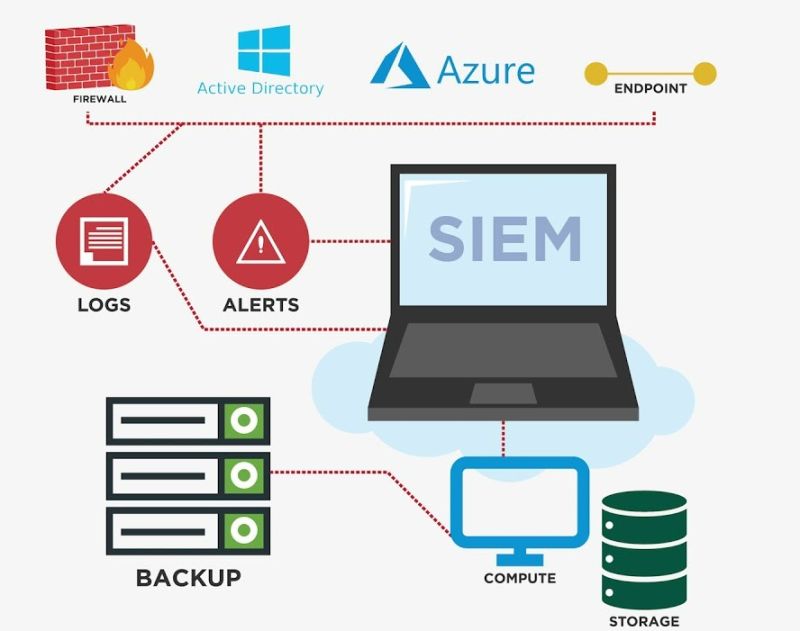
Simple Home-Lab (Active Directory) to Practice SOC Analysis.

  
  
👉 Download Virtualbox: <https://lnkd.in/g8Cfjys9>  
👉 Download Windows 10  
👉 Install Windows Server 2019 [180 days Trial] -<https://lnkd.in/dt4aS_xA>  
👉 Set up Domain Controller for Active Directory -<https://rb.gy/ynojh>  
  
🛡️ Download any one of them (ELK, QRadar)SIEM  
  
🔰 Elastic ELK SIEM  
👉 Download and Installation - <https://lnkd.in/dkf3Vb7B>  
👉 Elastic Free Courses - <https://lnkd.in/dKUtFcF7>  
  
🔰 QRadar SIEM  
👉 Download and Installation -<https://lnkd.in/dCtbkk-H>  
👉QRadar SIEM Free Courses- <https://lnkd.in/dw6aVSj9>  
👉 Get logs to Qradar - <https://lnkd.in/dAMBnXvf>  
👉QRadar - Jose Bravo - <https://lnkd.in/dXbWAQ3R>  
  
🔰 SOC SIEM Use Cases  
🛡️ Below is a list of sample use cases. You can categorize it in multiple ways.  
👉 Windows Use Cases  
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 the same source  
Logins outside normal business hours  
Logins to multiple users accounts from the same source.  
Brute force attempt from the same source with a successful login.  
Windows Account Created Deleted  
Windows Hardware Failure  
Failed Login to Multiple Destinations 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 a Short time period  
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 were created/removed within a short period of time  
\_\_\_\_\_\_\_\_\_\_\_  
  
🛡️ SOC Investigation Microsoft Events Log Analysis -  
<https://lnkd.in/eYPaUV6v>?  
  
  
🎯 For more content - <https://lnkd.in/d2pYU-84>  
  
🔰 Does it work? Great! That is a mini SOC. Document it somewhere and link it to your resume.🙏

Notes:

While using ELK use File Beat, Winlog Beat, Heartbeat so that you can track health resource usages, file changes and track windows logs, use syslog from sysinternals to track system logs, configure GPO and enable audit logs, command execution and PowerShell log, remote connection logs. After configuring these you will have tons of informations in ELK. If you woul like you can configure software execution policy in GPO as well so that you can track software execution as well.

Instead of so many software .... it was better you could have used wazuh virtuabox image and done all the required testing.