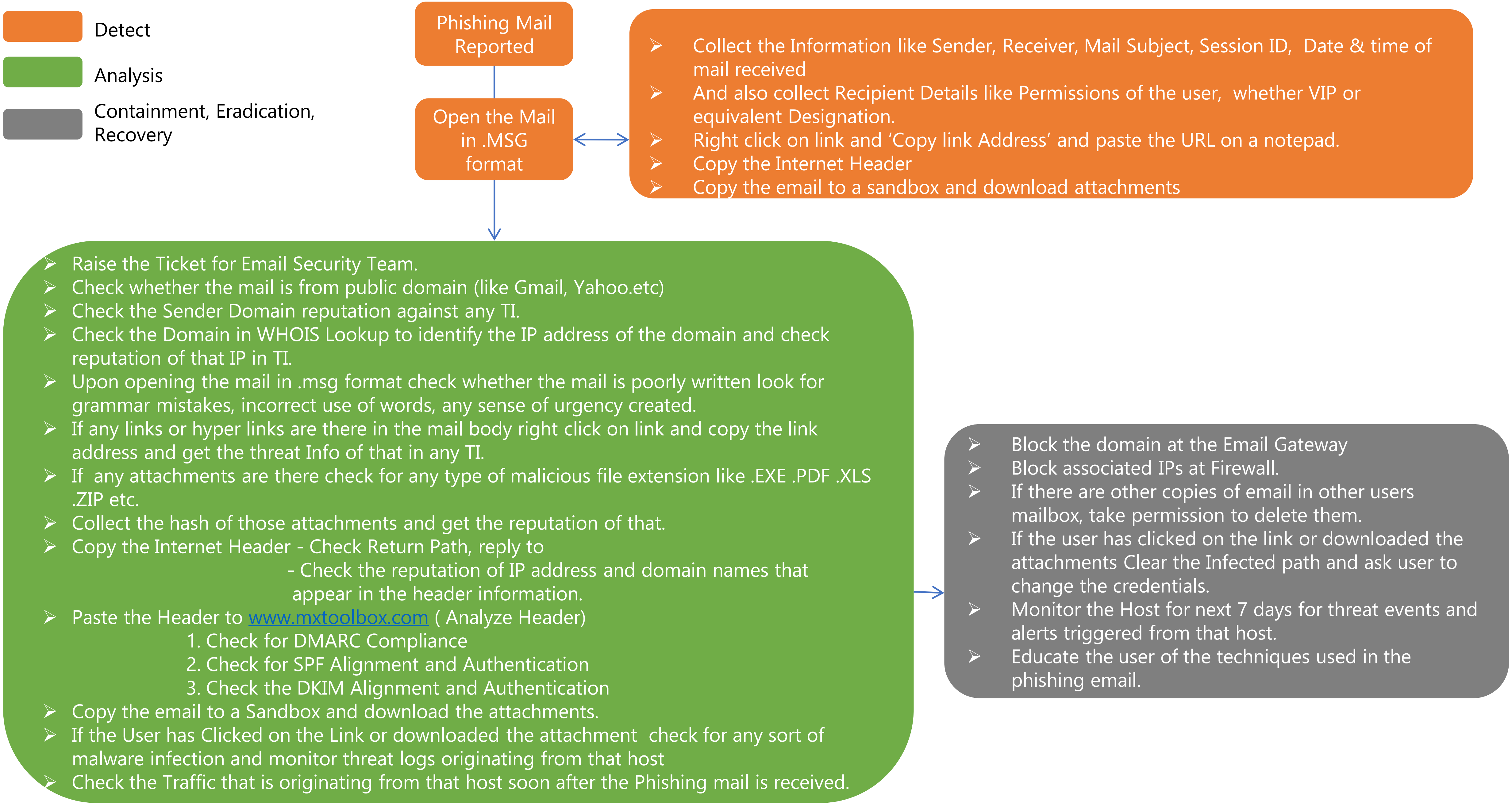
- Raise an incident to manually remove the malware
- Check the hash reputation against the TI.
- Check the Designation or Permission of user in AD

  --If the detection was made in Administrator system Inform the AD Team to take actionas it may lead to severe infection.

  --If the Detection was made in VIP or equivalent systems need to raise the P1
- Observe the File path to know entry point of malware whether the it was downloaded or by USB or by Email
- Continue Analysis and keep adding notes to the incident
- Check if AV has up-to-date signatures
- Check for any file modification, registry modifications, user account creations, privilege escalation and audit logs of the affected host

Manually remove the malware and rescan the host

How do you work on a Phishing Alert?



