Investigation steps for suspicious *processes and commands*

- Does the executing process have a valid signature?
- Should this parent process spawn this child process?
- Should this process be making network connections?
- Is the directory from which the process executed unusual?
- Are there processes with odd names or grammatical errors?
- Are there processes from unusual applications that start at login?
- Is the process count higher than normal for this binary?
- Is the parent count for this process unusual?
- Is the process tree unusual?
- Is the process path abnormally long?
- What commands were used before and after execution of the process?
- Do the commands occur in less than 1% of executions in this environment?
- Do the commands show evidence of obfuscation?
- Do the commands contain paths to executables in unprivileged directories?
- Do the commands contain files with suspicious extensions?
- Do the commands reference a public or blacklisted IP?
- Do the commands contain network discovery-related strings?
- Do the commands contain arguments to modify critical processes?
- Do the commands contain arguments to load DLLs?
- Do the commands contain scheduled task-related strings?
- Do the commands contain arguments to modify the registry?
- Do the commands contain dump or exfiltration-related strings?
- Is the command length abnormally long?
- Do the commands have a high degree of entropy?

Investigation steps for suspicious *users and accounts*

- Is the account privileged (such as admin or system)?
- To what user does the account belong?
- What is the users' role within the organization?
- What are the typical working hours for this user?
- From where does this user typically log in?
- Does this user normally log into or access this device?
- How does this user typically authenticate?
- Does the account have other open alerts?
- Does the account have repeated failed logons?
- Does this user have the required privileges to execute this process?
- Was the account authorized to access the resources it did?
- Are there accounts that were created and deleted in a short time window?
- Are there accounts that do not follow an established naming convention?
- Is the account being logged into from multiple sources within a short timeframe?
- Are there attempts to reset an account's password?
- Are there accounts that have been locked out?
- Are there remote users who are trying to access administrative shares?

Investigation steps for suspicious *network traffic*

- Is there traffic to or from known-bad or suspicious domains?
- Do these domains have odd names or have high entropy?
- Are these young—recently registered—domains?
- Is there traffic to external IPs without DNS query?
- What are the top source and destination IP addresses?
- What layer 4 protocol was used?
- What ports were used?
- What are the geographical zones of the source and destination traffic?
- Is traffic from these geographical zones expected?
- Is the volume of traffic typical in this context?
- What is the volume of bytes and packets that were blocked?
- Where was the traffic blocked? DMZ, Public, Internal?
- Was traffic allowed to internal hosts?
- Have these suspicious IPs triggered any other alerts?
- For how long have these suspicious IPs been seen?
- Is there outbound non-DNS traffic allowed on port 53?
- Do DNS packets have a query length greater than 40 bytes?
- Do DNS packets have a frequency per domain greater than 30 packets?
- Are there any abnormally long sessions (over 24 hours)?
- Is there a large number of POST requests to servers that have not been seen before?
- Is encrypted traffic being transmitted via an unencrypted channel (HTTP or FTP)?
- Is there traffic between clients?
- Are there clients that are sending significantly more data than they receive?