

Splunk Forum

Splunk Korea – December 2020



splunk > Forum

Forward- Looking Statements



During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Data-to-Everything, D2E 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. © 2020 Splunk Inc. All rights reserved

splunk> turn data into doing™

**Securing
the Cloud Journey**

**Unified Security
Operation**

**Analyst Productivity/
Efficiency**

Securing the Cloud Journey

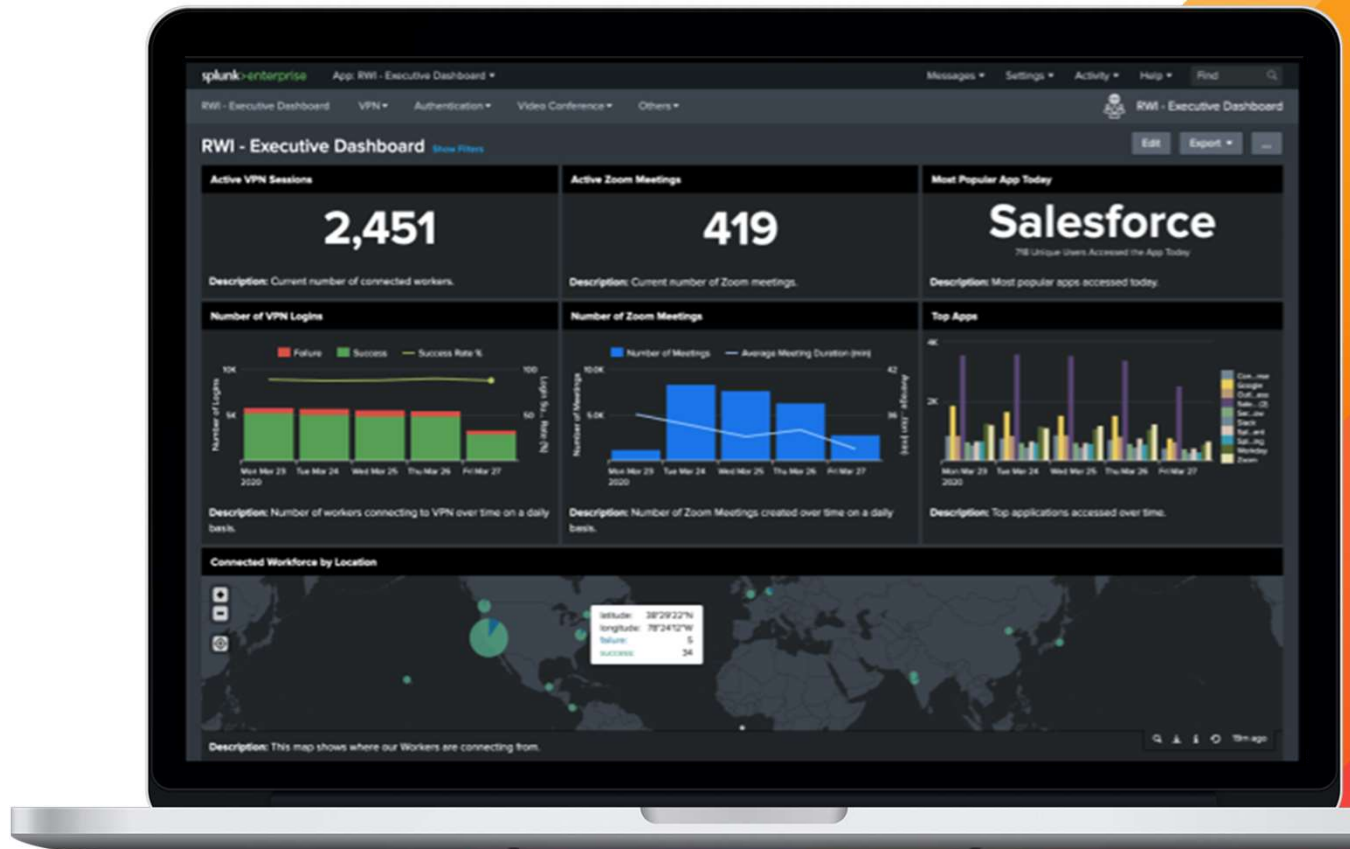
splunk > turn data into doing™

스플링크 엔터프라이즈 시큐리티
100 TB/Day 이상 확장

스플링크 팬텀
50k Events/Hour 이상 확장

ML 유연성
With SMLE and Jupyter 노트북

Remote Work Insights





Splunk의 Remote Work Insights
앱 덕분에 2 주 만에 직접
대면에서 원격으로
전환했습니다.”

