**Splunk Enterprise Security & Elastic SIEM built-in Machine Learning based rules.**This list was compiled for reference purposes only by Efi Kaufman.   
All errors are mine.   
<https://www.linkedin.com/in/efik/>

**Machine Learning Toolkit Searches in Splunk Enterprise Security**

<https://docs.splunk.com/Documentation/ES/6.6.0/Admin/MLTKsearches>

DA-ESS-AccessProtection

1. MLTK: Access - Total Access Attempts

DA-ESS-EndpointProtection

1. MLTK: Change - Abnormally High Number of Endpoint Changes By User – Rule
2. MLTK: Endpoint - Host Sending Excessive Email – Rule
3. MLTK: Malware - Total Infection Count

DA-ESS-IdentityManagement

1. MLTK: Identity - High Volume Email Activity with Non-corporate Domains – Rule
2. MLTK: Identity - Web Uploads to Non-corporate Domains - Rule

DA-ESS-NetworkProtection

1. MLTK: Network - Unusual Volume of Network Activity - Rule
2. MLTK: Web - Abnormally High Number of HTTP Method Events By Src - Rule

SA-AccessProtection

1. MLTK: Access - Authentication Failures By Source - Model Gen
2. MLTK: Access - Authentication Failures By Source Per Day - Model Gen
3. MLTK: Access - Authentication Volume Per Day - Model Gen
4. MLTK: Access - Brute Force Access Behavior Detected – Rule
5. MLTK: Access - Brute Force Access Behavior Detected Over 1d - Rule

SA-EndpointProtection

1. MLTK: Change - Total Change Count By User By Change Type Per Day - Model Gen
2. MLTK: Endpoint - Emails By Destination Count - Model Gen
3. MLTK: Endpoint - Emails By Source - Model Gen
4. MLTK: Endpoint - Malware Daily Count - Model Gen

SA-IdentityManagement

1. MLTK: Identity - Email Activity to Non-corporate Domains by Users Per 1d - Model Gen
2. MLTK: Identity - Web Uploads to Non-corporate Domains by Users Per 1d - Model Gen

SA-NetworkProtection

1. MLTK: Network - Event Count By Signature Per Hour - Model Gen
2. MLTK: Network - Port Activity By Destination Port - Model Gen
3. MLTK: Network - Substantial Increase In Intrusion Events – Rule
4. MLTK: Network - Substantial Increase in Port Activity – Rule
5. MLTK: Network - Traffic Source Count Per 30m - Model Gen
6. MLTK: Network - Traffic Volume Per 30m - Model Gen
7. MLTK: Web - Web Event Count By Src By HTTP Method Per 1d - Model Gen

