How to Delete the Malware

In order to kill the malicious process and quarantine the malware, We Use MDE

- Search the file using the hash value collected.
- Check “Observed In organisation” to see how many hosts in network are infected with the same malware.
- Stop and Quarantine feature helps to stop all malicious process run by the malware and quarantines the malicious file as well.
- Use add the indicator feature in MDE to feed the hash value and avoid getting malware infection again.

RCA – Root Cause Analysis

RCA- How did the malicious file end up in the user machine.

1. Check the mails received by the user in last 4 hours before the Incident.

- Segregate them as received from external and internal users.
- Further segregate the external emails and having attachment and not having attachment emails.
- Now do the phishing email analysis and dynamic malware analysis to see if the malware was downloaded by any other email received.

2. Check for the URL activity.

- Check URLs visited by the user in last couple of hours and segregate.
- See if the URL is the culprit.

3. Check with user , if he/she has used the USB before the incident and copied an files

- If so, Ask them to submit the USB to IT helpdesk.
- Communicate with IT helpdesk via INC to see If USB was the reason for malware infection.

4. If None of the options where the Root cause of malware infection – then Raise the INCIDENT to IR team to find the Root cause.

Remediate the Root Cause

Fix the Root Cause.

1. If Email was the RC- Purge the email using knowbe4, block the sender on email gateway and block the Ip on F/w.
2. If URL was the RC- Block the URL on Proxy/webgatway.
3. If USB- Educate the user

Unhandled Malware

This Alert is triggered when the AV detects the malware but is unable to clean, Delete or Quarantine

Once the conditions are met the alert triggers in Splunk.

The alert is Forwarded to your monitoring tool- Where you assign the alert to yourself and start to investigate.

Analyse the AV logs of the user for which the alert is triggered.
Collect the Hash value, File Name and File Path from the AV logs of user.

Check the file hash reputation on TI tools.
If need you can download the file sample on your host using MDE- “download file” feature and perform the dynamic malware analysis to confirm if the file is malware.

In order to kill the malicious process initiating the traffic to malicious Ip- We Use MDE , Search the file using the hash value collected-

- Check “Observed In organisation” to see how many hosts in network are infected.
- Stop and Quarantine feature helps to stop all malicious process run by the malware and quarantines the malicious file as well.
- Use add the indicator feature in MDE to feed the hash value and avoid getting malware infection again.

RCA- How did the malicious file end up in the user machine.

1. Check the mails received by the user in last 4 hours before the Incident.
   - Segregate them as received from external and internal users.
   - Further segregate the external emails and having attachment and not having attachment emails.
   - Now do the phishing email analysis and dynamic malware analysis to see if the malware was downloaded from these emails.
2. Check for the URL activity.
   - Check URLs visited by the user in last couple of hours and segregate.
   - See if the URL is the culprit.
3. Check with user , if he/she has used the USB before the incident and copied an files
   - If so, Ask them to submit the USB to IT helpdesk.
   - Communicate with IT helpdesk via INC to see If USB was the reason for malware infection.
4. If None of the options where the Root cause of malware infection – then Raise the INCIDENT to IR team to find the Root cause.

Fix the Root Cause.

1. If Email was the RC- Purge the email using knowbe4, block the sender on email gateway and block the Ip on F/w.
2. If URL was the RC- Block the URL on Proxy/webgatway.
3. If USB- Educate the user

Once INC raised to NOC team, IT helpdesk team, IR team is closed.
Go-ahead and close the alert on monitoring tool.

Same Malware Found on Multiple host

This Alert is triggered when the AV detects the same malware in multiple host in short span of time- This indicates several users are targeted via an email or a commonly used URL.

Once the conditions are met the alert triggers in Splunk.

The alert is Forwarded to your monitoring tool- Where you assign the alert to yourself and start to investigate.

Analyse the AV logs of the users for which the alert is triggered.
Collect the Hash value, File Name and File Path from the AV logs of user.

