SOC SIEM USE CASES

What are use cases?

The use cases are critical to identifying any of the early, middle, and end-stage operations of the adversary. A small abnormal event can be a clue to a larger attack. There also needs to be a playbook on how to respond. A use case can be technical rules or conditions applied on logs which are ingested into the SIEM. E.g. – malicious traffic is seen hitting critical servers of the infra, too many logins attempt in last 1 min etc.

Best practises

1. Ensure to have a clear list of your use cases handy always.
2. The use cases need to be mapped to the MITRE ATT&CK phases so you can know how much the adversary succeeded in his objective. Tagging and mapping to the MITRE ATT&CK Matrix would help detection (what logs to be tapped into) and mitigation. Also helps attribution to an APT group.
3. Each use case to have a clear priority based on your organisation.
4. Each use case to have the log source which must be ingested into your SIEM.

Why it is important to have a large set of use cases and have playbooks for them?

1. Real cyber-attacks are complex. It is actually very hard for the attacker to be invisible to a SOC who has enabled the right set of use cases.
2. Use cases are rules that trigger alerts. You need playbooks or instruction on how to respond to them, steps to analyse and mitigate.
3. The process of creation of playbooks is very important. It helps a lot for you to be prepared for handling a cyber-attack.

Below is a list of sample use cases. You can categorize it in multiple ways and refer to your SIEM-specific documentation to get the list of rules that come bundled.

Windows

- Server Shutdown/ Reboot
- Removable media detected
- Windows abnormal shutdown
- Login attempts with the same account from different source desktops
- Detection of Server shutdown-reboot after office hours
- Administrative Group Membership Changed
- Unauthorized Default Account Logins
- Interactive use of service account
- Remote access login – success & failure
- Windows Service Stop-Restart
- ACL Set on Admin Group members
- Windows Account Enabled Disabled
- Multiple Windows Account Locked out
- Multiple Windows Logins by Same User
- Brute force attempt from same source

- Logins outside normal business hours
- Logins to multiple user accounts from the same source
- Brute force attempt from same source with successful login
- Windows Account Created Deleted
- Windows Hardware Failure
- Failed Login to Multiple Destination from Same Source
- Administrative Accounts- Multiple Login failure
- Detection of user account added/removed in admin group
- Detection of system time changes (Boot time)
- Detection of use of default product vendor accounts
- User Deleted Within 24hrs of Being Created
- Critical service stopped on Windows Servers
- Windows Security Log is full
- Multiple Password Changes in Short time
- Windows group type was changed
- Audit Policy change
- Audit Log cleared
- Windows Security Log is full
- Detection of user account added
- Logon Failure-A logon attempt was made using an expired account
- High number of users created/ removed within a short period of time
- Outbound Traffic observed from Severs to Internet
- Failed Logins/Attempt with Disabled/Ex-Employee/Expired Accounts
- Windows File-Folder Delete
- Windows-File Folder Permission Changes
- High number of users created/removed within a short period of time

Unix

- Unix FTP File Import and Export Events
- Unix File system full
- Server shutdown
- Users Created /Deleted within short period
- Users Group Created /Removed within short period
- Unix-Login attempts with the same account from different source desktops
- Failed Logins
- Failed Logins with disabled accounts
- Unix FTP Login Access
- Unix multiple SFTP Connection
- Failed logins from root access
- Unix Multiple SU login failures
- Remote Logon Attempts using Root User on Production Node
- Sudo access from Non sudo users

- Detection of use of default product vendor accounts
- Adding or Removing users to the group “root”
- Critical Service Stop
- Unix-High number of login failure for the same account within a short time
- Password Changed
- Adding, removing and modifying cron jobs
- SU login failures
- Detection of change in syslog configuration
- Detection of change in network configuration