Lanita Collette

Deputy Chief Information Officer & CISO,
University of Arizona

splunk > turn data into doing™

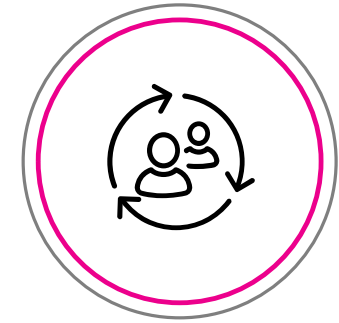
Workload Pricing



**Cloud
Native
Experiences**



**Secure
the Cloud**

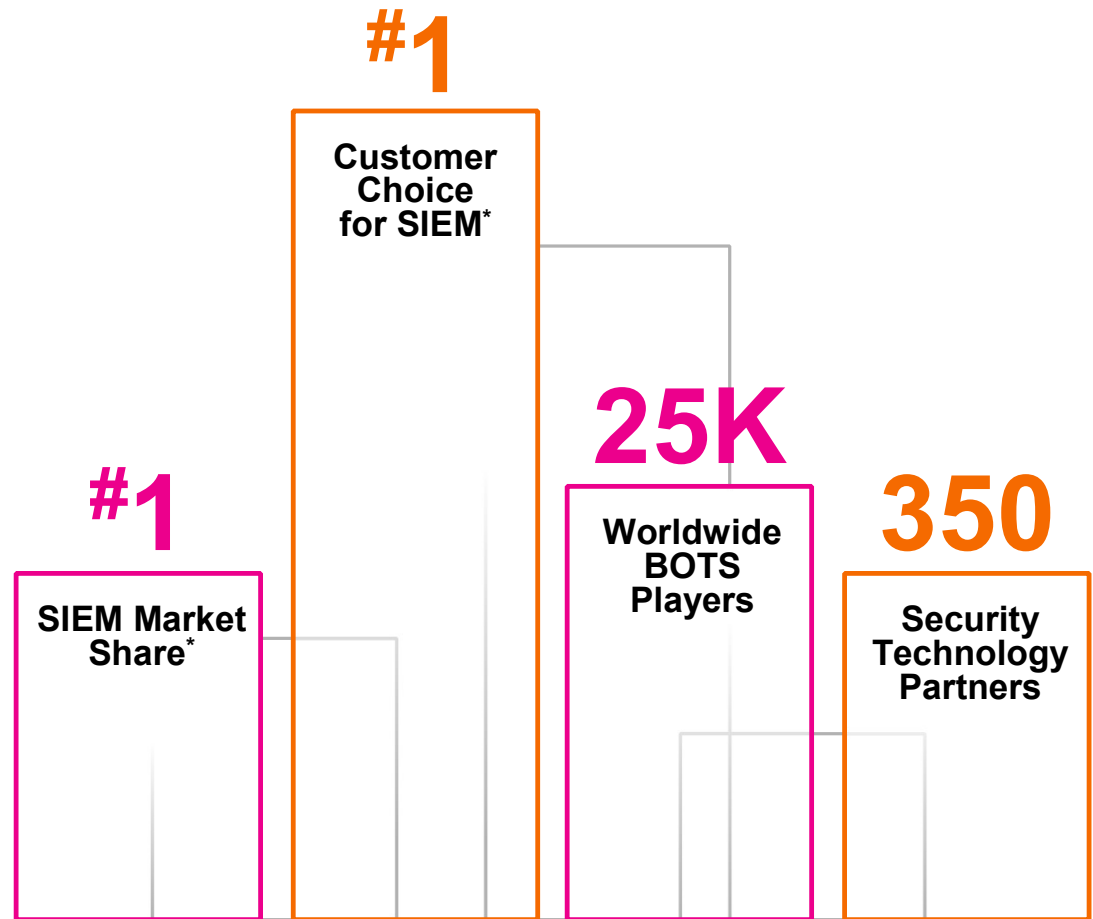


**Analyst
Experience**

Splunk Security Community

* Source: Gartner Inc. Gartner Magic Quadrant Security Incident and Event Management, K. Kavanagh, T. Bussa, G. Sadowski, February 2020

† <https://www.gartner.com/reviews/market/security-information-eventmanagement/vendor/splunk>





스플링크를 처음 사용해
보았는데, 툴이 가지고 있는
깊이에 매우 놀랐습니다.”

Mangatas Tondang

BOTS participant

splunk > turn data into doing™

3 Years of Digital Transformation in 6 Months

Splunk Helps You **Secure Your Cloud Journey**

Simpler, More Flexible

생산성에 집중

보안 포스처 향상

Keep attackers out
Bolster your defenses

규정 준수를 보다
쉽게

Soar through
compliance audits

가치 실현 시간
단축

Pilot to production

**데이터 볼륨을
어떻게 관리해야 하나?**

**비즈니스 위험을
어떻게 인지할 수 있는가?**

**IT 보안 운영을
어떻게 향상시킬 수 있는가?**

마켓을 선도하는 보안 포트폴리오



Security Portfolio

Investigation and Forensics
SIEM/Security Analytics
Automation and Orchestration
Security Incident Response
Unified Security Operations

Security Products

Splunk Cloud / Splunk Enterprise
Splunk Enterprise Security
Splunk UBA
Splunk Phantom
Splunk Mission Control