- 🟧 Detect
- 🟩 Analysis
- ⬛ Containment, Eradication, Recovery

Phishing Mail Reported

Open the Mail in .MSG format

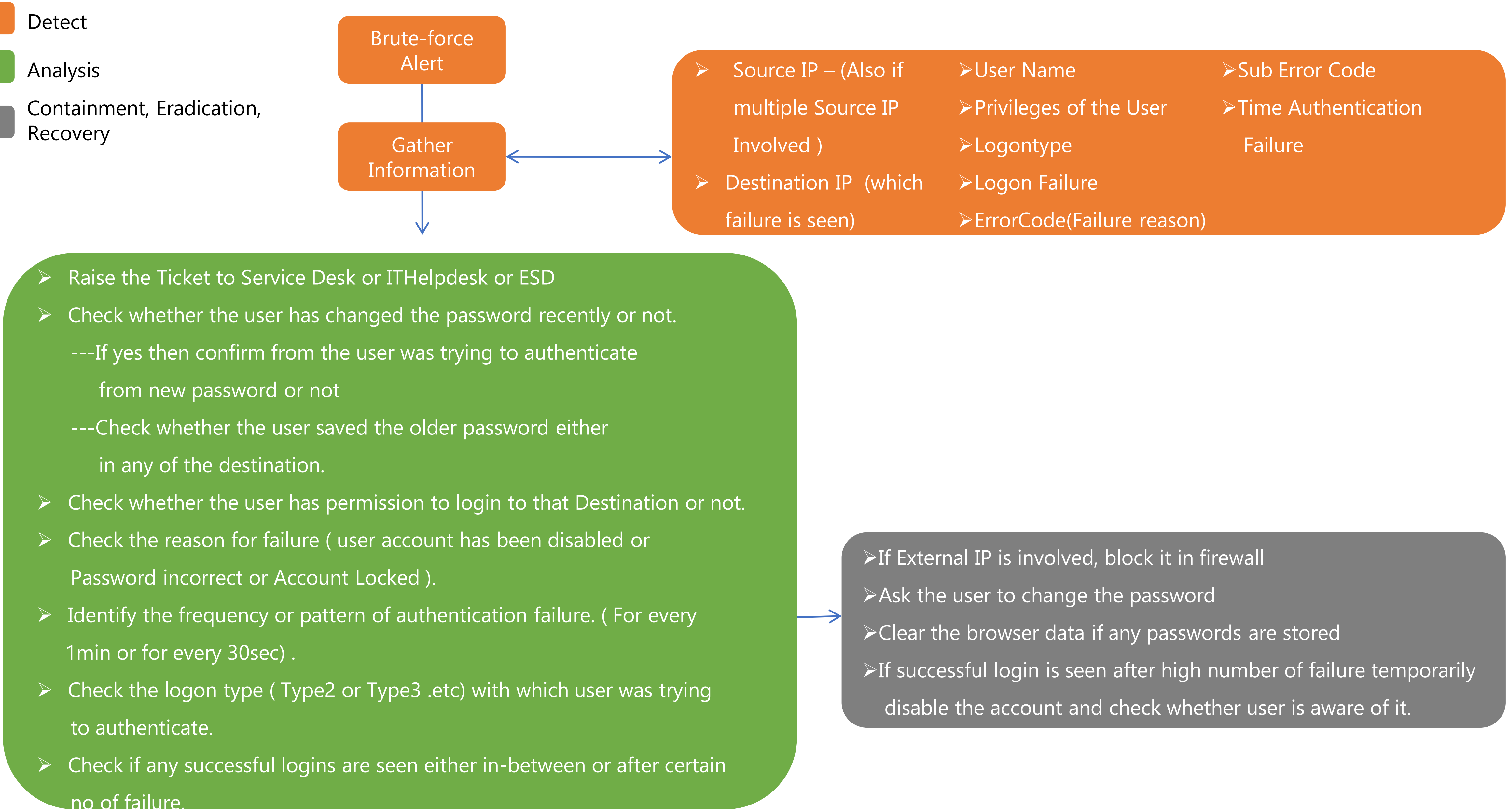
- Collect the Information like Sender, Receiver, Mail Subject, Session ID, Date & time of mail received
- And also collect Recipient Details like Permissions of the user, whether VIP or equivalent Designation.
- Right click on link and 'Copy link Address' and paste the URL on a notepad.
- Copy the Internet Header
- Copy the email to a sandbox and download attachments

- Raise the Ticket for Email Security Team.
- Check whether the mail is from public domain (like Gmail, Yahoo.etc)
- Check the Sender Domain reputation against any TI.
- Check the Domain in WHOIS Lookup to identify the IP address of the domain and check reputation of that IP in TI.
- Upon opening the mail in .msg format check whether the mail is poorly written look for grammar mistakes, incorrect use of words, any sense of urgency created.
- If any links or hyper links are there in the mail body right click on link and copy the link address and get the threat Info of that in any TI.
- If any attachments are there check for any type of malicious file extension like .EXE .PDF .XLS .ZIP etc.
- Collect the hash of those attachments and get the reputation of that.
- Copy the Internet Header - Check Return Path, reply to
  - Check the reputation of IP address and domain names that appear in the header information.
- Paste the Header to www.mxtoolbox.com (Analyze Header)
  1. Check for DMARC Compliance
  2. Check for SPF Alignment and Authentication
  3. Check the DKIM Alignment and Authentication
- Copy the email to a Sandbox and download the attachments.
- If the User has Clicked on the Link or downloaded the attachment check for any sort of malware infection and monitor threat logs originating from that host
- Check the Traffic that is originating from that host soon after the Phishing mail is received.

- Block the domain at the Email Gateway
- Block associated IPs at Firewall.
- If there are other copies of email in other users mailbox, take permission to delete them.
- If the user has clicked on the link or downloaded the attachments Clear the Infected path and ask user to change the credentials.
- Monitor the Host for next 7 days for threat events and alerts triggered from that host.
- Educate the user of the techniques used in the phishing email.