**MLTK searches in Enterprise Security Content Update (ESCU)**

<https://github.com/splunk/security_content/search?q=MLTK+path%3Adetections%2F>

1. Abnormally High AWS Instances Launched by User – MLTK  
   (AWS Cryptomining, Suspicious AWS EC2 Activities)  
   Uses Probably Density Function (PDF)  
   [Baseline of Excessive AWS Instances Launched by User – MLTK](https://github.com/splunk/security_content/blob/2c9e7b58a8a785b1b1a516083b20673abc4c70a1/detections/cloud/baseline_of_excessive_aws_instances_launched_by_user___mltk.yml)  
   **description**: This search is used to build a Machine Learning Toolkit (MLTK) model  
   for how many RunInstances users do in the environment. By default, the search uses  
   the last 90 days of data to build the model. The model created by this search is  
   then used in the corresponding detection search, which identifies subsequent outliers  
    in the number of RunInstances performed by a user in a small time window.
2. Abnormally High AWS Instances Terminated by User – MLTK  
   (Suspicious AWS EC2 Activities)  
   Uses Probably Density Function (PDF)  
   [Baseline of Excessive AWS Instances Terminated by User - MLTK](https://github.com/splunk/security_content/blob/2c9e7b58a8a785b1b1a516083b20673abc4c70a1/detections/cloud/baseline_of_excessive_aws_instances_terminated_by_user___mltk.yml)  
   **description**: This search is used to build a Machine Learning Toolkit (MLTK) model  
   for how many TerminateInstances users do in the environment. By default, the   
   search uses the last 90 days of data to build the model. The model created by this   
   search is then used in the corresponding detection search, which identifies subsequent outliers in the number of TerminateInstances performed by a user in a   
   small time window.
3. Emotet Malware DHS Report TA18-201A  
   (Hidden Cobra Malware , Ransomware)  
   Uses Probably Density Function (PDF)  
   [SMB Traffic Spike - MLTK](https://github.com/splunk/security_content/blob/08ed88bd88259c03c771c30170d2934ed0a8f878/detections/experimental/network/smb_traffic_spike___mltk.yml)  
   **Description**: This search uses the Machine Learning Toolkit (MLTK) to identify spikes  
    in the number of Server Message Block (SMB) connections.
4. Possible Backdoor Activity Associated With MUDCARP Espionage Campaigns  
   ( Ransomware, Suspicious Command-Line Executions, Suspicious MSHTA Activity, Unusual Processes)  
   Uses Probably Density Function (PDF)  
   [Baseline of Command Line Length - MLTK](https://github.com/splunk/security_content/blob/2c9e7b58a8a785b1b1a516083b20673abc4c70a1/detections/endpoint/baseline_of_command_line_length___mltk.yml)  
   **description**: This search is used to build a Machine Learning Toolkit (MLTK) model  
   to characterize the length of the command lines observed for each user in the   
   environment.  
   By default, the search uses the last 30 days of data to build the model. The model  
   created by this search is then used in the corresponding detection search, which

identifies outliers in the length of the command line.