Data-to-Everything™ Platform

속도

깊이

유연성

대응 시간 단축

주요 경보에 중요한
컨텍스트를 추가

속도

깊이

유연성

하이브리드와 멀티클라우드
스트리밍과 머신 러닝

속도

깊이

유연성

에코시스템 생태계

개방성

Securing
the Cloud Journey

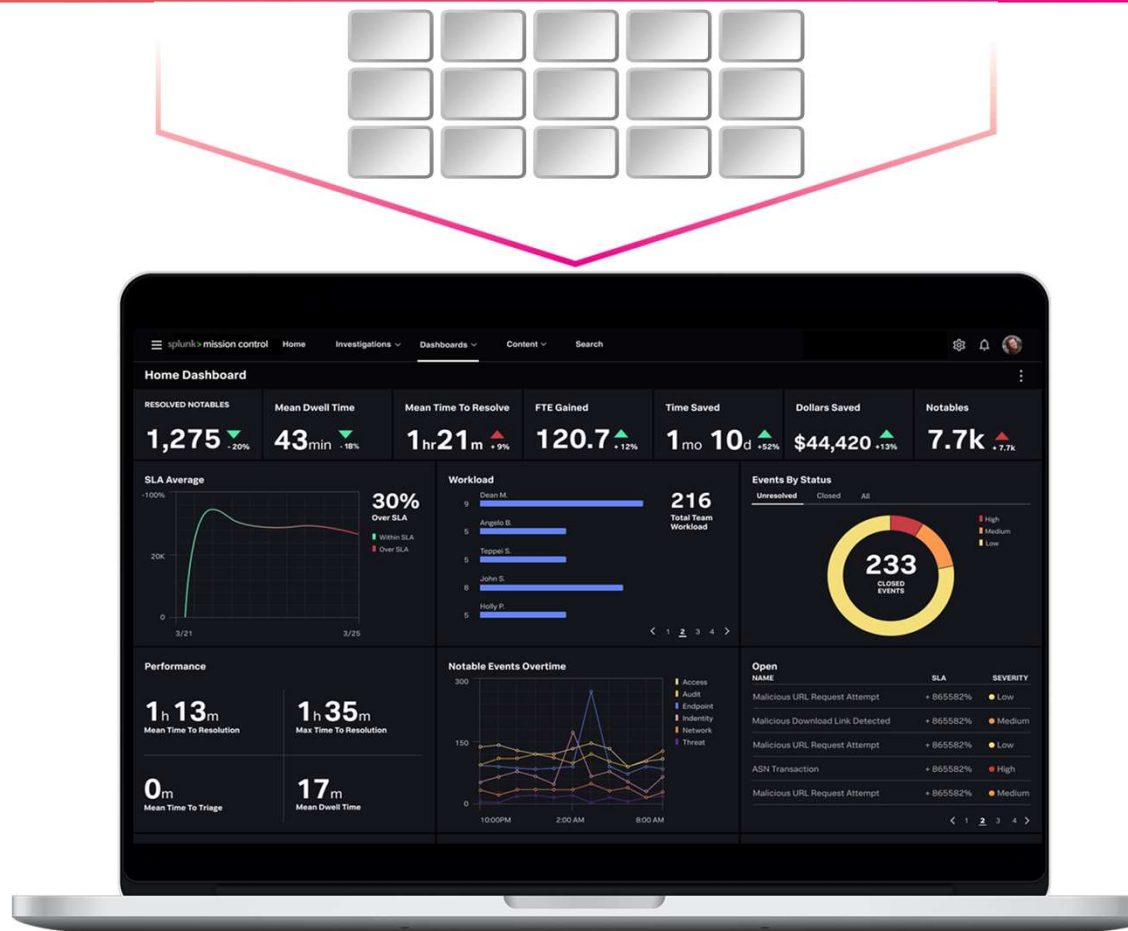
Unified Security
Operation

Analyst Productivity/
Efficiency

Unified Security Operation

splunk> turn data into doing™





단일 플랫폼?

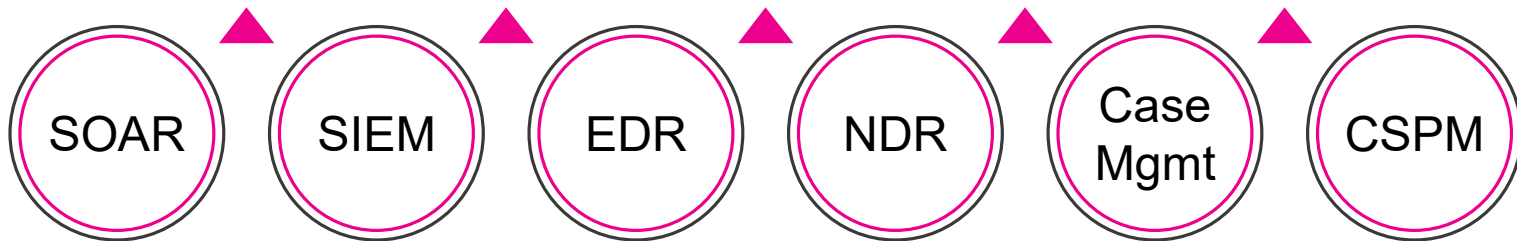
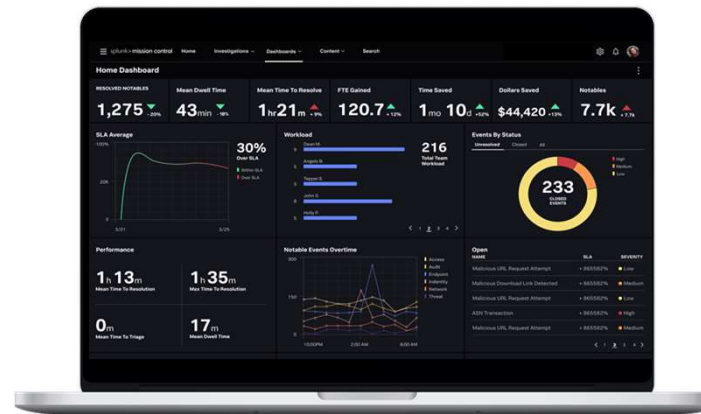
클라우드 기반, 통합 보안 운영 플랫폼



Mission Control

Splunk Mission Control

플러그인 프레임워크



최초의 플러그인 프레임워크 파트너



splunk> mission control Home Investigations Dashboards Content Search

Notables

Search for something... Last 24 Hrs Saved filters Saved_View_02 + Notable

Critical x ES Notable x Glenn Galien x Clear All Save

Notable activity 347 notables from 10/10/20 12:00 am - 10/13/20 12:00 am

Notables by Status

- Unassigned
- New
- In Progress
- Pending
- Resolved
- Closed

Notables by Severity

- High
- Low
- Critical
- Medium
- Info
- Nil

Notables by Sensitivity

- Green
- Red
- Amber
- White

Top Owners

Wilson Drake	20
Mel Yan	20
Glenn Galien	12
Dan Tranter	10
Bob Longlath	3

SLAs Exceeded

Total Count: **56** +20%

347 Notables 3 new updates 1-10 of 347 Show 10

ID	Case	Name	Severity	Sensitivity	Data sou.	Label	Type	Event	Created	Due	Owner	Status	Parent No.	Child Not.
10	No	Unusual IAM Activity	Critical	Critical	ES_O1	AWS Sec...	Notable	10	Oct 12, 3:26 am, PST	Oct 12, 3:26 am, PST	Glenn Gal...	New		
10	No	CSM Policy Violation - Ensure no security g...	Critical	Critical	ES_O1	CSM	Notable	10	Oct 12, 3:26 am, PST	Oct 12, 3:26 am, PST	Glenn Gal...	New		
10	No	Possible infected Host	Critical	Critical	ES_O1	ES Not...	Notable	10	Oct 12, 3:26 am, PST	Oct 12, 3:26 am, PST	Glenn Gal...	New		
10	Yes	Remote Account Takeover	Critical	Critical	ES_O1	ES Not...	Notable	10	Oct 12, 3:26 am, PST	Oct 12, 3:26 am, PST	Glenn Gal...	New		4
10	No	Data Exfiltration by User	Critical	Critical	ES_O1	ES Not...	Notable	10	Oct 12, 3:26 am, PST	Oct 12, 3:26 am, PST	Glenn Gal...	New		
10	No	Phishing attempt	Critical	Critical	ES_O1	ES Not...	Notable	10	Oct 12, 3:26 am, PST	Oct 12, 3:26 am, PST	Glenn Gal...	New		2
10	No	Host with Multiple infections (10.11.36.12)	Critical	Critical	ES_O1	ES Not...	Notable	10	Oct 12, 3:26 am, PST	Oct 12, 3:26 am, PST	Glenn Gal...	New		
10	No	Host with Multiple infections (10.11.36.12)	Critical	Critical	ES_O1	ES Not...	Notable	10	Oct 12, 3:26 am, PST	Oct 12, 3:26 am, PST	Glenn Gal...	New		
10	No	Host with Multiple infections (10.11.36.12)	Critical	Critical	ES_O1	ES Not...	Notable	10	Oct 12, 3:26 am, PST	Oct 12, 3:26 am, PST	Glenn Gal...	New		



미션 컨트롤을 사용하면,
팀 협업을 위해 다른 보안 도구로
전환할 필요가 없습니다”

Jared Born

Team Lead, Cyber Incident Response
Team (CIRT), Grainger

splunk > turn data into doing™

스플링크는
통합 보안 운영을 위한
최상의 선택지를
제공합니다.