How do you investigate a Brute-force Attack?

- 🟧 Detect
- 🟩 Analysis
- ⬛ Containment, Eradication, Recovery



Brute-force Alert

Gather Information

- Source IP – (Also if multiple Source IP Involved)
- Destination IP (which failure is seen)
- User Name
- Privileges of the User
- Logontype
- Logon Failure
- ErrorCode(Failure reason)
- Sub Error Code
- Time Authentication Failure

- Raise the Ticket to Service Desk or ITHelpdesk or ESD
- Check whether the user has changed the password recently or not.
  ---If yes then confirm from the user was trying to authenticate from new password or not
  ---Check whether the user saved the older password either in any of the destination.
- Check whether the user has permission to login to that Destination or not.
- Check the reason for failure (user account has been disabled or Password incorrect or Account Locked).
- Identify the frequency or pattern of authentication failure. (For every 1min or for every 30sec) .
- Check the logon type (Type2 or Type3 .etc) with which user was trying to authenticate.
- Check if any successful logins are seen either in-between or after certain no of failure.

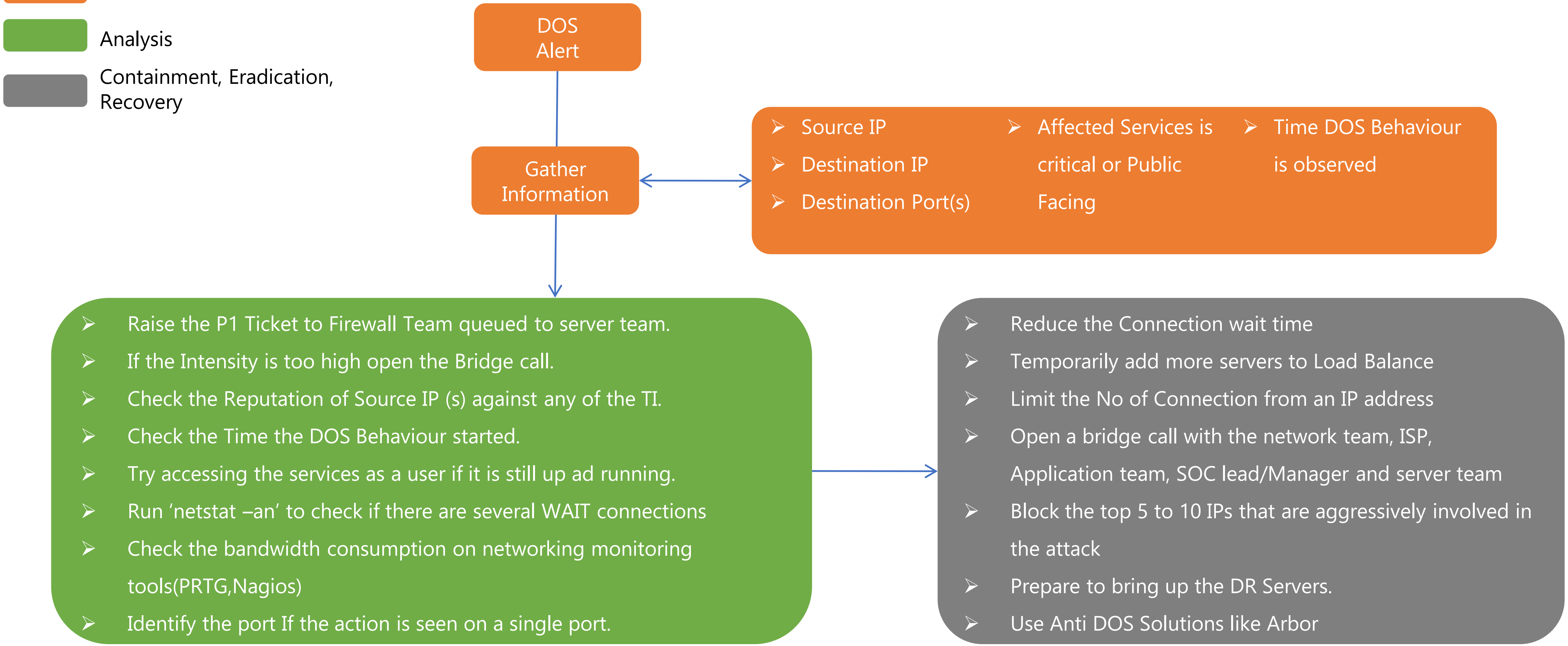
- If External IP is involved, block it in firewall
- Ask the user to change the password
- Clear the browser data if any passwords are stored
- If successful login is seen after high number of failure temporarily disable the account and check whether user is aware of it.

How do you analyze a DOS attack?

