## Splunk

Enhancing security

**Sven Vande Cappelle** 

Presales consultant



### Forward-Looking Statements



This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2023 Splunk Inc. All rights reserved.





### **Sven Vande Cappelle**

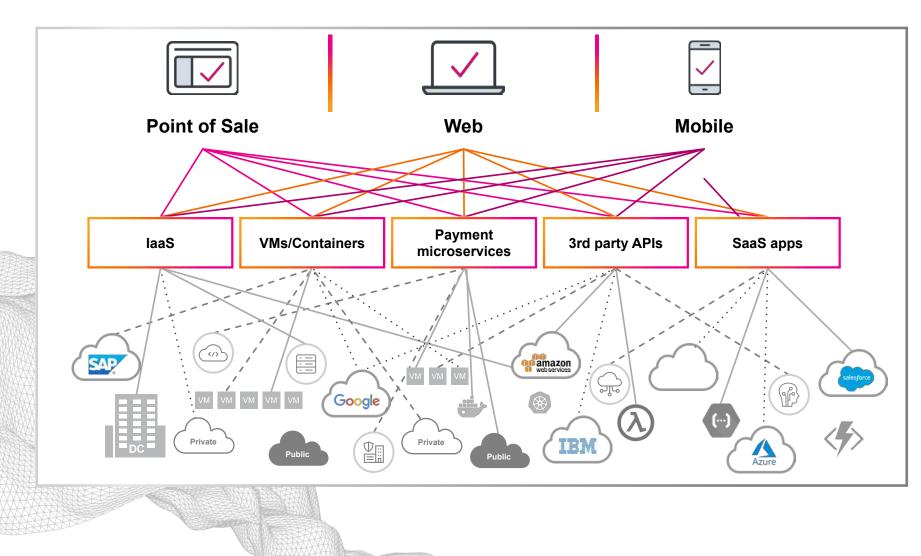
Presales consultant



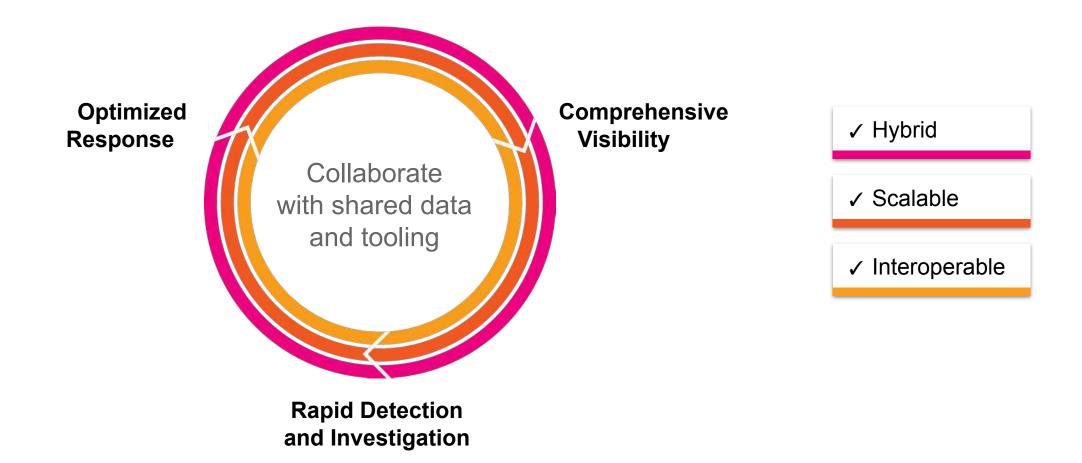
### How can we rethink our approach to keeping systems secure, reliable and performing?

# Build a foundation of **RESILIENCE**

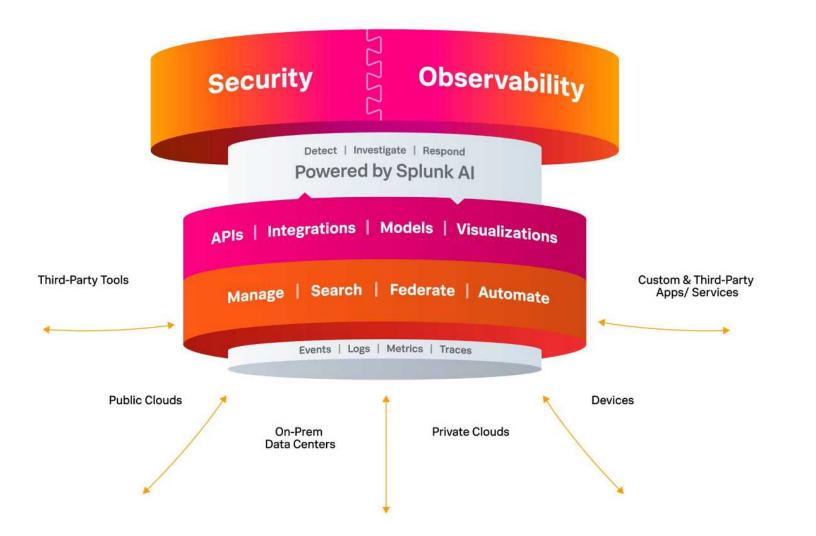
### Hybrid and Multi Cloud Systems Create Complexity



# Splunk enables faster detection, investigation and response



### The Unified Security and Observability Platform



#### **PLATFORM**

### Enable Unified Security and Observability

Monitor, investigate and respond rapidly at scale with comprehensive visibility and shared tooling. <complex-block><complex-block><complex-block>

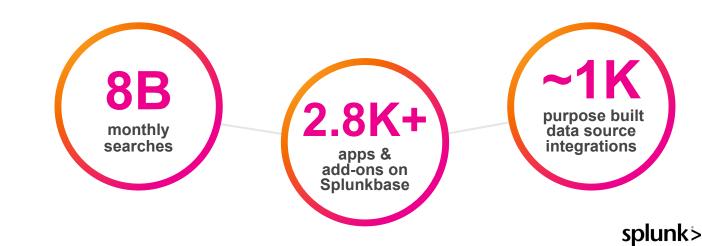
Streaming

**Machine learning** 

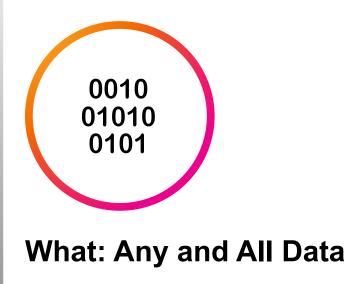
Scalable index

Search and visualization

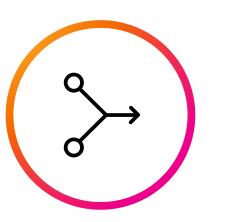
**Collaboration and orchestration** 



### Scalable Index



 Index Any and All streaming, machine, and historical data



#### How: Point it at a Source

 Point Splunk at a data source-tell it a bit about the source-that source becomes a data input

