Threat Hunting with Splunk

-by Vinay Gujar & Ronak Bhatt

Outline

- Threat Hunting
- ATT&CK Framework
- Splunk

Threat Hunting

- Threat hunting is, quite simply, the pursuit of abnormal activity on servers and endpoints that may be signs of compromise, intrusion, or exfiltration of data.
- With threat hunting, you use humans to go “find stuff” versus waiting for technology to alert you.
- We look for anomalies — things that don’t usually happen.

What to look for?

- **Processes:** Hunters are looking for processes with certain names, file paths, checksums, and network activity.
- **Binaries:** Here hunters look for binaries with certain checksums, file names, paths, metadata, specific registry modifications, and many other characteristics.
- **Network activity:** This threat attribute includes network activity to specific domain names and IP addresses.
- **Configuration modifications:** Hunters can look for specific configuration additions and modifications.

MITRE ATT&CK Framework

- ATT&CK provides the most comprehensive model of modern attacker behavior.
- Tactics represent the “why” of an ATT&CK technique. The tactic is the adversary’s tactical objective for performing an action.
- Techniques represent “how” an adversary achieves a tactical objective by performing an action.
- The framework binds the “why “ and “how” of the threats to create a matrix .

How ATT&CK framework works?

- Each tactic has a UID which can be traced back in the matrix
- Threat hunting is performed using this matrix of framework
- ATT&CK specifics of what to hunt for in different threat conditions
    - Initial access
    - Execution
    - Persistence
    - Privilege escalation
    - Defense evasion
    - Credential access etc.

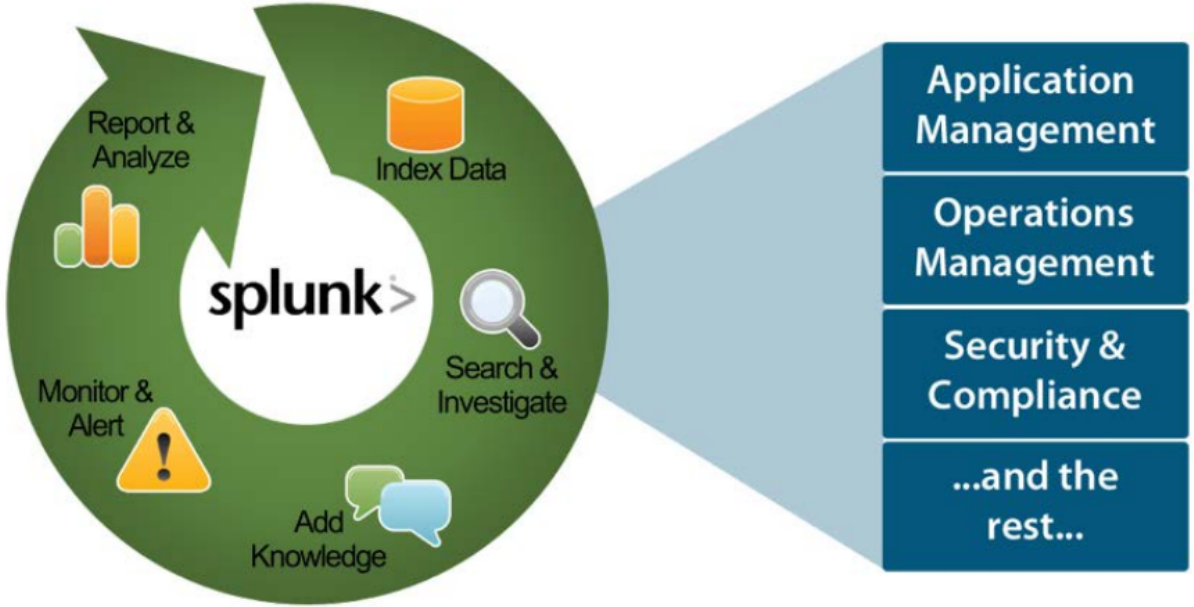
ATT&CK tactics and techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items	9 items	14 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking		DLL Search Order Hijacking	Password Filter DLL	System Information Discovery			Remote Access Tools		
	Regsvcs/Regasm	External Remote Services		DLL Side-Loading	Private Keys	System Network Configuration Discovery			Remote File Copy		
	Regsvr32			Execution Guardrails	Securityd Memory	System Network					
	Rundll32			Exploitation for Defense Evasion	Two-Factor						
				Extra Window Memory Injection							

Splunk

- Analyzes the aggregate of logs from a big service cluster
- Finds real-time logs and with faster speed
- Generates report and alerts for the desired search
- Provides enhanced GUI and real-time visibility in dashboard in various formats
- Provides quick results by reducing the time to troubleshoot and resolve issues
- Works like a monitoring, reporting and analysis tool and provides insights

What is Splunk?



