

멀티 클라우드 환경에서 통합 보안 관제 및 자동화 대응 방안

Splunk



멀티 클라우드 환경에서 통합 보안 관제 및 자동화 대응 방안

최대수 이사 (Ph.D. CISSP, CISA, GMON)
Splunk Korea

Agenda

1. Splunk 소개
2. Splunk 보안 솔루션 및 특징점
3. Trend Micro XDR + Splunk 연동 활용
4. 멀티 클라우드 환경 통합보안관제 방안
5. 주요 화면

1. Splunk 소개

Splunk 소개

- 글로벌 HQs:
 - 샌프란시스코(AMER)
 - 런던(EMEA)
 - 홍콩(APAC)
- 직원수 전세계 8,000+명
- 연 매출 약 2조 4천억원 (\$1,803 YoY +30%)
- 나스닥 상장 : SPLK

- 2003년 시작
- 제품 구성:
 - Splunk Enterprise
 - Splunk Cloud
 - Premium Solutions
 - Enterprise Security
 - IT Service Intelligence
 - UBA, Splunk SOAR, O11y

- 고객사 (전체): 16,000+
- 국가기준: 110개국+
- Fortune 100대 기업: 92+
- 고객사 (한국): 400+
 - 중소기업, 대기업, 그룹 계열사
- 최대 라이선스: 10+ PB/일

splunk >

turn data into doing™

“머신데이터를 아무런 제약 없이 수집>저장>분석>시각화 할 수 있는 실시간 분산 플랫폼”

머신데이터 (Machine Data)

- 서버/NW 로그
- 각종 설비 데이터
- 애플리케이션 로그
- 기타 모든 텍스트 형태의 데이터

제약 없음 (No Limits)

- 반정형/정형 데이터
- 데이터 포맷 무관
- 데이터 용량 무관
- 데이터 속도 무관
- 제약 없이 수용

엔드 투 엔드 (End-to-End)

- 외부 솔루션 불필요
- 복잡한 코딩 및 SI 개발이 필요 없음
- 데이터의 생성부터 가치 획득까지 모두

실시간 및 분산 (Real-time)

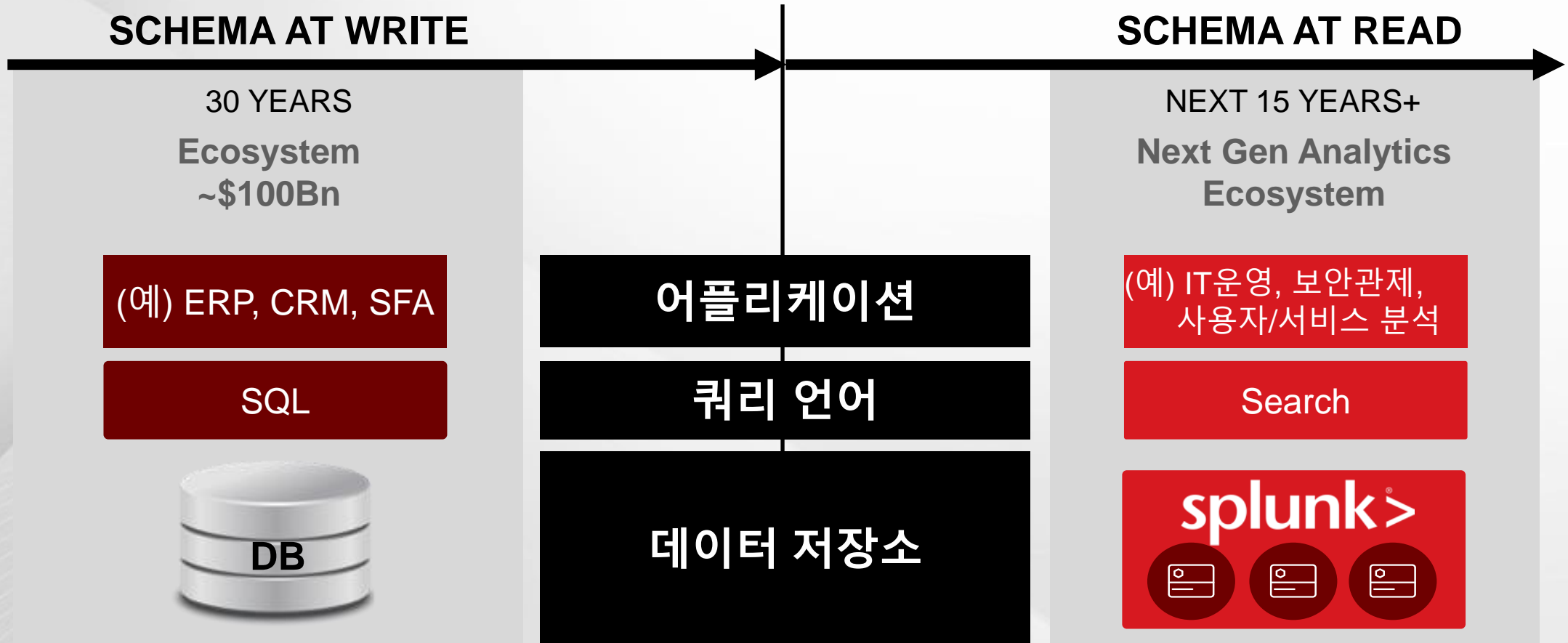
- 모든 데이터 실시간 처리, 즉시 결과 확인
- 분산 저장, 분산 검색
- 성능 및 용량의 선형적 확장

플랫폼 (Platform)

- 커스터마이징 용이
- 외부 시스템과 손쉬운 연동
- 2,800여 무료 앱을 통한 기능 확장

Splunk 특징점 - 로그 저장 및 검색 방식

머신데이터 분석 환경의 새로운 패러다임

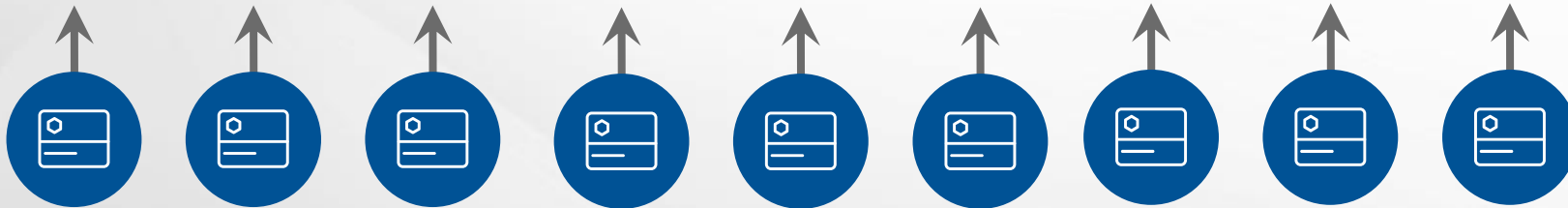


Splunk 특징점 - 확장성

성능 요구 사항에 따라 **횡적 확장성** 제공



Search head로 검색 워크로드 오프로딩



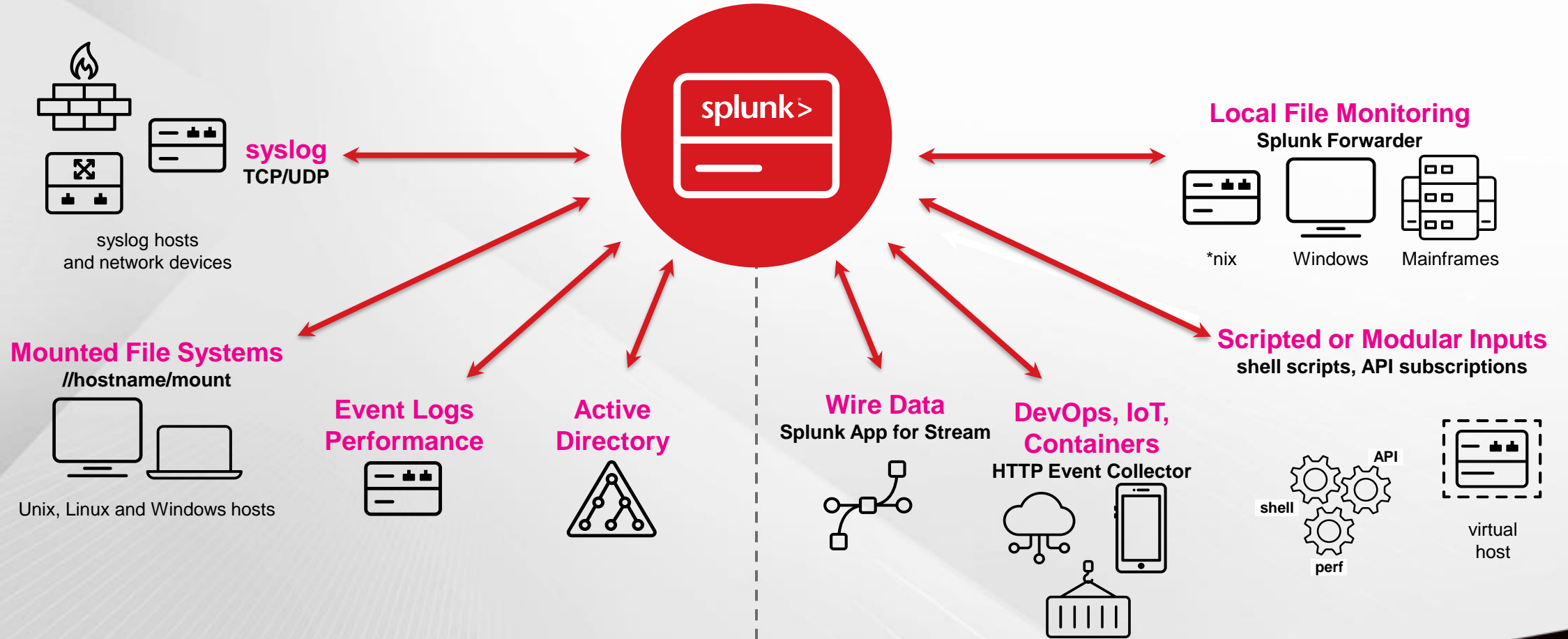
Splunk Indexer 들로 자동 부하 분산하여 균등하게 데이터 압축 저장



Splunk Forwarder 를 통해 수천대 서버에서 데이터를 전송

Splunk 특징점 - 로그 수집

다양한 이기종 데이터 소스로부터 제약없는 수집



Splunk 특징점 - 로그 검색

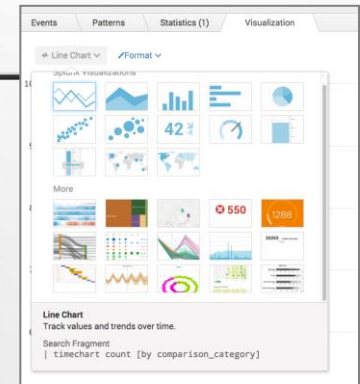
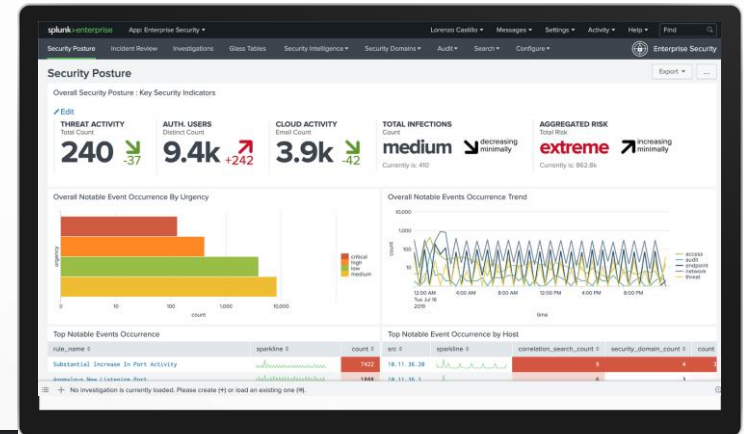
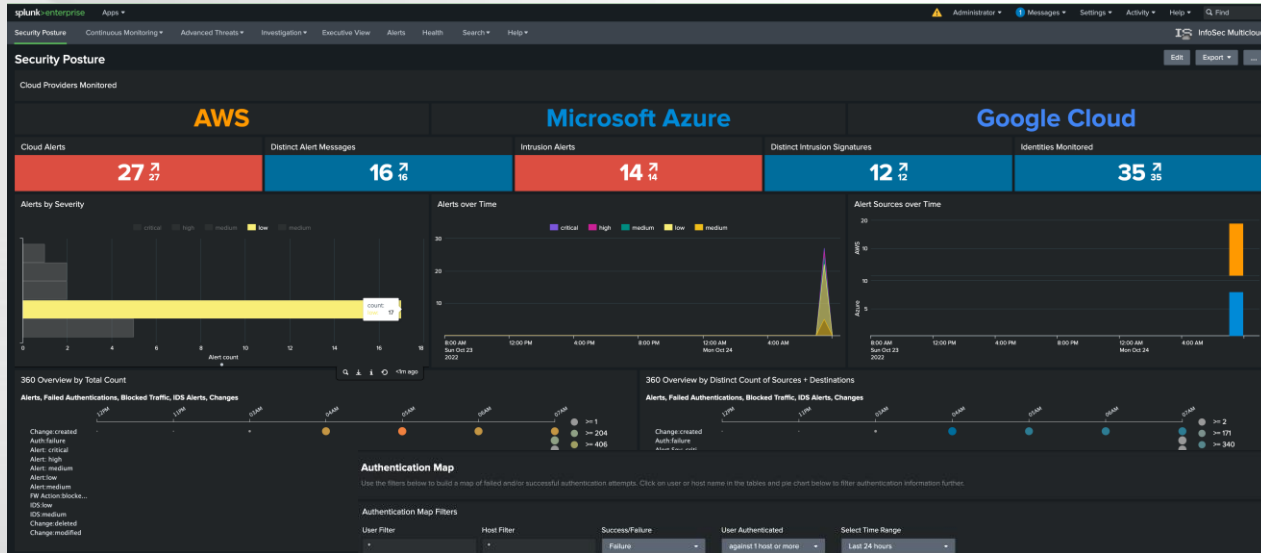
강력한 검색 기능(SPL)

- SQL 과 Unix 파이프라인 구문이 결합된 최적의 검색 언어 SPL(Search Processing Language)
- 검색, 상호 연관, 분석 및 시각화 관련된 150 개 이상의 명령어
- 통계, 그래프, 각종 연산 함수를 활용한 분석
- 별도의 correlation key 설정 없이 상관관계 분석
- 신속하게 필요한 데이터를 찾아 분석하여 사고의 근본 원인을 파악

The screenshot displays the Splunk Search & Reporting interface. At the top, the search bar contains the query `index=_internal`, highlighted with a yellow box and labeled "검색어". Below the search bar, a bar chart visualization shows the distribution of search results over time, labeled "시계열 데이터 분포". The main content area displays a table of search results with columns for Time and Event. The table is highlighted with a yellow box and labeled "검색 데이터". On the left side, the "Selected Fields" panel shows a list of fields, with "자동 필드 추출" (Automatic Field Extraction) highlighted in yellow.

Time	Event
7/28/20 12:24:50.822 AM	07-28-2020 00:24:50.822 +0000 INFO PeriodicHealthReporter - feature="Searches Skipped" color=green due_to_stanza="feature:searches_skipped" node_type=feature node_path=splunkd.search_scheduler.searches_skipped
7/28/20 12:24:50.822 AM	07-28-2020 00:24:50.822 +0000 INFO PeriodicHealthReporter - feature="Searches Delayed" color=green due_to_stanza="feature:searches_delayed" node_type=feature node_path=splunkd.search_scheduler.searches_delayed
7/28/20 12:24:50.822 AM	07-28-2020 00:24:50.822 +0000 INFO PeriodicHealthReporter - feature="Search Lag" color=green due_to_stanza="feature:search_lag" node_type=feature node_path=splunkd.search_scheduler.search_lag