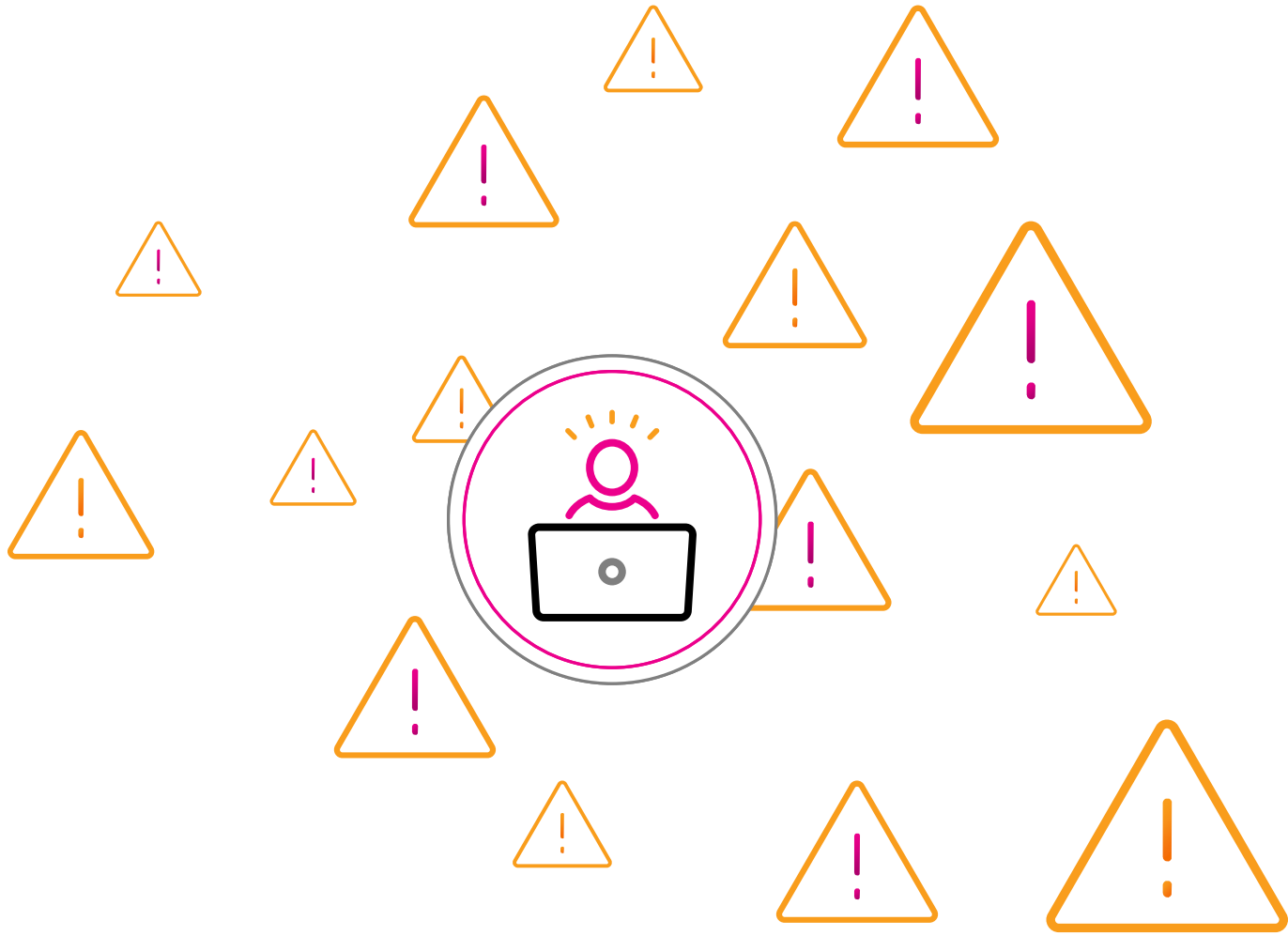
Securing
the Cloud Journey

Unified Security
Operation

Analyst Productivity/
Efficiency

Analyst Productivity/ Efficiency

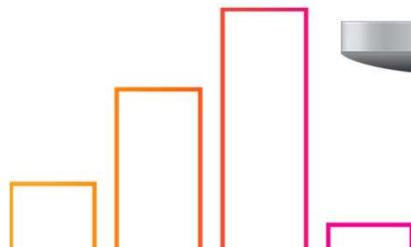
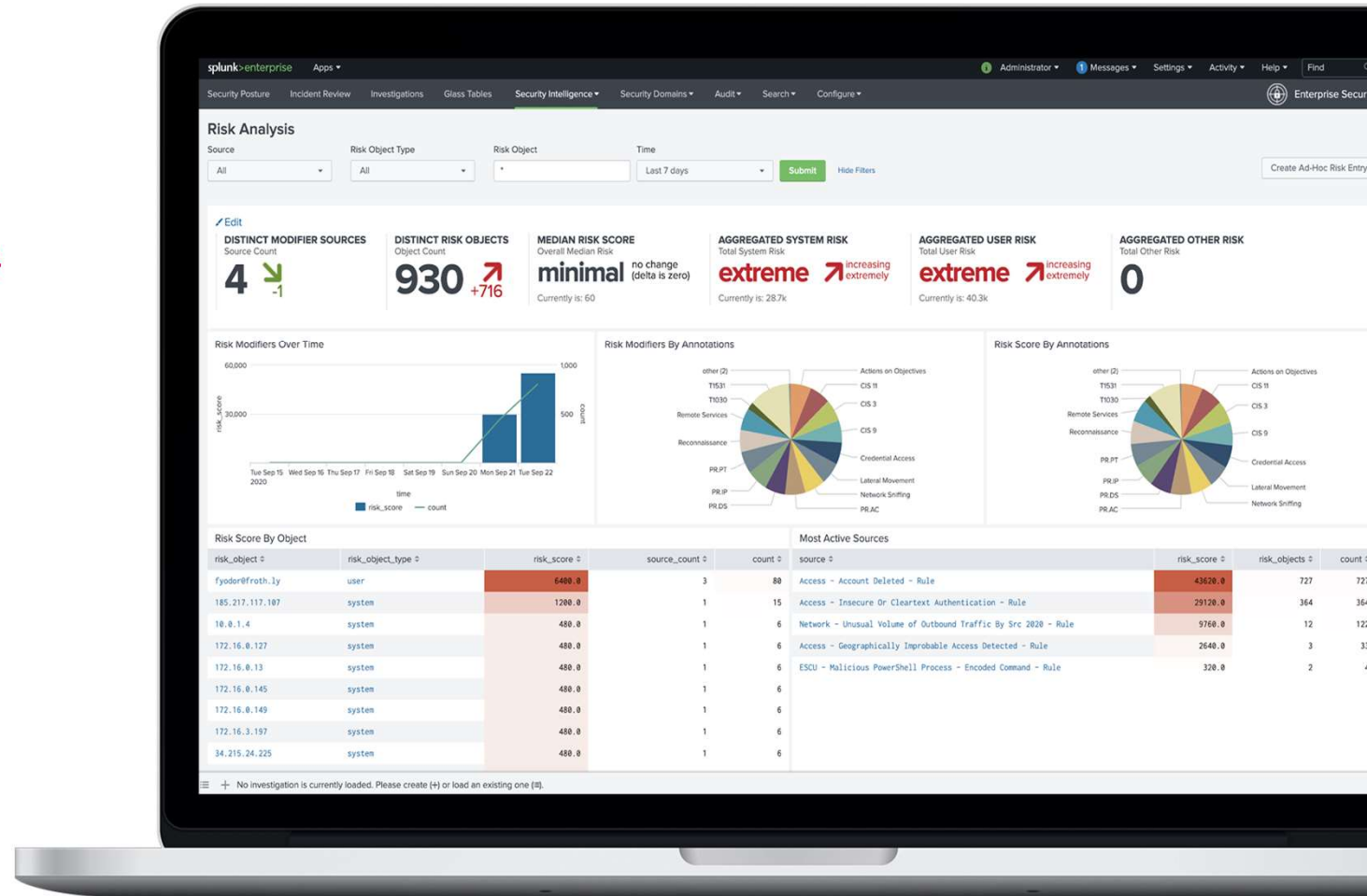
splunk > turn data into doing™



Risk-Based Alerting

Splunk Enterprise Security 6.4

- 오탐을 대폭 줄여 분석가의 시간을 절약하고 두통을 줄여줍니다
- 기존의 상관 관계 검색 방법이 놓치는 'low-and-slow' 공격과 같은 위협 탐지
- 프레임 워크를 탐지에 매핑하여, 보안 운영을 MITER ATT&CK와 같은 산업 프레임 워크에 맞게 조정합니다



Incident Review

Urgency

CRITICAL 3

HIGH 0

MEDIUM 0

LOW 0

INFO 0

Status

New x

Owner

Select...

Security Domain

Select...

Tag

Type...

Correlation Search Sequenced Event

ESCU - Malicious PowerShell Process x

Geographically Improbable Access Det. x

Unusual Volume of Outbound Traffic B... x

Search

fyodor* OR 10.0.14

Time Associations

Last 48 hours

Submit



Incident Review Events

0/3 Selected | Edit All 3 Matching Events | Add Selected to Investigation

Time	Security Domain	Title	Urgency	Status	Owner	Actions
9/15/20 3:26:13.000 PM	Network	Unusual Volume of Network Activity	Critical	New	unassigned	
9/15/20 6:05:12.000 PM	Access	Geographically Improbable Access Detected For fyodor@froth.ly	Critical	New	unassigned	
9/15/20 4:30:15.000 PM	Endpoint	Malicious PowerShell Process - Encoded Command On FYODOR.L@froth.ly	Critical	New	unassigned	

Risk-Based Alerting

SOC를 최적화 하고
가장 높은 위협을
탐지합니다.

