

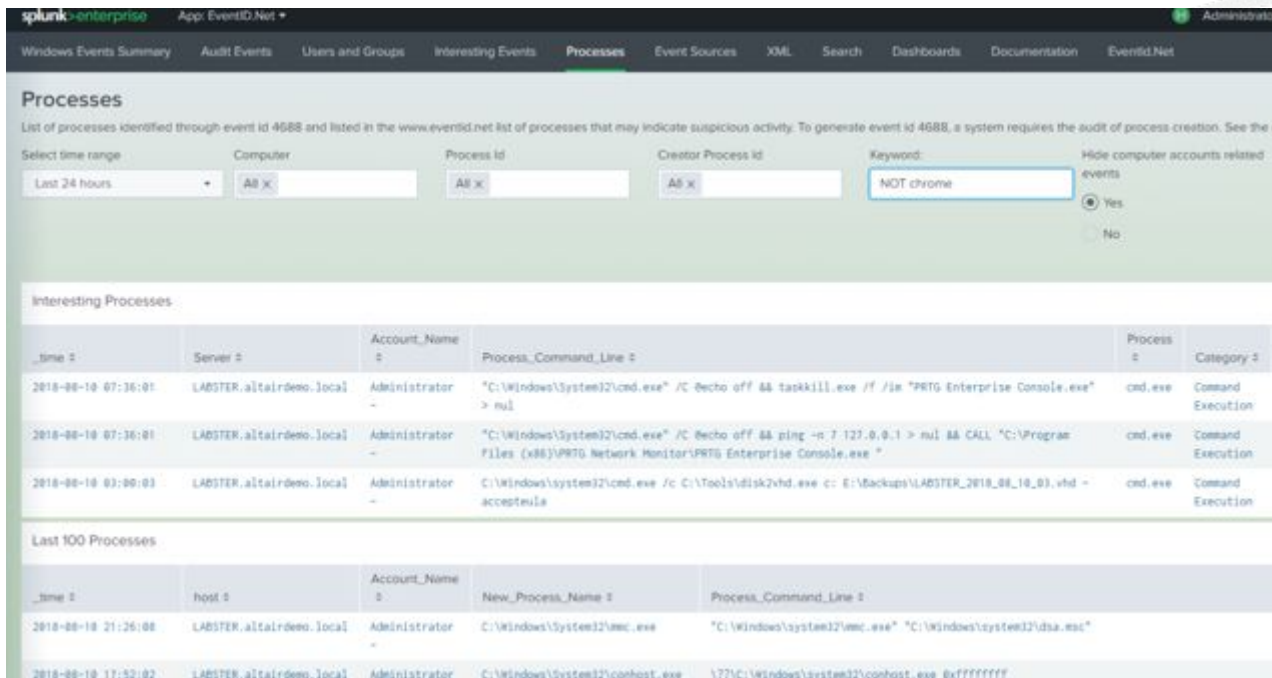
Logging & Monitoring

Farrukh Ali

What are Logs?

- Raw data that is produced by a system or application
- Reveal information about activity, health and functionality
- Records of time-stamped events generated by system and applications
 - Different types of events, times, origins and more
 - Can be used to debug, identify issues, identify breaches & provide details
- Vital to understanding health of system/applications, network infrastructure and security issues

Splunk Logs



The screenshot shows the Splunk Enterprise interface for the 'EventID:Net' app. The 'Processes' section is active, displaying a list of processes identified through event ID 4688. The search criteria include a time range of 'Last 24 hours', computer 'LABSTER.altairdemo.local', and a keyword 'NOT chrome'. The 'Interesting Processes' table shows three entries with their respective timestamps, servers, account names, and command lines. The 'Last 100 Processes' table shows two entries with their timestamps, hosts, account names, and process names.