1. Baseline of SMB Traffic – MLTK  
   (DHS Report TA18-074A, Disabling Security Tools, 'Emotet Malware DHS Report , TA18-201A ', Hidden Cobra Malware, Netsh Abuse, Ransomware)  
   Uses Probably Density Function (PDF)  
   [Baseline of SMB Traffic - MLTK](https://github.com/splunk/security_content/blob/2c9e7b58a8a785b1b1a516083b20673abc4c70a1/detections/network/baseline_of_smb_traffic___mltk.yml)  
   **description**: This search is used to build a Machine Learning Toolkit (MLTK) model  
   to characterize the number of SMB connections observed each hour for every day of  
   week. By default, the search uses the last 30 days of data to build the model. The  
   model created by this search is then used in the corresponding detection search  
   to identify outliers in the number of SMB connections for that hour and day of the  
   week.
2. Suspicious Command-Line Executions  
   (Unusual Processes, Possible Backdoor Activity Associated With MUDCARP , Espionage Campaigns, Ransomware)  
   Uses Probably Density Function (PDF)  
   [Unusually Long Command Line - MLTK](https://github.com/splunk/security_content/blob/08ed88bd88259c03c771c30170d2934ed0a8f878/detections/experimental/endpoint/unusually_long_command_line___mltk.yml)  
   **description**: Command lines that are extremely long may be indicative of malicious  
   activity on your hosts. This search leverages the Machine Learning Toolkit (MLTK)  
   to help identify command lines with lengths that are unusual for a given user.
3. [Baseline of DNS Query Length - MLTK](https://github.com/splunk/security_content/blob/2c9e7b58a8a785b1b1a516083b20673abc4c70a1/detections/network/baseline_of_dns_query_length___mltk.yml)  
   (Command and Control, Hidden Cobra Malware ,Suspicious DNS Traffic)  
   Uses Probably Density Function (PDF)  
   **description**: This search is used to build a Machine Learning Toolkit (MLTK) model  
   to characterize the length of the DNS queries for each DNS record type observed  
   in the environment. By default, the search uses the last 30 days of data to build  
   the model. The model created by this search is then used in the corresponding   
   detection search, which uses it to identify outliers in the length of the DNS query.
4. [DNS Query Length Outliers - MLTK](https://github.com/splunk/security_content/blob/08ed88bd88259c03c771c30170d2934ed0a8f878/detections/experimental/network/dns_query_length_outliers___mltk.yml)  
   (Hidden Cobra Malware, Suspicious DNS Traffic, Command and Control)  
   Uses Probably Density Function (PDF)  
   description: This search allows you to identify DNS requests that are unusually large  
   for the record type being requested in your environment.
5. [Baseline Of Cloud Instances Destroyed](https://github.com/splunk/security_content/blob/2c9e7b58a8a785b1b1a516083b20673abc4c70a1/detections/cloud/baseline_of_cloud_instances_destroyed.yml)  
   (Suspicious Cloud Instance Activities, Cloud Cryptomining)  
   Uses Probably Density Function (PDF)  
   **description**: This search is used to build a Machine Learning Toolkit (MLTK) model  
    for how many instances are destroyed in the environment. By default, the search  
    uses the last 90 days of data to build the model and the model is rebuilt weekly.  
    The model created by this search is then used in the corresponding detection   
   search, which identifies subsequent outliers in the number of instances destroyed in   
   a small time window.
6. [Baseline Of Cloud Security Group API Calls Per User](https://github.com/splunk/security_content/blob/2c9e7b58a8a785b1b1a516083b20673abc4c70a1/detections/cloud/baseline_of_cloud_security_group_api_calls_per_user.yml)  
   (Suspicious Cloud User Activities)  
   Uses Probably Density Function (PDF)  
   **description**: This search is used to build a Machine Learning Toolkit (MLTK) model  
   for how many API calls for security groups are performed by each user. By default,  
   the search uses the last 90 days of data to build the model and the model is rebuilt  
   weekly.
7. [Baseline Of Cloud Infrastructure API Calls Per User](https://github.com/splunk/security_content/blob/2c9e7b58a8a785b1b1a516083b20673abc4c70a1/detections/cloud/baseline_of_cloud_infrastructure_api_calls_per_user.yml)  
   (Suspicious Cloud User Activities)  
   Uses Probably Density Function (PDF)  
   **description**: This search is used to build a Machine Learning Toolkit (MLTK) model  
   for how many API calls are performed by each user. By default, the search uses the  
   last 90 days of data to build the model and the model is rebuilt weekly. The model  
   created by this search is then used in the corresponding detection search, which  
   identifies subsequent outliers in the number of instances created in a small time  
   window.
8. [Baseline Of Cloud Instances Launched](https://github.com/splunk/security_content/blob/2c9e7b58a8a785b1b1a516083b20673abc4c70a1/detections/cloud/baseline_of_cloud_instances_launched.yml)  
   (Cloud Cryptomining, Suspicious Cloud Instance Activities)  
   Uses Probably Density Function (PDF)  
   **description**: This search is used to build a Machine Learning Toolkit (MLTK) model  
   for how many instances are created in the environment. By default, the search uses  
   the last 90 days of data to build the model and the model is rebuilt weekly. The  
   model created by this search is then used in the corresponding detection search,  
   which identifies subsequent outliers in the number of instances created in a small  
   time window.
9. [Abnormally High AWS Instances Terminated by User - MLTK](https://github.com/splunk/security_content/blob/08ed88bd88259c03c771c30170d2934ed0a8f878/detections/deprecated/abnormally_high_aws_instances_terminated_by_user___mltk.yml)  
   (Suspicious AWS EC2 Activities)  
   Uses Probably Density Function (PDF)  
   **description**: This search looks for AWS CloudTrail events where a user successfully  
   terminates an abnormally high number of instances. This search is deprecated and  
   have been translated to use the latest Change Datamodel.
10. [Abnormally High AWS Instances Launched by User - MLTK](https://github.com/splunk/security_content/blob/08ed88bd88259c03c771c30170d2934ed0a8f878/detections/deprecated/abnormally_high_aws_instances_launched_by_user___mltk.yml)  
    (AWS Cryptomining, Suspicious AWS EC2 Activities)  
    **description**: This search looks for AWS CloudTrail events where a user successfully  
    launches an abnormally high number of instances. This search is deprecated and   
    have been translated to use the latest Change Datamodel.