내장 UI 컴포넌트를 활용한 쉽고 빠른 대시보드 제작



Splunk 특징점 – 앱 생태계 제공

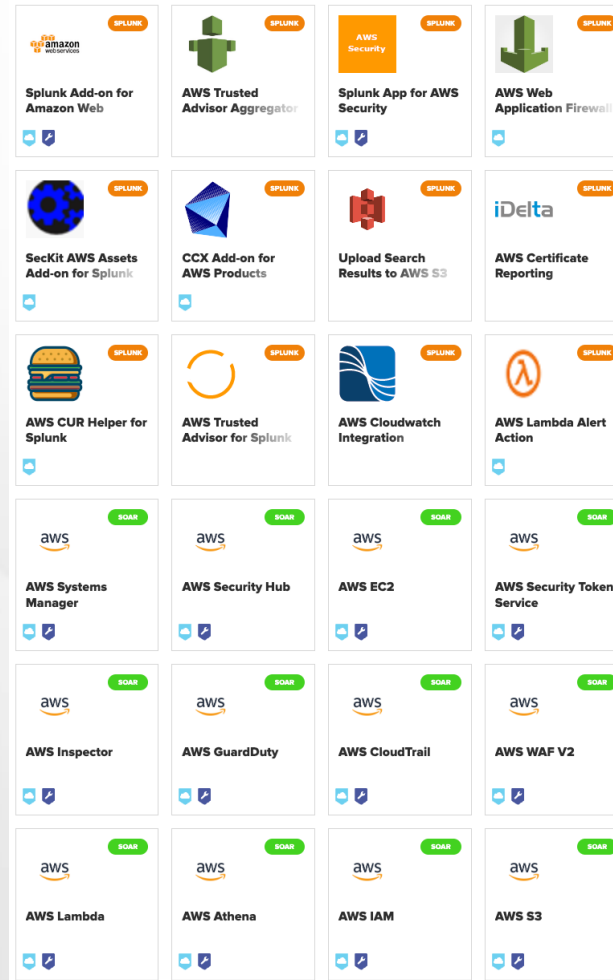
앱 생태계를 제공하여 최소의 리소스로 빠르게 요구사항을 구현

splunkbase.com **2,800**개 이상의 다양한 앱

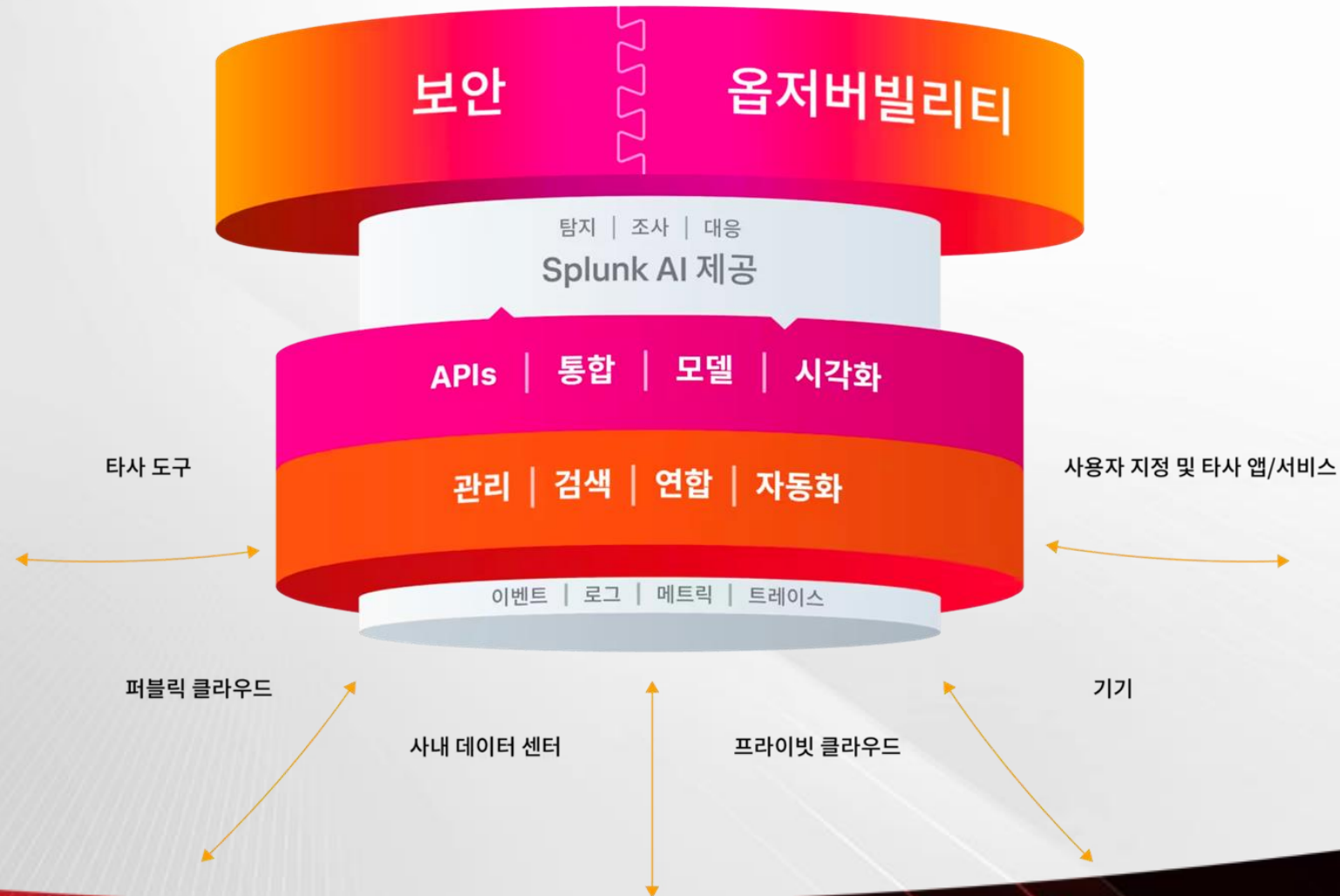
answers.splunk.com **12만건**의 Q&A

전세계 **138**개 user groups

825 여개의 partners

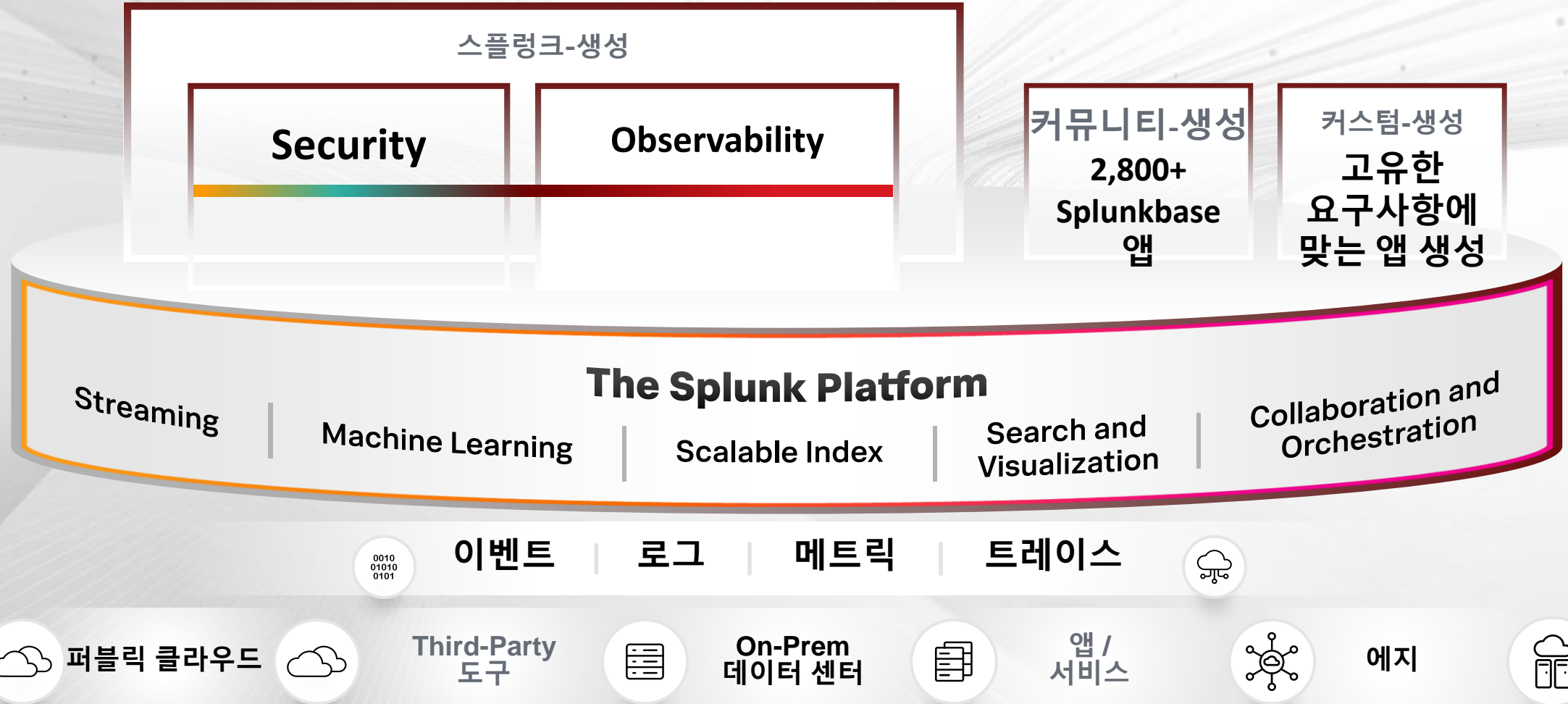


The Unified Security and Observability Platform



2. Splunk 보안 솔루션 및 특징점

통합된 Security 및 Observability 플랫폼



보안 관제(운영)에서 SIEM 과 SOAR 역할

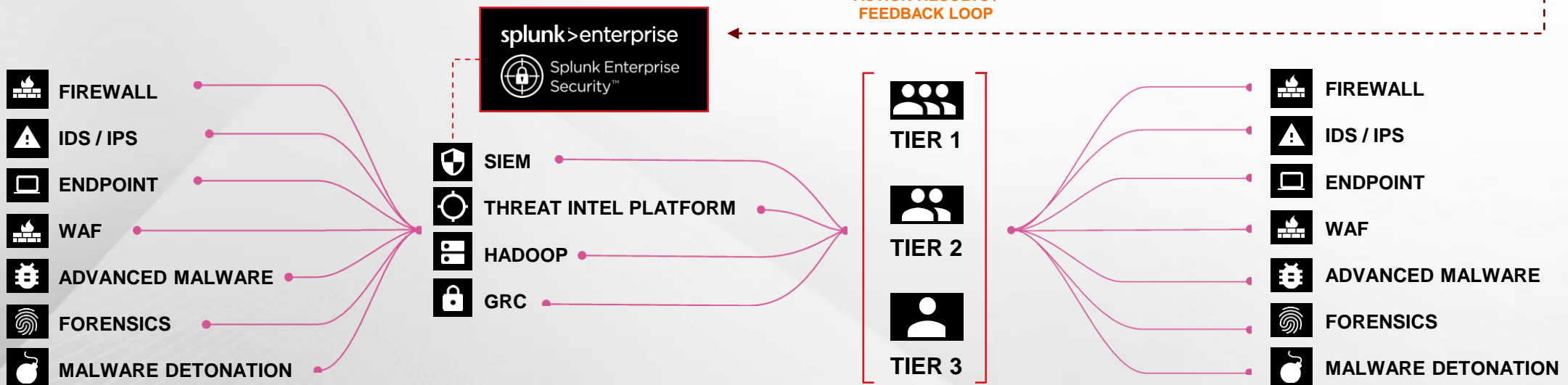
OODA Loop를 통한 빠른 실행으로 보안 향상

Observe(관찰) → Orient(상황판단) → Decide(의사결정) → Act(실행)

Point Products

Analytics

ACTION RESULTS /
FEEDBACK LOOP



splunk>enterprise

자동화
(로그 수집/저장/분석/시각화)

SOAR를 통한 보안 업무 자동화

Splunk 보안 솔루션

분석 중심의 보안운영 솔루션으로 주요 보안 Use Cases 제공

활용 사례

보안 관제 모니터링

고수준 위협 탐지

내부자 위협 탐지

사기 분석 및 탐지

컴플라이언스 관리

침해사고 조사 및 포렌식

위협 사냥 및 사고 대응

SOC 자동화

어플리케이션



Splunk Enterprise Security™

(SIEM)



Splunk User Behavior Analytics™

(UEBA)



SOAR

(SOAR)

TRU*STAR

(TIP)

twinwave
(Attack Analyzer)
...

플랫폼

splunk>

데이터 소스

(머신 데이터)

다양한 로그/이벤트(on-prem/cloud) 네트워크 와이어 데이터 위협 인텔리전스 ...

Splunk ES 주요 기능

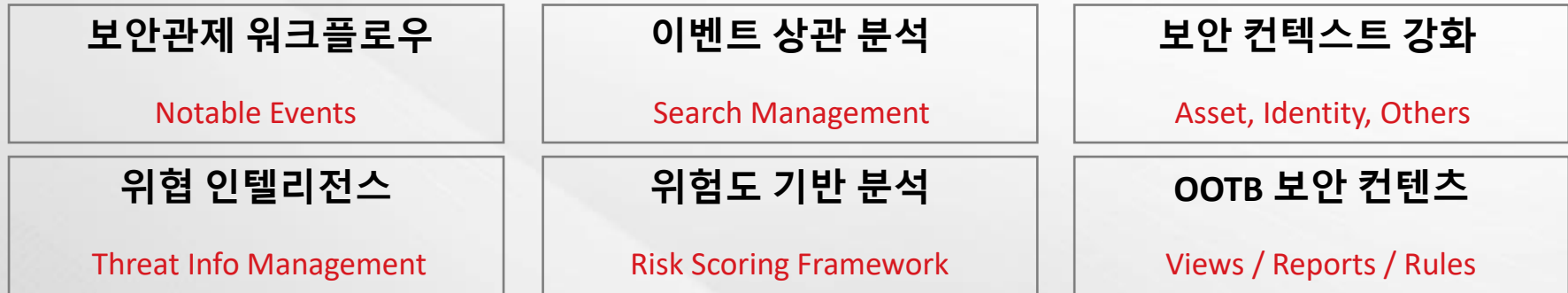
주요기능



프로세스



주요 기능



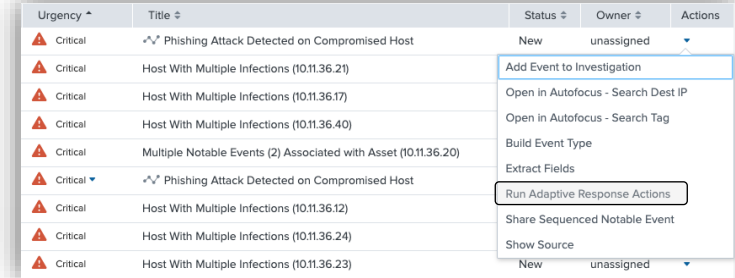
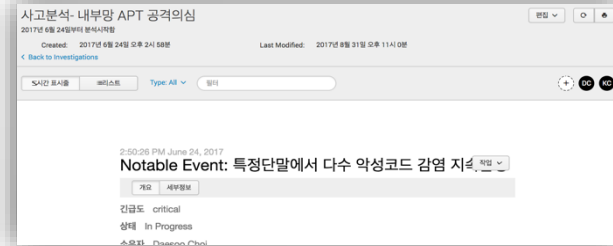
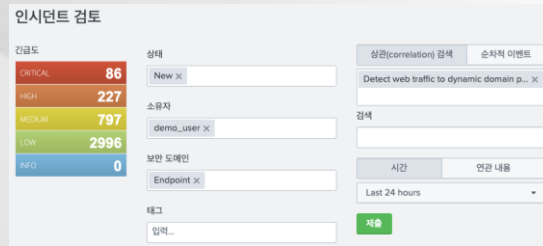
① 보안 포스처(Security Posture)

- 기업의 전체적인 보안 상태를 모니터링. 긴급도별, 위협별, 호스트별 주목할 만한 이벤트를 표시하며
- 중요 보안 지표(KSI)는 보안 포스처별로 실시간 트렌드를 모니터링



② 분석기반 SIEM 솔루션- 빠른 탐지 및 분석/대응

스플링크는 위협 인텔리전스와 상관분석 룰에 의하여 위협을 탐지하고, 침해사고를 분석 처리하고, 자동 대응하는 일련의 보안 관제 업무를 단일 플랫폼에서 지능적으로 빠르게 처리하고 관리



1 위협탐지

인시던트 검토 및 분석
상관관계분석 결과에 따른 긴급도 지원

3 침해사고 조사케이스 등록

첩보 및 장기간 분석 필요한 조사 등록
글래스테이블/핵심보안지표기반
심층분석이 필요한 항목 등록

5 즉각적 대응

단위보안솔루션에
조회, 차단, 블랙리스트 등록 등
대응 기능 수행 (Adaptive Response)

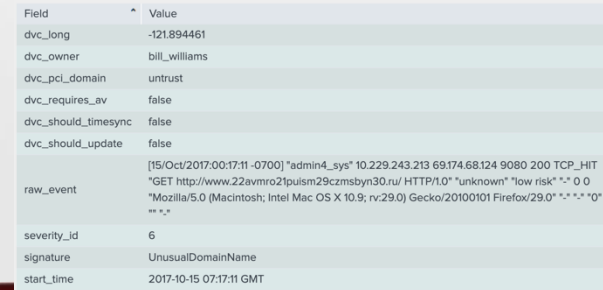
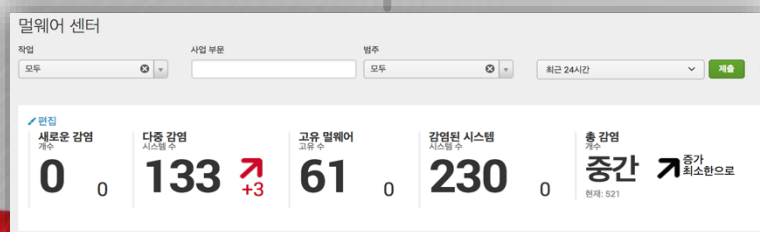


2 관제현황 시각화

핵심보안지표
글래스테이블, 임계치초과,
이상패턴 탐지

4 Deep-Dive 분석

조사 대상 (예, 웹공격탐지 등) 보안
컨텐츠와 관련된 대시보드를 결합하여
심층분석 업무 수행



③ 보안 콘텐츠 – ES Content Update

Use Case Library

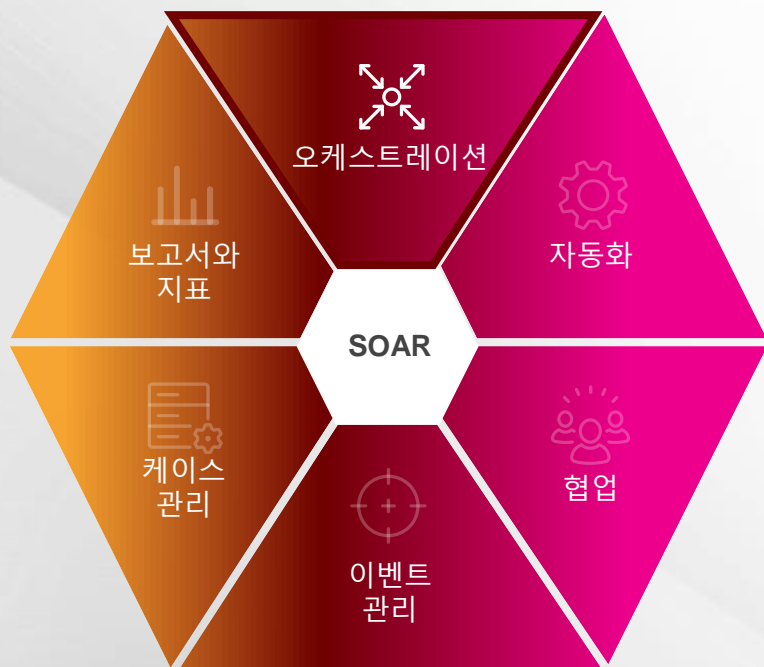
Explore the Analytic Stories included with Enterprise Security that provide analysis guidance on how to investigate and take actions on threats that ES detects.

Use Cases

Framework Mapping: All Data Model: All App: All In Use: All Bookmarked: All filter...