Interesting Processes

_time	Server	Account_Name	Process_Command_Line	Process	Category
2018-08-18 07:36:01	LABSTER.altairdemo.local	Administrator	"C:\Windows\System32\cmd.exe" /C echo off && taskkill.exe /f /im "PRTO Enterprise Console.exe" > nul	cmd.exe	Command Execution
2018-08-18 07:36:01	LABSTER.altairdemo.local	Administrator	"C:\Windows\System32\cmd.exe" /C echo off && ping -n 7 127.0.0.1 > nul && CALL "C:\Program Files (x86)\PRTO Network Monitor\PRTO Enterprise Console.exe"	cmd.exe	Command Execution
2018-08-18 03:00:03	LABSTER.altairdemo.local	Administrator	C:\Windows\System32\cmd.exe /c C:\Tools\disk2vhd.exe c: E:\Backups\LABSTER_2018_08_18_03.vhd -acceptuila	cmd.exe	Command Execution

Last 100 Processes

_time	host	Account_Name	New_Process_Name	Process_Command_Line
2018-08-18 21:26:08	LABSTER.altairdemo.local	Administrator	C:\Windows\System32\vmc.exe	"C:\Windows\system32\vmc.exe" "C:\Windows\system32\dsa.exe"
2018-08-18 17:52:02	LABSTER.altairdemo.local	Administrator	C:\Windows\System32\conhost.exe	1771C:\Windows\system32\conhost.exe 6x77777777

Log Aggregation

- Process of gathering logs from all sources and centralizing them
- Reduces time spent & improves efficiency
- Log Aggregation Methods :
 - 1) Syslog – collects data through a standard logging protocol; syslog server receives logs from multiple sources and then stores them in a easy to read format
 - 2) Event Streaming – collects log data from network devices or applications through SNMP, Netflow, or IPFIX
 - 3) Log Collectors – collects logs in real-time through a third-party
 - 4) Direct Access – collects logs directly from devices or systems on a network using API or network protocol integration

Syslog Examples

```
syslog - System Log Viewer
Xorg.0.log Jun 30 22:15:53 ubuntu howto geek: Hello World
auth.log Jun 30 22:17:01 ubuntu CRON[4161]: (root) CMD ( cd / && run-parts --re
dpkg.log Jun 30 22:26:20 ubuntu dhclient: DHCPREQUEST of 192.168.164.129 on eth0
mail.log Jun 30 22:26:20 ubuntu dhclient: DHCPACK of 192.168.164.129 from 192.168
syslog Jun 30 22:26:20 ubuntu dhclient: bound to 192.168.164.129 -- renewal in
Jun 30 22:31:17 ubuntu ScriptName: Hello World
Jun 30 22:40:46 ubuntu dhclient: DHCPREQUEST of 192.168.164.129 on eth0
Jun 30 22:40:46 ubuntu dhclient: DHCPACK of 192.168.164.129 from 192.16
Jun 30 22:40:46 ubuntu dhclient: bound to 192.168.164.129 -- renewal in
```

```
All Messages
SYSTEM LOG QUERIES
All Messages 4:18:07 PM OmniOutliner: Warning: No identifier set on bundle MSBundle ~/Users/ach...
DIAGNOSTIC AND USAGE INFORMAT...
Diagnostic and Usage Messages
User Diagnostic Reports
System Diagnostic Reports
FILES
system.log
~/Library/Logs
~/Library/Logs
~/var/log
4000 messages from 12/30/15, 12:01:33 PM to 12/30/15, 4:20:40 PM
```

Event Properties - Event 4524: Microsoft Windows security auditing

General Details

An account was successfully logged on.

Subject	Security ID: SYSTEM
	Account Name: WIN-GG8JULGCKGO
	Account Domain: WIN-GG8JULGCKGO
	Login ID: 0x2
Logon Information	Logon Type: 2
	Requested Admin Mode: No
	Virtual Account: No
	Elevated Token: Yes
Impersonation Level	Impersonation
New Logon	Security ID: CONTOSO\Administrator
	Account Name: Administrator
	Account Domain: WIN-GG8JULGCKGO
	Login ID: 0x0
	Linked Logon ID: 0x0
	Network Account Name: -
	Network Account Domain: -
	Logon GUID: {00000000-0000-0000-0000-000000000000}
Process Information	Process ID: 0x44
	Process Name: C:\Windows\System32\cmd.exe
Network Information	Workstation Name: WIN-GG8JULGCKGO
	Source Network Address: 127.0.0.1
	Source Port: 0
Detailed Authentication Information	Logon Process: User32
	Authentication Package: Negotiate
	Transmitted Services: -
	Package Name (NTLM only): -
	Key Length: 0
Log Name: Security	Source: Microsoft Windows security
	Event ID: 4624
	Level: Information
	Task Category: Logon
	Keywords: Audit Success
	User: N/A
	Computer: WIN-GG8JULGCKGO
	OpCode: Info