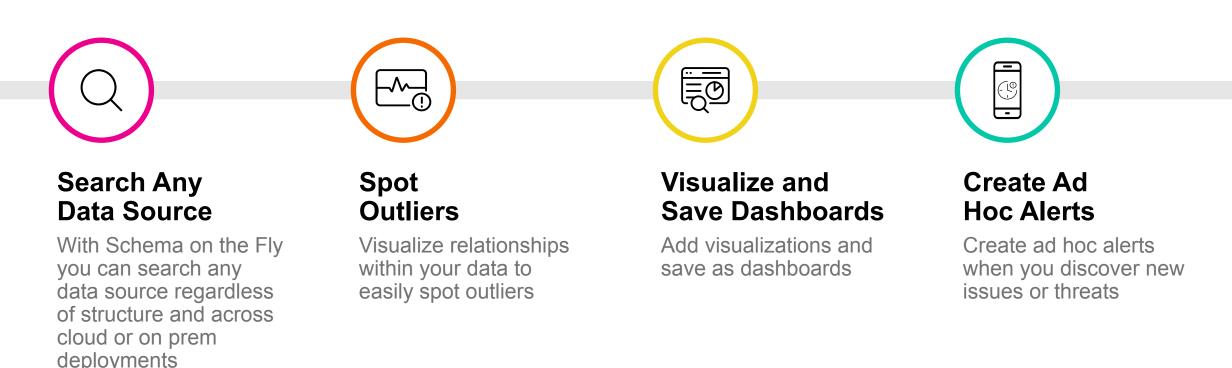


### Then: Turn Source into Stream of Events

 Splunk indexes the data stream and transforms it into a series of events-you can view and search those events right away

### **Search and Visualization**

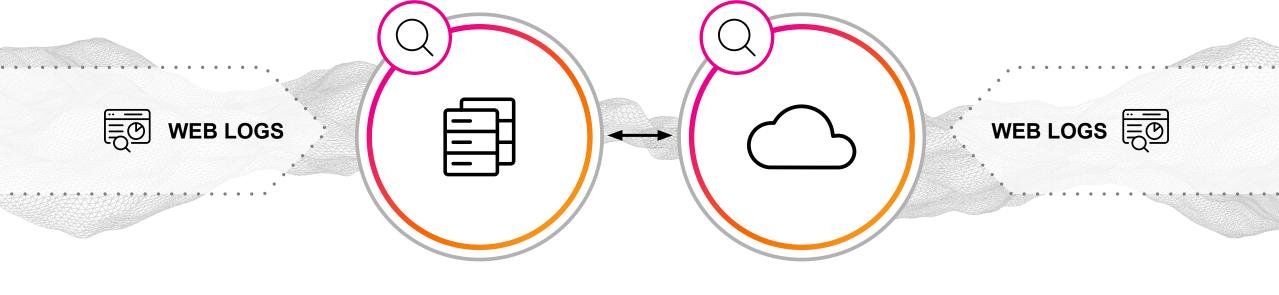
Use Search Process Language (SPL) to search and investigate your data across cloud or on prem deployments to find the needle in your haystack



### **Ubiquitous Machine Learning**

|                  | Turnkey   | Configurable  | Extensible   |
|------------------|---|---|--|
| Theme            | ML-powered Solutions: IT,<br>Security, Observability  | Extending use cases through streamlined ML application  | New frontier of use cases through DS development   |
| Splunk Solutions | <ul> <li>Enterprise Security</li> <li>User Behavioral Analytics</li> <li>Observability</li> <li>IT Service Intelligence (ITSI)</li> </ul> | <ul> <li>Machine Learning Toolkit (MLTK)</li> <li>Splunk app for Data Science and<br/>Deep Learning</li> </ul>              | <ul> <li>Machine Learning Toolkit (MLTK)</li> <li>Splunk App for Data Science and<br/>Deep Learning</li> </ul> |
| Examples         | <ul> <li>Anomaly Detection</li> <li>Adaptive Thresholding</li> <li>Predictive Insights</li> <li>Pipeline Drift Detection</li> </ul>       | <ul> <li>Outlier detection</li> <li>Forecast time series</li> <li>Predict fields</li> <li>Protect sensitive data</li> </ul> | <ul> <li>Fraud detection<br/>Predictive Maintenance</li> <li>Domain generated algorithms (DGA)</li> </ul>      |
| Target Users     | <ul> <li>Practitioners using embedded,<br/>low-touch ML</li> </ul>  | <ul> <li>Domain experts driving extended<br/>use cases</li> </ul>   | <ul> <li>Advanced data scientists building<br/>expansive custom use cases</li> </ul>                           |

# Search Across Environments with Federated Search



Splunk On-Prem Deployment Splunk Cloud Deployment

### Splunk Makes Data Accessible and Actionable From Anywhere

Extend Splunk beyond the desktop

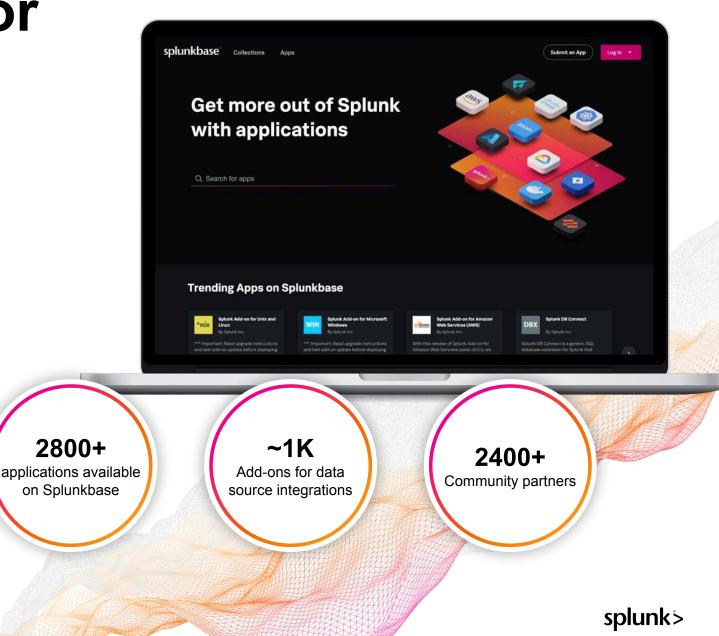


#### **Splunk Mobile**

#### **Splunk Augmented Reality (AR)**

# Access free apps, or build your own

- Build an essential security foundation and accelerate IT troubleshooting with free, high quality apps and add-ons to extend the power of your Splunk investment - and developer tooling to build your own!
- Access to the **2800+ solutions** from Splunk, partners, and the community
- Discover new tools for your use case with:
  - Collections Curated sets of top-rated apps for a variety of use cases and interests
  - App Directory Complete list of apps filterable by your specific needs



### **Unified Security and Observability Platform**

## **2M**<sup>+</sup>

Security threats blocked in 6 months

**99**%

Of threats are handled by automation

Affac.

## intel.

**100**%

Uptime despite 300% increase in traffic during Black Friday

Lenovo

## **1.5M<sup>+</sup> 96<sup>%</sup>**

COVID-19 tests administered and tracked with Splunk Cloud



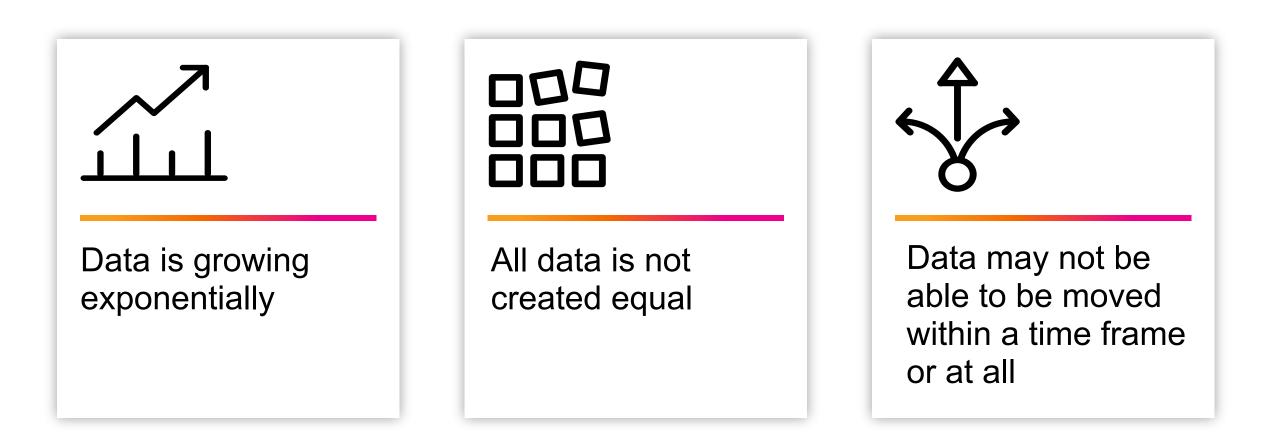
Faster application development powered by full-fidelity visibility