🟧 Detect

🟩 Analysis

⬛ Containment, Eradication, Recovery

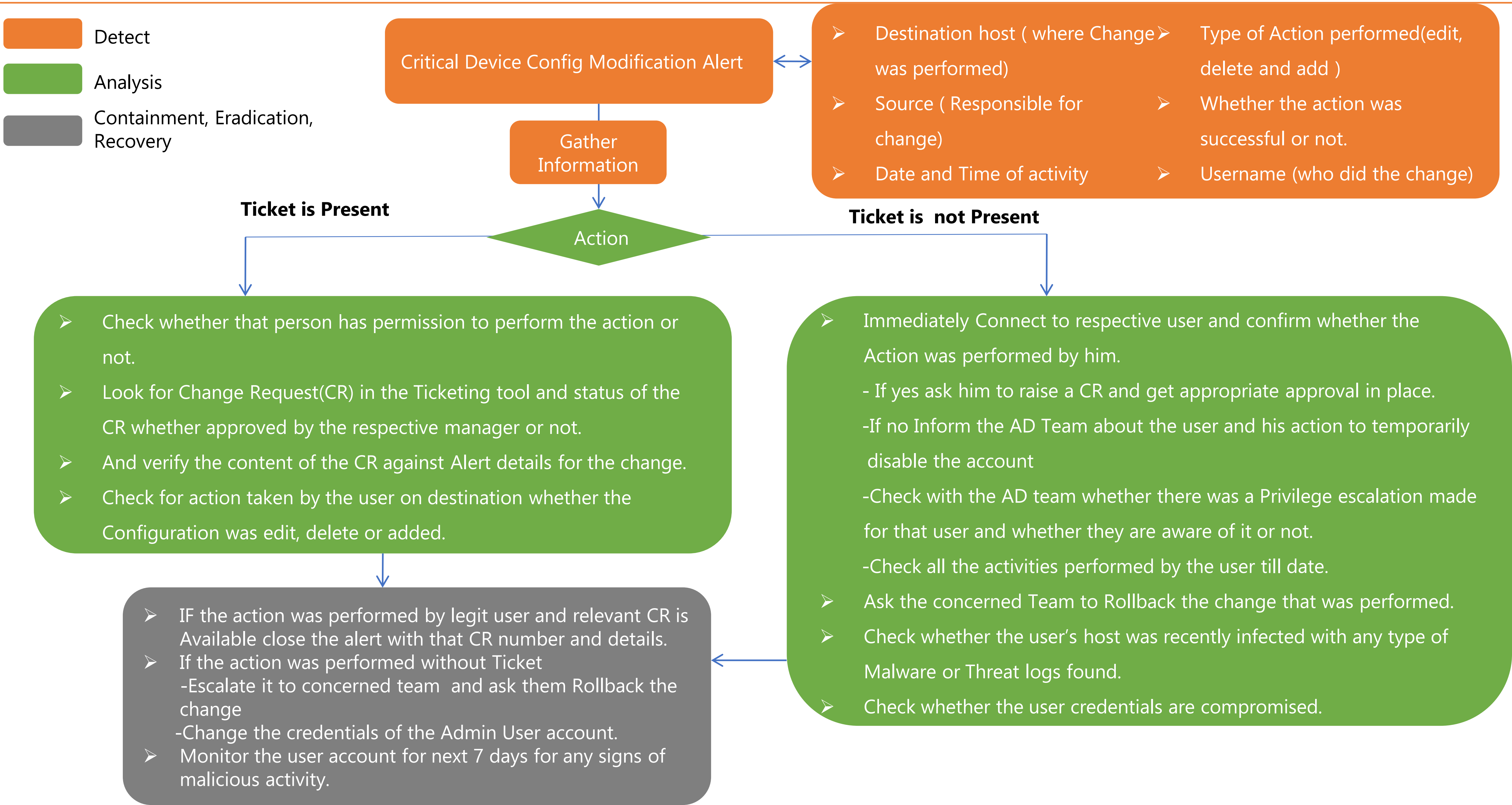


- ➢ Source IP
- ➢ Destination IP
- ➢ Destination Port(s)
- ➢ Affected Services is critical or Public Facing
- ➢ Time DOS Behaviour is observed

- ➢ Raise the P1 Ticket to Firewall Team queued to server team.
- ➢ If the Intensity is too high open the Bridge call.
- ➢ Check the Reputation of Source IP (s) against any of the TI.
- ➢ Check the Time the DOS Behaviour started.
- ➢ Try accessing the services as a user if it is still up ad running.
- ➢ Run ‘netstat –an’ to check if there are several WAIT connections
- ➢ Check the bandwidth consumption on networking monitoring tools(PRTG,Nagios)
- ➢ Identify the port If the action is seen on a single port.

- ➢ Reduce the Connection wait time
- ➢ Temporarily add more servers to Load Balance
- ➢ Limit the No of Connection from an IP address
- ➢ Open a bridge call with the network team, ISP, Application team, SOC lead/Manager and server team
- ➢ Block the top 5 to 10 IPs that are aggressively involved in the attack
- ➢ Prepare to bring up the DR Servers.
- ➢ Use Anti DOS Solutions like Arbor

Explain the analysis for Critical Device Config Modification



🟧 Detect

🟩 Analysis

▨ Containment, Eradication, Recovery

Critical Device Config Modification Alert

- Destination host (where Change was performed)
- Source (Responsible for change)
- Date and Time of activity
- Type of Action performed(edit, delete and add)
- Whether the action was successful or not.
- Username (who did the change)

Gather Information

Action

Ticket is Present

- Check whether that person has permission to perform the action or not.
- Look for Change Request(CR) in the Ticketing tool and status of the CR whether approved by the respective manager or not.
- And verify the content of the CR against Alert details for the change.
- Check for action taken by the user on destination whether the Configuration was edit, delete or added.

