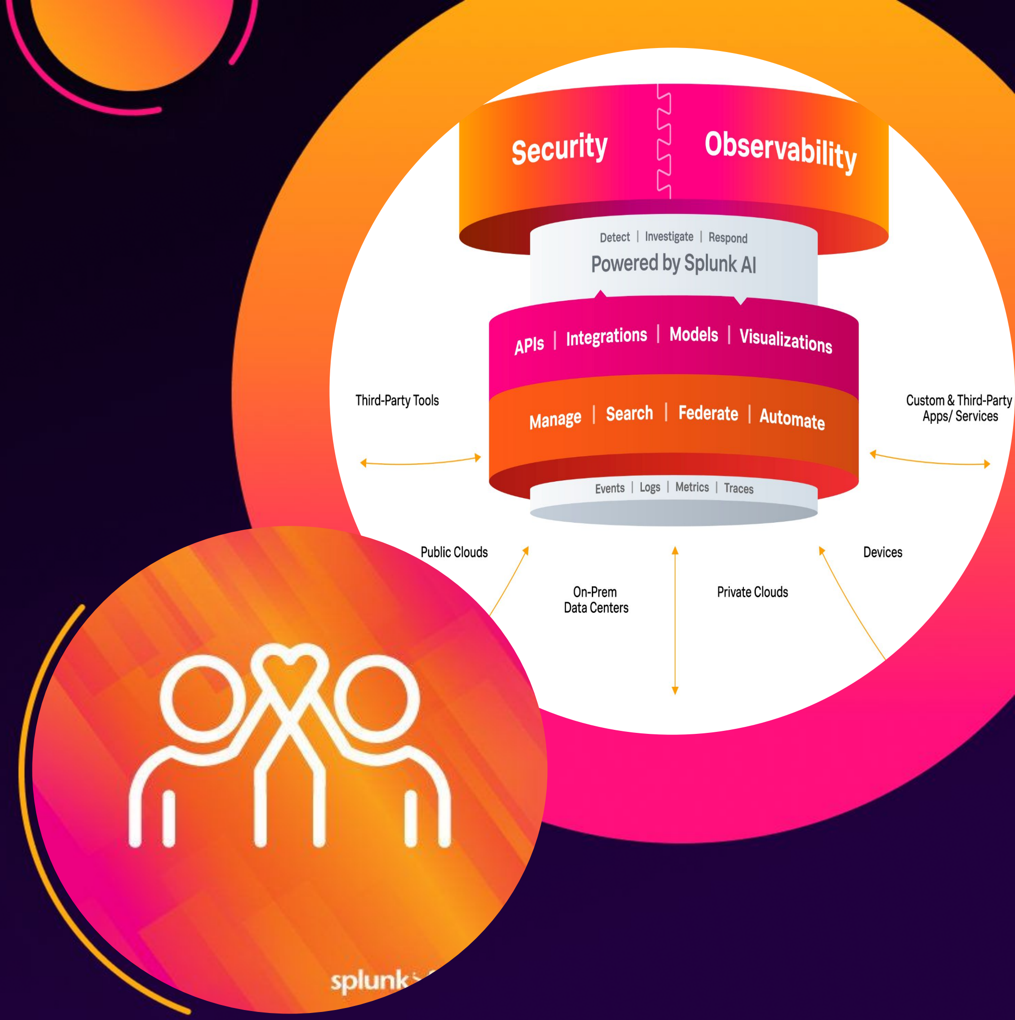
Nonprofit Splunkbase App and why do they matter?

Splunkbase Apps are free to nonprofit Splunk Users. There are significant applications that provide user interfaces that allow you to work with your data. This means that users can have more visibility and the opportunity to monitor their data in one central location.

Can you guess the top apps downloaded by nonprofits?

Our team has listed the most common Apps used by your peers in the slides provided below. *(Go to the last slide to find the answer)*

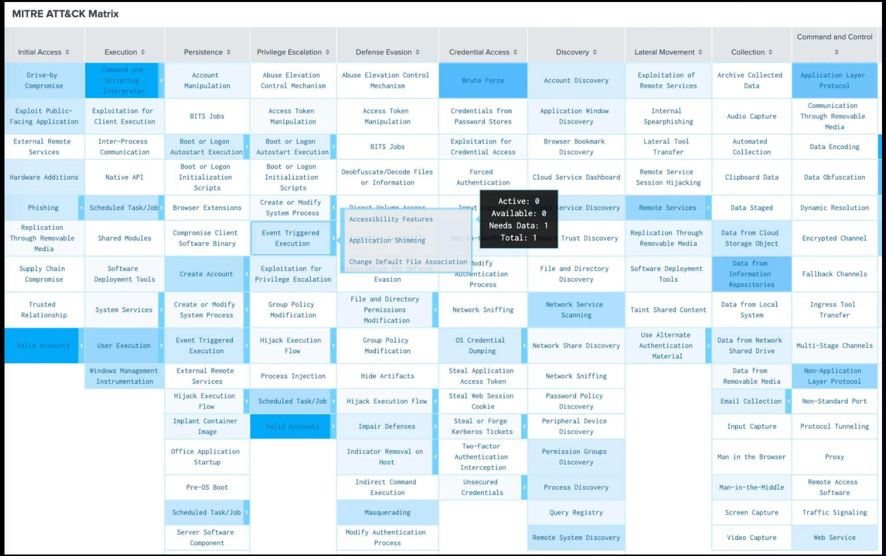


Security
Observability
Detect | Investigate | Respond
Powered by Splunk AI
APIs | Integrations | Models | Visualizations
Manage | Search | Federate | Automate
Events | Logs | Metrics | Traces
Third-Party Tools
Custom & Third-Party Apps/ Services
Public Clouds
On-Prem Data Centers
Private Clouds
Devices