167 Analytic Stories found in categories: Cloud Security, Best Practices, Malware, Adversary Tactics, Vulnerability, Abuse

	i	In use	Analytic Story	Use Case	Description	App	Last Updated	Bookmark
Abuse	>	<input type="checkbox"/>	AWS Cross Account Activity	Cloud Security	Track when a user assumes an IAM role in another AWS account to obtain cross-account access to services and resources in that account. Accessing new roles could be an indication of malicious activity.	Splunk Security Essentials	Jun 4, 2018	<input type="checkbox"/>
	>	<input type="checkbox"/>	AWS Cryptomining	Cloud Security	Monitor your AWS EC2 instances for activities related to cryptojacking/cryptomining. New instances that originate from previously unseen regions, users who launch abnormally high numbers of instances, or EC2 instances started by previously unseen users are just a few examples of potentially malicious behavior.	Splunk Security Essentials	Mar 8, 2018	<input type="checkbox"/>
Adversary Tactics	>	<input type="checkbox"/>	AWS Defense Evasion	Cloud Security	Identify activity and techniques associated with the Evasion of Defenses within AWS, such as Disabling CloudTrail, Deleting CloudTrail and many others.	Splunk Security Essentials	Jul 15, 2022	<input type="checkbox"/>
	>	<input type="checkbox"/>	AWS IAM Privilege Escalation	Cloud Security	This analytic story contains detections that query your AWS Cloudtrail for activities related to privilege escalation.	Splunk Security Essentials	Mar 8, 2021	<input type="checkbox"/>
	>	<input type="checkbox"/>	AWS Identity and Access Management Account Takeover	Cloud Security	Identify activity and techniques associated with accessing credential files from AWS resources, monitor unusual authentication related activities to the AWS Console and other services such as RDS.	Splunk Security Essentials	Aug 19, 2022	<input type="checkbox"/>
Best Practices	>	<input type="checkbox"/>	AWS Network ACL Activity	Cloud Security	Monitor your AWS network infrastructure for bad configurations and malicious activity. Investigative searches help you probe deeper, when the facts warrant it.	Splunk Security Essentials	May 21, 2018	<input type="checkbox"/>
	>	<input type="checkbox"/>	AWS Security Hub Alerts	Cloud Security	This story is focused around detecting Security Hub alerts generated from AWS	Splunk Security Essentials	Aug 4, 2020	<input type="checkbox"/>
	>	<input type="checkbox"/>	AWS Suspicious Provisioning Activities	Cloud Security	Monitor your AWS provisioning activities for behaviors originating from unfamiliar or unusual locations. These behaviors may indicate that malicious activities are occurring somewhere within your network.	Splunk Security Essentials	Mar 16, 2018	<input type="checkbox"/>
Cloud Security	>	<input type="checkbox"/>	AWS User Monitoring	Cloud Security	Detect and investigate dormant user accounts for your AWS environment that have become active again. Because inactive and ad-hoc accounts are common attack targets, it's critical to enable governance within your environment.	Splunk Security Essentials	Mar 12, 2018	<input type="checkbox"/>
	>	<input type="checkbox"/>	Access Protection	Best Practices	Monitoring account activity and securing authentication are critical to enterprise security. This use case includes searches that detect suspicious account activity and alert you to the use of cleartext	DA-ESS-AccessProtection	Sep 13, 2018	<input type="checkbox"/>



오케스트레이션

SOC 업무 전반에 대한 복잡한 워크플로우를 조율

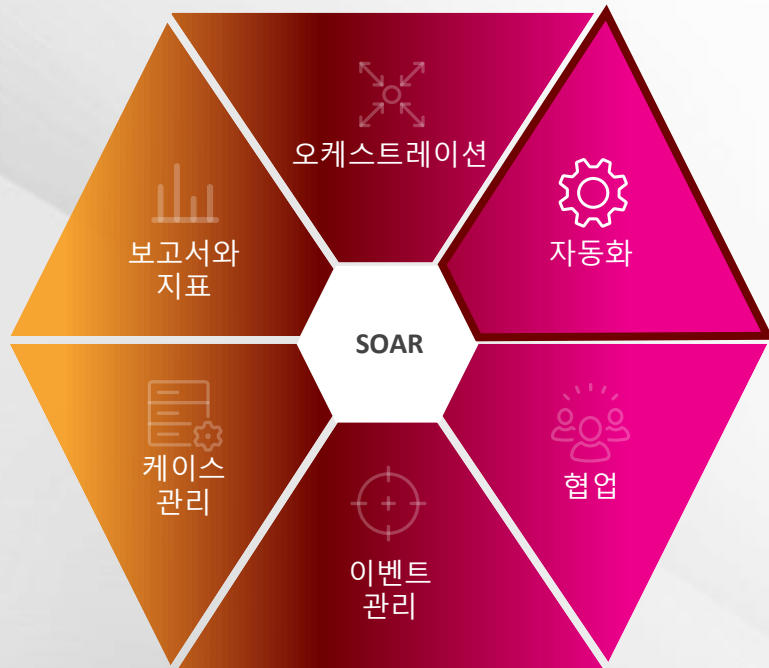
350+

APPS & GROWING

2150+

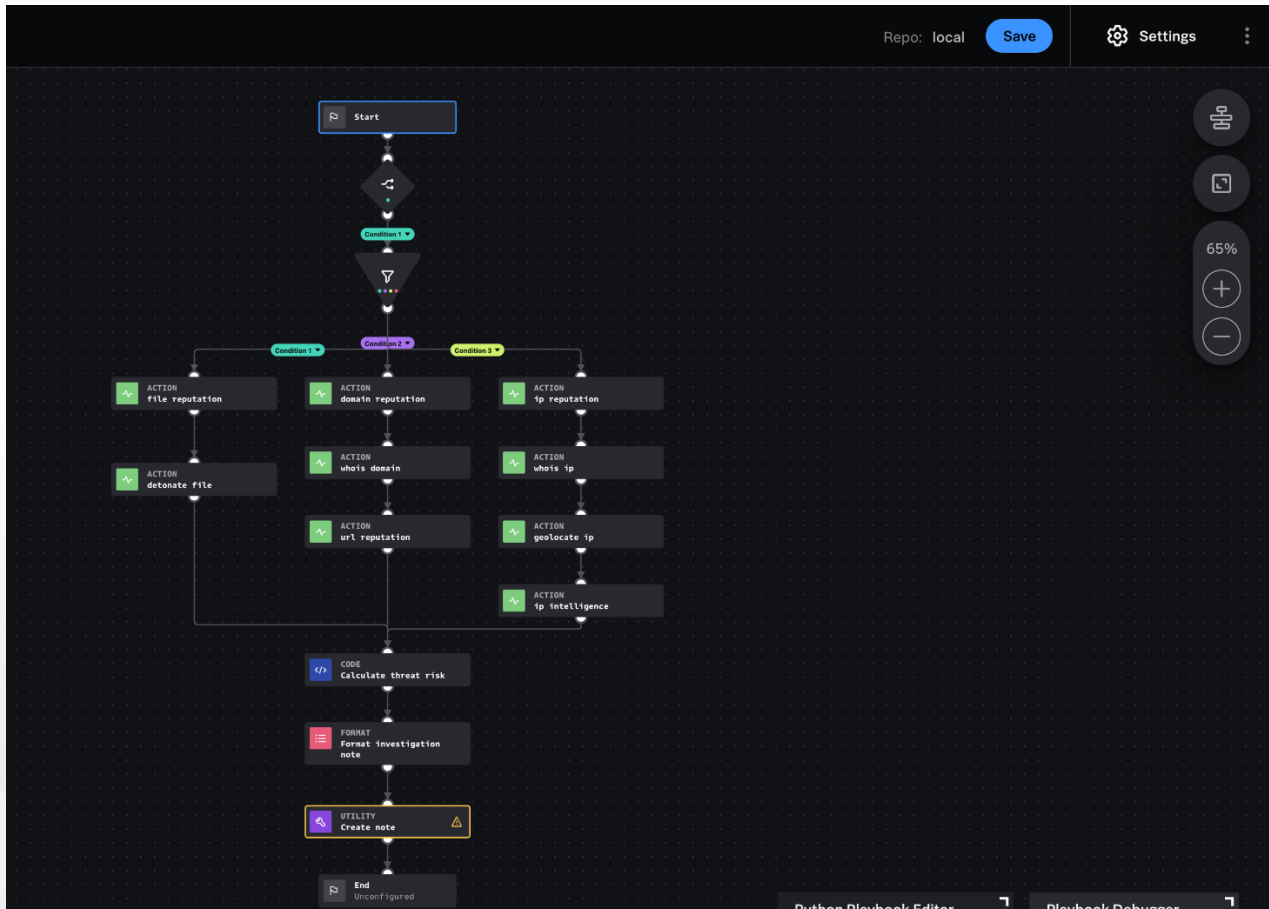
AUTOMATED ACTIONS





자동화

- 반복적 업무의 자동화를 통해 팀의 노력 대비 성과를 배가
- 자동화된 조치를 초 단위로 실행이 가능
- 사전 준비된 인텔리전스가 의사 결정을 지원



검증된 SIEM 솔루션

2022 IDC MarketScape for SIEM 에서 리더로 선정됨 (2022년 12월)

2022 Gartner MQ for SIEM 에서 리더로 9년 연속 선정됨 (2022년 6월)

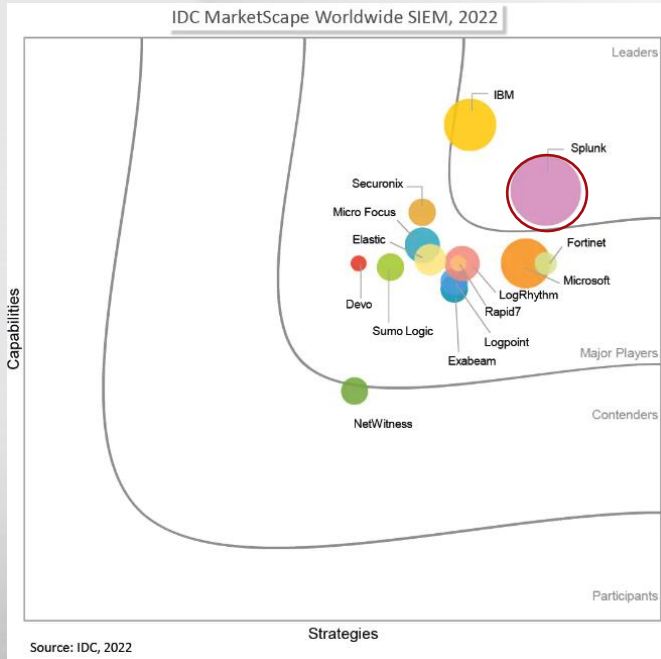
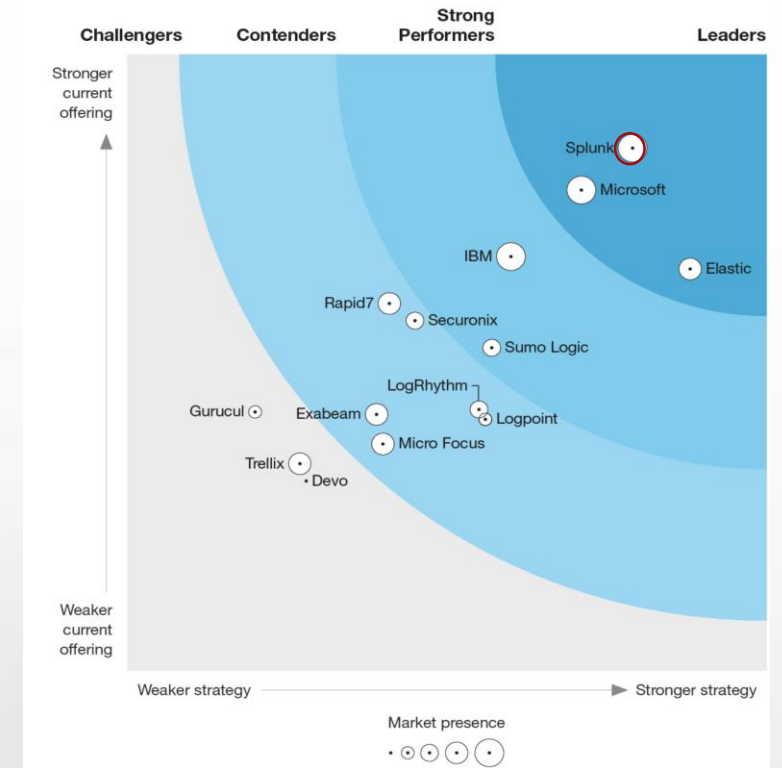


Figure 1: Magic Quadrant for Security Information and Event Management



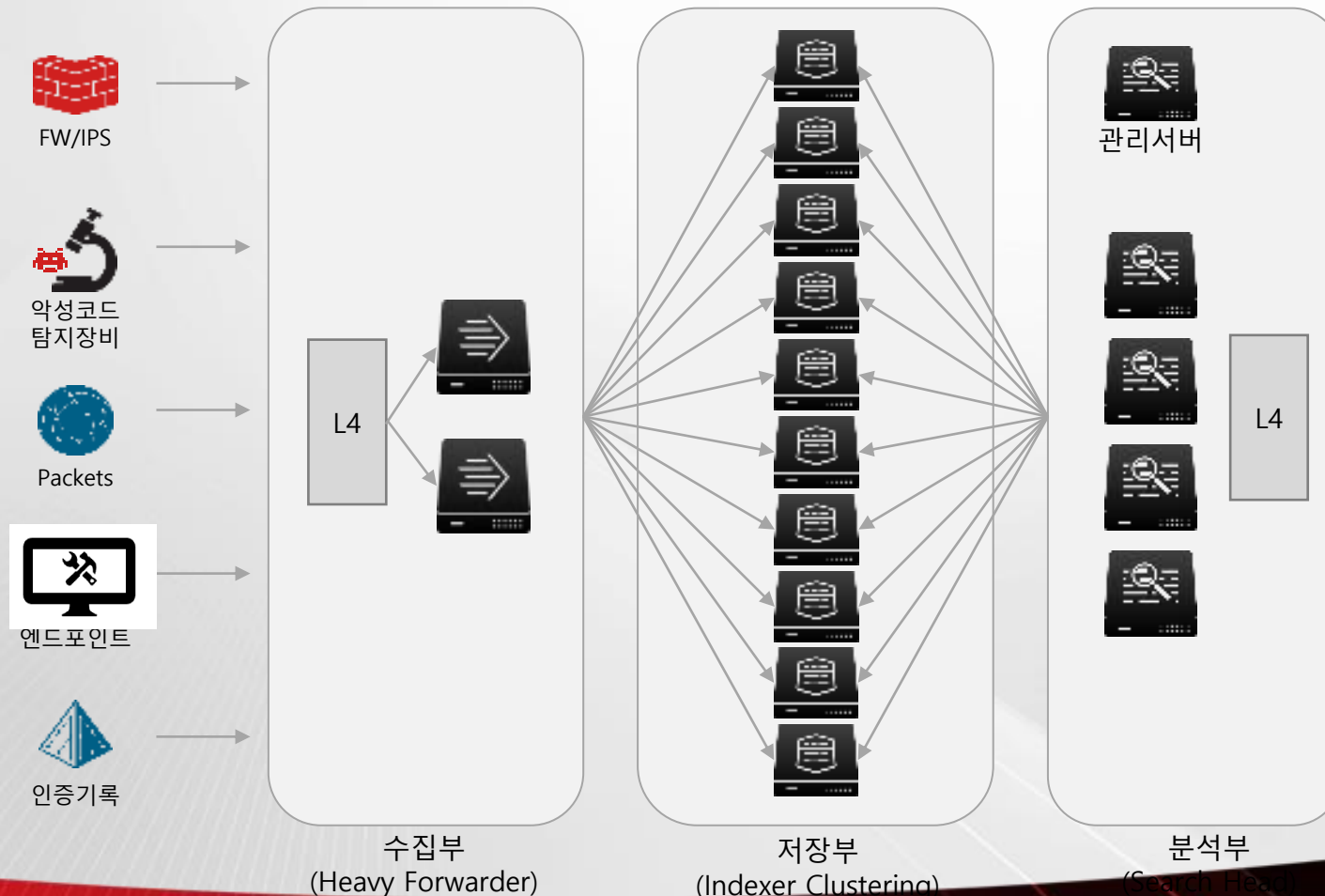
2022년 IDC 의 SIEM
Marketscape 최고 리더/마켓
쉐어 선정