**Elastic Anomaly Detection with Machine Learning: Prebuilt job reference**

<https://www.elastic.co/guide/en/security/current/prebuilt-ml-jobs.html#prebuilt-ml-jobs>

**1. linux\_anomalous\_network\_activity\_ecs**

Identifies OS processes that do not usually use the network but have unexpected network activity, which can indicate command-and-control, lateral movement, persistence, or data exfiltration activity.  
A process with unusual network activity can denote process exploitation or injection, where the process is used to run persistence mechanisms that allow a malicious actor remote access or control of the host, data exfiltration, and execution of unauthorized network applications.

**2. linux\_anomalous\_network\_port\_activity\_ecs**

Identifies unusual destination port activity that can indicate command-and-control, persistence mechanism, or data exfiltration activity.

Rarely used destination port activity is generally unusual in Linux fleets, and can indicate unauthorized access or threat actor activity.

**3. linux\_anomalous\_network\_service**

Searches for unusual listening ports that can indicate execution of unauthorized services, backdoors, or persistence mechanisms.

**4. linux\_anomalous\_network\_url\_activity\_ecs**

Searches for unusual web URL requests from hosts, which can indicate malware delivery and execution.

Wget and cURL are commonly used by Linux programs to download code and data. Most of the time, their usage is entirely normal. Generally, because they use a list of URLs, they repeatedly download from the same locations. However, Wget and cURL are sometimes used to deliver Linux exploit payloads, and threat actors use these tools to download additional software and code. For these reasons, unusual URLs can indicate unauthorized downloads or threat activity.

**5. linux\_anomalous\_process\_all\_hosts\_ecs**

Searches for rare processes running on multiple hosts in an entire fleet or network.

This reduces the detection of false positives since automated maintenance processes usually only run occasionally on a single machine but are common to all or many hosts in a fleet.

**6. linux\_anomalous\_user\_name\_ecs**

Searches for activity from users who are not normally active, which can indicate unauthorized changes, activity by unauthorized users, lateral movement, and compromised credentials.

In organizations, new usernames are not often created apart from specific types of system activities, such as creating new accounts for new employees. These user accounts quickly become active and routine.

Events from rarely used usernames can point to suspicious activity. Additionally, automated Linux fleets tend to see activity from rarely used usernames only when personnel log in to make authorized or unauthorized changes, or threat actors have acquired credentials and log in for malicious purposes. Unusual usernames can also indicate pivoting, where compromised credentials are used to try and move laterally from one host to another.

**7. linux\_network\_configuration\_discovery**

Looks for commands related to system network configuration discovery from an unusual user context. This can be due to uncommon troubleshooting activity or due to a compromised account. A compromised account may be used by a threat actor to engage in system network configuration discovery in order to increase their understanding of connected networks and hosts. This information may be used to shape follow-up behavior such as lateral movement or additional discovery.

**8. linux\_network\_connection\_discovery**

Looks for commands related to system network connection discovery from an unusual user context. This can be due to uncommon troubleshooting activity or due to a compromised account. A compromised account may be used by a threat actor to engage in system network connection discovery in order to increase their understanding of connected services and systems. This information may be used to shape follow-up behaviors such as lateral movement or additional discovery.

**9. linux\_rare\_kernel\_module\_arguments**Looks for unusual kernel modules which are often used for stealth.

**10. linux\_rare\_metadata\_process**

Looks for anomalous access to the metadata service by an unusual process. The metadata service may be targeted in order to harvest credentials or user data scripts containing secrets.

**11. linux\_rare\_metadata\_user**

Looks for anomalous access to the metadata service by an unusual user. The metadata service may be targeted in order to harvest credentials or user data scripts containing secrets.

**12. linux\_rare\_sudo\_user**

Looks for sudo activity from an unusual user context.