SECURITY APPS

Splunk Security Essentials

https://splunkbase.splunk.com/app/3435



MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media
External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding
Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation
Phishing	Scheduled Task/Job	Browser Extensions	Create or Modify System Process	Direct Volume Access	Input Capture	Cloud Service Discovery	Remote Services	Data Staged	Dynamic Resolution
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution	Execution Guardrails	Man-in-the-Middle	Domain Trust Discovery	Replication Through Removable Media	Data from Cloud Storage Object	Encrypted Channel
Supply Chain Compromise	Software Deployment Tools	Create Account	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process	File and Directory Discovery	Software Deployment Tools	Data from Information Repositories	Fallback Channels
Trusted Relationship	System Services	Create or Modify System Process	Group Policy Modification	File and Directory Permissions Modification	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Local System	Ingress Tool Transfer
Valid Accounts	User Execution	Event Triggered Execution	Hijack Execution Flow	Group Policy Modification	OS Credential Dumping	Network Share Discovery	Use Alternate Authentication Material	Data from Network Shared Drive	Multi-Stage Channels
	Windows Management Instrumentation	External Remote Services	Process Injection	Hide Artifacts	Steal Application Access Token	Network Sniffing		Data from Removable Media	Non-Application Layer Protocol
		Hijack Execution Flow	Scheduled Task/Job	Hijack Execution Flow	Steal Web Session Cookie	Password Policy Discovery		Email Collection	Non-Standard Port
		Implant Container Image	Valid Accounts	Impair Defenses	Steal or Forge Kerberos Tickets	Peripheral Device Discovery		Input Capture	Protocol Tunneling
		Office Application Startup		Indicator Removal on Host	Two-Factor Authentication Interception	Permission Groups Discovery		Man in the Browser	Proxy
		Pre-OS Boot		Indirect Command Execution	Unsecured Credentials	Process Discovery		Man-in-the-Middle	Remote Access Software
		Scheduled Task/Job		Masquerading		Query Registry		Screen Capture	Traffic Signaling
		Server Software Component		Modify Authentication Process		Remote System Discovery		Video Capture	Web Service

Accessibility Features

Application Shimming

Change Default File Association

Active: 0
Available: 0
Needs Data: 1
Total: 1

What does this app offer?

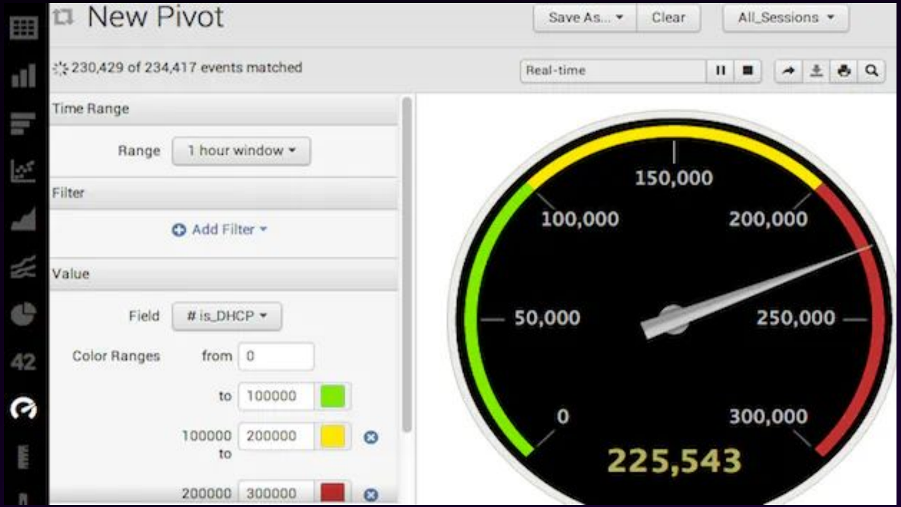
Splunk Security Essentials is a massive collection of security detection use cases to jump start your security journey with Splunk. Why start from scratch when you can stand on the shoulders of giants? This collection is masterfully curated on multiple dimensions including the MITRE ATT&CK framework, data sources involved, and stage of security maturity.

Why Does it Matter?

- Quickly operationalize high value detections with less work.
- Get the most from the data you collect by filtering on those data sources.
- Fuel your ideas for new detections and new data you may not have considered.
- Maximize your investment in the platform through quick adoption.

Splunk Common Information Model (CIM)

https://splunkbase.splunk.com/app/1621



230,429 of 234,417 events matched

Real-time

Time Range

Range: 1 hour window

Filter

Value

Field: # is_DHCP

Color Ranges: from 0 to 100000 🟩; 100000 to 200000 🟨; 200000 300000 🟥

225,543

What Does this App Offer?

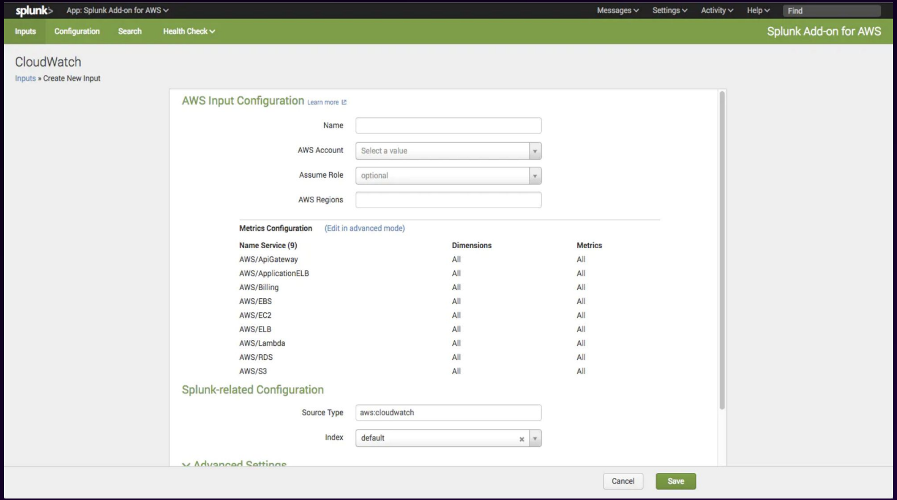
The Common Information Model is a set of field names and tags which are expected to define the least common denominator of a domain of interest. It is implemented as documentation on the Splunk docs website and JSON data model files in this add-on. Use the CIM add-on when modeling data or building apps to ensure compatibility between apps, or to just take advantage of these data models to pivot and report.