2022년 Gartner 의 SIEM
매직쿼더런트에서 리더로 선정

2022년 Q4, Forrester 의
보안 분석 플랫폼 리더로 선정

Splunk 아키텍처

스플링크 빅데이터 플랫폼은 서버 대수와 성능에 비례하여 수집 및 분석 성능을 제공하며, 무한대로 확장 가능한 유연한 아키텍처를 제공

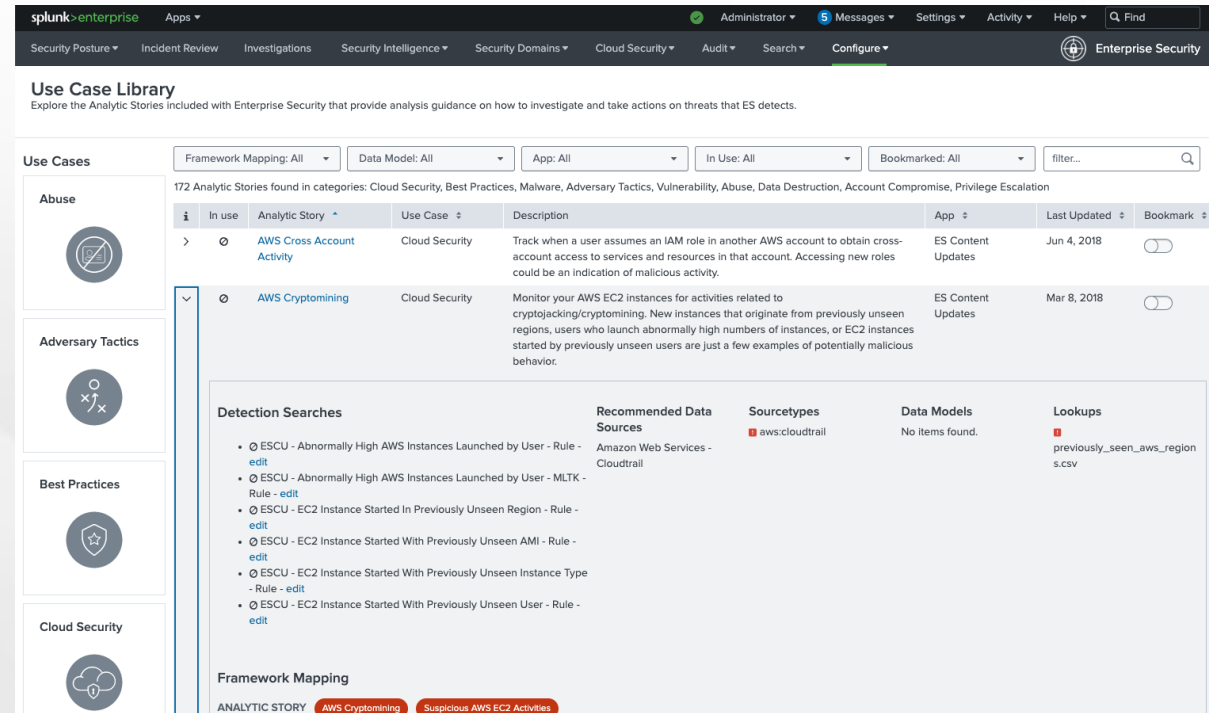
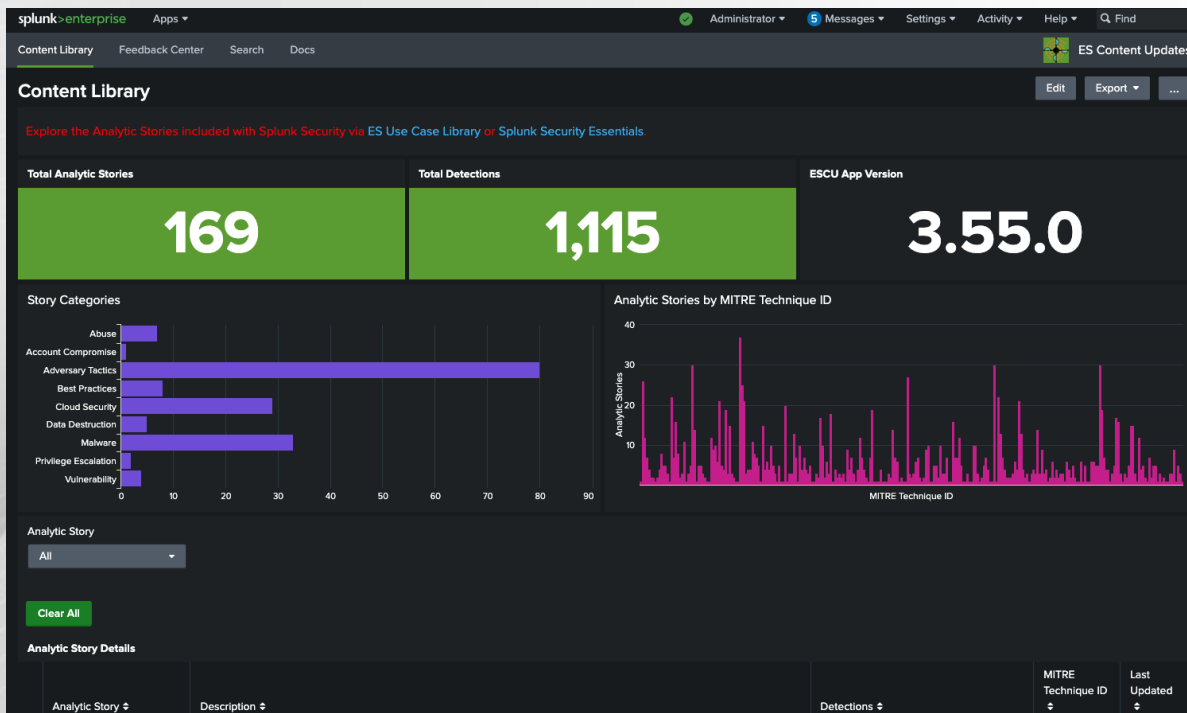


본 구성도는 예시로서 하루 데이터 수집 용량에 의해 변경됨. (1TB/일)

풍부한 보안컨텐츠 및 분석 기술

ESCU (Enterprise Security Content Update)

- Splunk ES 콘텐츠 업데이트(ESCU) 앱으로 사전 패키징된 보안 콘텐츠를 제공
- ESCU는 보안 실무자가 지속적으로 시간에 민감한 위협, 공격 방법 및 기타 보안 문제를 해결할 수 있도록 정기적인 보안 콘텐츠 업데이트를 제공 (약 월 2회)

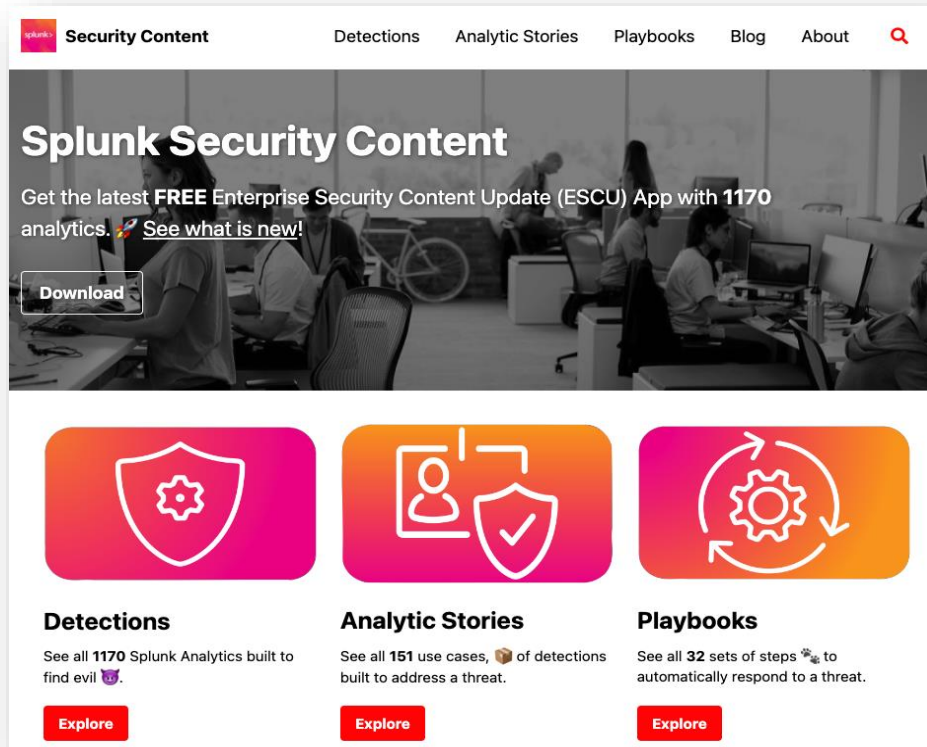


<https://github.com/splunk/security-content>.

신규 위협 연구 조직 및 공격 시뮬레이션 도구

STRT (Splunk Threat Research Team)

- 고객이 신규 위협을 빨리 탐지하고 조사 대응할수 있도록 지원하는 전문가 분석 및 인사이트 제공
- MITRE 프레임워크, Lockheed Martin Kill Chain 및 CIS 컨트롤에 매핑된 TTP에 대한 배경 정보를 함께 제공
 - ES Correlation Rules / Splunk SOAR Playbook 제공



Splunk Security Content

Get the latest **FREE** Enterprise Security Content Update (ESCU) App with **1170** analytics. [See what is new!](#)

[Download](#)

Detections
See all **1170** Splunk Analytics built to find evil 🦋.

[Explore](#)

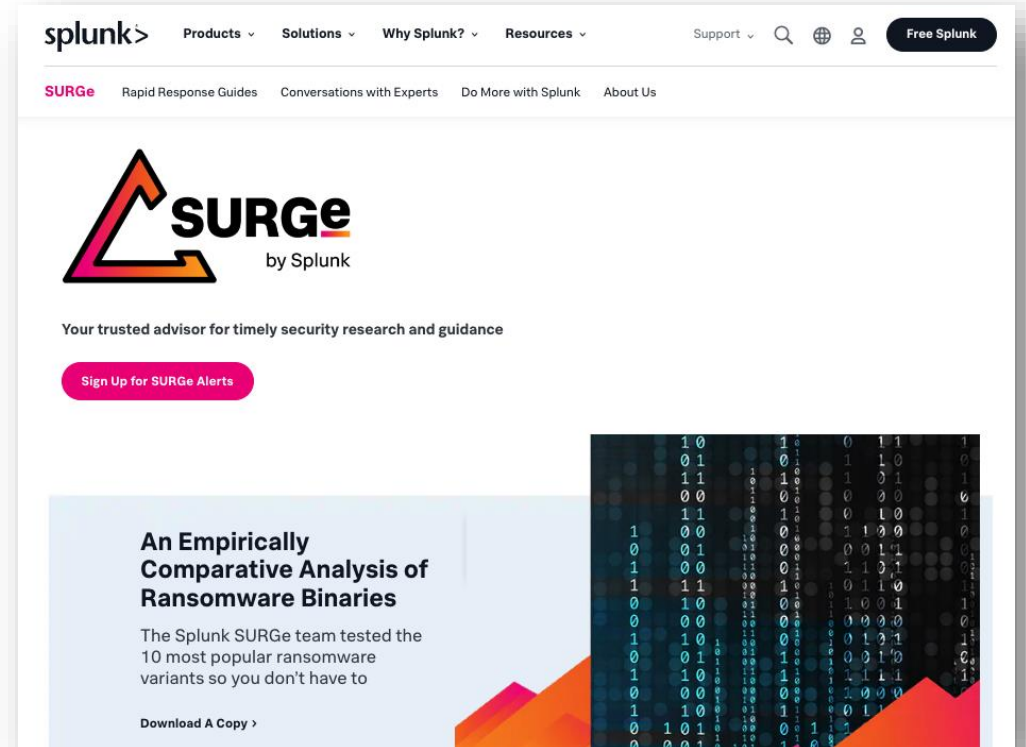
Analytic Stories
See all **151** use cases, 📦 of detections built to address a threat.

[Explore](#)

Playbooks
See all **32** sets of steps 🔄 to automatically respond to a threat.

[Explore](#)

<https://research.splunk.com/>



splunk> Products Solutions Why Splunk? Resources Support

SURGE Rapid Response Guides Conversations with Experts Do More with Splunk About Us

SURGE by Splunk

Your trusted advisor for timely security research and guidance

[Sign Up for SURGE Alerts](#)

An Empirically Comparative Analysis of Ransomware Binaries

The Splunk SURGE team tested the 10 most popular ransomware variants so you don't have to

[Download A Copy >](#)

<https://splunk.com/surge>

Log4j Respond

[Try in Splunk SOAR](#)

Description

Published in response to CVE-2021-44228, this playbook is meant to be launched after log4j_investigate. In this playbook, the risk from exploited hosts can be mitigated by optionally deleting malicious files from the hosts, blocking outbound network connections from the hosts, and/or shutting down the hosts

- **Type:** Response
- **Product:** Splunk SOAR
- **Apps:**
- **Last Updated:** 2021-12-14
- **Author:** Philip Royer, Splunk
- **ID:** e609d729-4076-421a-b8f7-9e545d000381

Associated Detections

- [Curl Download and Bash Execution](#)
- [Wget Download and Bash Execution](#)
- [Linux Java Spawning Shell](#)
- [Java Class File download by Java User Agent](#)
- [Outbound Network Connection from Java Using Default Ports](#)
- [Log4Shell JNDI Payload Injection Attempt](#)

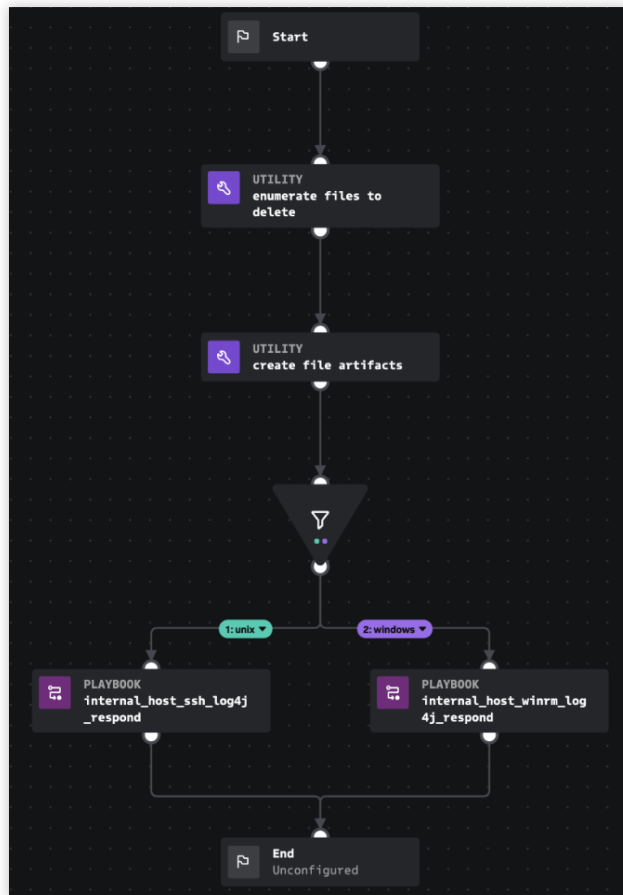
On this page

[Description](#)[Associated Detections](#)[How To Implement](#)[Explore Playbook](#)[Required field](#)[Reference](#)

How To Implement

To use this playbook, create a custom list called "log4j_hosts_and_files" with a format in which the first column should be an IP or hostname of a potentially affected log4j host, the second should be the operating system family (either unix or windows), and the third should be a full path to a file to delete if there are any. The first two are mandatory and the file is optional. In the block called "enumerate_files_to_delete", change the custom list name from "log4j_hosts_and_files" if needed. If ssh and/or winrm are not the preferred endpoint management methods, these playbooks could be ported to use Google's GRR, osquery, CrowdStrike's RTR, Carbon Black's EDR API, or similar tools. The artifact scope "all" is used throughout this playbook because the artifact list can be added to as the playbook progresses.

Explore Playbook



Required field

Splunk SOAR Playbook Explorer

Beta

Name
log4j_respond

Description
Published in response to CVE-2021-44228, this playbook is meant to be launched by log4j_investigate. In this playbook, the risk from an exploited host can be mitigated by optionally deleting malicious files from the hosts, blocking outbound network connections from the hosts, and/or shutting down the hosts.

Notes
* To use this playbook, create a custom list called "log4j_hosts_and_files" with a format like: hostname1 | unix | /full/path/to/delete/on/hostname_1 1.1.1.1 | windows | C:\\Full\\Path\\To\\Delete\\On\\1_1_1_1 * In other words, the first column should be an IP or hostname of a potentially affected log4j host, the second should be the operating system family (either unix or windows), and the third should be a full path to a file to delete if there are any. The first two are mandatory and the file is optional. * In the block called "enumerate_files_to_delete", change the custom list name from "log4j_hosts_and_files" if needed * If ssh and/or winrm are not the preferred endpoint management methods, these playbooks could be ported to use Google's GRR, osquery, CrowdStrike's RTR, Carbon Black's EDR API, or similar tools. * The artifact scope "all" is used throughout this playbook because the artifact list can be added to as the playbook progresses.

Playbook Type
automation

```
graph TD; Start[Start] --> Enumerate[UTILITY: enumerate_files_to_delete]; Enumerate --> Create[UTILITY: create_file_artifacts]; Create --> Filter{ }; Filter --> Unix[1: unix]; Filter --> Windows[2: windows]; Unix --> Ssh[PLAYBOOK: playbook_internal_host_ssh_log4j_respond_2]; Windows --> Winrm[PLAYBOOK: playbook_internal_host_winrm_log4j_respond_2]; Ssh --> End[End]; Winrm --> End;
```


신규 위협 연구 조직 및 공격 시뮬레이션 도구

Attack Range (공격 시뮬레이션 도구)

- 사용자는 프로덕션 환경에 최대한 가까운 소규모 랩 인프라를 신속하게 구축할
- 여러 보안 도구 및 로깅 구성이 미리 구성된 Windows 도메인 컨트롤러, Windows 워크스테이션 및 Linux 서버가 포함
- 인프라는 서로 다른 서버에서 여러 로그 소스를 수집하는 Splunk 서버와 함께 제공
- https://github.com/splunk/attack_range
- <https://attack-range.readthedocs.io/en/latest/>



테스트랩 구성



공격 시뮬레이션



탐지 테스트



3. Trend Micro XDR + Splunk 연동

Trend Micro App for Splunk ES, Splunk SOAR

PLATFORM Clear Showing 1-16 of 16 Results for **Trend Micro** × Sort By Best Match ▼

SPLUNK

> PRODUCT

> VERSION

SPLUNK SOAR

> PRODUCT

> VERSION

CATEGORY

- IT Operations
- Security, Fraud & Compliance
- Business Analytics
- Utilities
- IoT & Industrial Data
- DevOps
- Directory Service
- Email
- Endpoint
- Firewall
- Generic
- Identity Management
- Information
- Investigative
- Network Access Control

Filtered by: **Splunk** ×

<p>Trend Micro Risk Insights for Splunk By Trend Micro</p> <p>Trend Micro Risk Insights for Splunk extracts website access logs from Splunk and uploads the data to Trend...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ★★★★★ (2)</p> <p> DEVELOPER SUPPORTED APP</p>	<p>Trend Micro Threat Indicator Assessment for... By Trend Micro</p> <p>Trend Micro Threat Indicator Assessment for Splunk scans endpoint activity data for Splunk and uploads the data to Trend...</p> <p>PLATFORM Splunk Enterprise</p> <p>RATING ★★★★★ (0)</p> <p> DEVELOPER SUPPORTED APP</p>	<p>Trend Micro Vision One for Splunk (XDR) By Trend Micro</p> <p>The Trend Micro Vision One for Splunk (XDR) add-on allows you to view all your XDR data directly on the Splunk...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ★★★★★ (4)</p> <p> DEVELOPER SUPPORTED APP</p>
<p>Trend Micro Cloud App Security Add-On By Trend Micro</p> <p>The Trend Micro Cloud App Security Add-On allows you to view the security detection statistics of your protected...</p> <p>PLATFORM Splunk Enterprise</p> <p>RATING ★★★★★ (1)</p> <p> DEVELOPER SUPPORTED ADDON</p>	<p>Trend Micro Email Security for Splunk (TMES) By Anderson Silva</p> <p>The app Trend Micro Email Security (Formerly TMES) can help with a variety of situations. You can make a query faster...</p> <p>PLATFORM Splunk Enterprise</p> <p>RATING ★★★★★ (0)</p> <p> NOT SUPPORTED</p>	<p>TA for Trend Micro OfficeScan By Dmytro Sobolita</p> <p>This TA for Splunk provides field extractions from Trend Micro OfficeScan logs and mapping to the Malware CIM...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ★★★★★ (2)</p> <p> DEVELOPER SUPPORTED ADDON</p>
<p>CCX Unified Splunk Add-on for Trend Micro By Henrique Linsmeyer</p> <p>About Us: CyberCX is Australia's greatest force of cyber security experts. Our highly skilled professional services tea...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ★★★★★ (17)</p>	<p>Trend Micro - InterScan Messaging Security (IMSV...) By Splunk Works</p> <p>Trend InterScan Messaging Security (IMSV) Technology Add-on (TA) for Splunk provides knowledge object...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ★★★★★ (0)</p>	<p>Trend Micro Deep Security for Splunk By Trend Micro</p> <p>This package contains parsing logic, saved searches, and dashboards for monitoring Trend Micro Deep Security...</p> <p>PLATFORM Splunk Enterprise, Splunk Cloud</p> <p>RATING ★★★★★ (5)</p>