Firewall, Antivirus, IPS and VPN

- Administrator Login Failure
- Brute force with Successful Configuration Changes
- Firewall Failover event
- Successful connection from internet IP after repetitive blocks in firewall
- Access attempts on unidentified protocols & port
- Exploit Event followed by Scanning Host
- Outbound access to invalid destination Ips
- Successful logon between Non-Business Hours
- Firewalls reboot
- Detection of user account/group modifications
- User Added/Deleted to Firewall Database
- Detection of insecure traffic like FTP, telnet, on critical servers
- Detection of adding/deletion of a Firewall admin
- Login Denied (Brute Force)
- High number of Denied events
- Configuration Change detected
- The link to peer device is down either because of physical cabling issue or NSRP configuration issue
- Network and Host Port Scan Attempts
- Detection of Primary-Secondary Switch Over
- An admin has allowed/removed access to the firewall from a particular IP
- Detected P2P traffic
- Alerting high CPU utilization on firewall
- Firewall failed to allocate RAM memory
- Detection of any kind of failure related to Standby FW
- Top dropped traffic from DMZ, FW
- Outbound Traffic observed on Important Ports
- Successful Outbound Traffic to Blacklisted Threat IP Address
- Multiple Failed Outbound Traffic to Blacklisted Threat IP Address

Security Device – Checkpoint

- Firewall critical alert observed
- VPN configuration change observed
- Administrator Login Failure detected
- Successful logon between Non- Business Hours
- Successful access from Suspicious Countries
- Checkpoint Service restarts
- Firewall Cluster/Gateway Configuration Change
- CPU Utilization High
- Checkpoint Policy Installed
- High number of denied events
- Smart-Defense Signature Based Alert
- VPN Certificate Verification Failure
- Configuration Change detected
- Firewalls reboot

Email – Example – Exchange

- Top 10 users sending mails to external domains
- Top 10 Email Receivers/Senders
- Data Leakage Identified through
- Large files send via mail
- Malicious/Suspicious attachments identified
- Email Usage Group IDs
- Monitoring mails going out from the company domain to other domains after Office Hours
- High Email Bandwidth utilization by individual users
- Detection of Undelivered Messages
- Mailbox Access by Another user
- User sending a Message as another user
- User Sending a Message on behalf another user
- Detection of Users login to the Mailbox which is not their Primary Account
- Detection of Auto Redirected Mails
- Top 10 users sending mails internally
- SMTP gateway sudden spike in Incoming mails
- High number of rejected mails from single “from” address
- Detection of Users login to the Mailbox which is not their Primary Account
- Detection of Auto Redirected Mails

Wireless/VPN

- Rouge Network Traffic Detected
- Top VPN Account Logged in from Multiple Remote Locations
- Top VPN Account Logged in From VPN and on Local Network
- Wireless unauthorized login attempts

- Wireless authorization server is down
- Anonymous login from unknown IP address
- VPN Account logged in from multiple locations in short span of time, or from suspicious countries
- Simultaneous Login from Multiple Locations for Single User
- VPN Connection beyond 24 Hour
- VPN Access from Internal IP Address
- VPN access from overseas
- Wireless AP rebooted
- Wireless unsecure AP detected
- VPN access from onshore team
- VPN access and Access card on Onshore observed

IPS – Example device – Cisco IPS

- UNIX Password File Access Attempt
- IPS High Alert
- Possible Exploit of Vulnerability
- Probable Port Scanning in the network
- SQL Injection Attempt
- Virus Traffic in the network
- Signature Based Attacks

Proxy

- Access attempts on unidentified protocols & port
- Malware Domain Access Report
- Proxy Category based Summary Report
- Malware IP Access Report
- Potentially Unwanted Software access
- Dynamic DNS Host
- Malicious Sources/Malnets
- Malicious Outbound Data/Botnets
- Peer-to-Peer (P2P)
- Proxy Avoidance
- Remote Access Tools
- Access from unusual User Agent
- Post request to uncategorized sites after office hours
- Unwanted Internet Access
- Proxy configuration changes
- Proxy failed login attempt
- Content access violation
- Anonymous proxy access
- Hacker tool website access

- Access attempts by BOTNET identified by HTTP Request header

Oracle/DB

- Oracle password expired
- Critical command usage
- Critical commands executed on the database during non-business hours
- Oracle- Update or Insert Commands
- Oracle user Created/Deleted
- Multiple login failures observed for database
- Database Schema Creation/Modification
- Top Query Execution Failures
- Monitoring login attempts on database
- Use of default vendor accounts against policy
- Database access during non-business hours
- Login failures for sys/system or privileged accounts
- Connection to production databases from disallowed network segments