Why Does it Matter?

- The CIM helps you to normalize your data to match a common standard, using the same field names and event tags for equivalent events from different sources or vendors.
- The CIM acts as a search-time schema ("schema-on-the-fly") to allow you to define relationships in the event data while leaving the raw machine data intact.
- After you have normalized the data from multiple different source types, you can develop reports, correlation searches, and dashboards to present a unified view of a data domain. You can display your normalized data in the dashboards provided by other Splunk applications such as Splunk Enterprise Security and the Splunk App for PCI Compliance. The dashboards and other reporting tools in apps that support CIM compliance display only the data that is normalized to the tags and fields defined by the Common Information Model.

Splunk Add-on for Amazon Web Services (AWS)

https://splunkbase.splunk.com/app/1876



CloudWatch

Inputs » Create New Input

AWS Input Configuration

Name	
AWS Account	Select a value
Assume Role	optional
AWS Regions	

Metrics Configuration (Edit in advanced mode)

Name Service (9)	Dimensions	Metrics
AWS/ApiGateway	All	All
AWS/ApplicationELB	All	All
AWS/Billing	All	All
AWS/EBS	All	All
AWS/EC2	All	All
AWS/ELB	All	All
AWS/Lambda	All	All
AWS/RDS	All	All
AWS/S3	All	All

Splunk-related Configuration

Source Type	aws:cloudwatch
Index	default

Advanced Settings

What Does this App Offer?

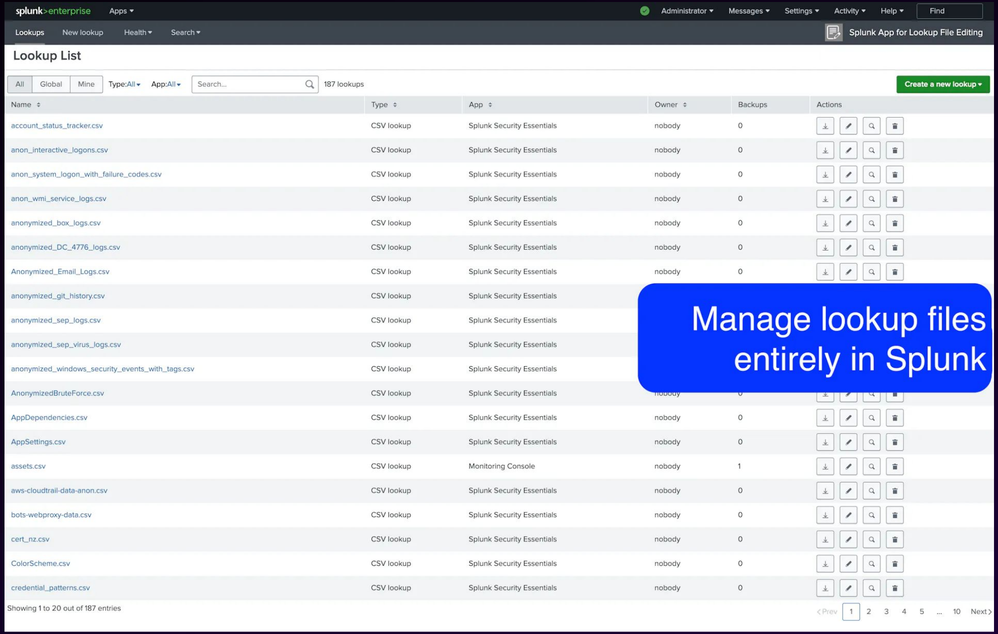
The Splunk Add-on for Amazon Web Services (AWS) allows a Splunk software administrator to collect performance, billing, raw or JSON, and IT and security data on AWS products using either a push-based (Amazon Kinesis Firehose) or Pull-based (API) collection method.

Why Does it Matter?

- Gain Insights into the cost of AWS usage
- Audit your AWS account by sending CloudTrail log data into Splunk
- Gain insights into your IT and Security environments by sending performance data and security logs to Splunk.
- Help power your Splunk Enterprise Security, and Splunk IT Service Intelligence by providing modular inputs and CIM compatible knowledge.

Splunk App for Lookup File Editing

https://splunkbase.splunk.com/app/1724



Lookup List

187 lookups

Name	Type	App	Owner	Backups	Actions
account_status_tracker.csv	CSV lookup	Splunk Security Essentials	nobody	0	⤓ ✎ 🔍 🗑
anon_interactive_logons.csv	CSV lookup	Splunk Security Essentials	nobody	0	⤓ ✎ 🔍 🗑
anon_system_logon_with_failure_codes.csv	CSV lookup	Splunk Security Essentials	nobody	0	⤓ ✎ 🔍 🗑
anon_wmi_service_logs.csv	CSV lookup	Splunk Security Essentials	nobody	0	⤓ ✎ 🔍 🗑
anonymized_box_logs.csv	CSV lookup	Splunk Security Essentials	nobody	0	⤓ ✎ 🔍 🗑
anonymized_DC_4776_logs.csv	CSV lookup	Splunk Security Essentials	nobody	0	⤓ ✎ 🔍 🗑
Anonymized_Email_Logs.csv	CSV lookup	Splunk Security Essentials	nobody	0	⤓ ✎ 🔍 🗑
anonymized_git_history.csv	CSV lookup	Splunk Security Essentials			
anonymized_sep_logs.csv	CSV lookup	Splunk Security Essentials			
anonymized_sep_virus_logs.csv	CSV lookup	Splunk Security Essentials			
anonymized_windows_security_events_with_tags.csv	CSV lookup	Splunk Security Essentials			
AnonymizedBruteForce.csv	CSV lookup	Splunk Security Essentials	nobody	0	
AppDependencies.csv	CSV lookup	Splunk Security Essentials	nobody	0	⤓ ✎ 🔍 🗑
AppSettings.csv	CSV lookup	Splunk Security Essentials	nobody	0	⤓ ✎ 🔍 🗑
assets.csv	CSV lookup	Monitoring Console	nobody	1	⤓ ✎ 🔍 🗑
aws-cloudtrail-data-anon.csv	CSV lookup	Splunk Security Essentials	nobody	0	⤓ ✎ 🔍 🗑
bots-webproxy-data.csv	CSV lookup	Splunk Security Essentials	nobody	0	⤓ ✎ 🔍 🗑
cert_nz.csv	CSV lookup	Splunk Security Essentials	nobody	0	⤓ ✎ 🔍 🗑
ColorScheme.csv	CSV lookup	Splunk Security Essentials	nobody	0	⤓ ✎ 🔍 🗑
credential_patterns.csv	CSV lookup	Splunk Security Essentials	nobody	0	⤓ ✎ 🔍 🗑