SOAR의 이점

▲
속도

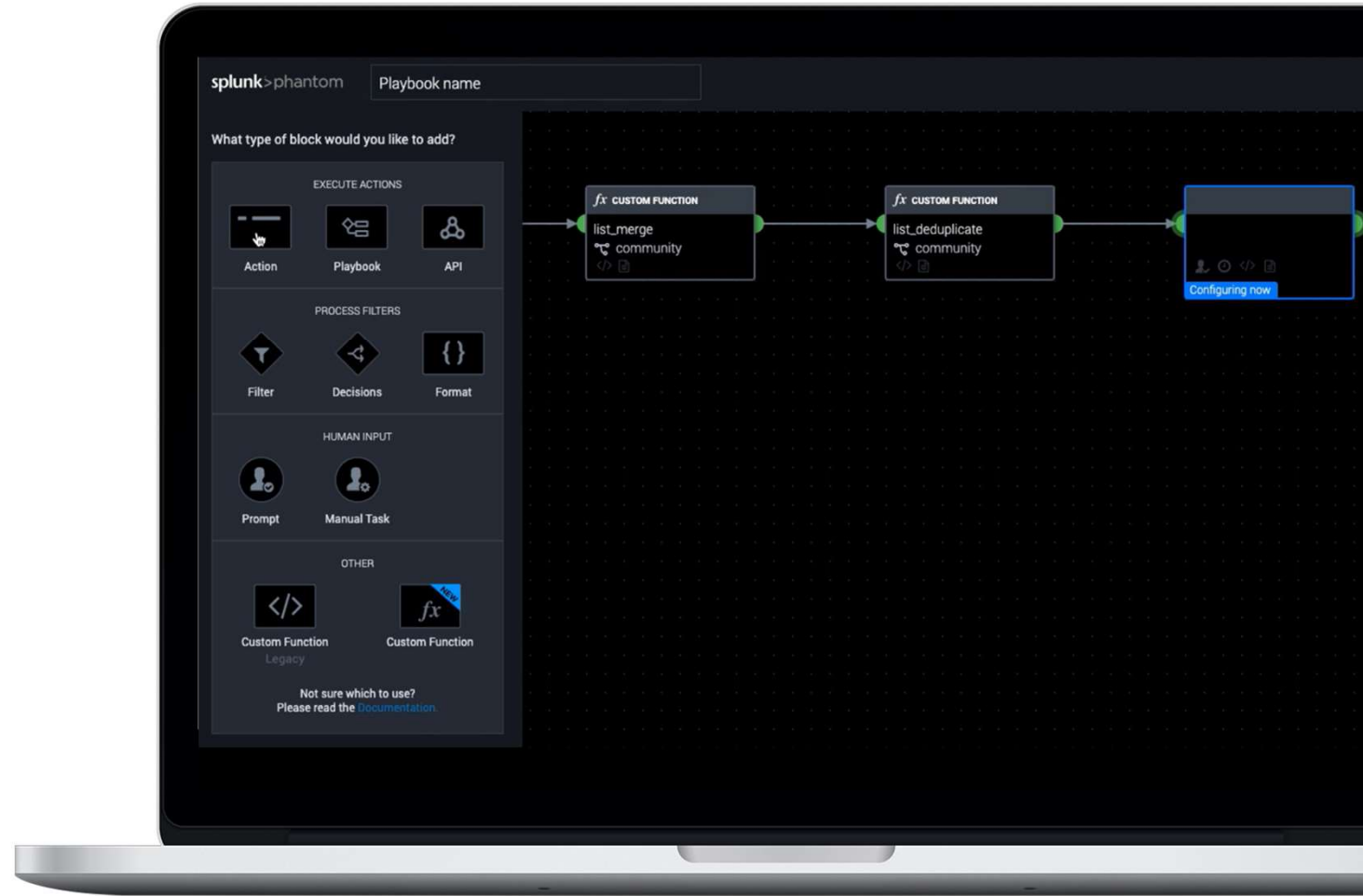
▲
생산성

자동화는 매우 유용합니다.
확장에 한계가 있습니다.

커스텀 함수

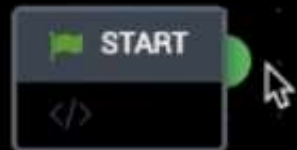
Splunk Phantom 4.9

- OOTB 커스텀 함수 블록으로 플레이북 생성을 더 쉽고 빠르게
- 플레이 북에서 커스텀 함수 재사용
- 코딩 요구 사항이 거의 없음
- 포함하거나 포함하지 않는 모든 플레이 북에 계단식 변경



splunk>phantom

Playbook name





새로운 Phantom 커스텀 함수 기능은 효율적인 플레이북 개발, 유지 및 관리를 용이하게 합니다. 이를 통해 보안 팀의 시간을 상당히 절약할 수 있습니다.”

Maria Elizabeth de Guzman

Director, EY Global Delivery Services,
Ernst & Young
splunk > turn data into doing™

자동화
보다
쉽게

Splunk Forum Korea 2020

클라우드 보안도 Splunk

○ 최재우 | Sales Engineer | Splunk Korea
17 Dec 2020

splunk > turn data into doing™

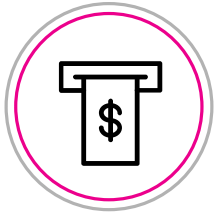
Challenges Cloud Security Operations



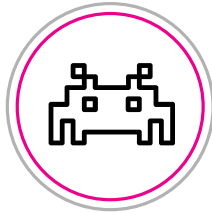
Unified Cloud Security

splunk > turn data into doing™

Cloud Enables Transformation, but Increases Complexity and Inhibits Visibility



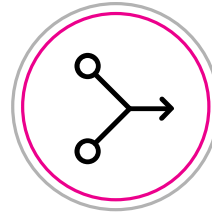
\$6T



Breach



Insider Threat



Compliance



Alert Fatigue

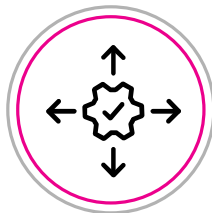


Enterprise Complexity

Compounded by



Multicloud Strategies



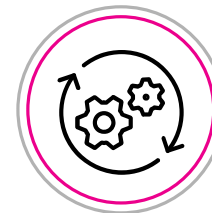
New Attack Surfaces



API/Microservices Interfaces



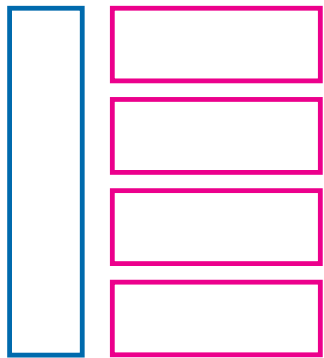
Cloud Workloads and Migrations



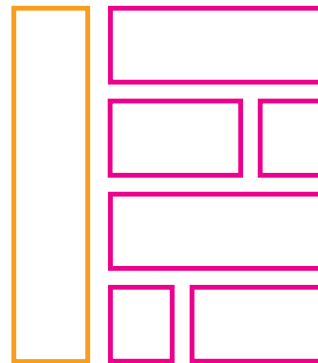
Ephemeral Processes

Secure the Journey to the Cloud

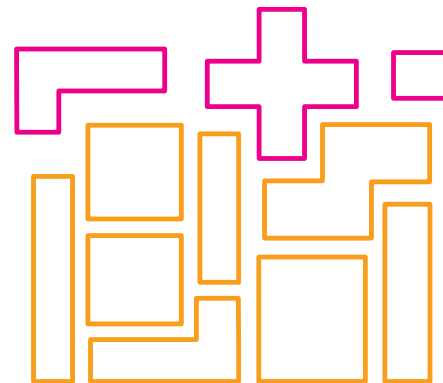
Retain and Optimize



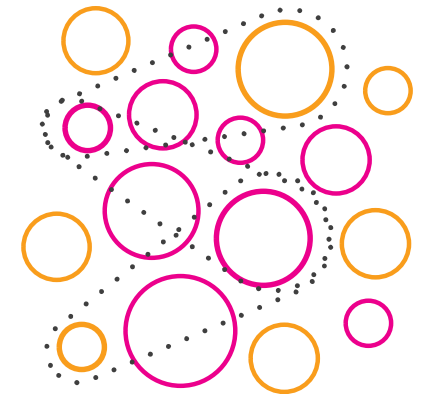
Lift and Shift



Refactor



**Rearchitect/
Cloud-Native**



Announcing

Cloud Security Monitoring

Splunk ES Cloud 6.4

통합 클라우드 보안을
구축하고 강화

멀티 클라우드
환경에서 데이터를
운영할 수 있도록

멀티 클라우드 환경에서
중요한 보안 이벤트를
분류하는 시간을 30-50%
단축

Incident Review

Urgency

- CRITICAL 2
- HIGH 0
- MEDIUM 1
- LOW 0
- INFO 0

Status

New x

Owner

Select...