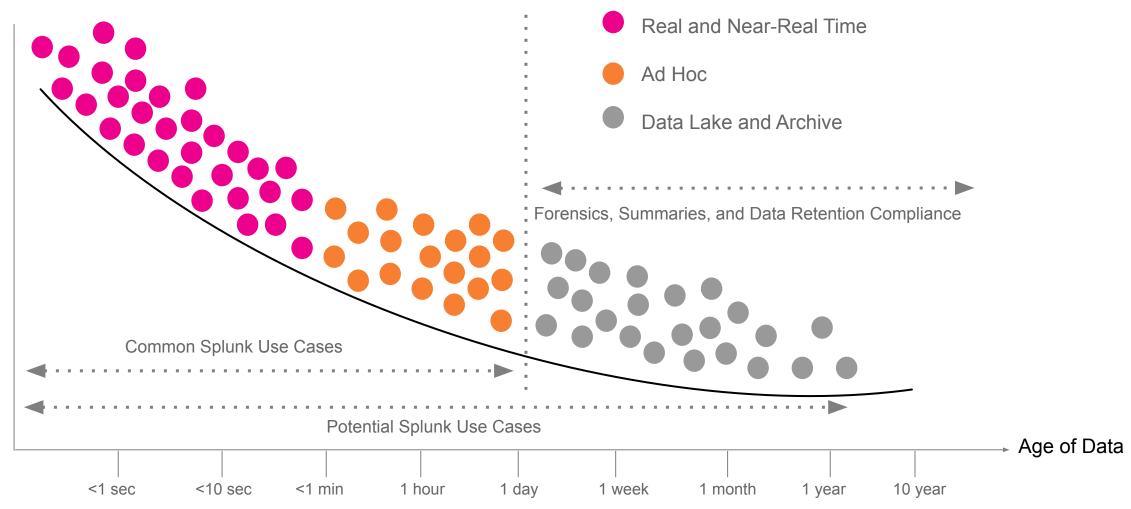


Data

## The World Of Data Is Changing

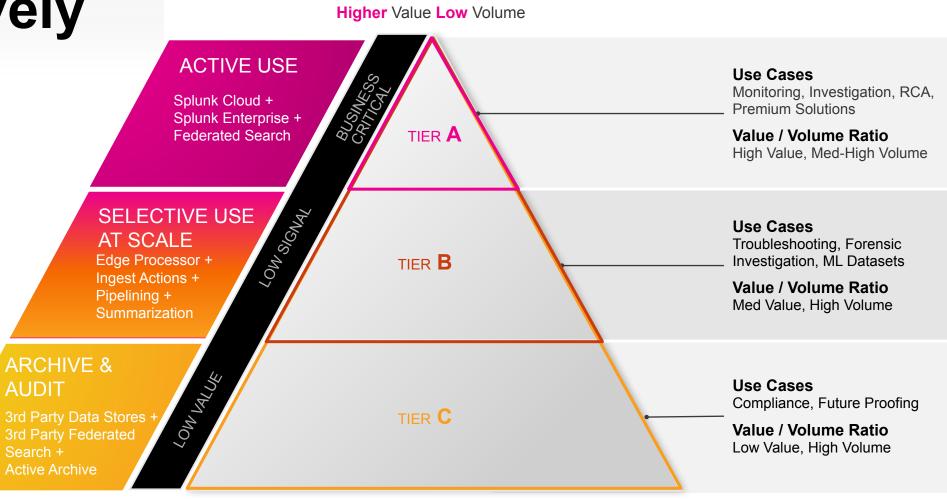


### **Data Value Changes With Age**



### Proactively tier by planned use

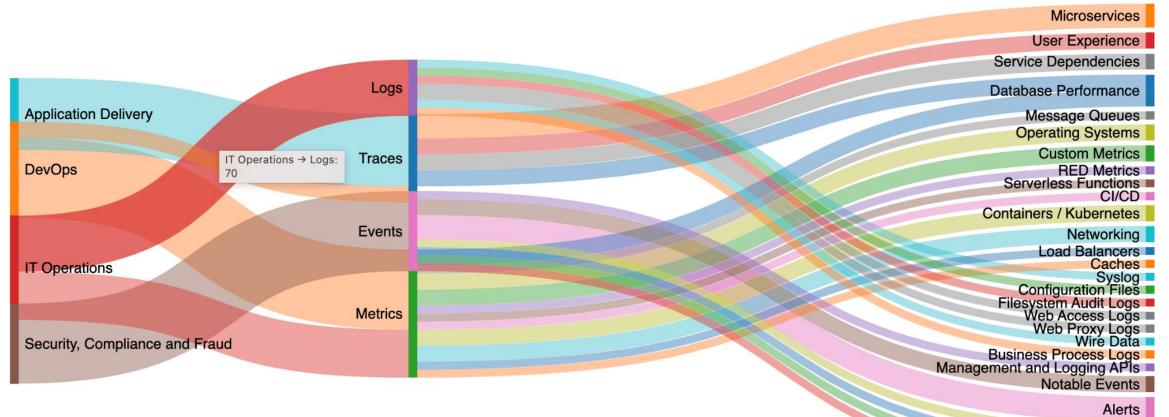
0010 01010 0101



Low Value High Volume

### **Multiple Use Cases On Common Data**

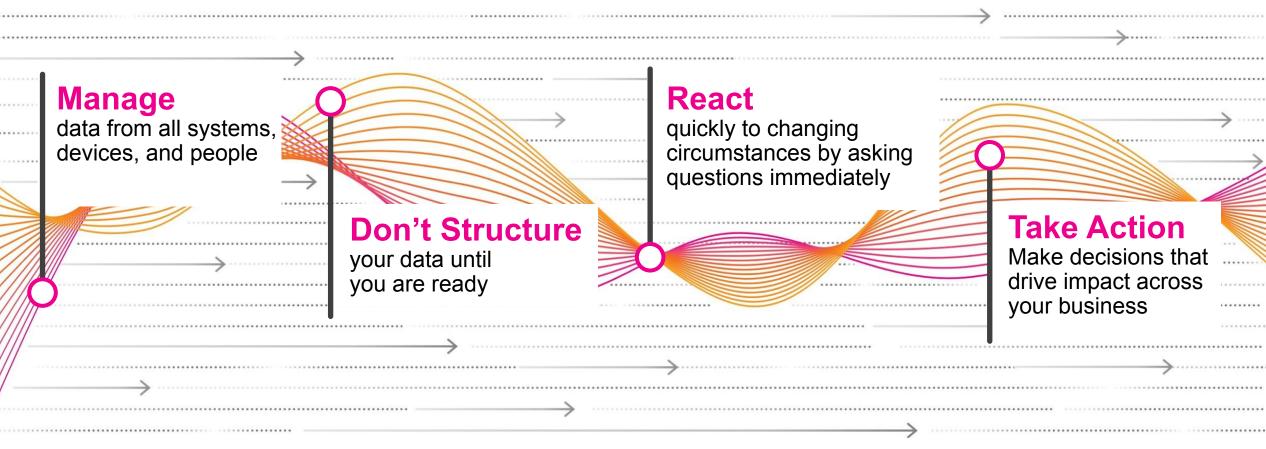
Drives system security and observability