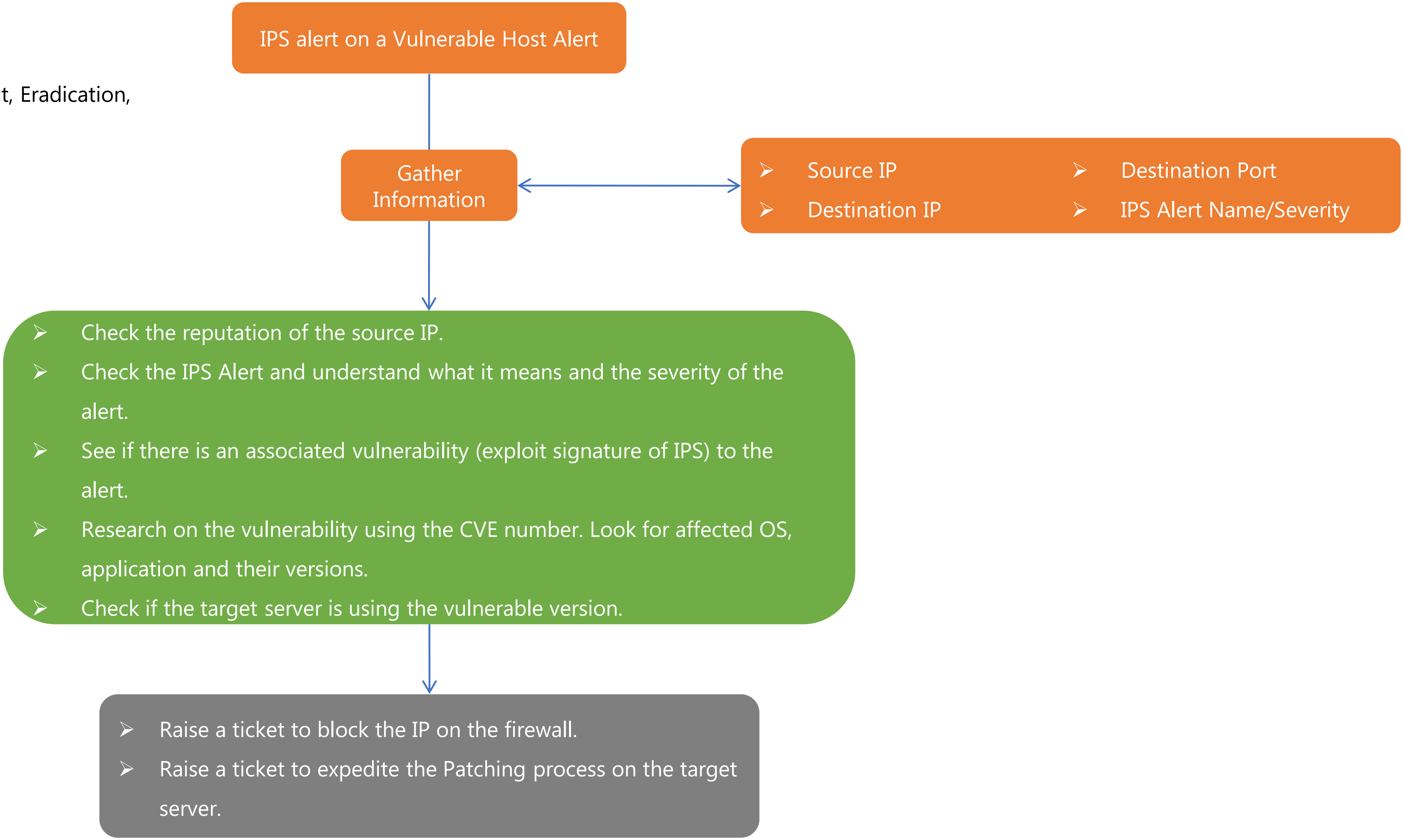
Ticket is not Present

- Immediately Connect to respective user and confirm whether the Action was performed by him.
  - If yes ask him to raise a CR and get appropriate approval in place.
  -If no Inform the AD Team about the user and his action to temporarily disable the account
  -Check with the AD team whether there was a Privilege escalation made for that user and whether they are aware of it or not.
  -Check all the activities performed by the user till date.
- Ask the concerned Team to Rollback the change that was performed.
- Check whether the user's host was recently infected with any type of Malware or Threat logs found.
- Check whether the user credentials are compromised.

- IF the action was performed by legit user and relevant CR is Available close the alert with that CR number and details.
- If the action was performed without Ticket
  -Escalate it to concerned team and ask them Rollback the change
  -Change the credentials of the Admin User account.
- Monitor the user account for next 7 days for any signs of malicious activity.

‘IPS alert on a Vulnerable Host’ rule is triggered, how do you analyze it ?

- 🟧 Detect
- 🟩 Analysis
- ⬛ Containment, Eradication, Recovery



IPS alert on a Vulnerable Host Alert

Gather Information

- Source IP
- Destination IP
- Destination Port
- IPS Alert Name/Severity

- Check the reputation of the source IP.
- Check the IPS Alert and understand what it means and the severity of the alert.
- See if there is an associated vulnerability (exploit signature of IPS) to the alert.
- Research on the vulnerability using the CVE number. Look for affected OS, application and their versions.
- Check if the target server is using the vulnerable version.