Security Domain

Select...

Tag

Type...

Correlation Search Sequenced Event

- ESCU - Malicious PowerShell Process - ... x
- Geographically Improbable Access DeL... x
- Unusual Volume of Outbound Traffic B... x

Search

10.0.1.4 OR fyodor*

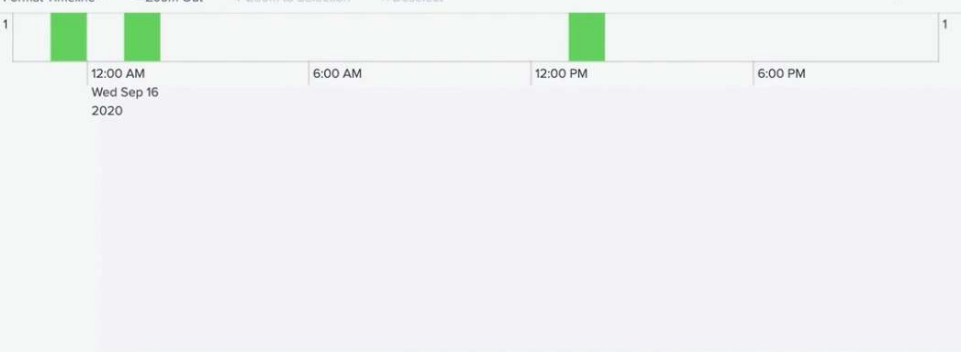
Time

Last 24 hours

Submit

3 events (9/15/20 10:00:00.000 PM to 9/16/20 10:04:51.000 PM)

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column



Incident Review Events

Edit Selected | Edit All 3 Matching Events | Add Selected to Investigation

i	<input type="checkbox"/>	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	<input type="checkbox"/>	9/16/20 1:00:58.000 PM	Network	Unusual Volume of Network Activity	Medium	New	unassigned	
>	<input type="checkbox"/>	9/16/20 1:05:12.000 AM	Access	Geographically Improbable Access Detected For fyodor@froth.ly	Critical	New	unassigned	
>	<input type="checkbox"/>	9/15/20 11:30:15.000 PM	Endpoint	Malicious PowerShell Process - Encoded Command On FYODOR-L.froth.ly	Critical	New	unassigned	

Successful security practices in AWS

Identify, investigate, and respond to threats in your AWS environments at scale

Main Services for Security Monitoring

AWS CloudTrail



Logs activity in your AWS environment

AWS GuardDuty



Native threat detection service

AWS Config



Inventory and configuration monitoring

Interesting CloudTrail Events

CloudTrail:

- DeleteTrail
- StopLogging
- UpdateTrail

VPCs:

- CreateVpcPeeringConnection
- AcceptVpcPeeringConnection
- CreateClientVpnEndpoint

GuardDuty:

- DeleteDetector
- DeleteMembers
- DisassociateFromMasterAccount
- DisassociateMembers
- StopMonitoringMembers

KMS:

- ScheduleKeyDeletion
- DisableKey

Security Groups:

- AuthorizeSecurityGroupEgress
- RevokeSecurityGroupEgress

NACLs:

- DeleteNetworkAcl
- CreateNetworkAclEntry
- DeleteNetworkAclEntry
- ReplaceNetworkAclEntry
- ReplaceNetworkAclAssociation

CloudTrail Use Cases

Root login detected:

```
... eventName=ConsoleLogin AND userIdentity.type=Root
```

Failed IAM Console Logins

```
... errorMessage="Failed*" eventName=ConsoleLogin
| stats count by sourceIPAddress
```

Brute Force Password Spraying:

```
... eventName="ConsoleLogin" action="failure"
| bin _time span=5m
| stats values(dest) values(eventType)
values(eventName) latest(_time) dc(userName) as
dc_users by src, _time
| where dc_users>=5
```

Encryption Key Protection Disabled

```
... eventName IN (ScheduleKeyDeletion,DisableKey)
errorCode=success
| stats values(dest) values(eventType)
values(eventName) by _time, userName, src
```

Unauthorized Call:

```
... errorCode="AccessDenied" OR
errorCode="UnauthorizedOperation"
| stats count by eventName userIdentity.arn
```

Interesting GuardDuty Events

EC2:

- Backdoor:EC2/DenialOfService
- Behavior:EC2/NetworkPortUnusual
- Recon:EC2/Portscan
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DropPoint
- UnauthorizedAccess:EC2/TorClient

IAM:

- Policy:IAMUser/RootCredentialUsage
- PrivilegeEscalation:IAMUser/AdministrativePermissions
- Recon:IAMUser/MaliciousIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration

S3:

- Discovery:S3/BucketEnumeration.Unusual
- Stealth:S3/ServerAccessLoggingDisabled
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- Impact:S3/ObjectDelete.Unusual

GuardDuty Use Cases

Logins From New IP Addresses:

```
...
detail.type="UnauthorizedAccess:IAMUser/ConsoleLogin"
| dedup
"detail.service.action.awsApiCallAction.remoteIpDetails.ipAddressV4"
| where
"detail.service.action.awsApiCallAction.remoteIpDetails.organization.org"!=<your org>
...
```

Credential Exfiltration:

```
...
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration
```

RDP Brute Forcing:

```
... detail.type IN
("UnauthorizedAccess:EC2/RDPBruteForce",
"UnauthorizedAccess:EC2/SSHBruteForce")
```