- Windows Events
- Packet / Flow Data
- Call Detail Records
  - Clickstream Data

### Dynamic and Complex Data Remain the Biggest Challenge & Opportunity

We solved one of the biggest challenges in data with our investigative approach



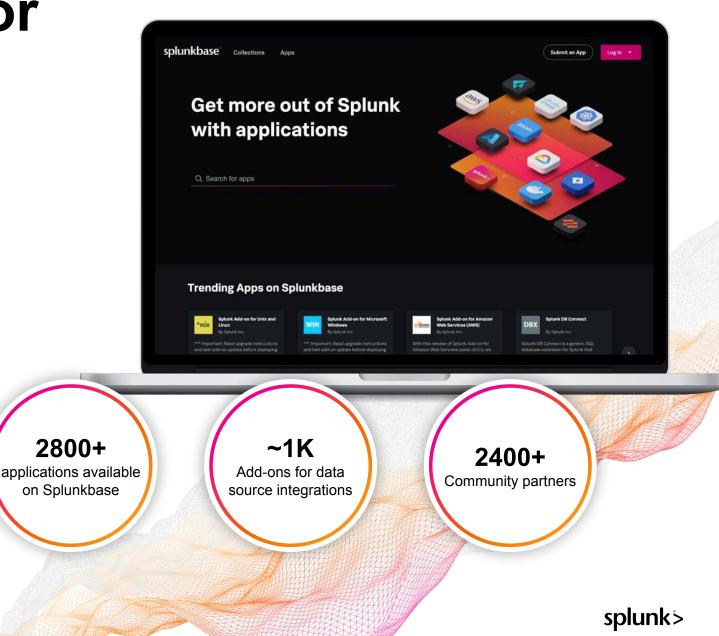
### Getting Data In (GDI)

- Universal Forwarder (UF)
- Splunk Stream
- DB Connect
- Data Manager
- HTTP Event Collector (HEC)
- OpenTelemetry Collector
- Splunk Connect for Syslog (SC4S)
- Splunk Connect for SNMP (SC4SNMP)
- Splunk OpenTelemetry Connect for Kubernetes
- Edge Processor
- Edge Hub
- eBPF
- Common Information Model / OCSF

- ...

# Access free apps, or build your own

- Build an essential security foundation and accelerate IT troubleshooting with free, high quality apps and add-ons to extend the power of your Splunk investment - and developer tooling to build your own!
- Access to the **2800+ solutions** from Splunk, partners, and the community
- Discover new tools for your use case with:
  - Collections Curated sets of top-rated apps for a variety of use cases and interests
  - App Directory Complete list of apps filterable by your specific needs





# Splunk & Security

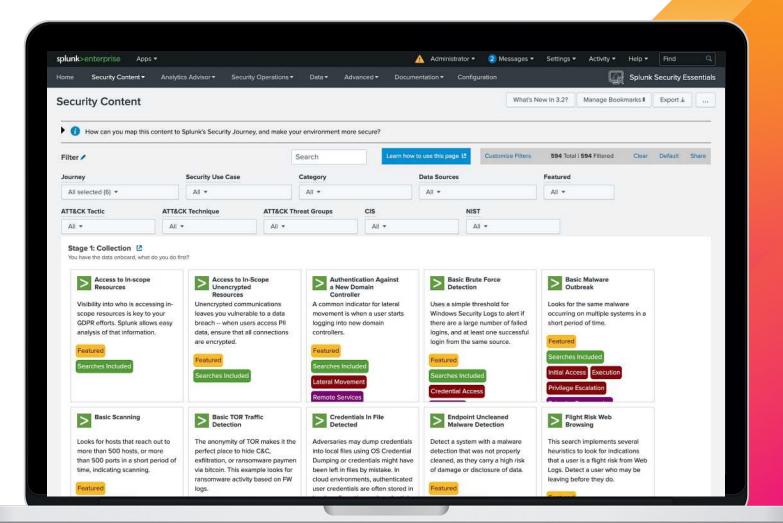


### Security Content Library

Browse, bookmark, and deploy 800+ security detections and analytic stories

#### ......

- Repository of Security Content for Splunk Cloud, Enterprise Security, UEBA, and SOAR
- Deploy security content within clicks
- Enrich notable events and run analytics with context from content library
- Stay up to date on ransomware + emerging threats

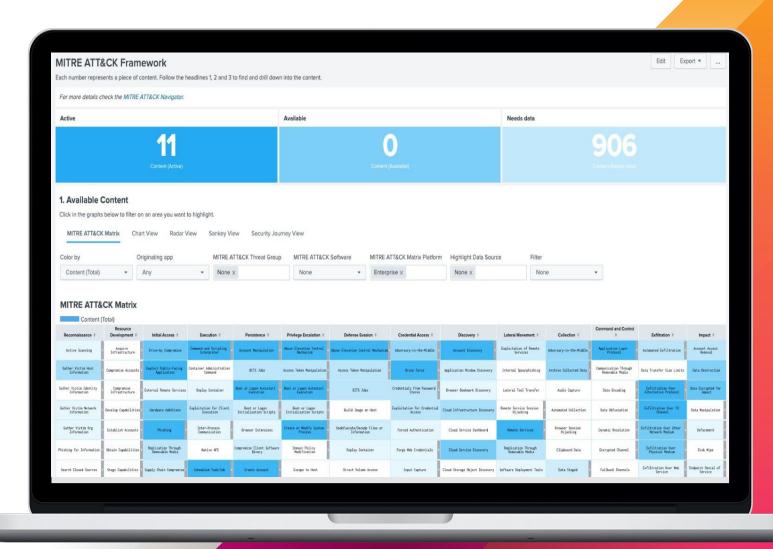




### Operationalize Security Frameworks

Identify gaps, improve threat detection, and reduce risks

- Develop an understanding of your security posture against MITRE ATT&CK® and Cyber Kill Chain® frameworks
- Ability to import 3rd party content and filter using the originating app
- Drilldown on known Tactics and Techniques and Kill Chain Phases to get a holistic view of all your security content





### Data and Content Introspection

Track data and saved searches to gain visibility

- Enrich saved searches with tags and metadata
- Automatic categorization by security products
- Visibility on ransomware related content and the ability to deploy directly from SSE

| Analytic Story Detail<br>hoose an Analytic Story from the<br>rop-down menu to view more<br>etail and run the searches.<br>AWS User Monitori • X                               | Hde Filers   |  |   |  | Export  |  |
|---|--|--|---|--|---|--|
|   | Category: Cloud Security   | Version: 1   | Created: 2018-03-12   |  |   |  |
| AWS User Monitoring   |  |  |   |  |   |  |
| Description:<br>Detect and investigate dorman<br>to enable governance within yo   |  | at have become active ag   | ain. Because inactive and ad-hoc accounts are common attack targets, it's critic  | ATTACK:  | Defense Evesion Discovery Initial Access Persistence<br>Privilege Excalation  |  |
| hoc accounts, leaving their sen<br>security of your data, when bac<br>usage, \ Fortunately, you can le<br>you increased visibility into you<br>source IP address from which t | vers vulnerable to attack. In fact, this was the<br>g actors leverage your compute resources, it<br>rverage Amazon Web Services (AWS) Cloud<br>ir user and resource activity by recording AM | very oversight that led to<br>can incur monumental cost<br>imil-a tool that helps you 4<br>/S Management Console e<br>imed.) The detection searc | sstructure. Nevertheless, it's all too common for enterprises to lose track of ad-<br>Teslak cryptojacking attack in February, 2018. In addition to compromising the<br>sts, since you will be billed for any new EC2 instances and increased bandwidth<br>enable governance, compliance, and inits auditing of your AWS account-to give<br>schors and API calls. You can identify which users and accounts called AWS, the<br>hes in this Analytic Story are designed to help you uncover AWS API activities | Kill Chain Phases:<br>Data Model:<br>References: | Actions on Objectives Exploitation<br>https://d0.avastatic.com/whitepapers/ava-security-best-practices.pdf<br>https://redlock.io/biog/cryptajacking-tesia |  |
| Analytic Story Detection  | n Searches   |  |   |  |   |  |
| + AWS Excessive Security Scan   | ning   |  |   |  |   |  |
| Detect API activity from users  | s without MFA  |  |   |  |   |  |
| security by forcing the u<br>MFA for privileged IAM u<br>Search   | sers to type a unique authentication code fro<br>users.  | m an approved authentica   | ong API calls and has not enabled Multi Factor authentication. Multi factor authent<br>ntion device when they access AWS websites or services. AWS Best Practices re<br>arch NOT [] inputlookup aws_service_accounts   fields identity  |  | ATT&CK<br>Kill Chain Phases<br>Evolution<br>CIS Controls<br>CIS 16<br>Data Models   |  |