More Information: [Event Log Online Help](#)

Processing Logs

- Raw logs converted into a standardized data source
- Steps to process logs:
 1. Log Parsing – Log formats are converted to structured data
 2. Log Normalization & Categorization – Events grouped together with common attributes
Ex.: time, function, IP address etc.
 3. Log Enrichment – Adding helpful information to logs to make them more useful
 4. Log Indexing – Creating an index of logs
 5. Log Storage – Finally, logs are stored

Log Types

- Endpoint Logs – Logs generated from endpoints. Different levels of logs produced from hardware, operating system, middleware, database and applications; used to understand status and activity of endpoint device
Ex. Devices in a network; laptops, smartphones, servers
- Router Logs – Logs generated from devices such as routers, switches and load balancers

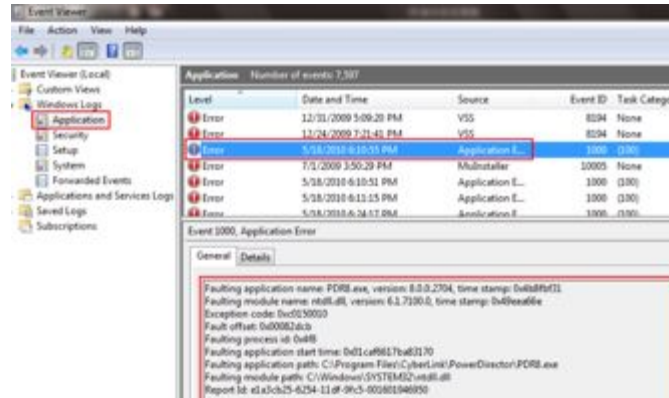


The screenshot shows the 'Log' page in the Netgear Genie Advanced interface. The page has a sidebar on the left with navigation options like 'ADVANCED Home', 'WiFi Wizard', 'Setup', 'Security', 'Administration', 'System Status', 'Router Mode', 'Attached Devices', 'Backup Settings', 'Set Password', 'Event Log', 'Diagnose', 'Wireless Channel', 'Wireless AP', and 'Advanced Setup'. The main content area displays a table of log entries with columns for Description, Count, Last, Target, and Source. The table contains several entries related to DHCP and DHCPv6 events.

Description	Count	Last	Target	Source
dhcpv6 logs from source 192.168.0.11	2	21:11:26 2017	0.0.0.0	192.168.0.11.0
[DHCPv6] net event: GetClientIPAddress from source 192.168.0.13	1	21:00:38 2017	0.0.0.0	192.168.0.13.0
[DHCPv6] net event: GetServerPortMappingInfo from source 192.168.0.13	6	21:00:38 2017	0.0.0.0	192.168.0.13.0
[DHCP] IP: 192.168.0.12 to MAC address	1	20:30:58 2017	0.0.0.0	0.0.0.0
[DHCP] net event: GetClientIPAddress from source 192.168.0.13	1	20:30:43 2017	0.0.0.0	192.168.0.13.0
[DHCP] net event: GetServerPortMappingInfo from source 192.168.0.13	6	20:30:38 2017	0.0.0.0	192.168.0.13.0
dhcpv6 logs from source 192.168.0.11	2	20:25:23 2017	0.0.0.0	192.168.0.11.0
dhcpv6 logs from source 192.168.0.11	1	20:21:57 2017	0.0.0.0	192.168.0.11.0

Log Types (cont.)