**13. linux\_rare\_user\_compiler**

Looks for compiler activity by a user context which does not normally run compilers. This can be ad-hoc software changes or unauthorized software deployment. This can also be due to local privilege elevation via locally run exploits or malware activity.

**14. linux\_system\_information\_discovery**

Looks for commands related to system information discovery from an unusual user context. This can be due to uncommon troubleshooting activity or due to a compromised account. A compromised account may be used to engage in system information discovery in order to gather detailed information about system configuration and software versions. This may be a precursor to selection of a persistence mechanism or a method of privilege elevation.

**15. linux\_system\_process\_discovery**

Looks for commands related to system process discovery from an unusual user context. This can be due to uncommon troubleshooting activity or due to a compromised account. A compromised account may be used to engage in system process discovery in order to increase their understanding of software applications running on a target host or network. This may be a precursor to selection of a persistence mechanism or a method of privilege elevation.

**16. linux\_system\_user\_discovery**

Looks for commands related to system user or owner discovery from an unusual user context. This can be due to uncommon troubleshooting activity or due to a compromised account. A compromised account may be used to engage in system owner or user discovery in order to identify currently active or primary users of a system. This may be a precursor to additional discovery, credential dumping or privilege elevation activity.

**17. rare\_process\_by\_host\_linux\_ecs**

Identifies rare processes that do not usually run on individual hosts, which can indicate execution of unauthorized services, malware, or persistence mechanisms.

Processes are considered rare when they only run occasionally as compared with other processes running on the host.

**18. suspicious\_login\_activity\_ecs**

Identifies an unusually high number of authentication attempts.

**Security: CloudTrailedit**

These configurations are only available if data exists that matches the recognizer query specified in the manifest file.

Detect suspicious activity recorded in your CloudTrail logs.

**19. high\_distinct\_count\_error\_message**

Looks for a spike in the rate of an error message. These spikes might simply indicate an impending service failure but they can also be byproducts of attempted or successful persistence, privilege escalation, defense evasion, discovery, lateral movement, or collection activity by a threat actor.

**20. rare\_error\_code**

Looks for unusual errors. Rare and unusual errors might simply indicate an impending service failure but they can also be byproducts of attempted or successful persistence, privilege escalation, defence evasion, discovery, lateral movement, or collection activity by a threat actor.

**21. rare\_method\_for\_a\_city**

Looks for AWS API calls that—​while not inherently suspicious or abnormal—​are sourcing from a geolocation (city) that is unusual. These calls can be the result of compromised credentials or keys.

**22. rare\_method\_for\_a\_country**

Looks for AWS API calls that—​while not inherently suspicious or abnormal—​are sourcing from a geolocation (country) that is unusual. These calls can be the result of compromised credentials or keys.

**23. rare\_method\_for\_a\_username**

Looks for AWS API calls that—​while not inherently suspicious or abnormal—​are sourcing from a user context that does not normally call the method. These calls can be the result of compromised credentials or keys as someone uses a valid account to persist, move laterally, or exfil data.

**24. v2\_linux\_anomalous\_network\_port\_activity\_ecs**

Identifies unusual destination port activity that can indicate command-and-control, persistence mechanism, or data exfiltration activity.

Rarely used destination port activity is generally unusual in Linux fleets, and can indicate unauthorized access or threat actor activity.

**25. v2\_linux\_anomalous\_process\_all\_hosts\_ecs**

Looks for processes that are unusual to all Linux hosts. Such unusual processes may indicate unauthorized services, malware, or persistence mechanisms.

This reduces the detection of false positives since automated maintenance processes usually only run occasionally on a single machine but are common to all or many hosts in a fleet.

**26. v2\_linux\_anomalous\_user\_name\_ecs**

Searches for activity from users who are not normally active, which can indicate unauthorized changes, activity by unauthorized users, lateral movement, and compromised credentials.

In organizations, new usernames are not often created apart from specific types of system activities, such as creating new accounts for new employees. These user accounts quickly become active and routine.