Showing 1 to 20 out of 187 entries

Manage lookup files entirely in Splunk

What Does this App Offer?

Ever want to edit a lookup within Splunk with a user interface? Now you can. This app provides an Excel-like interface for editing, importing, and exporting lookup files (KV store and CSV-based). This app also makes your lookups work in Search Head Clustered environments (edits to lookups will be propagated to other search heads). Revision history is maintained for lookups so that you can view or restore older lookups quickly in the interface.

Why Does it Matter?

Use the Splunk App for Lookup File Editing to add and edit lookup files within the Splunk platform. Using the app, you can edit, import, and export both KV store and CSV file lookups in an interface similar to Microsoft Excel.

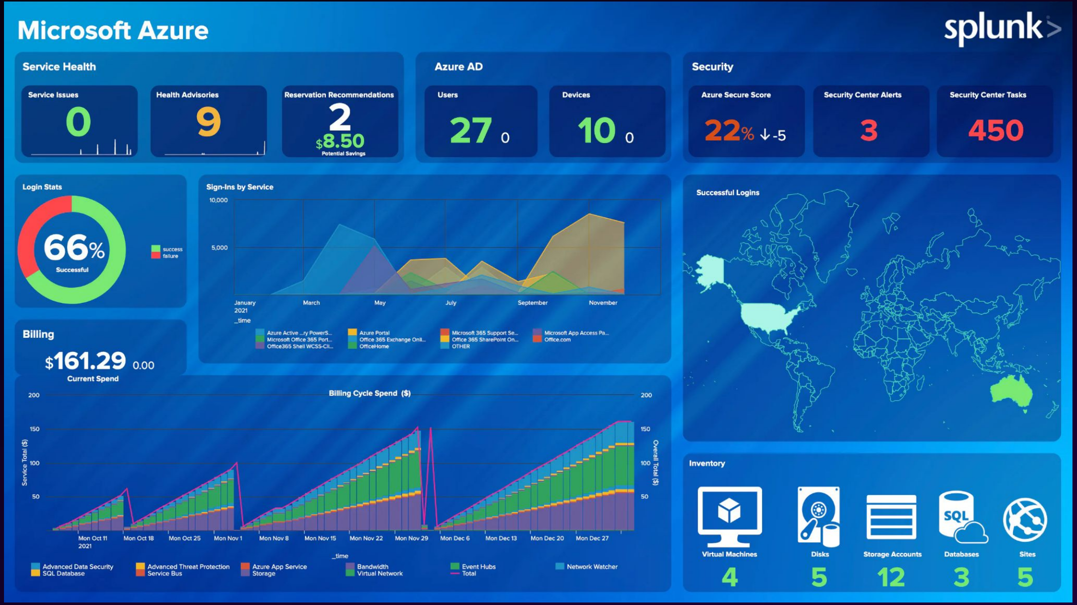
With the Splunk App for Lookup File Editing, you can do the following:

- Manage lookup files from within the Splunk platform
- Import CSV files into a lookup
- Import KV store data into a lookup
- Edit lookups within a GUI similar to Microsoft Excel
- Save a backup of a lookup and set a total backup size limit
- View or restore lookups using revision history

With the Splunk App for Lookup File Editing, you can also work with lookup files in search head cluster environments. Any edits you make to lookups propagate to your other search heads.

Splunk Add-On for Microsoft Azure

https://splunkbase.splunk.com/app/3757



What Does this App Offer?

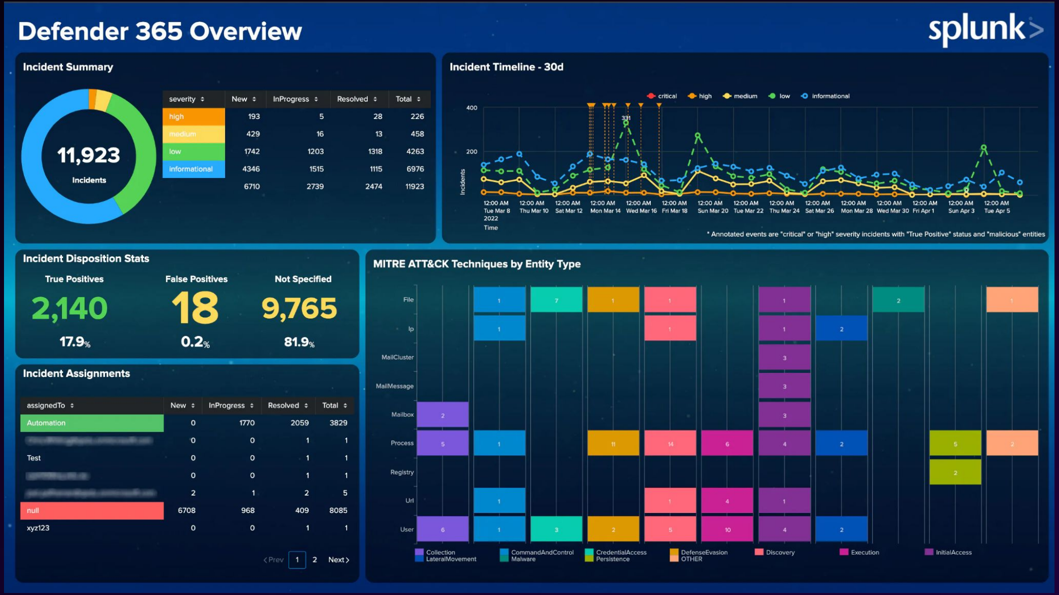
This add-on collects data from Microsoft Azure including the following: Azure AD Data - Users - Azure AD user data - Interactive Sign-ins - Azure AD sign-ins including conditional access policies and MFA - Directory audits - Azure AD directory changes including old and new values - Devices - Registered devices in Azure AD - Groups - Risk Detections Azure Log Analytics (KQL) Metrics Estimated billing and consumption - VM Reservation Recommendations Inventory metadata - Resource Groups - Resource group configuration - Virtual Machines - VM, Disk, Image, and Snapshot configurations - Virtual Networks - VNET, NSG, and Public IP configurations - Managed Disks - Subscriptions - Subscription name, ID, and type - Topology - IaaS relationships Azure Security Center - Alerts - Tasks Azure Resource Graph