- Application Event Logs – Logs generated by applications.
- IoT Logs– Logs generated from devices connected to the Internet of Things. Capturing these logs can be difficult because many devices have no logging at all or limit the ability to access these logs.
- Proxy Logs – Maintained by networks to provide details on traffic. Contain user, application and service requests.



Log Formats

- Log Formats
 - Key value pair, CSV, JSON, Common Event Format (CEF)

- **CSV Log Format**

5:39:55 → Time
[Fname, Lname, name@company] → User Credentials
Sign-in Failed → Authentication Event
173.0.0.0 → IP
/app/office365 → App User Signed Into

- **Common Event Format**

CEF:Version|Device Vendor|Device Product|Device Version|Signature
ID|Name|Severity|Extension

- **JSON Log Format**

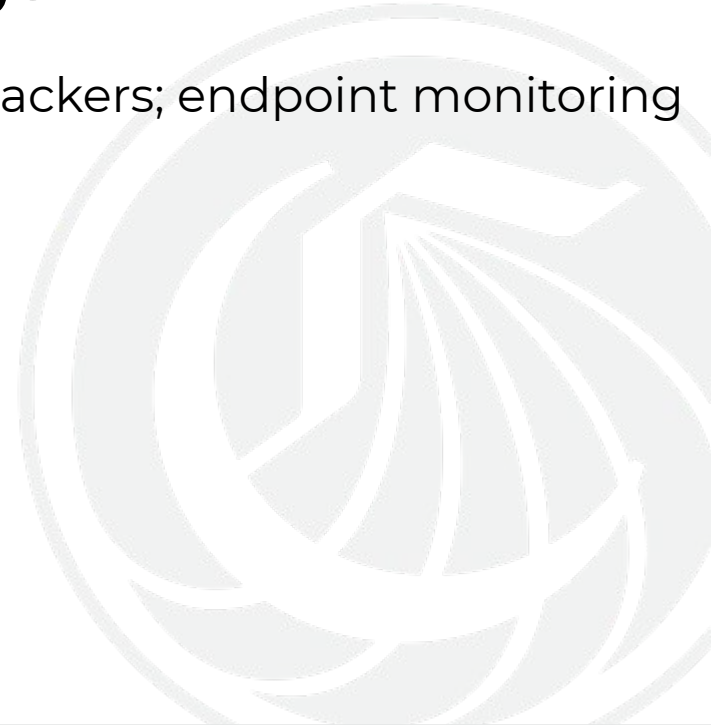
MachineName → User's host
Message → The event is a Kerberos service ticket (user already authenticated and sending access request for specific service)
TimeGenerated → Time of event
TargetUserName → Username attempting to login
TargetDomainName → Domain user attempted to login to
ServiceName → Service user attempted to log into

What is Log Monitoring?

- Use log files to scan and search for important events and irregular behavior
- Set rules and alerts
- Help identify issues, attacks or suspicious activity
- Events and incidents are the basic components of monitoring
 - Event – An occurrence or alert
 - Incident – Attack, broken rule, security violation, unauthorized access or change to data without consent

Endpoint Logs

- Endpoints have become a major target for attackers; endpoint monitoring is crucial
- Types of Endpoint Logs to monitor:
 - iOS Logs and iOS Crash Reports
 - Linux Event Logs
 - Windows Event Logs
 - Windows Security Logs



Endpoint Logs



















- iOS logs are not enabled by default, with the exception being application crash reports. With the introduction of iOS 10, Apple offered a logging API that allowed only pre-determined applications to send out events. These logs are still difficult to access which influenced third-parties to collect and aggregate them.
- Linux logs involve recording a timeline of events which occur on the operating system and its applications.
 - **What events are logged?** System events, kernel, package managers, boot processes and other common services.
- Windows OS provides event logs which showcase its own system and applications software and hardware events. These can be viewed through Windows Event Viewer. These contain events specified by the user using the system's audit policy.
 - **What events are logged?** Application installations, security management, startup programs and errors, System processes, system events, file access, policy changes, privilege access, logon, directory service access, account logon and account management.