Events from rarely used usernames can point to suspicious activity. Additionally, automated Linux fleets tend to see activity from rarely used usernames only when personnel log in to make authorized or unauthorized changes, or threat actors have acquired credentials and log in for malicious purposes. Unusual usernames can also indicate pivoting, where compromised credentials are used to try and move laterally from one host to another.

**27. v2\_linux\_rare\_metadata\_process**

Looks for anomalous access to the metadata service by an unusual process. The metadata service may be targeted in order to harvest credentials or user data scripts containing secrets.

**28.v2\_linux\_rare\_metadata\_user**

Looks for anomalous access to the metadata service by an unusual user. The metadata service may be targeted in order to harvest credentials or user data scripts containing secrets.

**29. v2\_rare\_process\_by\_host\_linux\_ecs**

Looks for processes that are unusual to a particular Linux host. Such unusual processes might indicate unauthorized services, malware, or persistence mechanisms.

Processes are considered rare when they only run occasionally as compared with other processes running on the host.

**30. high\_count\_by\_destination\_country**

Looks for an unusually large spike in network activity to one destination country in the network logs. This could be due to unusually large amounts of reconnaissance or enumeration traffic. Data exfiltration activity may also produce such a surge in traffic to a destination country which does not normally appear in network traffic or business work-flows. Malware instances and persistence mechanisms may communicate with command-and-control (C2) infrastructure in their country of origin, which may be an unusual destination country for the source network.

**31. high\_count\_network\_denies**

Looks for an unusually large spike in network traffic that was denied by network access control lists (ACL) or firewall rules. Such a burst of denied traffic is usually either a misconfigured application or firewall, or suspicious or malicious activity. Unsuccessful attempts at network transit, in order to connect to command-and-control (C2), or engage in data exfiltration, may produce a burst of failed connections. This could also be due to unusually large amounts of reconnaissance or enumeration traffic. Denial-of-service attacks or traffic floods may also produce such a surge in traffic.

**32.high\_count\_network\_events**

Looks for an unusually large spike in network traffic. Such a burst of traffic, if not caused by a surge in business activity, can be due to suspicious or malicious activity. Large-scale data exfiltration may produce a burst of network traffic; this could also be due to unusually large amounts of reconnaissance or enumeration traffic. Denial-of-service attacks or traffic floods may also produce such a surge in traffic.

**33.rare\_destination\_country**

Looks for an unusual destination country name in the network logs. This can be due to initial access, persistence, command-and-control, or exfiltration activity. For example, when a user clicks on a link in a phishing email or opens a malicious document, a request may be sent to download and run a payload from a server in a country which does not normally appear in network traffic or business work-flows. Malware instances and persistence mechanisms may communicate with command-and-control (C2) infrastructure in their country of origin, which may be an unusual destination country for the source network.

**34.packetbeat\_dns\_tunneling**

Searches for unusually large numbers of DNS queries for a single top-level DNS domain, which is often used for DNS tunneling.

DNS tunneling can be used for command-and-control, persistence, or data exfiltration activity. For example, dnscat tends to generate many DNS questions for a top-level domain as it uses the DNS protocol to tunnel data.

**35.packetbeat\_rare\_dns\_question**

Searches for rare and unusual DNS queries that indicate network activity with unusual domains is about to occur. This can be due to initial access, persistence, command-and-control, or exfiltration activity.

For example, when a user clicks on a link in a phishing email or opens a malicious document, a request may be sent to download and run a payload from an uncommon domain. When malware is already running, it may send requests to an uncommon DNS domain the malware uses for command-and-control communication.

**36.packetbeat\_rare\_server\_domain**

Searches for rare and unusual DNS queries that indicate network activity with unusual domains is about to occur. This can be due to initial access, persistence, command-and-control, or exfiltration activity.

For example, when a user clicks on a link in a phishing email or opens a malicious document, a request may be sent to download and run a payload from an uncommon HTTP or TLS server. When malware is already running, it may send requests to an uncommon DNS domain the malware uses for command-and-control communication.