Check the file hash reputation on TI tools.
If needed you can download the file sample on your host using MDE- "download file" feature and perform the dynamic malware analysis to confirm if the file is malware.

In order to kill the malicious process initiating the traffic to malicious Ip- We Use MDE , Search the file using the hash value collected-

- Check "Observed In organisation" to see how many hosts in network are infected.
- Stop and Quarantine feature helps to stop all malicious process run by the malware and quarantines the malicious file as well.
- Use add the indicator feature in MDE to feed the hash value and avoid getting malware infection again.

RCA- How did the malicious file end up in the user machine.
1. Check the mails received by the user in last 4 hours before the Incident.
- Segregate them as received from external and internal users.
- Further segregate the external emails as having attachment and not having attachment emails.
- Now do the phishing email analysis and dynamic malware analysis to see if the malware was downloaded from these emails.

2. Check for the URL activity.
- Check URLs visited by the user in last couple of hours and segregate.
- See if the URL is the culprit.

3. Check with user , if he/she has used the USB before the incident and copied an files
- If so, Ask them to submit the USB to IT helpdesk.
- Communicate with IT helpdesk via INC to see If USB was the reason for malware infection.

4. If None of the options where the Root cause of malware infection – then Raise the INCIDENT to IR team to find the Root cause.

Fix the Root Cause.
1. If Email was the RC- Purge the email using knowbe4, block the sender on email gateway and block the Ip on F/w.
2. If URL was the RC- Block the URL on Proxy/webgatway.
3. If USB- Educate the user

Once INC raised to NOC team, IT helpdesk team, IR team is closed.
Go-ahead and close the alert on monitoring tool.

Multiple Malware Found on Single host

This Alert is triggered when the AV detects multiple malware infection on single host in short span of time- This Indicates either user is trying to download or copy a malicious file over and over again, OR a malware is partially executed and trying to perform a activity that is being detected as malicious by AV

Once the conditions are met the alert triggers in Splunk.

The alert is Forwarded to your monitoring tool- Where you assign the alert to yourself and start to investigate.

Analyse the AV logs of the users for which the alert is triggered.
Collect the Hash values, File Names and File Paths from the AV logs of the user.

Check the file hash reputation on TI tools.
If needed you can download the file sample on your host using MDE- "download file" feature and perform the dynamic malware analysis to confirm if the file is malware.

In order to kill the malicious process initiating the traffic to malicious Ip- We Use MDE , Search the file using the hash value collected-

- Check "Observed In organisation" to see how many hosts in network are infected.
- Stop and Quarantine feature helps to stop all malicious process run by the malware and quarantines the malicious file as well.
- Use add the indicator feature in MDE to feed the hash value and avoid getting malware infection again.

RCA- How did the malicious file end up in the user machine.

1. Check the mails received by the user in last 4 hours before the Incident.
- Segregate them as received from external and internal users.
- Further segregate the external emails as having attachment and not having attachment emails.
- Now do the phishing email analysis and dynamic malware analysis to see if the malware was downloaded from these emails.