PLATFORM Clear Showing 1-2 of 2 Results for **Trend Micro** ×

SPLUNK

> PRODUCT

> VERSION

SPLUNK SOAR

▼ PRODUCT Clear

- SOAR On-Prem
- SOAR Cloud

> VERSION

Filtered by: **Splunk SOAR** × **Product > SOAR On-Prem** × **Product > SOAR Cloud** ×

<p>Trend Micro Vision One for Splunk SOAR By SOAR Community</p> <p>Trend Micro Vision One is a purpose-built threat defense platform that provides added value and new benefits beyond...</p> <p>PLATFORM SOAR On-Prem, SOAR Cloud</p> <p>RATING ★★★★★ (0)</p> <p> DEVELOPER SUPPORTED CONNECTOR</p>	<p>Trend Micro Apex One By SOAR Community</p> <p>This app provides investigative and containment actions for Trend Micro Apex One</p> <p>PLATFORM SOAR On-Prem, SOAR Cloud</p> <p>RATING ★★★★★ (0)</p> <p> NOT SUPPORTED</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Splunk 연동 - Vision One XDR app



Splunk Enterprise Security™

Splunk ES

Splunk SOAR

Vision One for Splunk (XDR)

Alert #	Score	Workbench ID #	Model #	Model severity	Created #	Details #	Link #
1	26	46-10707-20220820-00001	Suspicious SMB Connection Initiated	Low	2022-08-20 15:28:22	1	Open Trend Micro Vision One Console
2	26	46-10707-20220820-00001	Suspicious SMB Connection Initiated	Low	2022-08-20 15:28:12	1	Open Trend Micro Vision One Console
3	26	46-10707-20220820-00001	Suspicious SMB Connection Initiated	Low	2022-08-20 15:28:12	1	Open Trend Micro Vision One Console

Workbench

Score	Workbench ID	Model	Model severity	Impact scope
61	WB-10003-20220820-00001	Early Indicator of Lockbit Ransomware Attack	High	1
46	WB-10003-20220827-00000	Suspicious Internet Connection	Medium	1
21	WB-10003-20220820-00000	Hacking Tool Detection	Low	1

Observed Attack Techniques

Associated endpoint	Risk level	Detection filter	Description	Tactic	Technique
XDR-TOM-PC (2400:4010:413...	Low	Service Modification Via Pow...	Service Modification vi...	TA0003, TA00...	T1543.003
XDR-SAM-PC (2400:4010:413...	Low	Dll Loading From Uncommo...	Detects dll loaded form...	TA0004, TA00...	T1548.002
XDR-SAM-PC (2400:4010:413...	Medium	Auto-start Via Browser Helpe...	Detect created auto-sta...	TA0003, TA00...	T1547.001

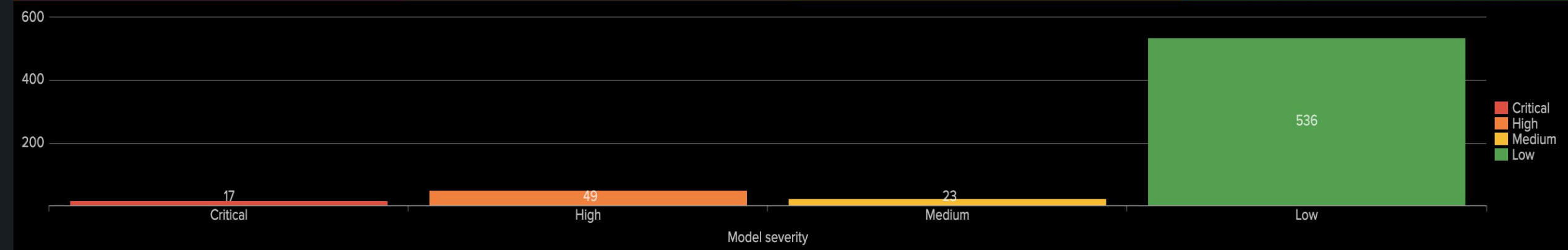
- Vision One의 SAE(보안 분석 엔진)에서 감지된 경고 및 로그를 API를 통해 SIEM에 동기화

Trend Micro의 분석 결과 경고를 포함한 보안 이벤트의 통합 관리 실현

Workbench Alerts

Period View graph

All time ▾ Show Hide



	Status ▾	Score ▾	Workbench ID ▾	Model ▾	Model severity ▾	Created ▾	Details ▾	Link ▾
1	New	47	WB-2-20230810-00013	Suspicious Web Access After Suspicious Email	Medium	2023-08-10T02:09:18Z	View	Open Trend Micro Vision One Console
2	New	87	WB-2-20230810-00014	Possible APT Attack	Critical	2023-08-10T02:09:17Z	View	Open Trend Micro Vision One Console
3	New	64	WB-2-20230810-00012	UAC Bypass - Windows Telemetry	High	2023-08-10T02:03:18Z	View	Open Trend Micro Vision One Console
4	New	64	WB-2-20230810-00011	Privilege Escalation via UAC Bypass	High	2023-08-10T02:03:18Z	View	Open Trend Micro Vision One Console
5	New	24	WB-2-20230810-00010	Suspicious Script Execution via LNK File with Double Extensions	Low	2023-08-10T02:02:54Z	View	Open Trend Micro Vision One Console

Observed Attack Techniques

Period View graph

Last 24 hours Show Hide



Generated	Detection	Risk level	Event ID	Endpoint	Techniques
1 2023-08-17T11:36:51Z	test filter	Critical	0215141c-bbfc-5698-b7cd-3c72fb16c52f	fe80::b8a8:ec0:9ed3:fe9a 169.254.44.176 fe80::7366:91a4:3ab:8532 169.254.0.2 fe80::6408:c3fc:5d8c:da86 10.64.18.189 fe80::6e90:c31a:b2f7:11b6 169.254.113.196 ::1 127.0.0.1	

Audit Logs

Period

Last 30 days ▾

	Logged ↕	Account ↕	Role ↕	Source ↕	Category ↕	Activity ↕	Result ↕	Details ↕
1	2023-08-10T08:44:51Z	XDR DEMO	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "18.162.171.88"}
2	2023-08-10T08:25:55Z	joya liu	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "18.162.103.100"}
3	2023-08-10T08:01:35Z	XDR DEMO	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "18.162.171.88"}
4	2023-08-10T07:38:39Z	XDR DEMO	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "18.162.171.88"}
5	2023-08-10T07:13:30Z	XDR DEMO	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "18.162.220.99"}
6	2023-08-10T06:55:37Z	XDR DEMO	Master Administrator	Console	API Keys	Add API Key	Successful	{"Name": "test jd", "RoleName": "Master Administrator"}
7	2023-08-10T06:51:02Z	API key	SIEM	API	Observed Attack Techniques	Register to data pipeline	Successful	{"riskLevels": ["high", "critical"], "hasDetail": true, "Description": "Trend Vision One for Splunk (XDR)"}
8	2023-08-10T06:27:53Z	XDR DEMO	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "18.162.171.88"}
9	2023-08-10T06:12:15Z	XDR DEMO	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "18.162.220.99"}
10	2023-08-10T05:34:18Z	XDR DEMO	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "18.162.171.88"}
11	2023-08-10T05:26:56Z	XDR DEMO	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "18.162.220.99"}
12	2023-08-10T05:15:22Z	FED Luwak	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "61.216.248.199"}
13	2023-08-10T04:36:22Z	XDR DEMO	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "142.126.80.105"}
14	2023-08-10T04:26:06Z	XDR DEMO	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "18.162.103.100"}
15	2023-08-10T03:33:17Z	XDR DEMO	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "142.126.80.105"}
16	2023-08-10T03:27:20Z	XDR DEMO	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "18.162.103.100"}
17	2023-08-10T03:23:18Z	joya liu	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "18.162.220.99"}
18	2023-08-10T03:16:17Z	XDR DEMO	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "18.162.220.99"}
19	2023-08-10T03:05:50Z	XDR DEMO	Master Administrator	Console	Logon and Logoff	Log on	Successful	{"IP address": "18.162.220.99"}



Trend Micro Vision One for Splunk SOAR Publisher: Trend Micro Version: 2.1.0 [Documentation](#)

[CONFIGURE NEW ASSET](#)[ASSOCIATED PLAYBOOKS](#)

Trend Micro Vision One is a purpose-built threat defense platform that provides added value and new benefits beyond XDR solutions, allowing you to see more and respond faster. Providing deep and broad extended detection and response (XDR) capabilities that collect and automatically correlate data across multiple security layers—email, endpoints, servers, cloud workloads, and networks—Trend Micro Vision One prevents the majority of attacks with automated protection

▼ 34 supported actions

- **get exception list** - Retrieves information about domains, file SHA-1, file SHA-256, IP addresses, sender addresses, or URLs in the Exception List and displays it in a paginated list
- **get suspicious list** - Retrieves information about domains, file SHA-1, file SHA-256, IP addresses, email addresses, or URLs in the Suspicious Object List and displays the information in a paginated list
- **sandbox investigation package** - Downloads the Investigation Package of the specified object
- **sandbox analysis result** - Displays the analysis results of the specified object
- **sandbox suspicious list** - Downloads the suspicious object list associated to the specified object
- **force password reset** - Signs the user out of all active application and browser sessions, and forces the user to create a new password during the next sign-in attempt
- **sign out account** - Signs the user out of all active application and browser sessions
- **restore email message** - Restore quarantined email messages
- **disable account** - Signs the user out of all active application and browser sessions, and prevents the user from signing in any new session
- **enable account** - Allows the user to sign in to new application and browser sessions
- **urls to sandbox** - Submits URLs to the sandbox for analysis
- **get alert details** - Displays information about the specified alert
- **update status** - Updates the status of an existing workbench alert
- **add note** - Adds a note to an existing workbench alert
- **start analysis** - Submit file to sandbox for analysis
- **forensic file info** - Get the download information for collected forensic file
- **collect forensic file** - Collect forensic file
- **download analysis report** - Get the analysis report of a file based on report id
- **check analysis status** - Get the status of file analysis based on task id
- **delete from suspicious** - Delete the suspicious object from suspicious list
- **add to suspicious** - Add suspicious object to suspicious list
- **delete from exception** - Delete object from exception list
- **add to exception** - Add object to exception list
- **terminate process** - Terminate the process running on the endpoint
- **delete email message** - Delete the email message
- **quarantine email message** - Quarantine the email message
- **remove from blocklist** - Removes an item from the Suspicious Objects list
- **add to blocklist** - Adds an item to the Suspicious Objects list in Vision One
- **status check** - Checks the status of a task
- **on poll** - Callback action for the on_poll ingest functionality
- **unquarantine device** - Unquarantine the endpoint
- **quarantine device** - Quarantine the endpoint
- **get endpoint info** - Gather information about an endpoint
- **test connectivity** - Validate the asset configuration for connectivity using supplied configuration

4. 멀티 클라우드 환경 통합보안관제 방안

Multi-Cloud Visibility

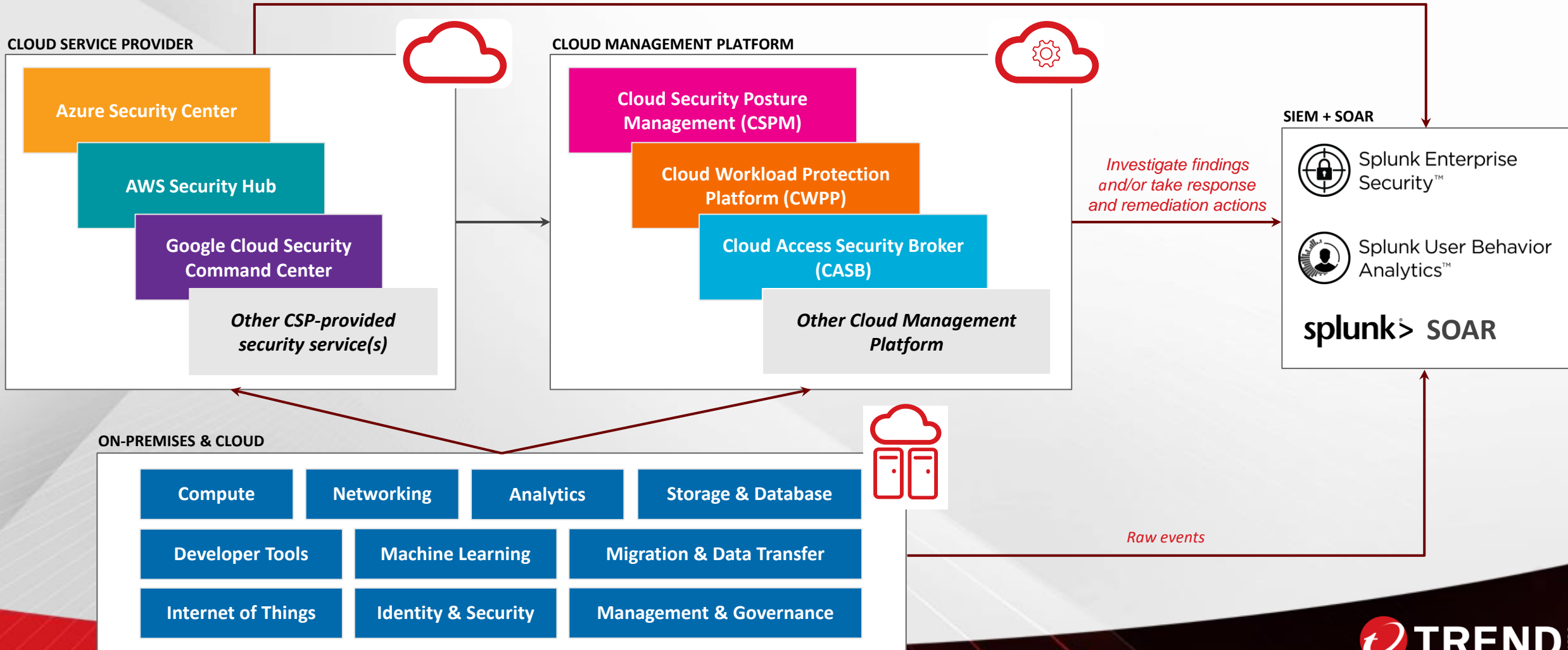


Monitor, investigate and detect vulnerabilities & misconfigurations across cloud environments

Visualize and analyze multi-cloud threat surfaces and vulnerabilities

Establish & enhance tools for cloud auditing across multiple cloud providers

Centralize Data and Findings From All Providers

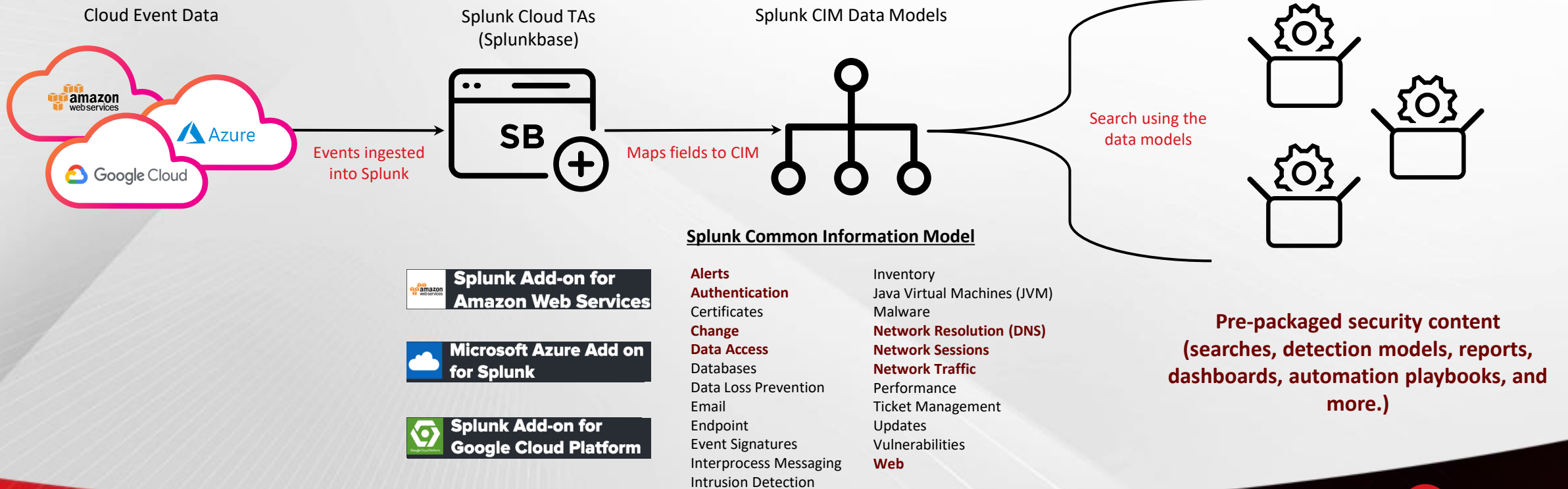


Cloud Data Flow

Data Collection

Data Normalization

Investigate, Monitor,
Analyze, Act



MITRE Cloud Matrix

Initial Access 5 techniques	Execution 1 techniques	Persistence 5 techniques	Privilege Escalation 2 techniques	Defense Evasion 6 techniques	Credential Access 5 techniques	Discovery 10 techniques	Lateral Movement 2 techniques	Collection 4 techniques	Exfiltration 1 techniques	Impact 6 techniques
<ul style="list-style-type: none"> Drive-by Compromise Exploit Public-Facing Application Phishing (1) Trusted Relationship Valid Accounts (2) 	<ul style="list-style-type: none"> User Execution (1) 	<ul style="list-style-type: none"> Account Manipulation (3) Create Account (1) Implant Internal Image Office Application Startup (6) Valid Accounts (2) 	<ul style="list-style-type: none"> Domain Policy Modification (1) Valid Accounts (2) 	<ul style="list-style-type: none"> Domain Policy Modification (1) Impair Defenses (3) Modify Cloud Compute Infrastructure (4) Unused/Unsupported Cloud Regions Use Alternate Authentication Material (2) Valid Accounts (2) 	<ul style="list-style-type: none"> Brute Force (4) Forge Web Credentials (2) Steal Application Access Token Steal Web Session Cookie Unsecured Credentials (2) 	<ul style="list-style-type: none"> Account Discovery (2) Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Network Service Scanning Permission Groups Discovery (1) Software Discovery (1) System Information Discovery System Location Discovery System Network Connections Discovery 	<ul style="list-style-type: none"> Internal Spearphishing Use Alternate Authentication Material (2) 	<ul style="list-style-type: none"> Data from Cloud Storage Object Data from Information Repositories (2) Data Staged (1) Email Collection (2) 	<ul style="list-style-type: none"> Transfer Data to Cloud Account 	<ul style="list-style-type: none"> Data Destruction Data Encrypted for Impact Defacement (1) Endpoint Denial of Service (3) Network Denial of Service (2) Resource Hijacking