**37.packetbeat\_rare\_urls**

Searches for rare and unusual URLs that indicate unusual web browsing activity. This can be due to initial access, persistence, command-and-control, or exfiltration activity.

For example, in a strategic web compromise or watering hole attack, when a trusted website is compromised to target a particular sector or organization, targeted users may receive emails with uncommon URLs for trusted websites. These URLs can be used to download and run a payload. When malware is already running, it may send requests to uncommon URLs on trusted websites the malware uses for command-and-control communication. When rare URLs are observed being requested for a local web server by a remote source, these can be due to web scanning, enumeration or attack traffic, or they can be due to bots and web scrapers which are part of common Internet background traffic.

**38.packetbeat\_rare\_user\_agent**

Searches for rare and unusual user agents that indicate web browsing activity by an unusual process other than a web browser. This can be due to persistence, command-and-control, or exfiltration activity. Uncommon user agents coming from remote sources to local destinations are often the result of scanners, bots, and web scrapers, which are part of common internet background traffic.

Much of this is noise, but more targeted attacks on websites using tools like Burp or SQLmap can sometimes be discovered by spotting uncommon user agents. Uncommon user agents in traffic from local sources to remote destinations can be any number of things, including harmless programs like weather monitoring or stock-trading programs. However, uncommon user agents from local sources can also be due to malware or scanning activity.

**39.v2\_rare\_process\_by\_host\_windows\_ecs**

Detects unusually rare processes on Windows hosts, which can indicate execution of unauthorized services, malware, or persistence mechanisms.

Processes are considered rare when they only run occasionally as compared with other processes running on the host.

**40. v2\_windows\_anomalous\_network\_activity\_ecs**

Looks for unusual processes using the network which could indicate command-and- control, lateral movement, persistence, or data exfiltration activity.

A process with unusual network activity can denote process exploitation or injection, where the process is used to run persistence mechanisms that allow a malicious actor remote access or control of the host, data exfiltration, and execution of unauthorized network applications.

**41. v2\_windows\_anomalous\_path\_activity\_ecs**

Looks for activity in unusual paths, which might indicate execution of malware or persistence mechanisms.

Windows payloads often execute from user profile paths. In corporate Windows environments, software installation is centrally managed and it is unusual for programs to be executed from user or temporary directories. Processes executed from these locations can denote that a user downloaded software directly from the internet or a malicious script/macro executed malware.

**42. v2\_windows\_anomalous\_process\_all\_hosts\_ecs**

Looks for processes that are unusual to all Windows hosts. Such unusual processes may indicate execution of unauthorized services, malware, or persistence mechanisms.

This reduces the detection of false positives since automated maintenance processes usually only run occasionally on a single machine but are common to all or many hosts in a fleet.

**43. v2\_windows\_anomalous\_process\_creation**

Identifies unusual process relationships that can indicate malware execution or persistence mechanisms.

Malicious scripts often call on other applications and processes as part of their exploit payload. For example, when a malicious Office document runs scripts as part of an exploit payload, Excel or Word may start a script interpreter process, which, in turn, runs a script that downloads and executes malware. Another common scenario is Outlook running an unusual process when malware is downloaded in an email.

Monitoring and identifying anomalous process relationships is an excellent way of detecting new and emerging malware that is not yet recognized by anti-virus scanners.

**44. v2\_windows\_anomalous\_user\_name\_ecs**

Searches for activity from users who are not normally active, which can indicate unauthorized changes, activity by unauthorized users, lateral movement, and compromised credentials.

In organizations, new usernames are not often created apart from specific types of system activities, such as creating new accounts for new employees. These user accounts quickly become active and routine.

Events from rarely used usernames can point to suspicious activity. Additionally, automated Linux fleets tend to see activity from rarely used usernames only when personnel log in to make authorized or unauthorized changes, or threat actors have acquired credentials and log in for malicious purposes. Unusual usernames can also indicate pivoting, where compromised credentials are used to try and move laterally from one host to another.