Sysmon

- Windows system service and device driver that monitors and logs system activity to the Windows Event Log
- Provides detailed information about:
 - Process creations with full command line for both current and parent processes
 - Includes process GUID in each event to allow correlation even with reused process IDs
 - Includes session GUID in each event to allow correlation on logon session
 - Records hash of process image files
 - Logs loading of drivers or DLLs with signatures and hashes
 - Logs opens for raw read access of disks and volumes
 - Logs network connections, includes source process, Ips, ports, hostnames and port names
 - Changes to file creation time to understand when a file was really created

Sysmon Events

Operational Number of events: 64,198 (0) New events available

Level	Date and Time	Source	Event ID	Task Category
 Information	7/11/2019 11:36:29 AM	Sysmon	13	Registry value set (rule: RegistryEvent)
 Information	7/11/2019 11:36:29 AM	Sysmon	12	Registry object added or deleted (rule: Regis...
 Information	7/11/2019 11:36:29 AM	Sysmon	12	Registry object added or deleted (rule: Regis...
 Information	7/11/2019 11:36:29 AM	Sysmon	13	Registry value set (rule: RegistryEvent)
 Information	7/11/2019 11:36:29 AM	Sysmon	13	Registry value set (rule: RegistryEvent)
 Information	7/11/2019 11:36:29 AM	Sysmon	10	Process accessed (rule: ProcessAccess)
 Information	7/11/2019 11:36:29 AM	Sysmon	10	Process accessed (rule: ProcessAccess)
 Information	7/11/2019 11:36:27 AM	Sysmon	10	Process accessed (rule: ProcessAccess)
 Information	7/11/2019 11:36:27 AM	Sysmon	10	Process accessed (rule: ProcessAccess)
 Information	7/11/2019 11:36:27 AM	Sysmon	10	Process accessed (rule: ProcessAccess)
 Information	7/11/2019 11:36:27 AM	Sysmon	10	Process accessed (rule: ProcessAccess)
 Information	7/11/2019 11:36:27 AM	Sysmon	10	Process accessed (rule: ProcessAccess)
 Information	7/11/2019 11:36:27 AM	Sysmon	10	Process accessed (rule: ProcessAccess)
 Information	7/11/2019 11:36:27 AM	Sysmon	10	Process accessed (rule: ProcessAccess)
 Information	7/11/2019 11:36:27 AM	Sysmon	10	Process accessed (rule: ProcessAccess)
 Information	7/11/2019 11:36:27 AM	Sysmon	10	Process accessed (rule: ProcessAccess)
 Information	7/11/2019 11:36:27 AM	Sysmon	10	Process accessed (rule: ProcessAccess)
 Information	7/11/2019 11:36:27 AM	Sysmon	10	Process accessed (rule: ProcessAccess)

