Cybersecurity Playbook for SOC

1. Attack utilizing a known vulnerability

An attacker utilizing a known vulnerability has been detected.

Detection

- Network detection from IDS/IPS/network threat detection capability
- Endpoint detection from the targeted host

Verification

- The event is validated with the asset list. If the known vulnerable software/hardware is not present on the targeted asset this should be marked as false positive. If an accurate asset list is not available, this verification needs to be done manually by the support team of the targeted asset.
- The event is correlated with the end point security software (EDR/XDR) to confirm whether the attack is successful or not.

Communication

- For successful attacks, start triage using attack and asset criticality information. Perform escalation according to triage results and predefined escalation plan.
- For unsuccessful attacks and false positives, no immediate communication required.

Action

- For successful attacks, perform containment on affected hosts. Run vulnerability scan on the same vulnerability across all IT assets.
- There can be different containment strategies according to the business criticality of the asset. It ranges from auto-containment and cutting it off completely from the network to a milder limited connectivity to selected IPs and ports. The strategy to apply requires discussion between SOC, risk management, and business teams.
- For unsuccessful attacks, add to backlog to study why and what additional actions are required.
- For false positives, log as statistics.

2. New vulnerability from Threat Intelligence

Undoubtedly the one you will execute most, a new vulnerability from threat intelligence.

Detection

- Threat intelligence indicates there is a new vulnerability impacting your assets.
- Here I assume the threat intelligence is already tuned to only include information relevant to your assets instead of a news broadcast of all vulnerabilities in the world.

Again, this relies on an accurate and up-to-date inventory and signifies the importance of keeping the house in order.

Verification

- If there are IOC/TTP, check for attacks already happened. If attack already happened, follow no 1.
- Use vulnerable version/configuration information to confirm the assets are vulnerable or not.
- Check firewall rules and other security configurations to confirm possible attack vectors. This can be partially done using automated tools.

Communication

- Start triage using available vulnerability and asset criticality information. Perform escalation according to triage results and predefined escalation plan.
- Discuss mitigation strategy between SOC, risk management, and IT support teams. That can range from an immediate shutdown to wait till the next patching window, depending on many factors such as the triage result and the availability and impact of the patch/workaround.
- The mitigation strategy also needs to include preventive actions for new builds of assets in the future, such as updating patch level of system images or templates.

Action

- Execute agreed mitigation strategy.
- Track the mitigation actions to completion.
- Rescan the vulnerability to confirm closure.

3. Unauthorized privileged access

Many organizations are using privileged access management systems and we can make use of it to identify unauthorized use, which is very useful to detect stolen credentials.

Detection

- Correlate privileged access management (PAM) logs to authentication logs of relevant end points. Trigger alerts on any privileged account logon without a corresponding PAM approval entry.
- While these are unauthorized access, they may not always be attacks. For example, if PAM is not set to reset password after every use, the system administration may memorize the password and use it to logon multiple times, or there may be scripts using those credentials to logon. Nevertheless, these alerts will be useful for cyber hygiene and gently remind people on the proper usage of privileged accounts.

Verification

- Check with relevant system administrators if they have used the accounts in the relevant time. If no administrator knows about the usage, widen the collaboration to related application support teams. If there is still no conclusion, treat as successful attack and follow no 1.

Communication

- For non-attacks, report to security/risk management teams and relevant IT teams to resolve improper usage of the concerned accounts.

Action

- If there are risk-accepted exceptions, update the correlation rules.

4. Phishing email

Here we deal with phishing emails with malicious payload or links. Those with text content only (e.g., account payable scams) can be dealt with another simpler playbook.

Detection

- Alert from email security solution.
- Email security solutions are good at blocking phishing email when they see one. The problem is that many adversaries now use a tactic to evade them:

    i. Prepare a phishing email with a link pointing to nothing, or even better to a normal, harmless page.
    ii. Send the phishing email in non-office hours, getting it past the email security controls and hoping the receiver won't be there to open it up yet.
    iii. At start of day, put up malicious content onto the linked website.
    iv. End user starts checking emails and click on the now malicious link.

- Email security solutions can check the links passed through them periodically to mitigate this, but there will always be a time gap between the checking and user clicking on the link.
- Alert from end points that traced back to payload from phishing email/link.
- Report from end users.

Verification

- Check if there are similar emails (e.g., same source email server) delivered to other inboxes.
- If web proxy is enforced for outgoing web requests, check web proxy logs to confirm if the malicious link is visited. The user should also be contacted to understand if the link was forwarded to other places (e.g., personal email) and potentially clicked over there.