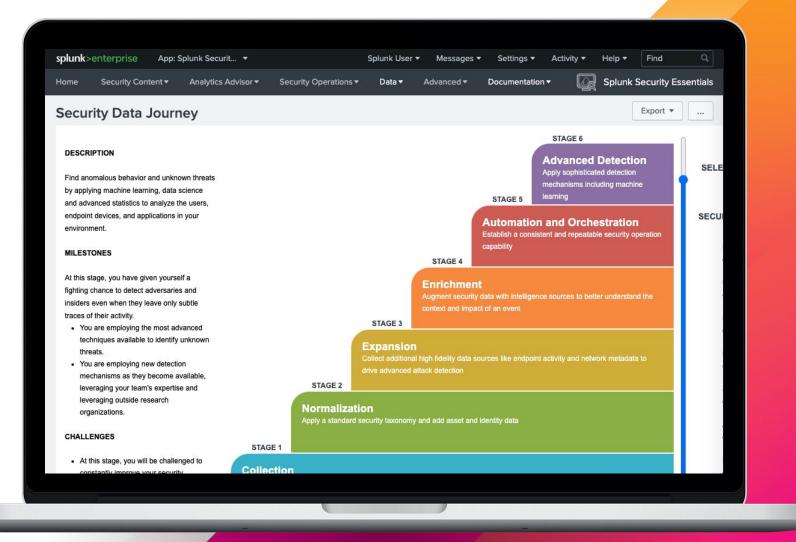


### Security Data Journey

Use data to bring context to security

\_\_\_\_\_

- Identify data and security milestones and challenges
- View analytics stories and their related contents easily in SSE
- Curate security detections to level up your security maturity
- Easily export content from SSE into Splunk ES





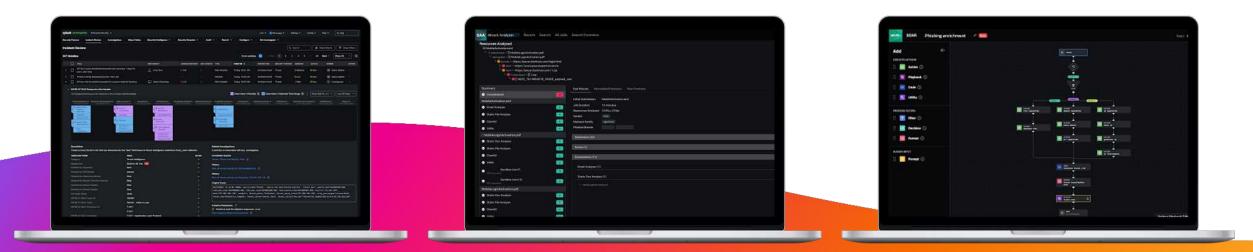
### **The Industry-Defining TDIR Solution**

#### SPLUNK MISSION CONTROL

#### Splunk Enterprise Security

#### Splunk Attack Analyzer

#### Splunk SOAR



Detect | Investigate | Respond

#### Splunk Enterprise Security

#### A data-centric, modern SIEM

- Gain insight into your security posture and investigate with speed and flexibility
- Reduce false positives by up to 80%, detect more sophisticated threats, and align security operations to industry frameworks
- Use pre-built detection and investigation content to more easily secure your AWS, Azure, and Google Cloud Platform data
- Scale to search and monitor terabytes of data per day