**45. v2\_windows\_rare\_metadata\_process**

Looks for anomalous access to the metadata service by an unusual process. The metadata service may be targeted in order to harvest credentials or user data scripts containing secrets.

**46. v2\_windows\_rare\_metadata\_user**

Looks for anomalous access to the metadata service by an unusual user. The metadata service may be targeted in order to harvest credentials or user data scripts containing secrets.

**47. rare\_process\_by\_host\_windows\_ecs**

Identifies rare processes that do not usually run on individual hosts, which can indicate execution of unauthorized services, malware, or persistence mechanisms.

Processes are considered rare when they only run occasionally as compared with other processes running on the host.

**48. windows\_anomalous\_network\_activity\_ecs**

Identifies OS processes that do not usually use the network but have unexpected network activity, which can indicate command-and-control, lateral movement, persistence, or data exfiltration activity.

A process with unusual network activity can denote process exploitation or injection, where the process is used to run persistence mechanisms that allow a malicious actor remote access or control of the host, data exfiltration, and execution of unauthorized network applications.

**49. windows\_anomalous\_path\_activity\_ecs**

Identifies processes started from atypical folders in the file system, which might indicate malware execution or persistence mechanisms.

In corporate Windows environments, software installation is centrally managed and it is unusual for programs to be executed from user or temporary directories. Processes executed from these locations can denote that a user downloaded software directly from the internet or a malicious script/macro executed malware.

**50. windows\_anomalous\_process\_all\_hosts\_ecs**

Searches for rare processes running on multiple hosts in an entire fleet or network.

This reduces the detection of false positives since automated maintenance processes usually only run occasionally on a single machine but are common to all or many hosts in a fleet.

**51. windows\_anomalous\_process\_creation**

Identifies unusual parent-child process relationships that can indicate malware execution or persistence mechanisms.

Malicious scripts often call on other applications and processes as part of their exploit payload. For example, when a malicious Office document runs scripts as part of an exploit payload, Excel or Word may start a script interpreter process, which, in turn, runs a script that downloads and executes malware. Another common scenario is Outlook running an unusual process when malware is downloaded in an email.

Monitoring and identifying anomalous process relationships is an excellent way of detecting new and emerging malware that is not yet recognized by anti-virus scanners.

**52. windows\_anomalous\_service**

Searches for unusual Windows services that can indicate execution of unauthorized services, malware, or persistence mechanisms.

In corporate Windows environments, hosts do not generally run many rare or unique services. This job helps detect malware and persistence mechanisms that have been installed and run as a service.

**53. windows\_anomalous\_user\_name\_ecs**

Searches for activity from users who are not normally active, which can indicate unauthorized changes, activity by unauthorized users, lateral movement, and compromised credentials.

In organizations, new usernames are not often created apart from specific types of system activities, such as creating new accounts for new employees. These user accounts quickly become active and routine.

Events from rarely used usernames can point to suspicious activity. Additionally, automated Linux fleets tend to see activity from rarely used usernames only when personnel log in to make authorized or unauthorized changes, or threat actors have acquired credentials and log in for malicious purposes. Unusual usernames can also indicate pivoting, where compromised credentials are used to try and move laterally from one host to another.

**54. windows\_rare\_metadata\_process**

Looks for anomalous access to the metadata service by an unusual process. The metadata service may be targeted in order to harvest credentials or user data scripts containing secrets.

**55. windows\_rare\_metadata\_user**

Looks for anomalous access to the metadata service by an unusual user. The metadata service may be targeted in order to harvest credentials or user data scripts containing secrets.

**56. windows\_rare\_user\_runas\_event**

Searches for unusual user context switches using the runas command or similar techniques, which can indicate account takeover or privilege escalation using compromised accounts. Privilege elevation using tools like runas is more common for domain and network administrators than professionals who are not members of the technology department.

**57. windows\_rare\_user\_type10\_remote\_login**

Searches for unusual remote desktop protocol (RDP) logins, which can indicate account takeover or credentialed persistence using compromised accounts. RDP attacks, such as BlueKeep, also tend to use unusual usernames.