Last modified: 29 April 2021

Source: <https://attack.mitre.org/matrices/enterprise/cloud/>

MITRE Cloud Matrix: **Change** Example

Initial Access 5 techniques	Execution 1 techniques	Persistence 5 techniques	Privilege Escalation 2 techniques	Defense Evasion 6 techniques	Credential Access 5 techniques	Discovery 10 techniques	Lateral Movement 2 techniques	Collection 4 techniques	Exfiltration 1 techniques	Impact 6 techniques
Drive-by Compromise	User Execution (1)	Account Manipulation (3)	Domain Policy Modification (1)	Domain Policy Modification (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing Use Alternate Authentication Material (2)	Data from Cloud Storage Object	Transfer Data to Cloud Account	Data Destruction
Exploit Public-Facing Application		Create Account (1)	Valid Accounts (2)	Impair Defenses (3)	Forge Web Credentials (2)	Cloud Infrastructure Discovery		Data from Information Repositories (2)		Data Encrypted for Impact
Phishing (1)		Implant Internal Image		Modify Cloud Compute Infrastructure (4)	Steal Application Access Token	Cloud Service Dashboard		Data Staged (1)		Defacement (1)
Trusted Relationship		Office Application Startup (6)	Unused/Unsupported Cloud Regions	Steal Web Session Cookie	Cloud Service Discovery	Network Service Scanning		Email Collection (2)		Endpoint Denial of Service (3)
Valid Accounts (2)		Valid Accounts (2)	Use Alternate Authentication Material (2)	Unsecured Credentials (2)	Permission Groups Discovery (1)	Software Discovery (1)				Network Denial of Service (2)
			Valid Accounts (2)			System Information Discovery			Resource Hijacking	
						System Location Discovery				
						System Network Connections Discovery				

Last modified: 29 April 2021

Source: <https://attack.mitre.org/matrices/enterprise/cloud/>

Detection Logic

Threat-Based Monitoring Plan: **Change**

INFRA COMPONENT	THREAT	SERVICE (VENDOR)	DETECTION LOGIC
CRUD ACTIVITIES	<i>Provisioning activity from unusual regions</i> (MITRE Cloud ATT&CK Matrix: Defense Evasion: Unsupported/Unused Cloud Regions)	EC2 (AWS)	Summarize a count per API (create/activate/run/attach) by source IP address. Examples: <ul style="list-style-type: none"> ● SSE/ESCU: Cloud Provisioning from Previously Unseen Country / City / Region
		Virtual Machines (Azure)	
		Compute Engine (GCP)	
	<i>Abnormally high number of instances launched by user</i> (MITRE Cloud ATT&CK Matrix: Impact: Resource Impact)	EC2 (AWS)	Summarize a count per API (create/activate/run/attach) by user. Examples: <ul style="list-style-type: none"> ● ESCU: Detect Spike in API Activity ● UBA: Multiple Cloud Operations
		Virtual Machines (Azure)	
		Compute Engine (GCP)	

SSE: Splunk Security Essentials App

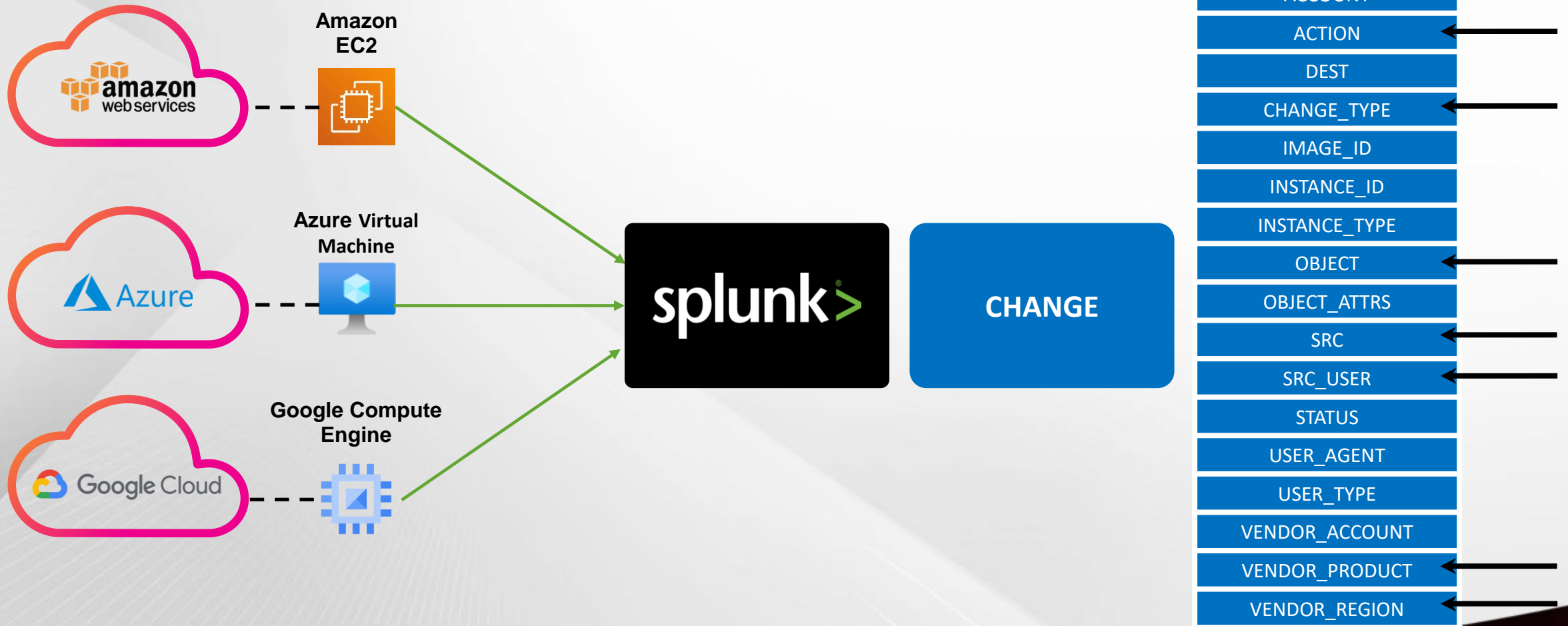
ESCU: Splunk Enterprise Security Content Update

UBA: Splunk User and Entity Behavior Analytics

and so on ...

Splunk Multi-Cloud Monitoring Example: **Change**

Monitor Create, Read, Update and Delete activities across environments



<https://docs.splunk.com/Documentation/CIM/latest/User/Change>

MITRE Cloud Matrix: Network (DNS) Example

Initial Access 5 techniques	Execution 1 techniques	Persistence 5 techniques	Privilege Escalation 2 techniques	Defense Evasion 6 techniques	Credential Access 5 techniques	Discovery 10 techniques	Lateral Movement 2 techniques	Collection 4 techniques	Exfiltration 1 techniques	Impact 6 techniques
Drive-by Compromise	User Execution (1)	Account Manipulation (3)	Domain Policy Modification (1)	Domain Policy Modification (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Cloud Storage Object	Transfer Data to Cloud Account	Data Destruction
Exploit Public-Facing Application		Create Account (1)	Valid Accounts (2)	Impair Defenses (3)	Forge Web Credentials (2)	Cloud Infrastructure Discovery		Use Alternate Authentication Material (2)		Data from Information Repositories (2)
Phishing (1)		Implant Internal Image		Modify Cloud Compute Infrastructure (4)	Steal Application Access Token	Cloud Service Dashboard	Data Staged (1)			Defacement (1)
Trusted Relationship		Office Application Startup (6)	Unused/Unsupported Cloud Regions	Steal Web Session Cookie	Cloud Service Discovery	Cloud Service Discovery	Email Collection (2)	Endpoint Denial of Service (3)		
Valid Accounts (2)		Valid Accounts (2)	Use Alternate Authentication Material (2)	Unsecured Credentials (2)	Network Service Scanning	Permission Groups Discovery (1)		Network Denial of Service (2)		
				Valid Accounts (2)		Software Discovery (1)		Resource Hijacking		
						System Information Discovery				
						System Location Discovery				
						System Network Connections Discovery				

Last modified: 29 April 2021

Source: <https://attack.mitre.org/matrices/enterprise/cloud/>

Detection Logic

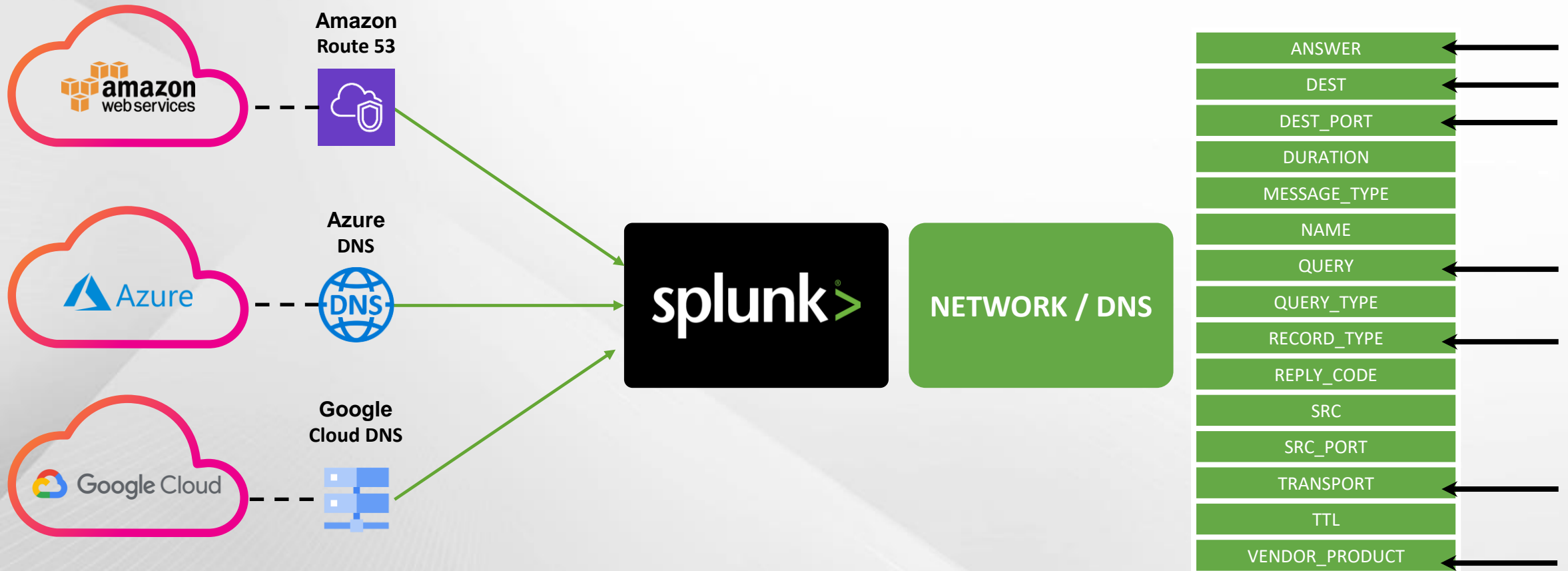
Threat-Based Monitoring Plan: Network (DNS)

INFRA COMPONENT	THREAT	SERVICE (VENDOR)	DETECTION LOGIC
DNS	<i>Query to suspicious (rare domains, young domains, non-existent domains, high entropy, etc.) / known-bad domains (CnC, bots, malware, cryptomining, etc.)</i>	Route 53 (AWS)	Collect DNS query and response data from endpoints (instances, VMs) and correlate resulting IP with threat intel, entropy analysis (DGA), registration data, etc.
		DNS (Azure)	
		Cloud DNS (GCP)	
	<i>Query spikes</i>	Route 53 (AWS)	Collect DNS query and response data from endpoints and provider DNS service to baseline domains queried by client as well as time of day.
		DNS (Azure)	
		Cloud DNS (GCP)	

and so on ...

Splunk Multi-Cloud Monitoring Example: Network (DNS)

Centralize network data across all cloud providers



<https://docs.splunk.com/Documentation/CIM/latest/User/NetworkResolutionDNS>

Cloud-based techniques for Azure AD, Office 365, Google Workspace, SaaS, IaaS (v9)

MITRE Cloud Matrix: Authentication Example

Initial Access 5 techniques	Execution 1 techniques	Persistence 5 techniques	Privilege Escalation 2 techniques	Defense Evasion 6 techniques	Credential Access 5 techniques	Discovery 10 techniques	Lateral Movement 2 techniques	Collection 4 techniques	Exfiltration 1 techniques	Impact 6 techniques
Drive-by Compromise	User Execution (1)	Account Manipulation (3)	Domain Policy Modification (1)	Domain Policy Modification (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Cloud Storage Object	Transfer Data to Cloud Account	Data Destruction
Exploit Public-Facing Application		Create Account (1)	Valid Accounts (2)	Impair Defenses (3)	Forge Web Credentials (2)	Cloud Infrastructure Discovery		Use Alternate Authentication Material (2)		Data from Information Repositories (2)
Phishing (1)		Implant Internal Image	Modify Cloud Compute Infrastructure (4)	Steal Application Access Token	Cloud Service Dashboard	Steal Web Session Cookie	Cloud Service Discovery	Data Staged (1)		Defacement (1)
Trusted Relationship		Office Application Startup (6)	Unused/Unsupported Cloud Regions	Use Alternate Authentication Material (2)	Network Service Scanning	Unsecured Credentials (2)	Cloud Service Discovery	Email Collection (2)		Endpoint Denial of Service (3)
Valid Accounts (2)		Valid Accounts (2)	Use Alternate Authentication Material (2)	Valid Accounts (2)	Permission Groups Discovery (1)	Software Discovery (1)	System Information Discovery		Network Denial of Service (2)	
						System Location Discovery			Resource Hijacking	
						System Network Connections Discovery				

Last modified: 29 April 2021

Source: <https://attack.mitre.org/matrices/enterprise/cloud/>

Detection Logic

Threat-Based Monitoring Plan: Authentication

INFRA COMPONENT	THREAT	SERVICE (VENDOR)	DETECTION LOGIC
AUTHENTICATION	<i>Console login from suspicious/unusual geolocation</i>	CloudTrail (AWS)	Detect when a user logs in from a new city, country or region. Examples: <ul style="list-style-type: none"> ● ESCU: Detect Console Login by User from New City, New Country, New Region
		AD (Azure)	
		Cloud Audit (GCP)	
	<i>Root/privileged user logins without MFA/key enforcement</i>	CloudTrail (AWS)	Detect when <code>userIdentity.type="Root"</code> , and <code>additionalEventData.MFAUsed="no"</code> .
		AD (Azure)	Audit user, role (Owner, *contributor, admin) and authentication details to determine if MFA request was satisfied or denied.
		Cloud Audit (GCP)	Audit <code>resourceManager.organizationAdmin</code> role for security keys (versus SMS or one-time passwords).

SSE: Splunk Security Essentials App

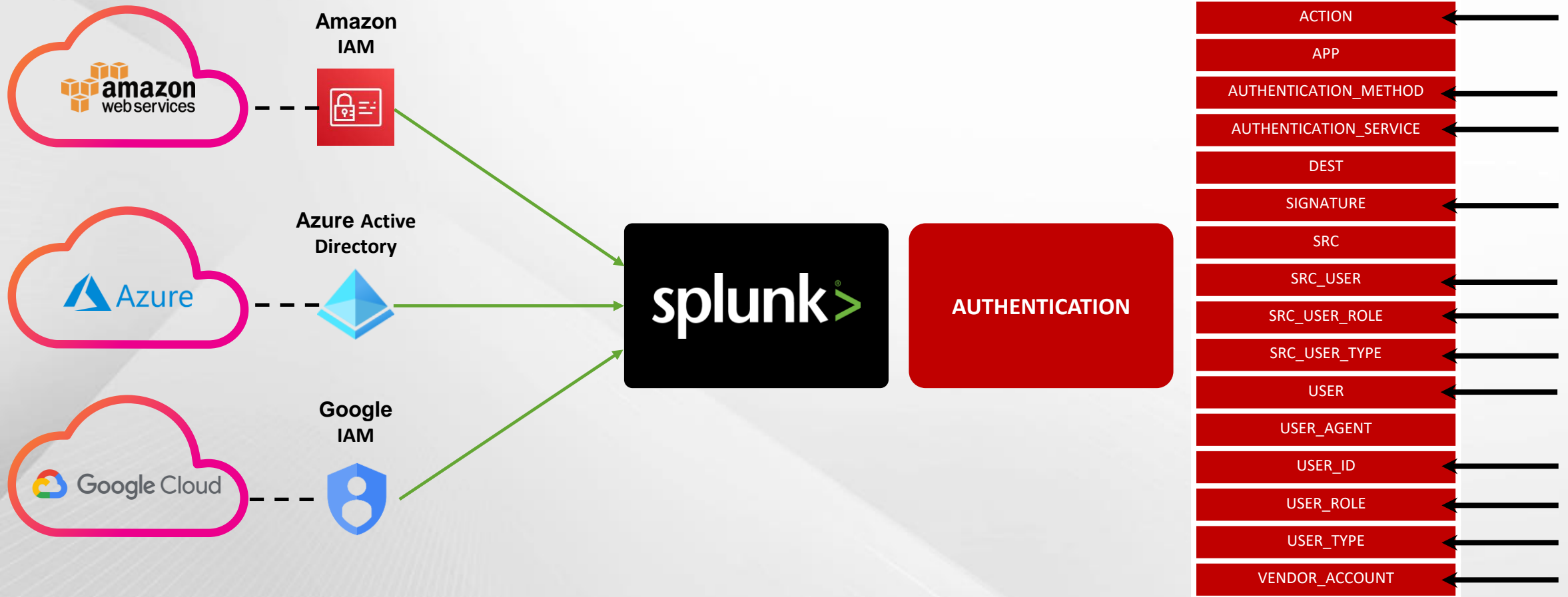
ESCU: Splunk Enterprise Security Content Update

UBA: Splunk User and Entity Behavior Analytics

and so on ...