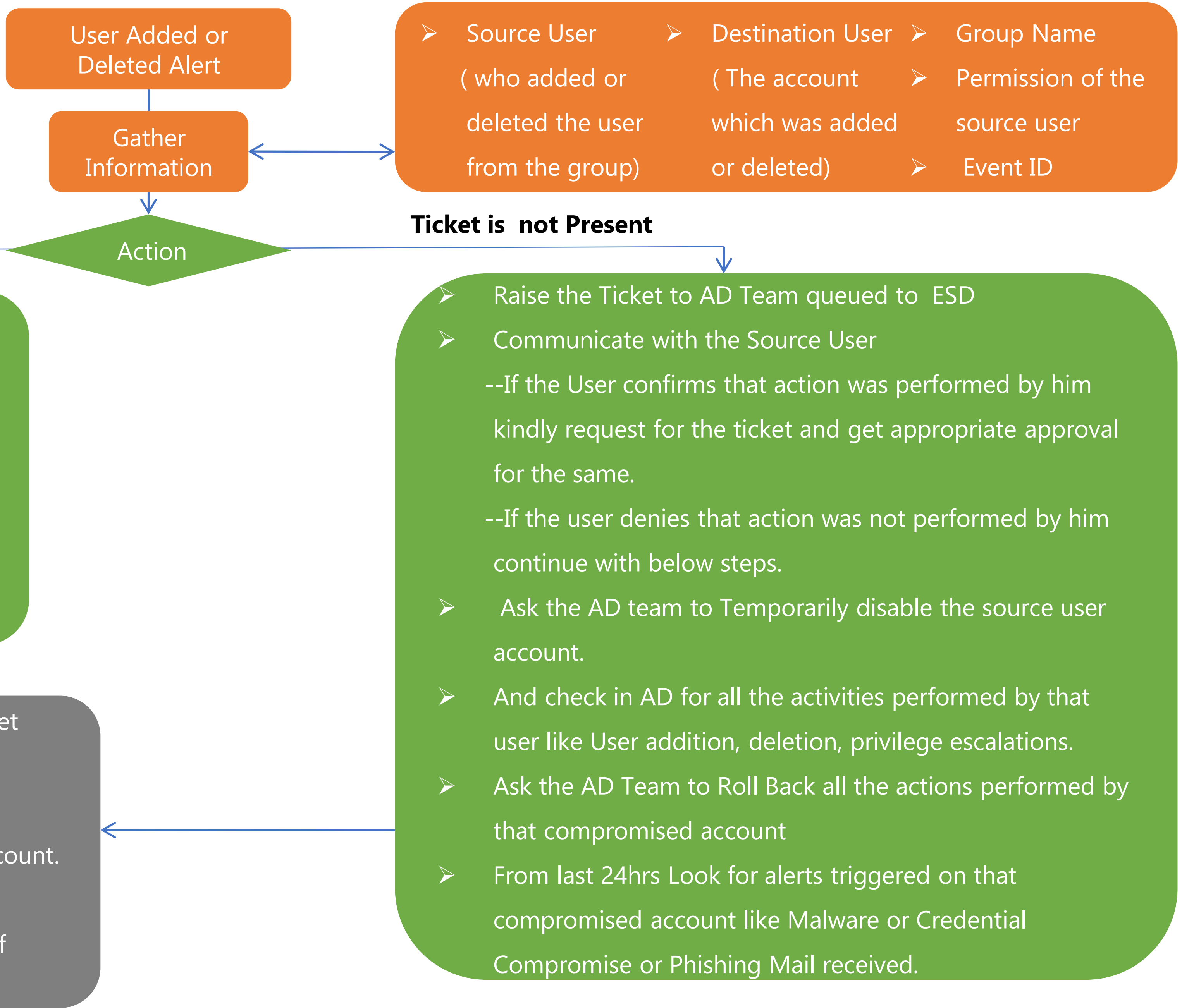
- Raise a ticket to block the IP on the firewall.
- Raise a ticket to expedite the Patching process on the target server.

How do you handle a User Added or deleted from the Universal Security Enabled group?

🟧 Detect

🟩 Analysis

▨ Containment, Eradication, Recovery



User Added or Deleted Alert

Gather Information

- Source User (who added or deleted the user from the group)
- Destination User (The account which was added or deleted)
- Group Name
- Permission of the source user
- Event ID

Action

Ticket is Present

- Check whether the source user has permission to perform the action or not.
- Check for relevant ticket in the Ticketing tool like (New hire request ticket or Termination of the user from HR Team) and whether the ticket has been approved or not
- Check the alert details against respective ticket whether the action performed matches in both.

- If the relevant ticket was found for that action use the ticket number and Alert can be closed.
- If relevant ticket is not found

  -- Ask the user to change the credentials of the Admin account.

  --Roll back the actions performed by that user account

  --Monitor the user account for next 7 days for any signs of malicious activity.

Ticket is not Present

- Raise the Ticket to AD Team queued to ESD
- Communicate with the Source User

  --If the User confirms that action was performed by him kindly request for the ticket and get appropriate approval for the same.