Why Does it Matter?

- This add-on contains the following alert actions: - Stop Azure VM - stops an Azure Virtual Machine. - Add member to group - adds a user to a group. This can be useful if you need to enable additional policies like MFA based on search results. - Dismiss Azure Alert - dismisses an Azure Security Center alert.

AddOn+ Splunk Add-On for Microsoft Office 365

https://splunkbase.splunk.com/app/4055



Defender 365 Overview

splunk>

Incident Summary

11,923
Incidents

severity	New	InProgress	Resolved	Total
high	193	5	28	226
medium	429	16	13	458
low	1742	1203	1318	4263
informational	4346	1515	1115	6976
	6710	2739	2474	11923

Incident Timeline - 30d

* Annotated events are "critical" or "high" severity incidents with "True Positive" status and "malicious" entities

Incident Disposition Stats

True Positives	False Positives	Not Specified
2,140	18	9,765
17.9%	0.2%	81.9%

Incident Assignments

assignedTo	New	InProgress	Resolved	Total
Automation	0	1770	2059	3829
[redacted]	0	0	1	1
Test	0	0	1	1
[redacted]	0	0	1	1
[redacted]	2	1	2	5
null	6708	968	409	8085
xyz123	0	0	1	1

‹ Prev 1 2 Next ›

MITRE ATT&CK Techniques by Entity Type

What Does this App Offer?

The Splunk Add-on for Microsoft Office 365 allows a Splunk software administrator to pull service status, service messages, and management activity logs from the Office 365 Management API.

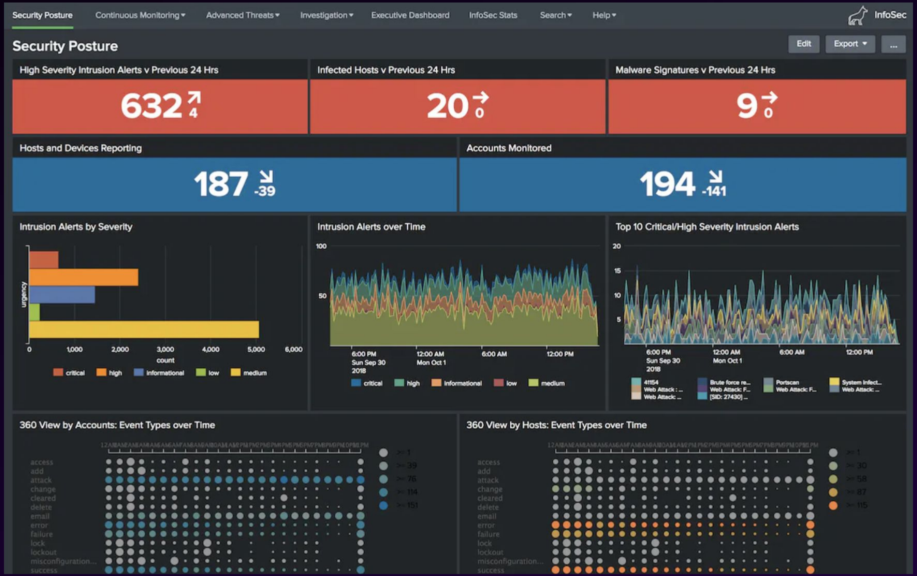
Why Does it Matter?

- * Audit logs for Azure Active Directory, Sharepoint Online, and Exchange Online, supported by the Office 365 Management API. * Historical and current service status, and service messages for the corresponding Microsoft Office 365 Management API. * Data Loss Prevention on Microsoft Office 365 Management API. After the Splunk platform indexes the events, you can then directly analyze the data or use it as a contextual data feed to correlate with other data in the Splunk platform

splunk>

InfoSec App for Splunk

https://splunkbase.splunk.com/app/4240



What Does this App Offer?

InfoSec app is designed to address the most common security use cases, including continuous monitoring and security investigations. InfoSec app also includes a number of advanced threat detection use cases.