Splunk Multi-Cloud Monitoring Example: Auth

Highlight user behavior across cloud instances



<https://docs.splunk.com/Documentation/CIM/latest/User/Authentication>

Change, Authentication & Network Traffic Data Model Support



Bring data from AWS, GCP and Azure into your existing detections and investigative workflows with **pre-built content for authentication, network traffic, and configuration changes**, as well as other data, such as CSP native alerts.

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Security Posture Incident Review Investigations Glass Tables Security Intelligence Security Domains Audit Search Configure 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 Framework Mapping: All Data Model: All App: All In Use: All Bookmarked: All filter...

16 Analytic Stories found in category: Cloud Security

	In use	Analytic Story	Use Case	Description	App	Last Updated	Bookmark
Abuse	>	<input type="checkbox"/> AWS Cross Account Activity	Cloud Security	Track when a user assumes an IAM role in another AWS account to obtain cross-account access to services and resources in that account. Accessing new roles could be an indication of malicious activity.	ES Content Updates	Jun 4, 2018	<input type="checkbox"/>
	>	<input type="checkbox"/> AWS Cryptomining	Cloud Security	Monitor your AWS EC2 instances for activities related to cryptojacking/cryptomining. New instances that originate from previously unseen regions, users who launch abnormally high numbers of instances, or EC2 instances started by previously unseen users are just a few examples of potentially malicious behavior.	ES Content Updates	Mar 8, 2018	<input type="checkbox"/>
Adversary Tactics	>	<input type="checkbox"/> AWS Network ACL Activity	Cloud Security	Monitor your AWS network infrastructure for bad configurations and malicious activity. Investigative searches help you probe deeper, when the facts warrant it.	ES Content Updates	May 21, 2018	<input type="checkbox"/>
	>	<input type="checkbox"/> AWS Suspicious Provisioning Activities	Cloud Security	Monitor your AWS provisioning activities for behaviors originating from unfamiliar or unusual locations. These behaviors may indicate that malicious activities are occurring somewhere within your network.	ES Content Updates	Mar 16, 2018	<input type="checkbox"/>
	>	<input type="checkbox"/> AWS User Monitoring	Cloud Security	Detect and investigate dormant user accounts for your AWS environment that have become active again. Because inactive and ad-hoc accounts are common attack targets, it's critical to enable governance within your environment.	ES Content Updates	Mar 12, 2018	<input type="checkbox"/>
Best Practices	>	<input type="checkbox"/> Cloud Cryptomining	Cloud Security	Monitor your cloud compute instances for activities related to cryptojacking/cryptomining. New instances that originate from previously unseen regions, users who launch abnormally high numbers of instances, or compute instances started by previously unseen users are just a few examples of potentially malicious behavior.	ES Content Updates	Oct 2, 2019	<input type="checkbox"/>
	>	<input type="checkbox"/> Container Implantation Monitoring and Investigation	Cloud Security	Use the searches in this story to monitor your Kubernetes registry repositories for upload, and deployment of potentially vulnerable, backdoor, or implanted containers. These searches provide information on source users, destination path, container names and repository names. The searches provide context to address Mitre T1525 which refers to container implantation upload to a company's repository either in Amazon Elastic Container Registry, Google Container Registry and Azure Container Registry.	ES Content Updates	Feb 20, 2020	<input type="checkbox"/>
	>	<input type="checkbox"/> Kubernetes Scanning Activity	Cloud Security	This story addresses detection against Kubernetes cluster fingerprint scan and attack by providing information on items such as source ip, user agent, cluster names.	ES Content Updates	Apr 15, 2020	<input type="checkbox"/>
Cloud Security	>	<input type="checkbox"/> Kubernetes Sensitive Object Access Activity	Cloud Security	This story addresses detection and response of accounts accessing Kubernetes cluster sensitive objects such as configmaps or secrets providing information on items such as user user, group, object, namespace and authorization reason.	ES Content Updates	May 20, 2020	<input type="checkbox"/>
	>	<input type="checkbox"/> Kubernetes Sensitive Role Activity	Cloud Security	This story addresses detection and response around Sensitive Role usage within a Kubernetes clusters against cluster resources and namespaces.	ES Content Updates	May 20, 2020	<input type="checkbox"/>
	>	<input type="checkbox"/> Suspicious AWS EC2 Activities	Cloud Security	Use the searches in this Analytic Story to monitor your AWS EC2 instances for evidence of anomalous activity and suspicious behaviors, such as EC2 instances that originate from unusual locations or those launched by previously unseen users (among others). Included investigative searches will help you probe more deeply, when the information warrants it.	ES Content Updates	Feb 9, 2018	<input type="checkbox"/>
Compliance	>	<input type="checkbox"/> Suspicious AWS Login Activities	Cloud Security	Monitor your AWS authentication events using your CloudTrail logs. Searches within this Analytic Story will help you stay aware of and investigate suspicious logins.	ES Content Updates	May 1, 2019	<input type="checkbox"/>
	>	<input type="checkbox"/> Suspicious AWS S3 Activities	Cloud Security	Use the searches in this Analytic Story to monitor your AWS S3 buckets for evidence of anomalous activity and suspicious behaviors, such as detecting open S3 buckets and buckets being accessed from a new IP. The contextual and investigative searches will give you more information, when required.	ES Content Updates	Jul 24, 2018	<input type="checkbox"/>
	>	<input type="checkbox"/> Suspicious AWS Traffic	Cloud Security	Leverage these searches to monitor your AWS network traffic for evidence of anomalous activity and suspicious behaviors, such as a spike in blocked outbound traffic in your virtual private cloud (VPC).	ES Content Updates	May 7, 2018	<input type="checkbox"/>

Security Posture

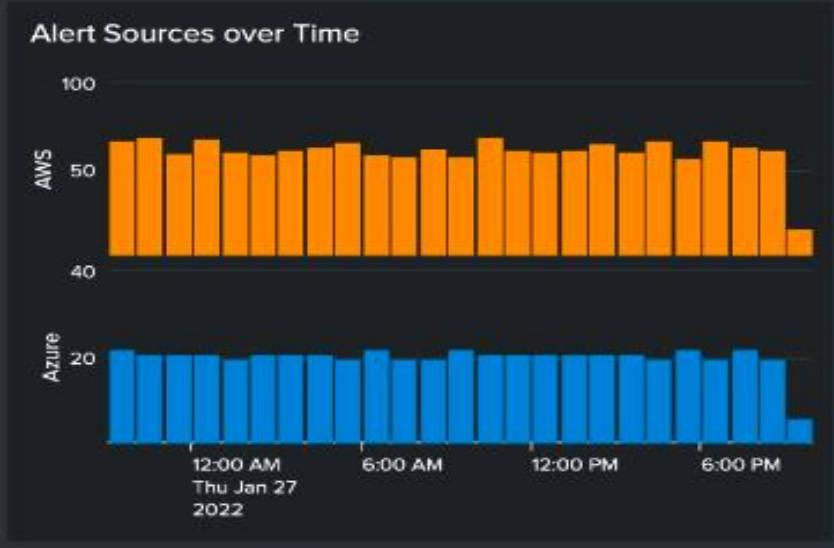
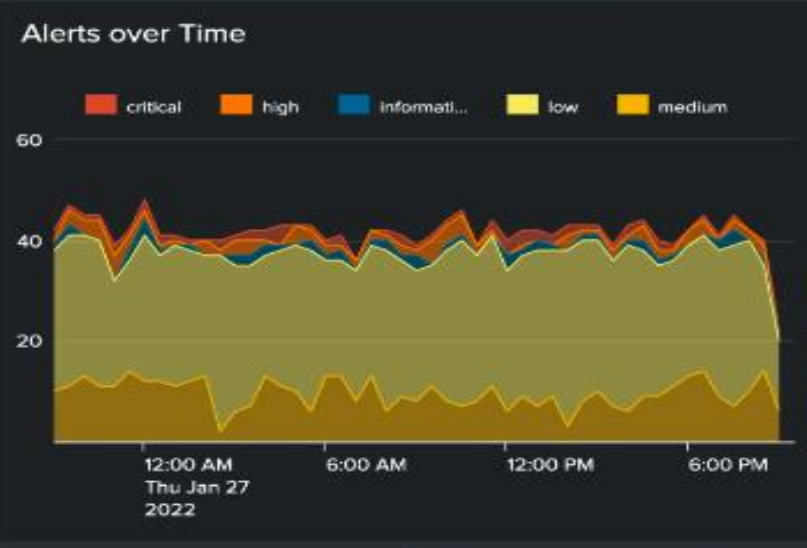
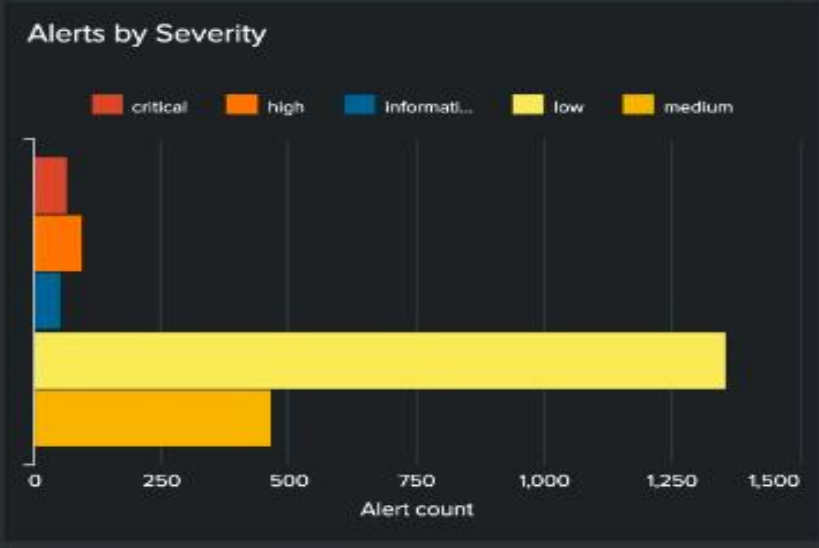
Edit Export ...

Cloud Providers Monitored

AWS

Microsoft Azure

Google Cloud



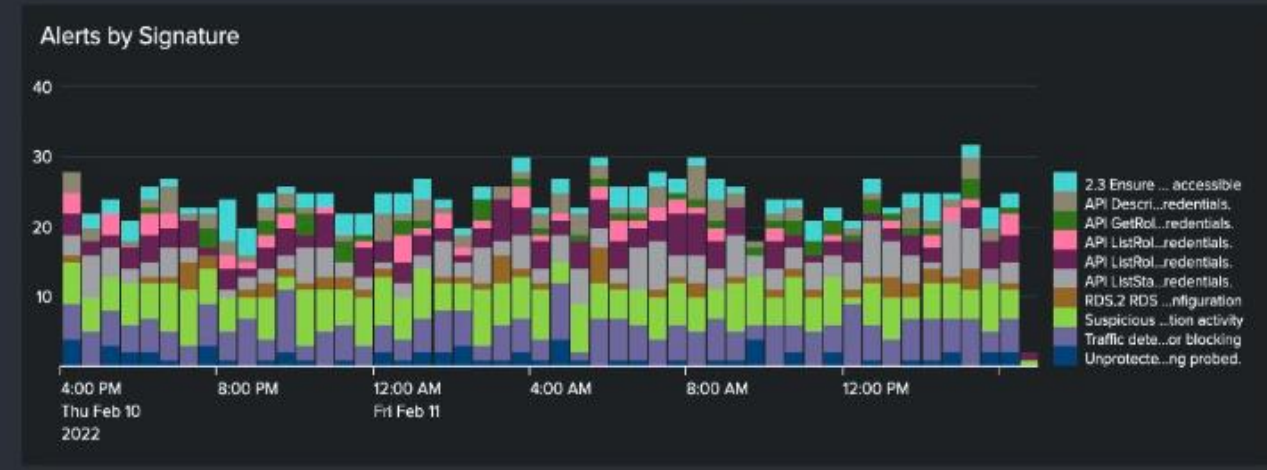
Cloud Alerts [Show Filters](#) Edit Export ...



List of Alerts

severity	cloud	count	signature
critical	AWS	27	2.3 Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible
critical	AWS	18	API ListStacks was invoked using root credentials.
critical	AWS	9	RDS.2 RDS DB Instances should prohibit public access, determined by the PubliclyAccess
critical	AWS	7	Unprotected port on EC2 instance i-89f82cd2ca06f46c5 is being probed.
high	AWS	16	2.3 Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible
high	AWS	16	API ListStacks was invoked using root credentials.
high	AWS	36	Amazon S3 Public Anonymous Access was granted for S3 bucket GeneratedFindingS3Bucket.

< Prev 1 2 3 4 5 6 7 8 9 10 Next >



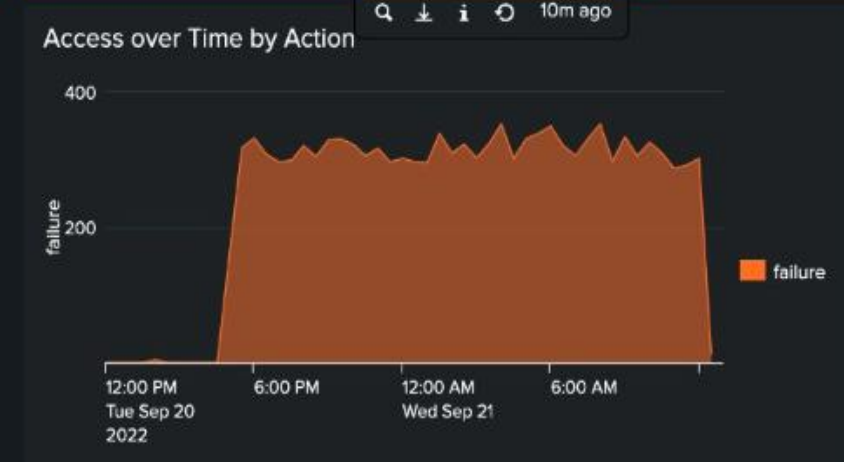
Many Attacks from Same Source

Many Attacks from Same Source by Source Location

Authentication [Show Filters](#)

Edit Export ...

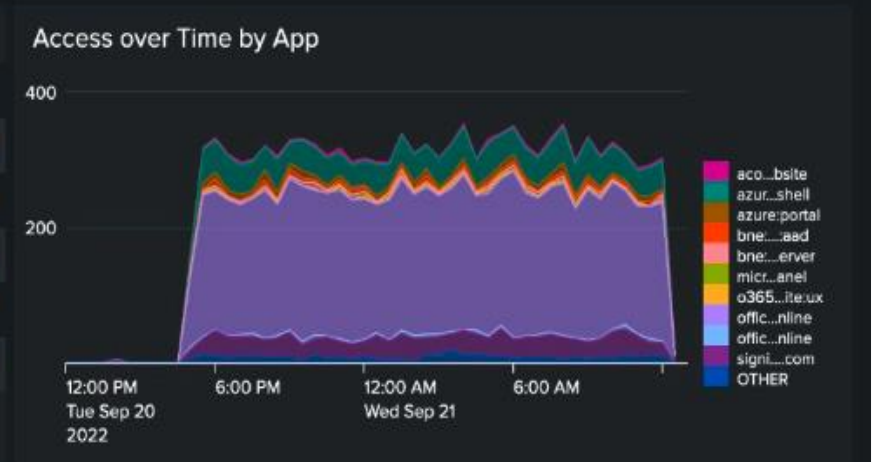
Failed Authentications	Successful Authentications	Applications	Users
12,137	17,647	50	256



Authentication Attempts by Application

app	count
azure:devops	2
graph:explorer	9
my:profile	10
splunk_o365	10
frothly_phantom	14

« Prev 1 2 3 4 5 Next »



Top Authentications by Source

src	sparkline	count
171.12.224.14		3086
34.215.24.225		2620
96.247.194.3		2038
122.4.40.35		856
218.73.119.158		719
114.239.29.80		442
110.175.8.139		363

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Top Authentication Sources by Unique User Count

src	sparkline	user_count
96.247.194.3		17
10.154.1.20		4
10.154.1.5		4
10.154.12.101		4
10.154.12.76		4
10.154.131.210		4
10.154.167.183		4

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

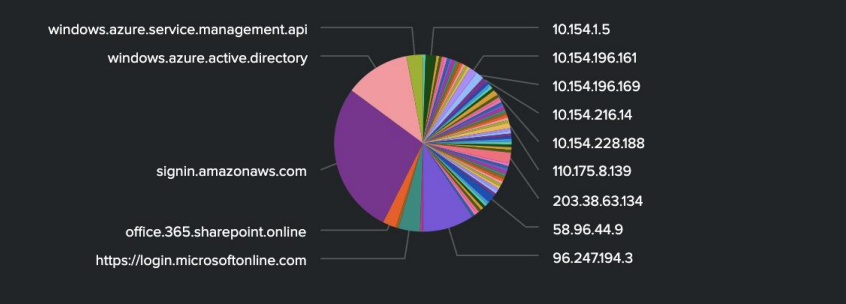
Users (with Filters Applied)

user	hosts_authenticated
HSJG6AIAIDAI3UOW26C5KA	19
DBC6AIAIDAI3UOW26C5KA	16
AUODN4TKSW26C5KA	14
NDHIDAI3UKSW26C5KA	11
ebelford@ellingson.group	10

Source and Destination Hosts (with Filters Applied)

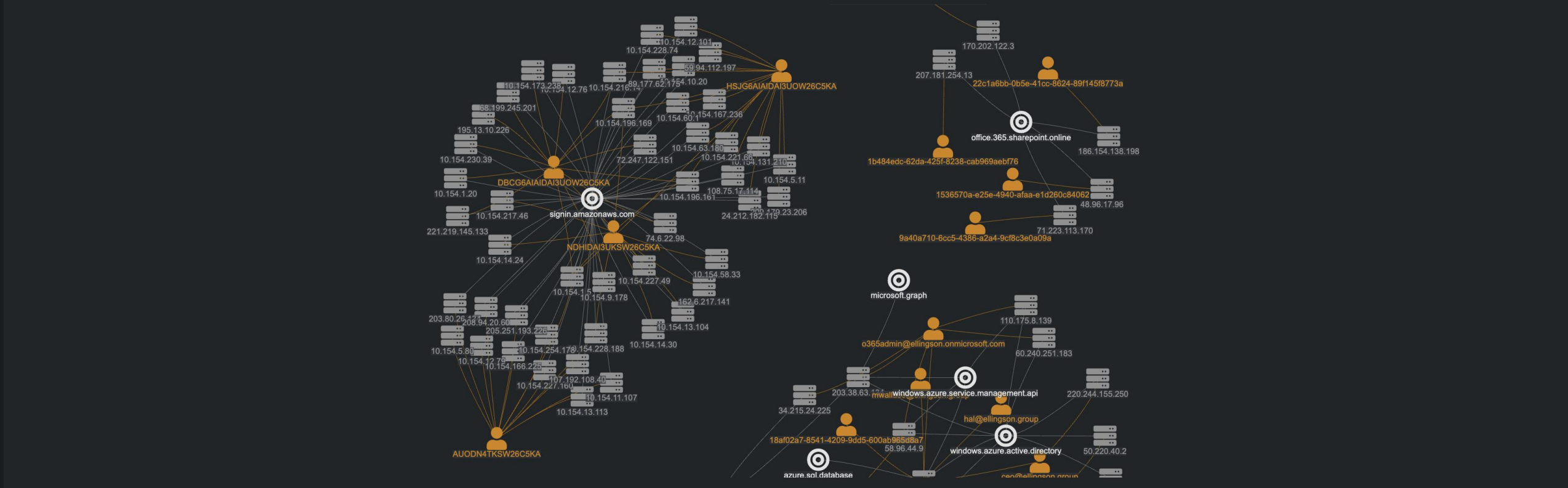
source&destination	count
171.12.224.14	190
https://login.microsoftonline.com	151
34.215.24.225	50
https://login.microsoftonline.com	50

Source and Destination Hosts (with Filters Applied)

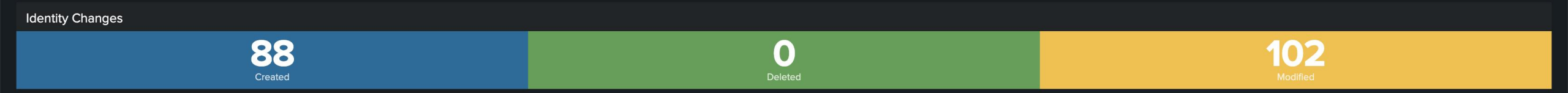


Authentications Map (Map Shows up to 300 Authentication Source+Destination Pairs)

Double-click to drill down. Server icon = authentication source. Circle icon = authentication destination.