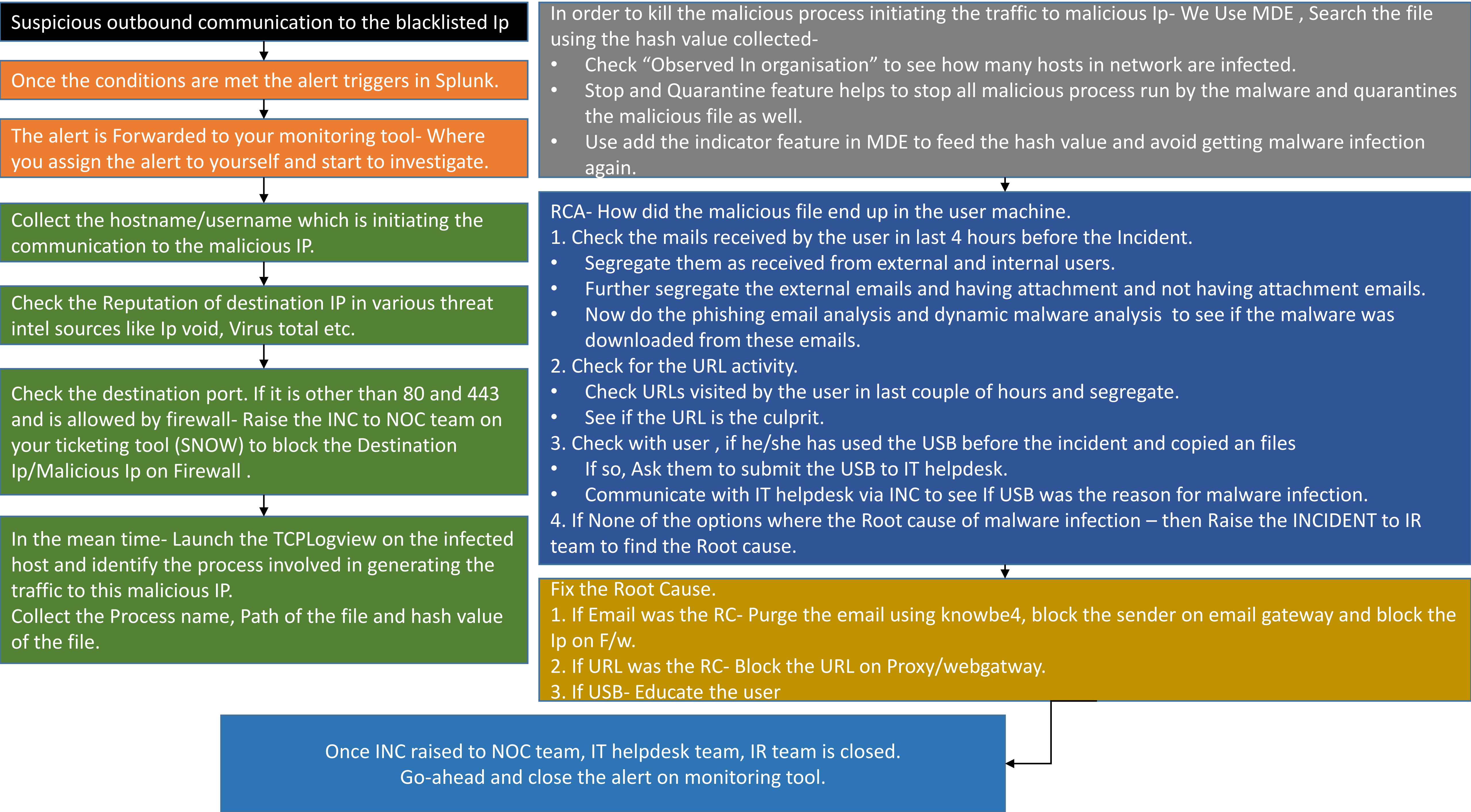
2. Check for the URL activity.
- Check URLs visited by the user in last couple of hours and segregate.
- See if the URL is the culprit.

3. Check with user , if he/she has used the USB before the incident and copied an files
- If so, Ask them to submit the USB to IT helpdesk.
- Communicate with IT helpdesk via INC to see If USB was the reason for malware infection.

4. If None of the options where the Root cause of malware infection – then Raise the INCIDENT to IR team to find the Root cause.

Fix the Root Cause.
1. If Email was the RC- Purge the email using knowbe4, block the sender on email gateway and block the Ip on F/w.
2. If URL was the RC- Block the URL on Proxy/webgatway.
3. If USB- Educate the user

Once INC raised to NOC team, IT helpdesk team, IR team is closed.
Go-ahead and close the alert on monitoring tool.



Suspicious outbound communication to the blacklisted Ip

Once the conditions are met the alert triggers in Splunk.

The alert is Forwarded to your monitoring tool- Where you assign the alert to yourself and start to investigate.

Collect the hostname/username which is initiating the communication to the malicious IP.