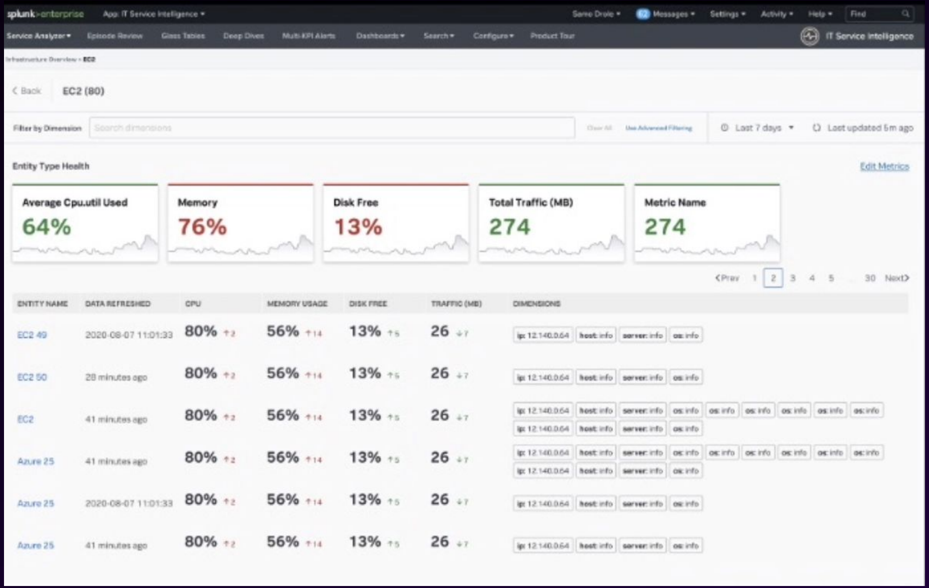
Why Does it Matter?

- Quickly operationalize high value detections with less work.
- 3 Data Sources:
  - **Firewall data** like Cisco ASA, Palo Alto Networks, Check Point, Juniper, Fortinet, etc.
  - **Active Directory security logs** (make sure that your audit policy enables logging failed and successful authentication attempts)
  - **Antivirus/Malware data** like McAfee, Symantec, Trend Micro, etc.

IT Apps

IT Essentials Work

https://splunkbase.splunk.com/app/5403



EC2 (80)

Filter by Dimension: Search dimensions

Last 7 days ▾ | Last updated 5m ago

Entity Type Health

Average Cpu.util Used	Memory	Disk Free	Total Traffic (MB)	Metric Name
64%	76%	13%	274	274

ENTITY NAME	DATA REFRESHED	CPU	MEMORY USAGE	DISK FREE	TRAFFIC (MB)	DIMENSIONS
EC2 49	2020-08-07 11:01:33	80% ↑2	56% ↑14	13% ↑5	26 ↓7	ip: 12.140.0.64 host: info server: info os: info
EC2 50	28 minutes ago	80% ↑2	56% ↑14	13% ↑5	26 ↓7	ip: 12.140.0.64 host: info server: info os: info
EC2	41 minutes ago	80% ↑2	56% ↑14	13% ↑5	26 ↓7	ip: 12.140.0.64 host: info server: info os: info os: info os: info os: info os: info os: info ip: 12.140.0.64 host: info server: info os: info
Azure 25	41 minutes ago	80% ↑2	56% ↑14	13% ↑5	26 ↓7	ip: 12.140.0.64 host: info server: info os: info os: info os: info os: info os: info os: info ip: 12.140.0.64 host: info server: info os: info
Azure 25	2020-08-07 11:01:33	80% ↑2	56% ↑14	13% ↑5	26 ↓7	ip: 12.140.0.64 host: info server: info os: info
Azure 25	41 minutes ago	80% ↑2	56% ↑14	13% ↑5	26 ↓7	ip: 12.140.0.64 host: info server: info os: info

What Does this App Offer?

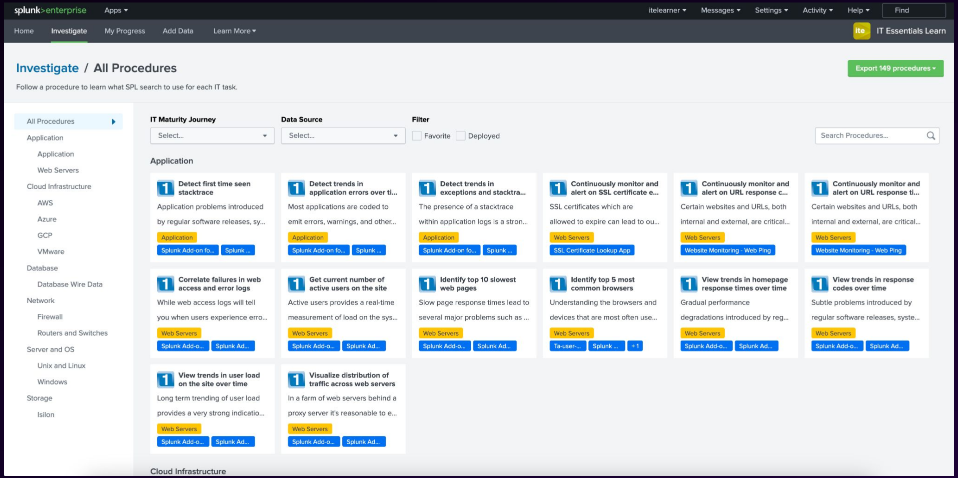
This is a free app that helps customers start monitoring and analyzing their IT infrastructure. ITE Work includes data integrations and investigation tools for operating systems, virtual infrastructures and containers.

Why Does it Matter?

- Helps observe and understand performance of infrastructure
- Automatically discover and bring in data in the form of entities
- Direct upgrade path to ITSI
    - “Feature flagged” version of ITSI

IT Essentials Learn

https://splunkbase.splunk.com/app/5390



Investigate / All Procedures

Follow a procedure to learn what SPL search to use for each IT task.

Application

Detect first time seen stacktrace
Application problems introduced by regular software releases, sy...
Application | Splunk Add-on fo... | Splunk ...

Detect trends in application errors over ti...
Most applications are coded to emit errors, warnings, and other...
Application | Splunk Add-on fo... | Splunk ...

Detect trends in exceptions and stacktra...
The presence of a stacktrace within application logs is a stron...
Application | Splunk Add-on fo... | Splunk ...

Continuously monitor and alert on SSL certificate e...
SSL certificates which are allowed to expire can lead to ou...
Web Servers | SSL Certificate Lookup App

Continuously monitor and alert on URL response c...
Certain websites and URLs, both internal and external, are critical...
Web Servers | Website Monitoring - Web Ping

Continuously monitor and alert on URL response ti...
Certain websites and URLs, both internal and external, are critical...
Web Servers | Website Monitoring - Web Ping

Correlate failures in web access and error logs
While web access logs will tell you when users experience erro...
Web Servers | Splunk Add-o... | Splunk Ad...