Router and Switches

- Emergency router error messages
- BGP Neighbour Relationship Status Change
- Router-Power supply failure
- Configuration Change
- Critical messages observed from the SWITCH
- Alert messages observed from the SWITCH
- Detection of Antispam
- File Dropped due to large size
- Detection of application process proxy
- Detection of land attack
- Detection of Ping of death attack
- Detection of new policy addition
- Detection of policy violation
- Virus traffic
- Content filtering detected
- Authentication failure/success

Anti-Virus (AV)

- AV Virus Detected
- AV Detection of Backdoor traffic in the network
- Removable Storage Identified
- AV Malware Infection Identified (Not quarantined/cleaned/deleted/moved)
- Multiple AV Malware Infection Identified from Same Host
- Multiple Sources accessing the same Malware URL

- Multiple Types of AV Malware Infection Identified from Same Host
- Detection failure of Antivirus DAT update in end user machines
- Detection of Worm outbreak in the network
- Detection of Virus Outbreak
- Attempt to stop the Ad hoc/daily scan schedules
- Detection of Backdoor traffic in the network
- Attempt to stop the AV Services
- Attempt to stop the critical AV modules
- AV identified the Rogue machines in the network
- Detection of the scan which is stopped before it completes
- Detection of the scheduled scan is stopped/paused (delayed)
- Detection of the computer which is not protected with latest definitions
- Detection of the new client software installed
- Detection of the client software uninstalled
- AV Malware Breakout Identified across multiple machines on same Subnet/ Different Subnet Multiple re-occurrences of same Infection identified from same machine (AL and Trend – Historical)
- Multiple re-occurrences of unique Infection identify ed from same machine (AL and Trend – Historical)
- Blacklist Domain/IP Addresses monitoring of traffic emerging to/from the Infected machine (AL and Trend – Real Time)
- Brute Force/port or host scan/privilege elevation access attempt from the Infected machine (AL and Trend – Real Time)
- Attempt to restart AV service or process, AV modules from Infected machine
- Access to critical file share, network path, SSH or Remote RDP attempt from the Infected Host

Uncategorized:

- Default User Account Usage
- Inactive User Accounts
- After Hour VPN Assess Monitoring
- Firewall Top Talkers
- P2P Traffic
- Distributed Host Port Scan
- Distributed Network Host Scan
- SYN Flood by IDS/Firewall
- High Number of Denied Connections for a Single Host
- Worm/Virus Outbreak Detected
- Outbound/Inbound Network Sweep
- AV Update Failed
- Malware IP Access
- Malware URL Access

- Hacking attempt on web portal
- Data Leakage
- Detection of BOTNET infection in Internal LAN
- Unauthorised access from Third Party or vendor networks
- Infected Host Activities
- Suspicious, Adware, Phishing and Hacking Activities
- Unwanted Software's
- AV Malware Breakout Identified across multiple machines
- Monitor Development team's access to Production systems
- Blacklisted IP
- Blacklisted IP Pass after multiple Firewall Block
- Blacklisted URL
- Data Overview Trend
- Outbound Traffic to Suspicious Countries
- Outbound Traffic to Suspicious port
- Outbound Traffic to Suspicious Services
- Terminated User Activity
- Malicious Traffic to Vulnerable Asset
- Communications to Bad Domains
- Communications to Blacklisted Domains/IP's
- Data Transfer involved on Blacklisted Domains/IP's
- Outbound traffic involving Database
- Cross Site Scripting
- Script Injection
- Malicious Activity
- Detection of FW Interface Status Changes/Failures
- Insecure Protocol Usage – Detection of insecure traffic like FTP, telnet, VNC on critical servers
- VPN Access from Outside Country
- Suspicious VPN Login Attempts
- Detection of service stop on ESX servers
- Detection of multiple user failed logins on ESX servers from the same source
- Detection of ESX server shutdown/restart
- Detection of virtual machine start/stop/resume/reboot
- Detection of addition/removal of a host on vCenter
- Detection of virtual machine creation/removal on vCenter
- Probable XSS attack observed
- Probable Directory Traversal attack observed
- Suspicious HTTP methods observed
- HTTP Request Other Than GET, POST, HEAD and OPTIONS
- Probable SQL Injection attack observed
- Web Attack- Vulnerability scanning using Nessus