- Check if the end point is exempted from web proxy or web isolation. If so other logs (e.g., firewall logs) need to be checked to ascertain the link is clicked or not.
- If the link is visited, check web proxy log for anything downloaded to the end point.
- If there are files downloaded, check endpoint security events for malicious actions and malware analysis is also recommended. Your XDR vendor should be able to perform the analysis if you do not have an in-house expert on this.
- It is often very tempting to just run an AV scan or upload the downloaded files to virus total to check if the endpoint is clean or not. Unfortunately, these aren't too effective if the adversaries are not using well known vulnerabilities or malicious code. This is especially true for spear phishing, where everything is customised.

Communication

- Follow playbook no 1 if there is a confirmed compromise.
- Feedback to the end user receiving the phishing email on the action taken (not clicked the link, reported to SOC, etc.).
- Report to security/risk management teams on the scope of phishing and advise general communication to everyone if this looks like a phishing campaign.

Action

- Follow playbook no 1 if there is a confirmed compromise.
- Delete all phishing emails from other inboxes (or advise the end users to delete them).
- Triggers rebuild of the endpoint if you are unsure of the downloaded content.
- Revisit phishing mitigation controls such as web filtering (new domains, IP addresses), web isolation/sandboxing, email security (DMARC), and end user security awareness to see if any improvement is required.

5. Confidential data on Internet

It describes what to do on notable data discovered by threat intelligence on the Internet.

Detection

- Threat intelligence found non-public data about your organization on the Internet, such as in open S3 buckets, Pastebin, or even "hidden" directories on your own web server.
- Report from peoples through public and internal channels.

Verification

- Download a snapshot of the data to check.
- Identify potential owner of the data and contact relevant business teams to review the data. Only the data owner can confirm if the data is genuine and intended for public consumption or not.

Communication

- If it is confirmed a leak, alert relevant business teams and security/risk management team.
- Get instruction from business teams on whether legal, compliance, law enforcement liaison, and other control functions should be involved for next steps. (e.g., leakage of stock price sensitive data, or personal data of staff or customers may have legal and regulatory reporting requirements).

Action

- Remove the confidential data if it is under your control (e.g., on your own tenancy or web servers).
- Otherwise, use all available channels to take down the confidential data as soon as possible. This includes brand protection services, national CERT, abuse contact of the hosting service provider, or even personal security contacts you have with the hosting organization. Effectiveness of each channel differs in almost every case, so it is worthwhile to try them all before resorting to legal actions.
- Find out who has previously downloaded the data.
- If the data contains authentication credentials, change the credentials immediately.
- Report to data owner after the take down is completed.
- Continue to monitor the data for a period. Repeat the removal actions if it resurfaces.

6. Fraudulent Websites

These pretends to be your organization and tries to spread false information, collect your customers data, spread malicious software, or more.

Detection

- Brand protection service alerts.
- Threat intelligence.
- In my experience there is no perfect detection mechanism for fraudulent websites. Some can be found by web searches, some by brand protection services, and some are only reported by customers and third parties. When collecting threat intelligence be aware of language limitations of search engines, and different communication medium spreading the fraudulent websites. This can include email and instant messages.

Verification

- Download a deep copy of the fraudulent website. Differentiate between externally hosted content and pass-through content on the genuine website.
- Take screenshots of the fraudulent website as well. It is useful to include the screenshot in communications, and as a record in case the website goes offline quickly.
- Navigate in the fraudulent website and confirm if it:

    I. Contain false information (e.g., contact email and phone numbers)

II. Harvest customer information (credentials and personal data)
III. Contain malicious code (e.g., CSRF, drive-by downloads)

Communication

- Inform compliance team on regulatory reporting required.
- Work with law enforcement liaison on police reporting.
- Discuss with security team and corporate communication team on the impact of the fraudulent website to customers and publish customer alerts accordingly. Advise should be given on actions they need to take (e.g. change credentials). There should be a predefined channel of communication, such as SMS, website, and press release.

Action

- Invoke brand protection service and other channels to take down the website (see no 5).
- Continue to monitor the URL for a period. Repeat the removal actions if it resurfaces.
- Because of the uncertainties on completion of take down, it is often observed that these fraudulent websites went online and offline a few times before they drop dead for good.

7. Brute Force Authentication

The attacks can be against internal or Internet facing systems.

Detection

- SIEM alerts on number of failed authentication attempts.
- Related alerts from IPS and other security devices.

Verification

- Check if the logon was successful or not.
- Confirm if the targeted account(s) exist or not.
- Check the attack source IP:

    i. Confirm it is an internal host or external
    ii. Confirm owner/user of the source IP (if possible)

Communication

- If the attack is successful, escalate to security/risk management team and relevant IT support teams and discuss mitigation strategy. Inform the relevant account owner(s) on the password compromise and necessary reset.
- If the attacker is an internal IP, check with the owner/administrator to understand any recent action may have caused this. (e.g., downloaded software from Internet)
- For failed attacks report/escalate according to a pre-agreed threshold (e.g., based on number of accounts affected, number of attacks, etc).