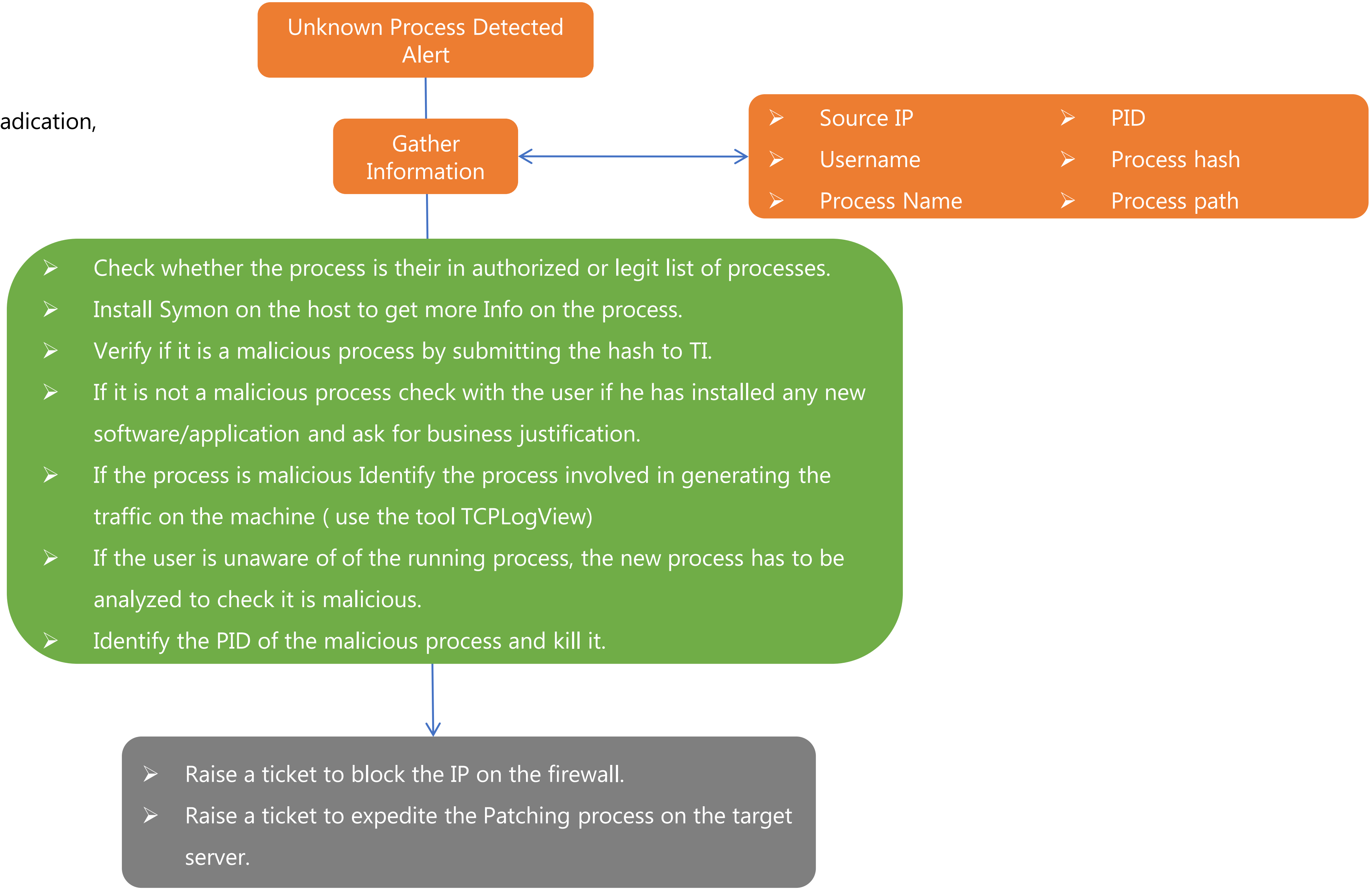
  --If the user denies that action was not performed by him continue with below steps.
- Ask the AD team to Temporarily disable the source user account.
- And check in AD for all the activities performed by that user like User addition, deletion, privilege escalations.
- Ask the AD Team to Roll Back all the actions performed by that compromised account
- From last 24hrs Look for alerts triggered on that compromised account like Malware or Credential Compromise or Phishing Mail received.

What are the Steps you take to analyze ‘Unknown Process Detected’ alert ?