Log Analysis with SIEM

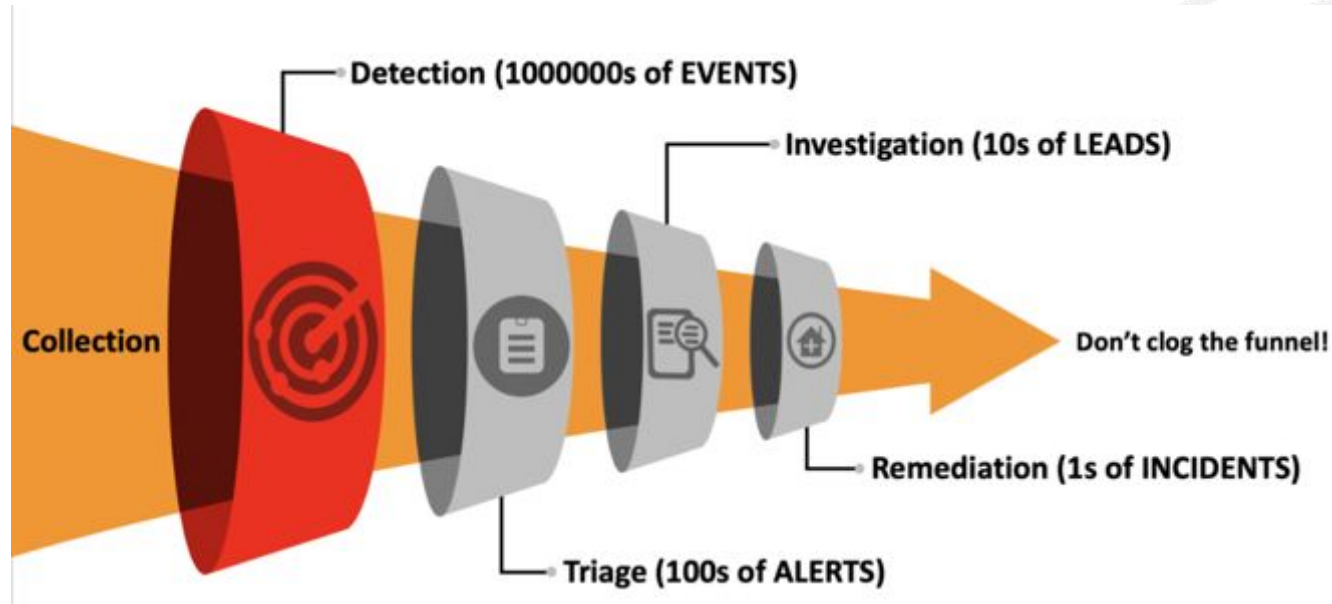
- Security Information and Event Management (SIEM) solution is the system that aggregates and monitors logs.
- Analyze data and form relationships which aid in finding anomalies, security gaps and incidents.
- Traditional SIEMs would use two techniques to generate alerts from log data: correlation rules and vulnerabilities and risk assessment.
 - Correlation rules specified an order of events that pointed to an anomaly, representing an attack or incident.
 - Vulnerabilities and risk assessment involve scanning networks for known vulnerabilities. These traditional techniques draw many false positives and are not efficient detecting new event types.

Log Analysis with SIEM (cont.)

- Modern SIEM utilizes machine learning to look at patterns and establish baselines, identify suspicious/anomalous activities. These techniques take the lead over the traditional ones as they can detect newer event types and threats.

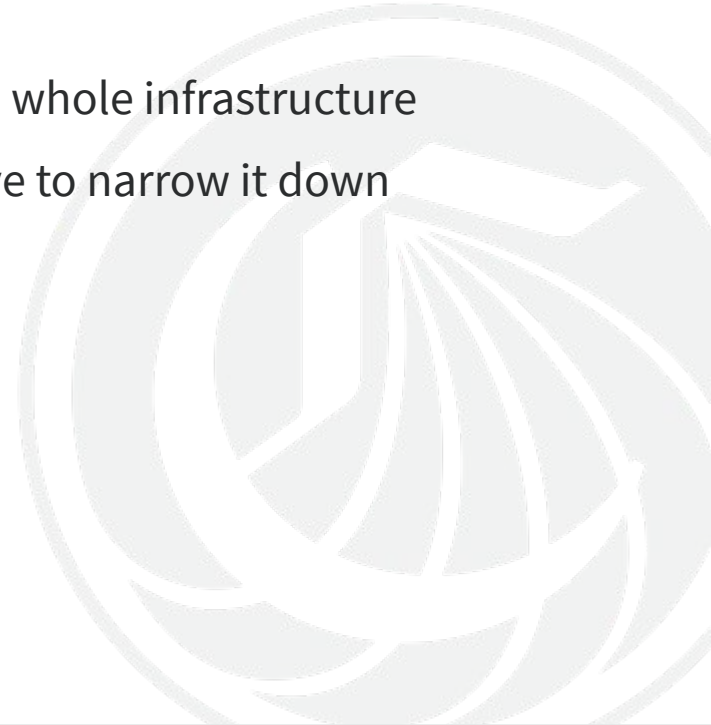


Funnel of Fidelity



Collection

- Events generated should give insight into activity of the whole infrastructure
- Data should be high quality, which is why it is imperative to narrow it down
- Data quality measured by:
 - Accuracy
 - Completeness
 - Consistency
 - Timeliness
 - Validity