Get current number of active users on the site
Active users provides a real-time measurement of load on the sys...
Web Servers | Splunk Add-o... | Splunk Ad...

Identify top 10 slowest web pages
Slow page response times lead to several major problems such as ...
Web Servers | Splunk Add-o... | Splunk Ad...

Identify top 5 most common browsers
Understanding the browsers and devices that are most often use...
Web Servers | Ta-user-... | Splunk ... | +1

View trends in homepage response times over time
Gradual performance degradations introduced by reg...
Web Servers | Splunk Add-o... | Splunk Ad...

View trends in response codes over time
Subtle problems introduced by regular software releases, syste...
Web Servers | Splunk Add-o... | Splunk Ad...

View trends in user load on the site over time
Long term trending of user load provides a very strong indicatio...
Web Servers | Splunk Add-o... | Splunk Ad...

Visualize distribution of traffic across web servers
In a farm of web servers behind a proxy server it's reasonable to e...
Web Servers | Splunk Add-o... | Splunk Ad...

Cloud Infrastructure

What Does this App Offer?

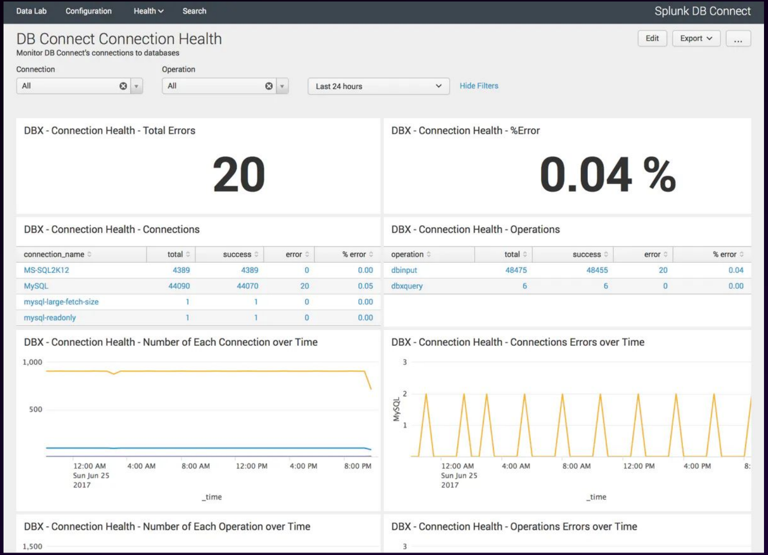
ITE Learn helps customers onboard and quickly gain value from IT monitoring use cases by providing curated, step-by-step guidance and a library of searches, dashboard templates, and recommended content based on their environment.

Why Does it Matter?

- Easy for customers to get started with IT use cases
- Prescriptive guidance to help data onboarding
- Can be curated based on IT maturity journey

Splunk DB Connect

https://splunkbase.splunk.com/app/2686



DB Connect Connection Health

Monitor DB Connect's connections to databases

Connection: All

Operation: All

Last 24 hours

DBX - Connection Health - Total Errors

20

DBX - Connection Health - %Error

0.04 %

DBX - Connection Health - Connections

connection_name	total	success	error	% error
MS-SQL2K12	4389	4389	0	0.00
MySQL	44090	44070	20	0.05
mysql-large-fetch-size	1	1	0	0.00
mysql-readonly	1	1	0	0.00

DBX - Connection Health - Operations

operation	total	success	error	% error
dbinput	48475	48455	20	0.04
dbxquery	6	6	0	0.00

DBX - Connection Health - Number of Each Connection over Time

DBX - Connection Health - Connections Errors over Time

DBX - Connection Health - Number of Each Operation over Time

DBX - Connection Health - Operations Errors over Time

What Does this App Offer?

Splunk DB Connect is a generic SQL database extension for Splunk that enables easy integration of database information with Splunk queries and reports. Splunk DB Connect supports DB2/Linux, Informix, MemSQL, MySQL, AWS Aurora, Microsoft SQL Server, Oracle, PostgreSQL, AWS RedShift, SAP SQL Anywhere, Sybase ASE, Sybase IQ, Teradata, InfluxDB and MongoDB Atlas. Use Splunk DB Connect's Inputs to import structured data for powerful indexing, analysis, and visualization. Use Outputs to export machine data insights to a legacy database to increase your organization's insight. Use Lookups to add meaningful information to your event data by referencing fields in an external database. Use query commands to build live dashboards mixing structured and unstructured data.

Why Does it Matter?