Aggregate, analyze, and get answers from your machine data

What Splunk can collect?

Index **ANY** data from **ANY** source

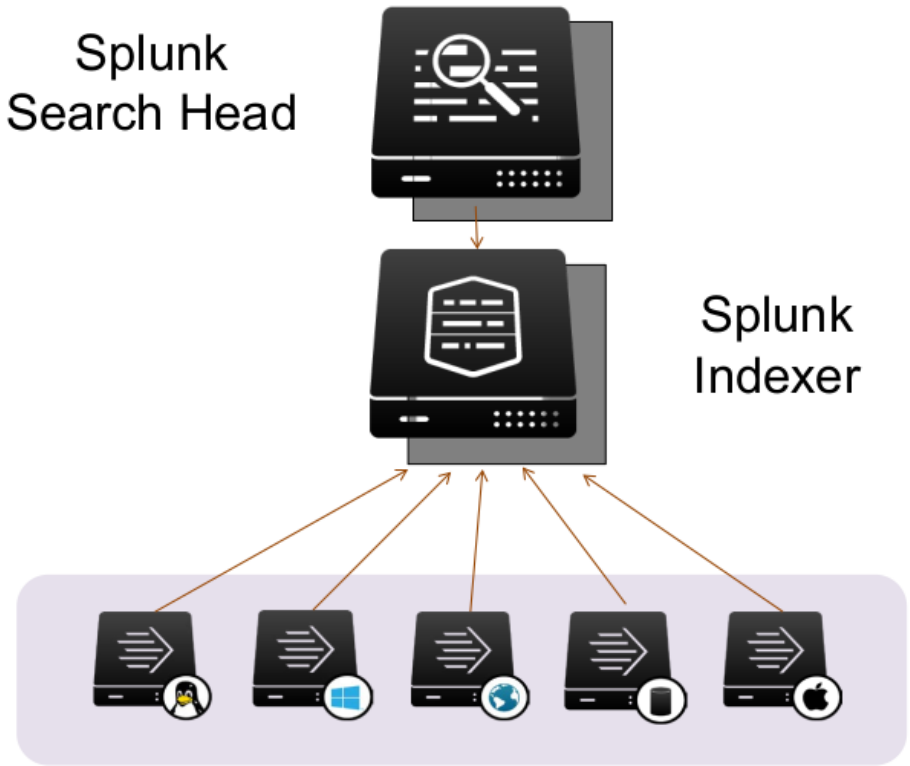
- Computers
- Network devices
- Virtual machines
- Internet devices
- Communication devices
- Sensors
- Databases

- Logs
- Configurations
- Messages
- Call detail records
- Clickstream
- Alerts
- Metrics
- Scripts
- Changes
- Tickets

Note

For **lots** of ideas on data to collect in your environment, get

How Splunk works?



How Is Splunk deployed?

- Splunk Enterprise

  Splunk components installed and administered on-premises

- Splunk Cloud
  - Splunk Enterprise as a scalable service
  - No infrastructure required

- Splunk Light

  Solution for small IT environments

What are Splunk Apps?

- Designed to address a wide variety of use cases and to extend the power of Splunk
- Collections of files containing data inputs, UI elements, and/or knowledge objects
- Allows multiple workspaces for different use cases/user roles to co-exist on a single Splunk instance
- 1000+ ready-made apps available on Splunkbase (splunkbase.com) or admins can build their own

What are Splunk Enhanced Solutions?

- **Splunk IT Service Intelligence (ITSI)**

– Next generation monitoring and analytics solution for IT Ops

– Uses machine learning and event analytics to simplify operations and prioritize problem resolution

- **Splunk Enterprise Security (ES)**

– Comprehensive Security Information and Event Management (SIEM) solution

– Quickly detect and respond to internal and external attacks

- **Splunk User Behavior Analytics (UBA)**

– Finds known, unknown, and hidden threats by analyzing user behavior and flagging unusual activity

Live Demo