Collection: Push vs. Pull

- Two methods of collecting data:
 - Push – software on the endpoint forwards data as it occurs
 - Must be installed on all monitored endpoints
 - Expensive
 - Pull – query the endpoint at the time of collection for data
 - Permanent install is not needed
 - Collects data at the point of query
- Many threat hunting strategies combine both pull and push

Detection

- Rooted in the analysis of centralized data
- Focus is to detect anomalous/malicious activity instead of detecting a method or tool
 - Ex. Detecting processes related to or accessing “SolarWinds.exe” instead of just detecting “SolarWinds.exe”
- Reduce noise in data to produce alerts in the next phase

Triage

- In this phase, this question comes up: Is this benign or malicious?
- Consumption of alerts from the Collection and Detection phases
 - Use of Additional sources
- Conclusions: **Benign, Suspicious, Malicious**
 - **Benign** - Known to be good
 - Tune detection
 - **Suspicious** – Known to be neither good nor bad
 - Passed to investigation
 - **Malicious** – Known to be bad
 - Passed to response phase

Investigation

- Gather additional data that is not available for centralization, or hard to collect at scale
 - Memory
 - Malware
 - Network
 - File System Collection & Analysis
- Determine if the event constitutes a security incident requiring response

Remediation

- Determining scope of incident
 - Category of incident
 - How many systems involved
 - Impact
- Actions taken to eradicate the malicious entity from the network
- Post Incident breakdown for future reference
 - Detection/Prevention at an earlier phase
 - Improve response time

Introduction to Threat Hunting

- Actively searching for malicious activity in the environment that has evaded current in place defenses
- Rooted in the assume breach mentality
- Focus on post-exploitation mentality
 - Many in place defenses focus on preventing/detecting the initial attack
 - Firewalls
 - Anti-Virus
 - Intrusion Detection/Prevention Systems
- End goal is to stop attacker before objective is achieved, not just at code execution

Traditional Security vs. Threat Hunting

- Traditional Security
 - Guard at front desk
 - Reliant on set controls
- Threat Hunting
 - Roving Security Guard
 - Actively searching for threats



Threat Hunt Campaign Types

- Where do we start?
- What techniques to use?
- Adopting multiple hunt campaign types can assist with selection of techniques to be hunted for

Threat Hunt Campaign: Data Driven

- Determine what to hunt for by looking at the data available
- Begin with a hypothesis based on data observations
- Example:
 - Identify the Windows Event IDs being collected in the environment.
 - What types of techniques do they allow you to detect?
 - Identifying the types of data sources available, mapping data sources to techniques using a framework like ATT&CK.

Threat Hunt Campaign: Intel Driven

- Threat hunting based on information gathered through threat intelligence channels
- Can be difficult to parse through information and apply to organization
- Example:
 - Threat intelligence has identified that APT29 is targeting the organization, the focus of campaign is around techniques that they know ATP29 likes to use.
 - Internal Threat Intel team identifies and tracks the types of initial access techniques used in recent phishing campaigns. Threat hunters focus their campaign around detecting those techniques.

Threat Hunt Campaign: Entity Driven

- Design hunts focusing on high risk/high value entities
- Focus on critical systems, intellectual property resources, and network infrastructure
- Requires identification of what is considered high value
- Threat may consider a target high value if it can be used as a means to an end
- Example:
 - Threat hunters are assigned to specifically monitor systems belonging to high value individuals
 - Threat hunters know that a specific file on a s specific system contains trade secrets which needs additional monitoring

Threat Hunt Campaign: TTP Driven

- Focus on TTPs in general rather than attacks against specific system
- Requires understanding of how a threat operates and uses TTPs
- Instead of searching critical systems for evidence, a hunter can search a large amount of systems for evidence of a specific TTP
- Example:
 - Hunting for credential access via powershell
 - Hunt team focuses on persistence, modification of an existing service via reg.exe