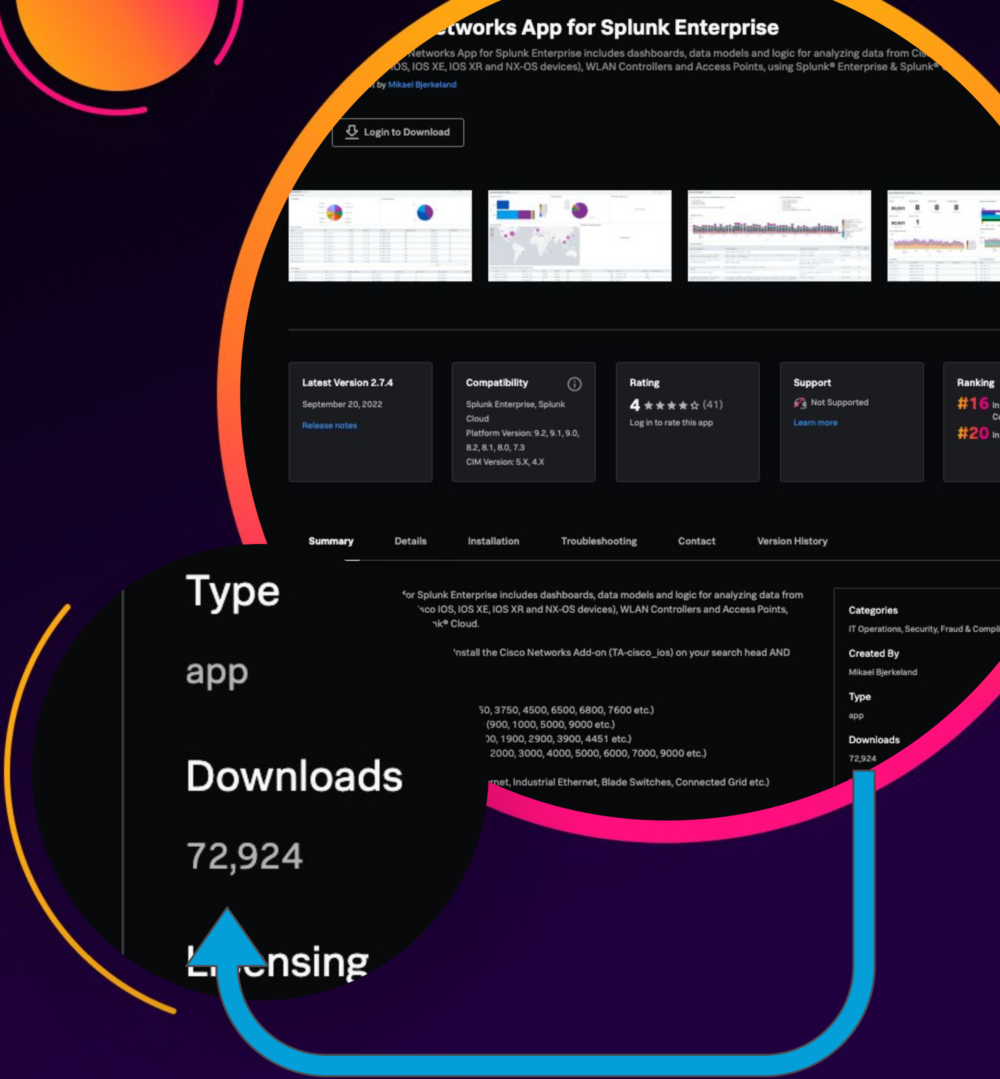
- Database import - Splunk DB Connect allows you to import tables, rows, and columns from a database directly into Splunk Enterprise, which indexes the data. You can then analyze and visualize that relational data from within Splunk Enterprise just as you would the rest of your Splunk Enterprise data.
- Database export - DB Connect also enables you to output data from Splunk Enterprise back to your relational database. You map the Splunk Enterprise fields to the database tables you want to write to.
- Database lookups - DB Connect also performs database lookups, which let you reference fields in an external database that match fields in your event data. Using these matches, you can add more meaningful information and searchable fields to enrich your event data.
- Database access - DB Connect also allows you to directly use SQL in your Splunk searches and dashboards. Using these commands, you can make useful mashups of structured data with machine data.

Cisco Networks App for Splunk

Splunkbase App

Analyze data from Cisco Switches & Routers (**Cisco IOS, IOS XE, IOS XR and NX-OS devices**), WLAN Controllers and Access Points, using Splunk® Enterprise & Splunk® Cloud.

- Cisco Catalyst series switches (2960, 3650, 3750, 4500, 6500, 6800, 7600 etc.)
- Cisco ASR - Aggregation Services Routers (900, 1000, 5000, 9000 etc.)
- Cisco ISR - Integrated Services Routers (800, 1900, 2900, 3900, 4451 etc.)
- Cisco Nexus Data Center switches (1000V, 2000, 3000, 4000, 5000, 6000, 7000, 9000 etc.)
- Cisco Carrier Routing System
- Other Cisco IOS based devices (Metro Ethernet, Industrial Ethernet, Blade Switches, Connected Grid etc.)
- Cisco Access Points
- Cisco WLC - WLAN Controller



etworks App for Splunk Enterprise

Networks App for Splunk Enterprise includes dashboards, data models and logic for analyzing data from Cis
IOS, IOS XE, IOS XR and NX-OS devices), WLAN Controllers and Access Points, using Splunk® Enterprise & Splunk®

by Mikael Bjerkeland

Login to Download

Latest Version 2.7.4
September 20, 2022
Release notes

Compatibility
Splunk Enterprise, Splunk Cloud
Platform Version: 9.2, 9.1, 9.0, 8.2, 8.1, 8.0, 7.3
CIM Version: 5.X, 4.X

Rating
4 ★★★★☆ (41)
Log in to rate this app

Support
Not Supported
Learn more

Ranking
#16 In
#20 In

for Splunk Enterprise includes dashboards, data models and logic for analyzing data from
sco IOS, IOS XE, IOS XR and NX-OS devices), WLAN Controllers and Access Points,
nk® Cloud.

nstall the Cisco Networks Add-on (TA-cisco_ios) on your search head AND

50, 3750, 4500, 6500, 6800, 7600 etc.)
(900, 1000, 5000, 9000 etc.)
00, 1900, 2900, 3900, 4451 etc.)
2000, 3000, 4000, 5000, 6000, 7000, 9000 etc.)
rnet, Industrial Ethernet, Blade Switches, Connected Grid etc.)

Categories
IT Operations, Security, Fraud & Compli

Created By
Mikael Bjerkeland

Type
app

Downloads
72,924

Type

app

Downloads

72,924

Licensing

Contact Adriana Erickson

Email: aerickson@splunk.com if your team needs technical details and support on how to utilize these free apps

Phone: 703-677-7405

Thank for staying to the end! Here are the answers:

1. Splunk Security Essential
2. Splunk Common Information Model (CIM)
3. Splunk Add-On for Amazon Web Services (AWS)
4. Splunk App for Lookup File Editing
5. Splunk Add-On for Microsoft Azure
6. Splunk Add-On for Microsoft Office 365
7. InfoSec App for Splunk
8. IT Essentials Work
9. IT Essentials Learn
10. Splunk DB Content