|          |      | oud Apps • Messages • Settings • Activit  | y = Q Find   |  |  |  |   |   |  | <u> </u>   | SOS Admin *  | Support 8   | a service  |
|----------|------|---|--|--|--|--|---|---|--|--|--|---|--|
| cunity   | Post | sture • Incident Review Investigations Securit  | y Intelligence • Security Dor  |  | Security =                                     | Audit• Se  |   |   |  |  | C  | Enterprise  | e Secu   |
| icid     | en   | nt Review   |  |  |  |  |   |   | Q Search   |  | III Hide Char  | ts T Hid  | le Filter  |
| rger     | ıcy  | <u>'</u>  | Status   |  |  |  | Owner   |   |  | Dom  | ain  |   |  |
|          |      | Informational<br>Line<br>Modure<br>Official   | 0  | Unassign<br>New<br>In Fropt<br>Percify<br>Resolved                           |  |  | C   | DIS Admin<br>SDAP Admin<br>Splane Could A<br>Uneskipped   | lulinin :  |  | Ο  | )   | Access<br>Endpol<br>Netwo<br>Titraut<br>Isteritty<br>Audit |
| ved filt |      | Ting Urgency Sta  |  | Security 0   |  |  | Search Type   |   | Time or Associations   |  |  |   |  |
| Selec    | t    | Add tags     Select.  | Select. • Select   | * Selec  | 1  | Select   | * Correlatio  | a ▼ ATT (2) ▼   | Time •   | * Last 24 - *  |  |   |  |
| 1.0      |      | Source: ATT&CK Tactic Threshold Exceeded For Object   | t Over Previous 7 Days x Risk  | Threshold Exceeded   | For Object Over 2                              | 4 Hour Period  | x Time Range:   |   |  |  |  |   |  |
| 8 N      | lota | tables Unselectal 1 Edit Selected 1 Edit All Matchin  |  |  |  |  |   |   |  | 2 Next >   | 20 per page  | · → Refr  | esh (  |
| 3        |      | THE -   | Risk Object +  | Risk Score •   | Risk Events -                                  | Type +   | ↓ Time +  | Disposition -   | Security Domain -  | Urgency +  | Status -   | Owner -   | Act  |
|          |      |   |  |  |  |  |   |   |  |  |  |   |  |
|          |      | 24 hour risk threshold exceeded for user=fyador@froth.ly  | / <u>A</u> fyodor@froth.ly   | 13978  | HS   | Risk Notable   | Today, 10:56 PM   | True Positive -<br>Suspicious Activity  | Threat   | A Critical   | Closed   | SOS Admin   | 1000   |
|          |      | 24 hour risk threshold exceeded for user-fyodar@froth.ly<br>24 hour risk threshold exceeded for<br>system=54.230.147.59   | ( 오 fyodor@froth.ly  | # 3978<br>#1360  |  |  |   | Suspicious Activity   |  |  | Closed<br>In<br>Progress   | SOS Admin<br>unassigned   |  |
|          |      | 24 hour risk threshold exceeded for<br>nystem=54.23014759   |  |  | 45   | Risk Notable   | Today, 10:56 PM   | Suspicious Activity<br>Undetermined   | Threat   | Critical   |  |   |  |
|          |      | 24 hour risk threshold exceeded for<br>system=54.22014759<br>24 hour risk threshold exceeded for<br>system=54.23014747  | ⊊ 54,230.147.59  | <mark>(</mark> 1360  | 145<br>17                                      | Risk Notable<br>Risk Notable   | Today, 10:56 PM<br>Today, 9:06 PM   | Suspicious Activity<br>Undetermined<br>Undetermined   | Threat<br>Threat   | A Figh   | in<br>Progress<br>In   | unassigned  |  |
|          |      | 24 hour risk threshold exceeded for<br>system=54,230147,59<br>24 hour risk threshold exceeded for<br>system=54,23014747<br>24 hour risk threshold exceeded for  | 54.230.147.59<br>54.230.147.47   | 1360<br>1360   | 145<br>17<br>17                                | Risk Notable<br>Risk Notable<br>Risk Notable   | Today, 10:56 PM<br>Today, 9:06 PM<br>Today, 9:06 PM   | Suspicious Activity<br>Undetermined<br>Undetermined<br>Undetermined   | Threat<br>Threat<br>Threat   | A Critical   | In<br>Progress<br>In<br>Progress<br>In   | unassigned<br>unassigned  |  |
|          |      | 24 hour risk threshold exceeded for<br>system=54.23014759<br>24 hour risk threshold exceeded for<br>system=54.23014747<br>24 hour risk threshold exceeded for<br>system=52.84.235102<br>24 hour risk threshold exceeded for   | 54.230.147.59<br>54.230.147.47<br>55.84.235.102  | (1360<br>(1360<br>(1360  | 145<br>17<br>17                                | Risk Notable<br>Risk Notable<br>Risk Notable<br>Risk Notable                                 | Today, 10:56 PM<br>Today, 9:06 PM<br>Today, 9:06 PM<br>Today, 9:06 PM   | Suspidous Activity<br>Undetermined<br>Undetermined<br>Undetermined<br>Undetermined  | Threat<br>Threat<br>Threat<br>Threat                               | A Critical<br>A High<br>A High<br>A High   | In<br>Progress<br>In<br>Progress<br>In<br>Progress<br>In   | unassigned<br>unassigned<br>unassigned  |  |
|          |      | 24 hour risk threshold exceeded for<br>system:54.230.147.59<br>24 hour risk threshold exceeded for<br>system:54.230.147.47<br>24 hour risk threshold exceeded for<br>system:52.84.235.102<br>24 hour risk threshold exceeded for<br>system:54.215.24.225  | 54.230.147.59<br>54.230.147.47<br>52.84.235.102<br>34.215.24.225<br>() 172.16.3197   | 11360<br>11360<br>(1360<br>11360   | 145<br>17<br>17<br>17                          | Risk Notable<br>Risk Notable<br>Risk Notable<br>Risk Notable<br>Risk Notable                 | Today, 10:56 PM<br>Today, 9:06 PM<br>Today, 9:06 PM<br>Today, 9:06 PM<br>Today, 9:06 PM   | Suspictous Activity<br>Undetermined<br>Undetermined<br>Undetermined<br>Undetermined   | Threat<br>Threat<br>Threat<br>Threat<br>Threat                     | <ul> <li>▲ Critical</li> <li>▲ High</li> <li>▲ High</li> <li>▲ High</li> <li>▲ High</li> <li>▲ High</li> </ul> | In<br>Progress<br>In<br>Progress<br>In<br>Progress<br>In<br>Progress<br>In                             | unassigned<br>unassigned<br>unassigned<br>unassigned                            |  |
|          |      | 24 hour risk threshold exceeded for<br>system:54.230.147.59<br>24 hour risk threshold exceeded for<br>system:54.230.147.47<br>24 hour risk threshold exceeded for<br>system:52.84.235.102<br>24 hour risk threshold exceeded for<br>system:34.215.24.225<br>24 hour risk threshold exceeded for system:172.16.3.197<br>ATT&CK tactic threshold exceeded over previous 7 days<br>for user:mvaltus@froth.ly   | 54.230.147.59<br>54.230.147.47<br>52.84.235.102<br>34.215.24.225<br>() 172.16.3197   | 1360<br>1360<br>1360<br>1360   | 145<br>17<br>17<br>17<br>17<br>17              | Risk Notable<br>Risk Notable<br>Risk Notable<br>Risk Notable<br>Risk Notable                 | Today, 10:56 PM<br>Today, 9:06 PM<br>Today, 9:06 PM<br>Today, 9:06 PM<br>Today, 9:06 PM   | Suspictous Activity<br>Undetermined<br>Undetermined<br>Undetermined<br>Undetermined<br>Undetermined<br>Thus Positive -  | Threat<br>Threat<br>Threat<br>Threat<br>Threat                     | A Critical<br>A High<br>A High<br>A High<br>A High<br>A High   | In<br>Progress<br>In<br>Progress<br>In<br>Progress<br>In<br>Progress<br>In<br>Progress                 | unassigned<br>unassigned<br>unassigned<br>unassigned<br>unassigned              |  |
|          |      | 24 hour risk threshold exceeded for<br>system=54.230147.59<br>24 hour risk threshold exceeded for<br>system=54.230147.47<br>24 hour risk threshold exceeded for<br>system=52.84.235.102<br>24 hour risk threshold exceeded for<br>system=54.24.24.25<br>24 hour risk threshold exceeded for system=172.16.3.197<br>ATT&CK tactic threshold exceeded over previous 7 days<br>for user=musilus@foth.ly  |  | 1 1360<br>1 1360<br>1 1360<br>1 1360<br>1 1360<br>1 137                      | 145<br>17<br>17<br>17<br>17<br>19              | Risk Notable<br>Risk Notable<br>Risk Notable<br>Risk Notable<br>Risk Notable<br>Risk Notable | Today, 10:56 PM<br>Today, 9:06 PM<br>Today, 9:06 PM<br>Today, 9:06 PM<br>Today, 9:06 PM<br>Today, 9:06 PM                                     | Suspictous Activity<br>Undetermined<br>Undetermined<br>Undetermined<br>Undetermined<br>Undetermined<br>True Positive -<br>Suspictous Activity<br>Undetermined | Threat<br>Threat<br>Threat<br>Threat<br>Threat<br>Threat           | A Critical<br>A High<br>A High<br>A High<br>A High<br>A High<br>A High<br>A Critical                           | In<br>Progress<br>In<br>Progress<br>In<br>Progress<br>In<br>Progress<br>Closed<br>In                   | unassigned<br>unassigned<br>unassigned<br>unassigned<br>SOS Admin               |  |
|          |      | 24 hour risk threshold exceeded for<br>system:54.230.147.59<br>24 hour risk threshold exceeded for<br>system:54.230.147.47<br>24 hour risk threshold exceeded for<br>system:52.84.235.102<br>24 hour risk threshold exceeded for<br>system:34.215.24.225<br>24 hour risk threshold exceeded for system:172.16.3.197<br>ATT&CK tactic threshold exceeded over previous 7 days<br>for user-movalluxs@foth.1y<br>ATT&CK tactic threshold exceeded over previous 7 days | □         54.230.147.59           □         54.230.147.47           □         52.84.235.102           □         34.215.24.225           □         172.36.3197           Q.         mvalkus@froth.ly           Q.         tyodor@froth.ly | 1 1360<br>1 1360<br>1 1360<br>1 1360<br>1 1360<br>1 1360<br>1 1377<br>1 4230 | 145<br>17<br>17<br>17<br>17<br>17<br>19<br>162 | Risk Notable<br>Risk Notable<br>Risk Notable<br>Risk Notable<br>Risk Notable<br>Risk Notable | Today, 10:56 PM<br>Today, 9:06 PM<br>Today, 9:06 PM<br>Today, 9:06 PM<br>Today, 9:06 PM<br>Today, 9:06 PM<br>Today, 7:53 PM<br>Today, 7:53 PM | Suspictous Activity<br>Undetermined<br>Undetermined<br>Undetermined<br>Undetermined<br>Undetermined<br>True Positive -<br>Suspictous Activity<br>Undetermined | Threat<br>Threat<br>Threat<br>Threat<br>Threat<br>Threat<br>Threat | A Critical<br>A High<br>A High<br>A High<br>A High<br>A High<br>A High<br>A Ortical<br>A Medium                | In<br>Progress<br>In<br>Progress<br>In<br>Progress<br>In<br>Progress<br>Closed<br>In<br>Progress<br>In | unassigned<br>unassigned<br>unassigned<br>unassigned<br>SOS Admin<br>unassigned |  |