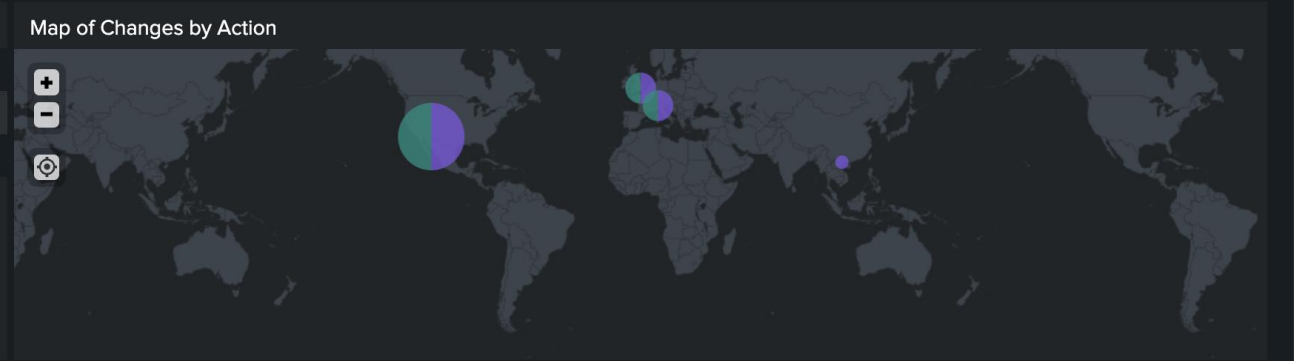


Changes [Show Filters](#) Edit Export ...



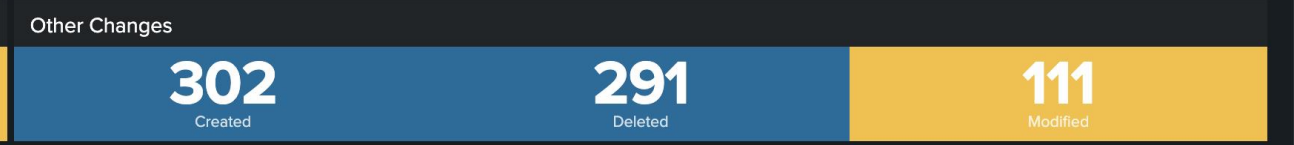
Identity Changes

action	sparkline	cloud	count	command
created		AWS	88	CreateUser
modified		AWS	102	UpdateUser



Instance Changes

action	sparkline	count	command
created		1,137	CreateBucket, CreateVolume, RunInstances
deleted		195	DeleteBucket, DeleteVolume, TerminateInstances
modified		292	AttachVolume, DetachVolume, PutBucketPublicAccessBlock, PutObject
restarted		34	RebootInstances
started		25	StartInstances
stopped		28	StopInstances

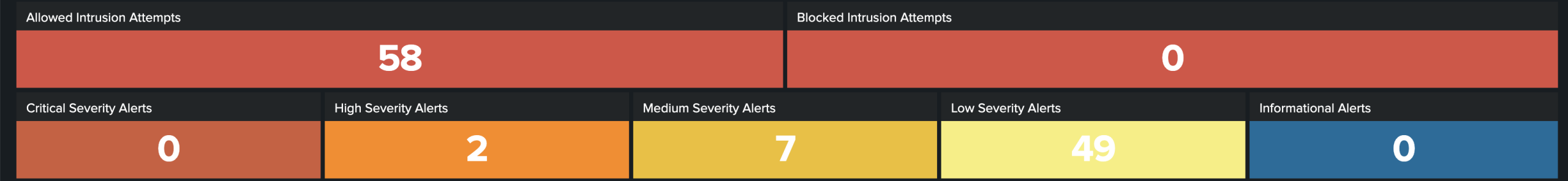


Other Changes

action	sparkline	count	command
created		302	CreateNetworkAcl, CreateNetworkAclEntry, CreateSecurityGroup
deleted		291	DeleteNetworkAcl, DeleteSecurityGroup, RevokeSecurityGroupEgress, RevokeSecurityGroupI
failure		69	ConsoleLogin
modified		111	ReplaceNetworkAclEntry



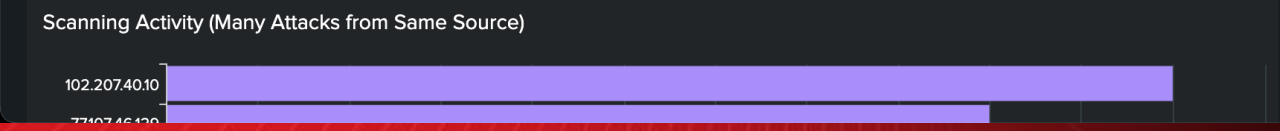
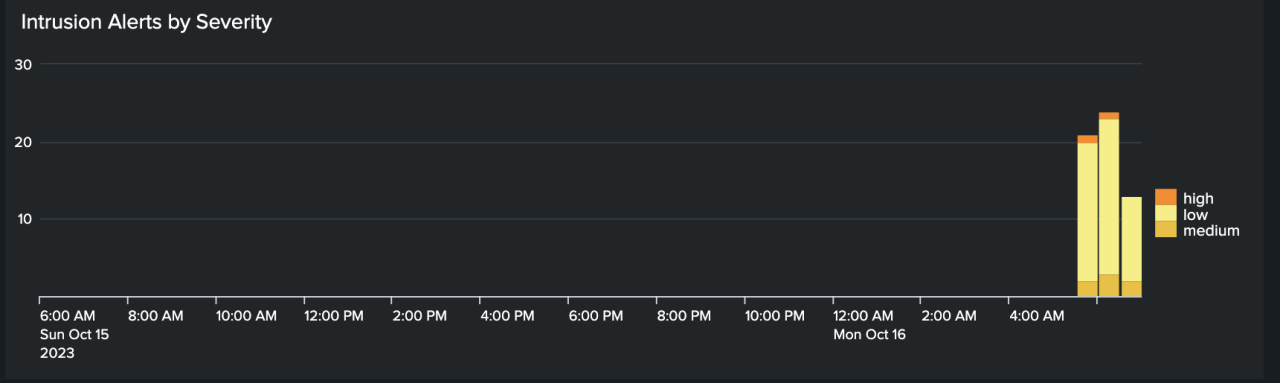
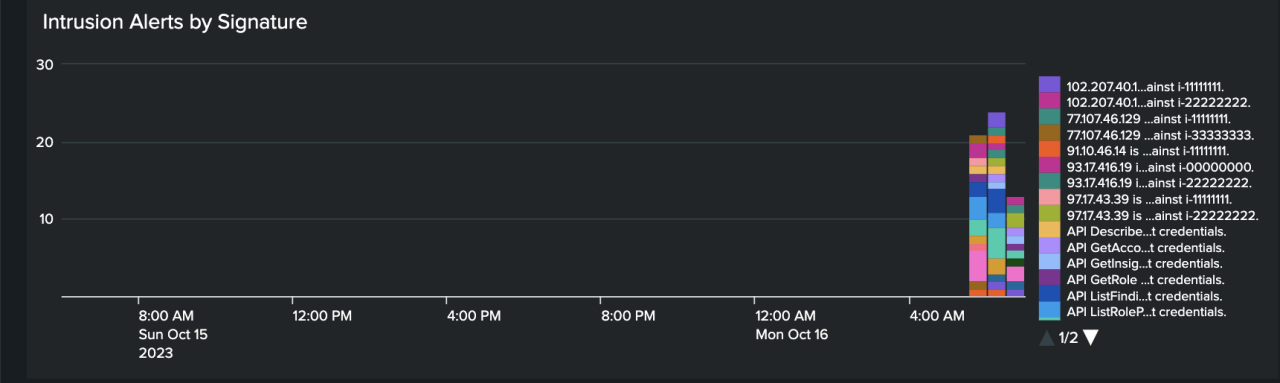
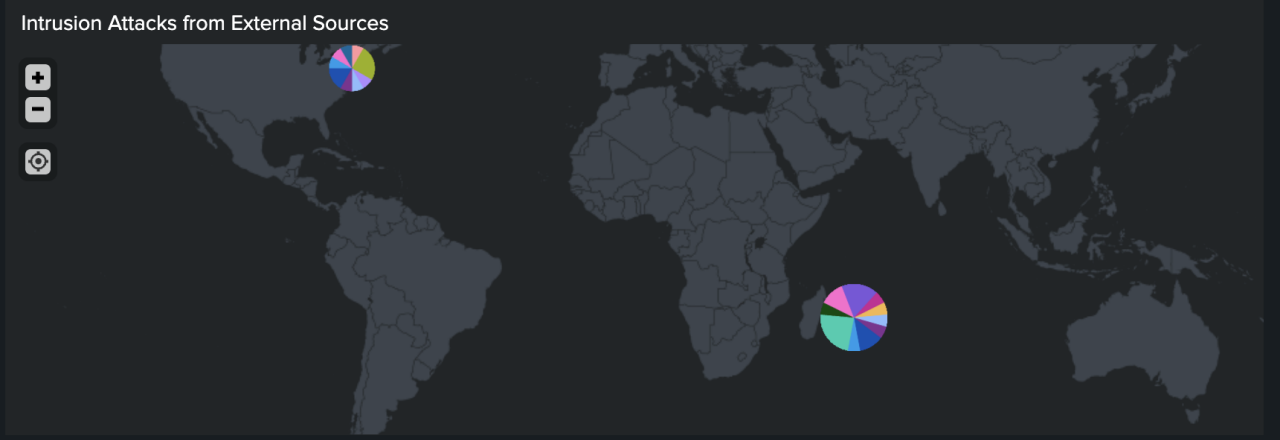
Intrusion Detection (IDS/IPS) [Show Filters](#) Edit Export ...



Intrusion Signatures

severity	count	signature
high	2	Amazon S3 Public Anonymous Access was granted for S3 bucket GeneratedFindingS3Bucket.
low	7	API ListRoles was invoked using root credentials.
low	6	Resource discovery API GeneratedFindingAPIName was invoked from a Tor exit node.
low	5	API ListFindings was invoked using root credentials.
low	5	API ListRolePolicies was invoked using root credentials.
low	3	93.17.416.19 is performing SSH brute force attacks against i-00000000.
low	3	97.17.43.39 is performing SSH brute force attacks against i-22222222.

« Prev 1 2 3 4 Next »



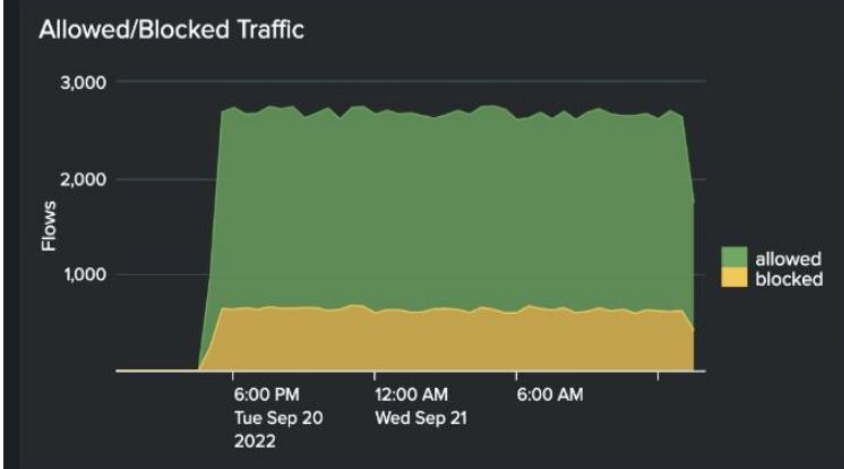
Scanning Activity (Many Attacks from Same Source) by Source Location

Country	City	src	attack_count
Mauritius	Ebene CyberCity	102.207.40.10	11

Network Traffic [Show Filters](#)

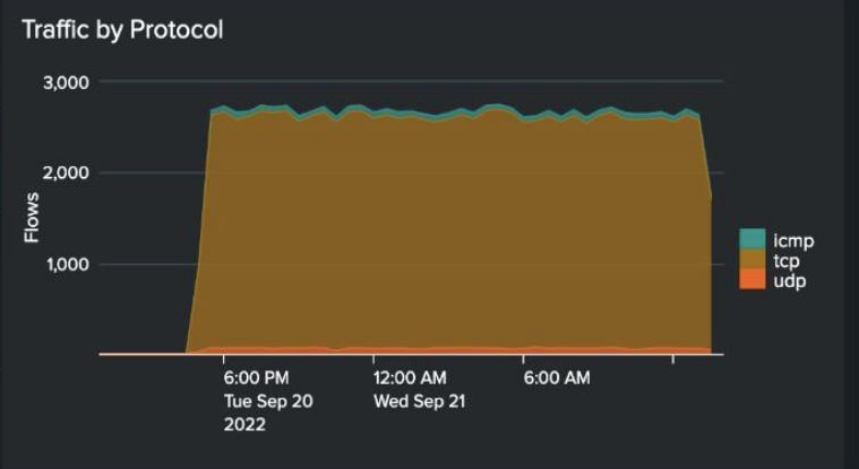
Edit Export ...

Blocked Connections 25,919	Allowed Connections 83,904	Traffic Sources 13,120	Traffic Destinations 13,749	Logged Traffic Volume 0.50 GB
--------------------------------------	--------------------------------------	----------------------------------	---------------------------------------	-----------------------------------------



Top Communication by Volume

src	dest	MBytes
10.154.196.169	137.145.204.10	3.88
10.154.196.169	10.154.196.169	3.53
10.154.196.169	10.154.1.5	2.13
10.154.196.169	192.42.93.30	1.96
10.154.196.169	10.154.196.161	1.95



Top Sources

src	count	num_dest_port	num_dest_ip
10.154.196.169	25,934	6478	1,463
10.154.196.161	5,118	3563	1,221
10.154.1.5	3,420	2655	1,028
10.154.229.167	2,066	1781	843
10.154.131.210	1,192	1089	602

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Top Destinations

dest	count	num_dest_port	num_src_ip
10.154.196.169	3,112	2495	543
137.145.204.10	3,071	2457	553
10.154.1.5	1,776	1580	414
10.154.196.161	1,720	1515	444
192.42.93.30	1,651	1480	413

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Top Destination Ports

dest_port	count	num_dest_ip	num_src_ip
1447	38	32	25
6486	34	31	20
3876	33	30	23
1283	32	30	23
4391	32	32	24

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

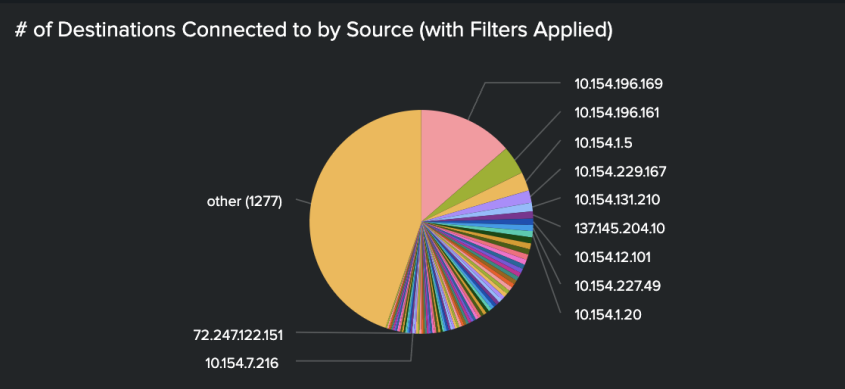
Network Communication Map

Use the filters below to build a host communication map. Click on host name or IP address in the tables and pie chart below to filter communication information further.

Network Communication Map Filters

Protocol Filter: *
 Source/Dest. Host Name or IP: *
 Allowed/Blocked: All
 Host Connected to: 1 host or more
 Select Time Range: Last 24 hours

Protocols (with Filters Applied)	flows
transport	flows
icmp	134
tcp	6,106
udp	120



Source and Destination (with Filters Applied)

source&destination	flows
10.154.196.169	38
137.145.204.10	
10.154.196.169	30
10.154.196.161	
10.154.196.169	28
10.154.1.5	

[Prev](#) 1 [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)

Communications Map (Map Shows up to 300 Connections)

Double-click to drill down



Free trials and downloads

Splunk Cloud Platform

See the power of the Splunk Platform in a Splunk-hosted cloud environment and get fast insights. Try up to 5GB of data/day for 14 days, no credit card required.

[Get My Free Trial](#)

[View Product](#)



Splunk Enterprise

Download and install Splunk Enterprise trial on your own hardware or cloud instance so you can collect, analyze, visualize and act on all your data — no matter its source. Try indexing up to 500MB/day for 60 days, no credit card required.

[Get My Free Trial](#)

[View Product](#)





감사합니다.