🟧 Detect

🟩 Analysis

⬛ Containment, Eradication, Recovery



Unknown Process Detected Alert

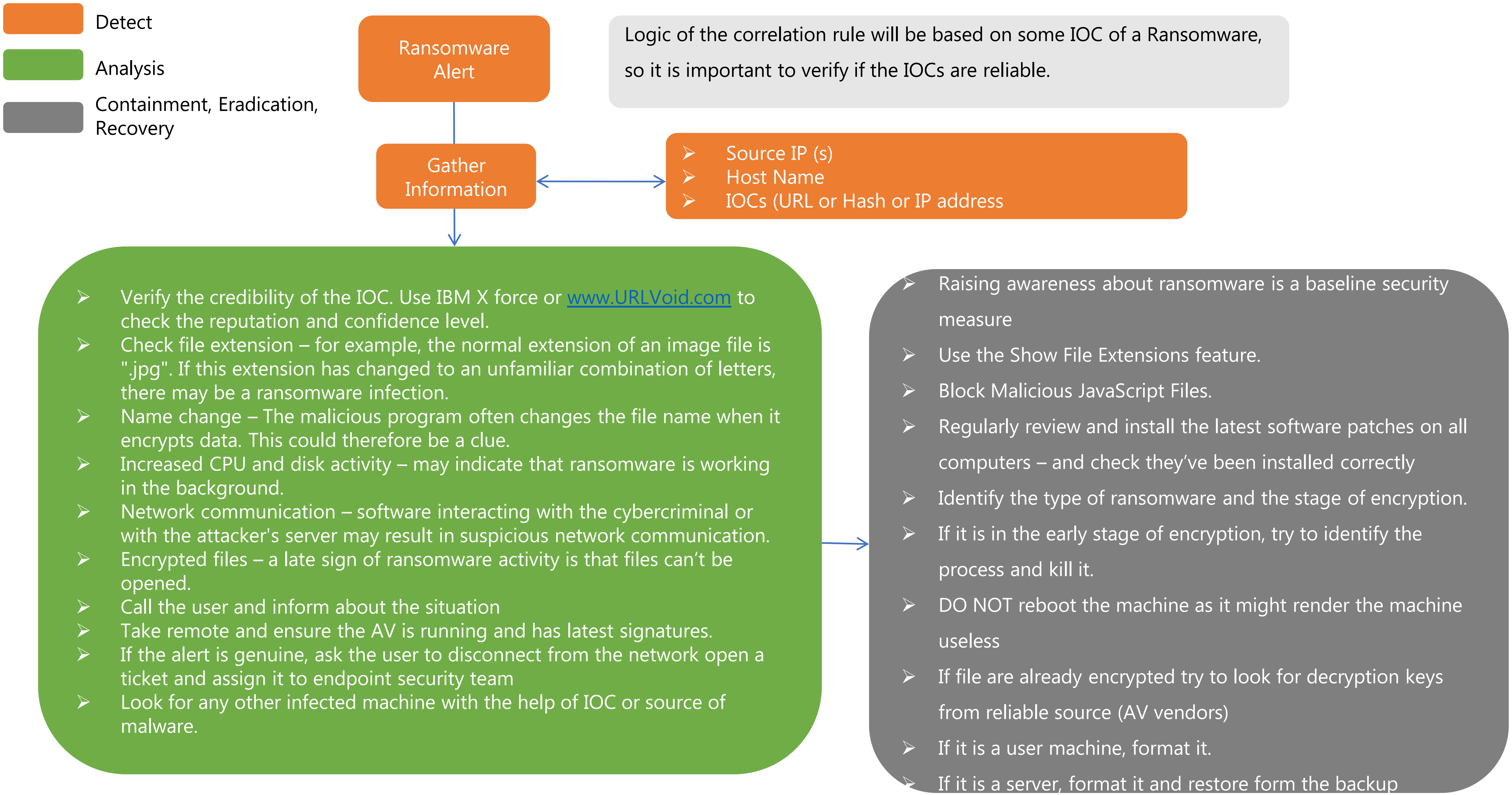
Gather Information

- Source IP
- Username
- Process Name
- PID
- Process hash
- Process path

- Check whether the process is their in authorized or legit list of processes.
- Install Symon on the host to get more Info on the process.
- Verify if it is a malicious process by submitting the hash to TI.
- If it is not a malicious process check with the user if he has installed any new software/application and ask for business justification.
- If the process is malicious Identify the process involved in generating the traffic on the machine (use the tool TCPLogView)
- If the user is unaware of of the running process, the new process has to be analyzed to check it is malicious.
- Identify the PID of the malicious process and kill it.

- Raise a ticket to block the IP on the firewall.
- Raise a ticket to expedite the Patching process on the target server.

How to work on a Ransomware alert ?



🟧 Detect

🟩 Analysis

▨ Containment, Eradication, Recovery

Ransomware Alert

Logic of the correlation rule will be based on some IOC of a Ransomware, so it is important to verify if the IOCs are reliable.

Gather Information

- Source IP (s)
- Host Name
- IOCs (URL or Hash or IP address

- Verify the credibility of the IOC. Use IBM X force or www.URLVoid.com to check the reputation and confidence level.
- Check file extension – for example, the normal extension of an image file is ".jpg". If this extension has changed to an unfamiliar combination of letters, there may be a ransomware infection.
- Name change – The malicious program often changes the file name when it encrypts data. This could therefore be a clue.
- Increased CPU and disk activity – may indicate that ransomware is working in the background.
- Network communication – software interacting with the cybercriminal or with the attacker's server may result in suspicious network communication.
- Encrypted files – a late sign of ransomware activity is that files can't be opened.
- Call the user and inform about the situation
- Take remote and ensure the AV is running and has latest signatures.
- If the alert is genuine, ask the user to disconnect from the network open a ticket and assign it to endpoint security team
- Look for any other infected machine with the help of IOC or source of malware.

- Raising awareness about ransomware is a baseline security measure
- Use the Show File Extensions feature.
- Block Malicious JavaScript Files.
- Regularly review and install the latest software patches on all computers – and check they've been installed correctly
- Identify the type of ransomware and the stage of encryption.
- If it is in the early stage of encryption, try to identify the process and kill it.
- DO NOT reboot the machine as it might render the machine useless
- If file are already encrypted try to look for decryption keys from reliable source (AV vendors)
- If it is a user machine, format it.
- If it is a server, format it and restore form the backup