### Data-Driven Insights

(i)

Full-breadth visibility

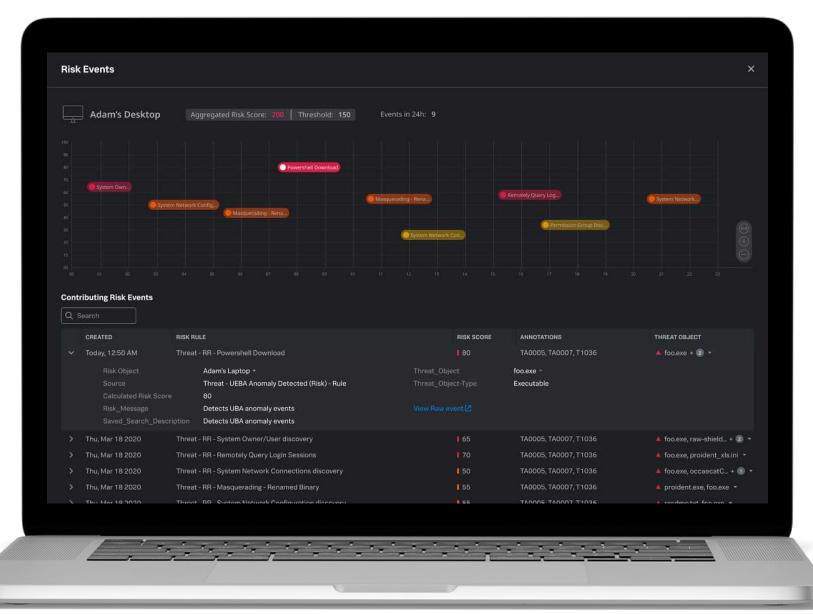
- Unlock the ability to ingest, normalize, and gain insights on any data from any source
- Schema-on-read and distributed indexing capabilities ensure fast, flexible investigations
- Perform continuous monitoring with pre-built and customizable dashboards, detections, content, reports, and frameworks
- Search and correlate across cloud, on-premises, or hybrid data sources and deployments



## Advanced Analytics

#### Boost productivity

- 1400+ detections with 100+ cloud-based detections
- 30% increase in true-positive alert rates with Risk-Based Alerting (RBA)
- Enrich and prioritize alerts with integrated threat intelligence (Splunk Intelligence Management)
- Align security operations to industry frameworks (MITRE ATT&CK, NIST, CIS 20, and Kill Chain)
- Dive deep with intuitive search and investigation capabilities



## Scale and Flexibility

#### Open and extensible

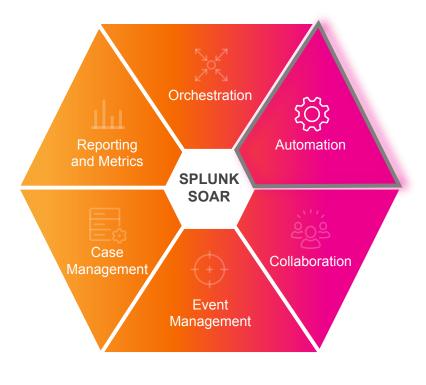
- Scale to search and monitor terabytes of data per day
- Gather context across your multi-vendor security and IT stack with technology integrations from Splunkbase
- Stay on top of new and emerging threats with automated content delivery from the Splunk Threat Research Team
- Customize and tune pre-built detections, content, frameworks to address what's critical

| splunk>cloud A     | Apps 👻 🔞 Mess   | sages • Settings | <ul> <li>Activity ▼</li> </ul> | Q Find                   |                  |         |          | 0           | 👤 SOS Admin 🔻 | ? Support & Services • |
|--------------------|-----------------|------------------|--------------------------------|--------------------------|------------------|---------|----------|-------------|---------------|------------------------|
| Security Posture - | Incident Review | Investigations   | Security Intelliger            | nce ▼ Security Domains ▼ | Cloud Security - | Audit 🕶 | Search 🕶 | Configure • | œ             | Enterprise Security    |

#### **Use Case Library**

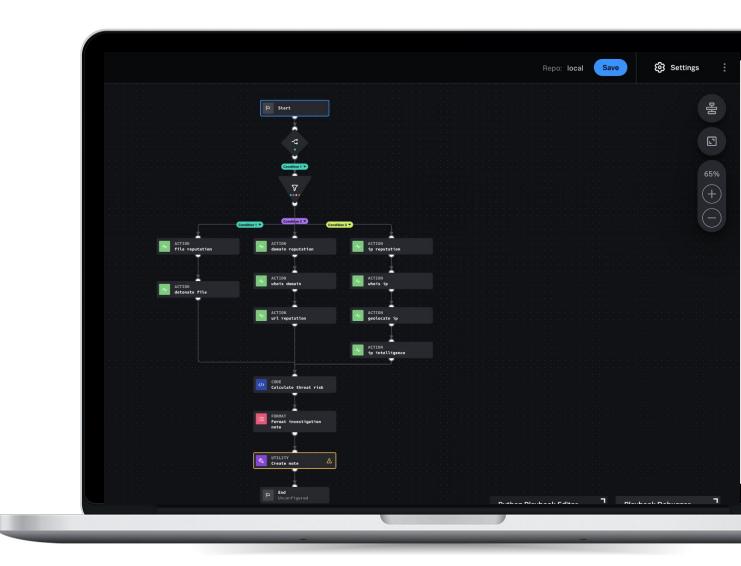
Explore the Analytic Stories included with Enterprise Security that provide analysis guidance on how to investigate and take actions on threats that ES detects.