Action

- If the attack is successful, reset passwords of all compromised accounts immediately. Treat target hosts as compromised and follow no 1. Extra care must be taken if the concerned account is an administrator account, where an in-depth investigation will be needed on the impact and containment actions required.
- If the attacker IP is internal, assume it is compromised and execute no 1.
- If the attacker is on the Internet, block the source IP on the network perimeter. You may consider reporting it to the IP/AS owner on their abuse contact.

8. VPN abnormalities

VPN is a popular way for attackers to maintain persistent access to your environment

Detection

- Identity management system alerts there are VPN accounts without the corresponding account creation approval record.
- If there is no identify management system available, the same check can be done by script or manually on exported VPN account list and the user account request ticketing system.
- User reported VPN password is reset, or the registered mobile device is changed without consent.
- It is a good practice to notify the user of VPN password reset and change of the registered VPN device. This can be done by email and SMS.

Verification

- Confirm with VPN administrator on the concerned account and activities are legit or not.
- Gather the access logs of the concerned VPN accounts and check source IPs of the connections. Confirm those are from the legit VPN user or not.
- Be cautious on overly relying on geo-IP information. Attackers are known to rent rack space close to your user base (e.g., data centre in the same city) to get around that.

Communication

- Inform VPN account owners and advise them to change passwords on other systems (including personal devices).
- Escalate to security/risk management teams and relevant IT teams to identify root cause, as the VPN system may not be the vector used by the attacker to get in.

Action

- If unauthorized account/activities are detected, treat the concerned accounts (and even the VPN system) as compromised. Reset passwords, rebuild system, and follow no 1 before resuming the VPN service.
- Perform further forensic analysis to identify root cause and other compromised systems.

9. DNS callback

DNS has become the de facto call back mechanism for many malwares.

Malware have evolved quite a bit for their call back channels:

- In the beginning they used custom high ports as UNIX allows non-root users to open them. Firewall came about and quickly put an end to them by the "deny any" default policy.
- Then malware moved to HTTP/HTTPS as these are frequently allowed by firewalls for legit users' web browsing. The widespread use of web proxies and sophisticated web filter filtering rules (e.g., block new domains, blacklists, IP only addresses) are making this channel less and less reliable for the attackers.
- Then there is DNS, which is an essential service on TCPIP networks. A great many internal hosts, even with no direct Internet connectivity, still can resolve Internet hostnames via DNS servers.

Detection

- DNS monitoring alerts on very-long-domain-name queries, known bad queries (IOC/TTP), DNS traffic volume and frequency, etc.
- Network security device (e.g., IPS/IDS) alert on abnormal DNS queries.

Verification

- Check DNS logs to establish the beginning date of the same kind of DNS queries and similar behaviour of other endpoints. Note some queries may be refused by the DNS servers (depending on the configuration), so the log review should include those as well.
- Check endpoint security event logs (e.g., XDR) of the relevant endpoints for malware.
- If necessary, run forensic analysis on the relevant endpoints to find out the offending process sending out the DNS queries.

Communication

- If this is a confirmed compromise escalate to security/risk management teams and relevant IT teams to identify how the malware got in.

Action

- Follow no 1 on compromised hosts.

- Perform further forensic analysis to identify root cause and other compromised systems.

10. Ransomware

Ransomware has been the top cyber security concern for many organizations in recent years.

Detection

- Network detection on attack traffics (e.g., Eternal Blue)
- Endpoint security detection on abnormal program behaviour or IOC.
- End user report on Ransomware screens.

Verification

- Check threat intelligence to find a match for the Ransomware. They are usually well known.
- Check SIEM and other security event source to understand how widespread the Ransomware and host is fast it is spreading.
- Investigate which end-point was the first point of intrusion and the probable root cause.

Communication

- Escalate to security/risk management teams and relevant IT teams to discuss containment strategy. Available options can be XDR containment, network containment, remote power down, or even (partial) network shutdown. The option to go for will depend on the prevalence of the root cause, availability of quick fix, difficulties on network containment, remote administration capability, and so on.
- Inform affected end-point users on the system unavailability.

Action

- Contain the infected endpoints immediately. Power them off if possible.
- If backup is available for all affected systems, rebuild them from last-known-good copy.
- It should be well known by now that an online data mirror cannot remediate the risk of Ransomware, as the copy can be corrupted as well. Only an offline copy with a suitable retention schedule can be safe from tampering and should be mandated on all data.
- Follow up on root cause of the Ransomware infection and track its remediation.