Check the Reputation of destination IP in various threat intel sources like Ip void, Virus total etc.

Check the destination port. If it is other than 80 and 443 and is allowed by firewall- Raise the INC to NOC team on your ticketing tool (SNOW) to block the Destination Ip/Malicious Ip on Firewall .

In the mean time- Launch the TCPLogview on the infected host and identify the process involved in generating the traffic to this malicious IP.
Collect the Process name, Path of the file and hash value of the file.

In order to kill the malicious process initiating the traffic to malicious Ip- We Use MDE , Search the file using the hash value collected-

- Check “Observed In organisation” to see how many hosts in network are infected.
- Stop and Quarantine feature helps to stop all malicious process run by the malware and quarantines the malicious file as well.
- Use add the indicator feature in MDE to feed the hash value and avoid getting malware infection again.

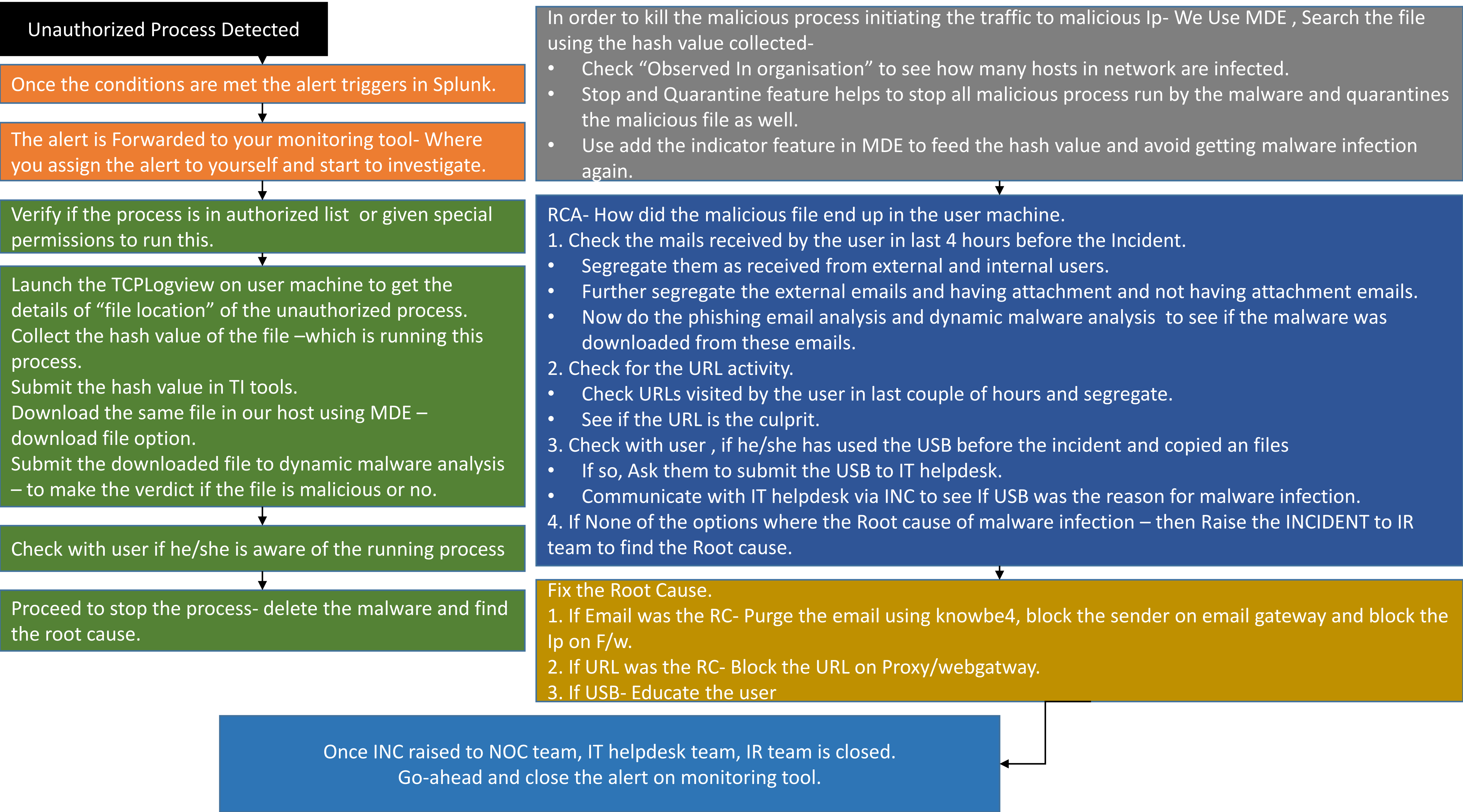
RCA- How did the malicious file end up in the user machine.