| Use Cases         |        |        |   | Nodel: All     | App: All  App: A |                             | Q filter       |          |
|-------------------|--------|--------|---|----------------|--|-----------------------------|----------------|----------|
| Abuse             | 135 AI | In use |   | Use Case -     | ces, adversary factics, vulnerability, maiware, Abuse, Data Destruction, Phyliege<br>Description   | App -                       | Last Updated 🗸 | Bookmark |
|                   | >      |        | AWS Cross Account<br>Activity             | Cloud Security | Track when a user assumes an IAM role in another AWS account to obtain<br>cross-account access to services and resources in that account. Accessing<br>new roles could be an indication of malicious activity.   | ES Content<br>Updates       | Jun 4, 2018    |          |
| Adversary Tactics | >      |        | AWS Cryptomining                          | Cloud Security | Monitor your AWS EC2 instances for activities related to<br>cryptojacking/cryptomining. New instances that originate from previously<br>unseen regions, users who launch abnormally high numbers of instances, or<br>EC2 instances started by previously unseen users are just a few examples of<br>potentially malicious behavior.  | ES Content<br>Updates       | Mar 8, 2018    |          |
| ×Ĵx               | >      |        | AWS IAM Privilege<br>Escalation           | Cloud Security | This analytic story contains detections that query your AWS Cloudtrail for<br>activities related to privilege escalation.  | ES Content<br>Updates       | Mar 8, 2021    |          |
|                   | >      |        | AWS Network ACL Activity                  | Cloud Security | Monitor your AWS network infrastructure for bad configurations and malicious<br>activity. Investigative searches help you probe deeper, when the facts warrant<br>it.  | ES Content<br>Updates       | May 21, 2018   |          |
| Best Practices    | >      |        | AWS Security Hub Alerts                   | Cloud Security | This story is focused around detecting Security Hub alerts generated from AWS  | ES Content<br>Updates       | Aug 4, 2020    |          |
|                   | >      |        | AWS Suspicious<br>Provisioning Activities | Cloud Security | Monitor your AWS provisioning activities for behaviors originating from<br>unfamiliar or unusual locations. These behaviors may indicate that malicious<br>activities are occurring somewhere within your network.   | ES Content<br>Updates       | Mar 16, 2018   |          |
| Cloud Security    | >      |        | AWS User Monitoring                       | Cloud Security | Detect and investigate dormant user accounts for your AWS environment that<br>have become active again. Because inactive and ad-hoc accounts are<br>common attack targets, it's critical to enable governance within your<br>environment.  | ES Content<br>Updates       | Mar 12, 2018   |          |
|                   | >      | ۴      | Access Protection                         | Best Practices | Monitoring account activity and securing authentication are critical to<br>enterprise security. This use case includes searches that detect suspicious   | DA-ESS-<br>AccessProtection | Sep 13, 2018   |          |



#### **Automation**

- Automate repetitive tasks to force multiply team efforts.
- Execute automated actions in seconds versus hours.
- Become proactive and focus on mission-critical objectives to protect your business.



### Splunk Attack Analyzer

Automatic analysis of active threats. Full-scope insights and rapid resolution.

### The newest member of the Splunk Security Family

Acquisition of TwinWave announced on November 8th, 2022

Take the manual work out of threat analysis

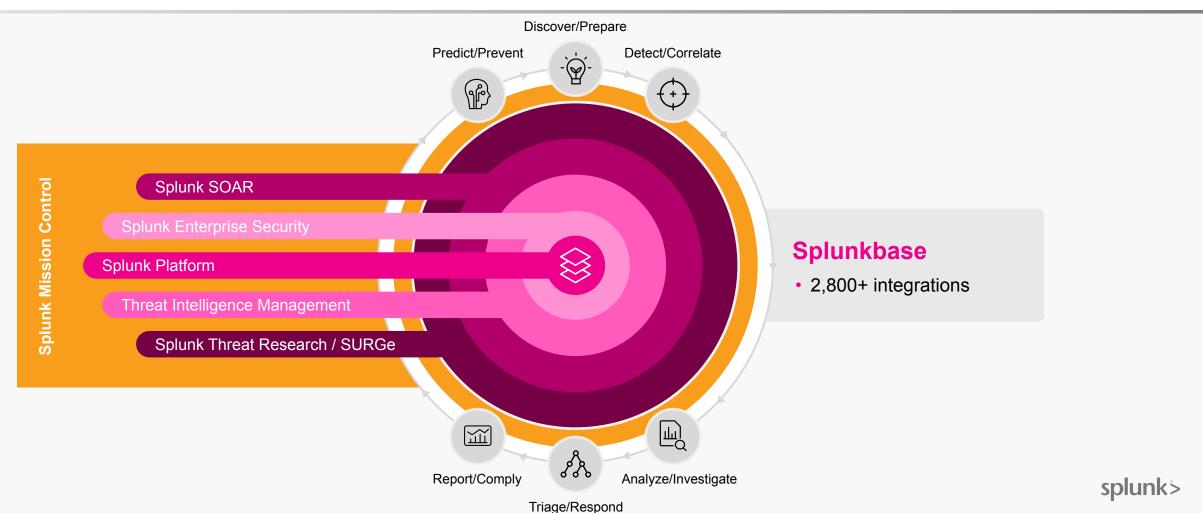
See through the eyes of the threat actor

Interact with malicious content in a dedicated, unattributable environment

Fully automate end-to-end threat analysis and response workflow

### Splunk Security for Threat Detection, Investigation and Response

The tools you need to build a modern, data-centric SOC





### Demo

### The path to greater resilience

#### Foundational Visibility

See across hybrid environments

Security SecOps

#### **Observability** ITOps, Engineering

Search and investigate

Troubleshoot with log analytics

#### Prioritized Actions

Understand risk and performance

Expand monitoring and alerting

Understand service health

#### Proactive Response

Get ahead of issues

Deliver situational awareness and automation

Ensure reliability of consumer-facing web applications

#### Optimized Experiences

Delight customers and build trust

Unify threat detection, investigation and response

Deliver exceptional digital customer experiences

**Digital Resilience at Enterprise Scale** 

### **Splunk Leads the Way**



# In One Platform Accessible to all Your Business' Consumers

Shared tooling to drive resilience across critical consumer groups

### Security Operations

Security Monitoring

æ,

- Incident Management
- Advanced Threat Detection
- Insider Threats
- Incident Investigation and Forensics
- SOC Automation & Orchestration
- Compliance
- ICS Security



#### **IT** Operations

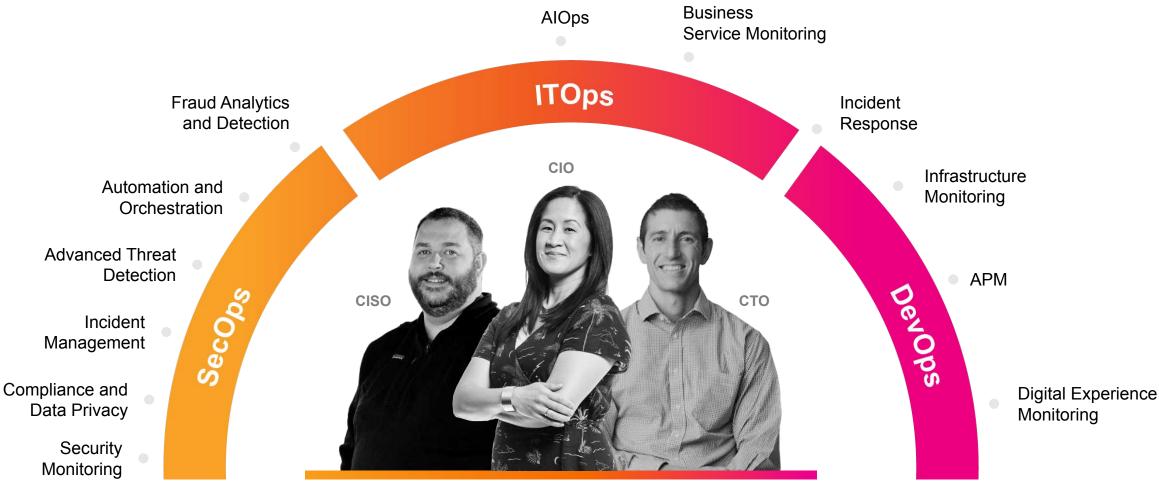
- Analytics for IT Troubleshooting
- Predictive Analytics
- SDKs for GO, Python, JavaScript
- Developer APIs
- Customer Experience Optimization
- Container Monitoring
- Infrastructure Monitoring
- High Volume, Low Cost Storage



#### DevOps

- Real-Time Observability with Monitoring and Diagnostics
- Infrastructure Monitoring
- Application Performance
   Monitoring
- Synthetics Monitoring
- Real User Monitoring
- Container Monitoring
- Distributed Tracing

### We Bring Your Digital Teams Together



The Unified Security and Observability Platform

# Thank You