1. Check the mails received by the user in last 4 hours before the Incident.
   - Segregate them as received from external and internal users.
   - Further segregate the external emails and having attachment and not having attachment emails.
   - Now do the phishing email analysis and dynamic malware analysis to see if the malware was downloaded from these emails.
2. Check for the URL activity.
   - Check URLs visited by the user in last couple of hours and segregate.
   - See if the URL is the culprit.
3. Check with user , if he/she has used the USB before the incident and copied an files
   - If so, Ask them to submit the USB to IT helpdesk.
   - Communicate with IT helpdesk via INC to see If USB was the reason for malware infection.
4. If None of the options where the Root cause of malware infection – then Raise the INCIDENT to IR team to find the Root cause.

Fix the Root Cause.

1. If Email was the RC- Purge the email using knowbe4, block the sender on email gateway and block the Ip on F/w.
2. If URL was the RC- Block the URL on Proxy/webgatway.
3. If USB- Educate the user

Once INC raised to NOC team, IT helpdesk team, IR team is closed.
Go-ahead and close the alert on monitoring tool.



Unauthorized Process Detected

Once the conditions are met the alert triggers in Splunk.

The alert is Forwarded to your monitoring tool- Where you assign the alert to yourself and start to investigate.

Verify if the process is in authorized list or given special permissions to run this.

Launch the TCPLogview on user machine to get the details of “file location” of the unauthorized process.
Collect the hash value of the file –which is running this process.
Submit the hash value in TI tools.
Download the same file in our host using MDE – download file option.
Submit the downloaded file to dynamic malware analysis – to make the verdict if the file is malicious or no.

Check with user if he/she is aware of the running process

Proceed to stop the process- delete the malware and find the root cause.

In order to kill the malicious process initiating the traffic to malicious Ip- We Use MDE , Search the file using the hash value collected-

- Check “Observed In organisation” to see how many hosts in network are infected.
- Stop and Quarantine feature helps to stop all malicious process run by the malware and quarantines the malicious file as well.
- Use add the indicator feature in MDE to feed the hash value and avoid getting malware infection again.

RCA- How did the malicious file end up in the user machine.
1. Check the mails received by the user in last 4 hours before the Incident.

- Segregate them as received from external and internal users.
- Further segregate the external emails and having attachment and not having attachment emails.
- Now do the phishing email analysis and dynamic malware analysis to see if the malware was downloaded from these emails.

2. Check for the URL activity.

- Check URLs visited by the user in last couple of hours and segregate.
- See if the URL is the culprit.

3. Check with user , if he/she has used the USB before the incident and copied an files

- If so, Ask them to submit the USB to IT helpdesk.
- Communicate with IT helpdesk via INC to see If USB was the reason for malware infection.

4. If None of the options where the Root cause of malware infection – then Raise the INCIDENT to IR team to find the Root cause.

Fix the Root Cause.
1. If Email was the RC- Purge the email using knowbe4, block the sender on email gateway and block the Ip on F/w.
2. If URL was the RC- Block the URL on Proxy/webgatway.
3. If USB- Educate the user

Once INC raised to NOC team, IT helpdesk team, IR team is closed.
Go-ahead and close the alert on monitoring tool.