Privilege Escalation: IAMUser/AdministrativePermissions

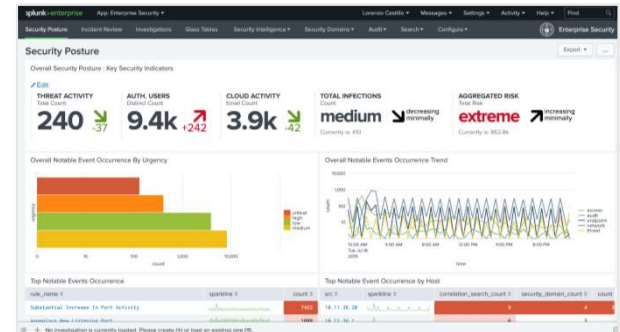
```
...
"detail.type"="PrivilegeEscalation:IAMUser/AdministrativePermissions"
```

FORUM 2020

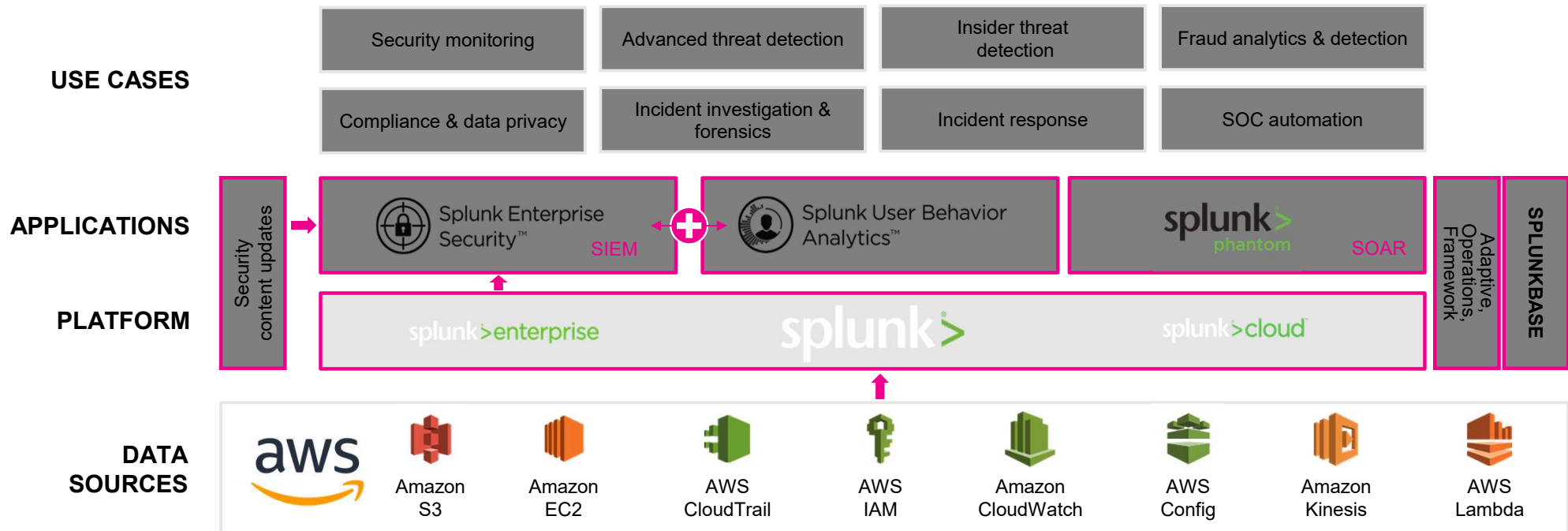


Security posture of your AWS workloads

Detection and Investigation Use Cases



Splunk Security Operations Suite



Let's look first at some detection and investigation use cases with **AWS** and **Splunk Enterprise Security (SIEM)**

Use Case 1: Protecting Your AWS Account

- API는 AWS 계정과 상호 작용하는 방식을 지원합니다.
- API에 대한 액세스 및 사용에 대한 제어가 중요합니다.
 - 비정상적인 위치에서 자격 증명을 사용하고 있습니까?
 - 현재 **휴면 자격 증명**이 사용되고 있습니까?
 - 자격 증명이 **비정상적인 방식**으로 사용되고 있습니까?



Use Case 1: Account Protection

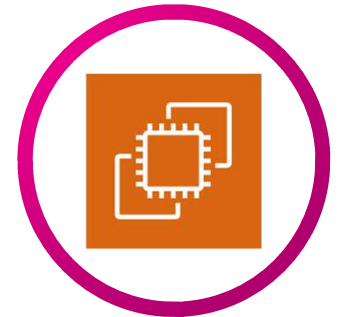
Essential data mapping and detection rules

AWS Data Source	Source type in Add-on	CIM Model	Detection in Splunk ES
CloudTrail	aws:cloudtrail aws:kinesis:firehose	Authentication Change Analysis	Any AWS Account Activity Notable in ES Use Case library ES Content Update pack
GuardDuty	aws:cloudwatch:guardduty	Alert Intrusion Detection	GuardDuty Finding as Notable Event in ES – common ones: UnauthorizedAccess:EC2/MaliciousIPCaller* UnauthorizedAccess:IAMUser/MaliciousIPCaller* Recon:IAMUser/MaliciousIPCaller Policy:IAMUser/RootCredentialUsage

Use Case 2: Protecting Virtual Compute Resources

Amazon EC2는 고객 워크로드의 핵심 구성 요소입니다.

EC2 기반 워크로드에 대한 위협을 이해하는 것이 중요합니다.



- 누군가 내 인스턴스를 스캔하여 침입하는 방법을 찾고 있습니까?
- 인스턴스가 비정상적인 방식으로 작동하기 시작 했습니까?
- 인스턴스가 알려진 위험(Command and control Server)과 통신을 시작 했습니까?

Use Case 2: Defending Compute Resources

Essential data mapping and detection rules

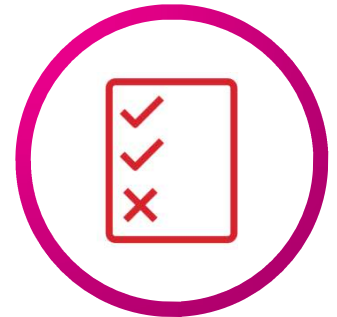
AWS Data Source	Source type in Add-on	CIM Model	Detection in Splunk ES
VPCFlow logs	aws:cloudwatchlogs:vpflow	Network_Traffic	Port Scanning activity Detect Spike in blocked Outbound Traffic from your AWS AWS Network Access Control List Created with All Open Ports
CloudTrail	aws:cloudtrail	Change Analysis	EC2 Instance Started In Previously Unseen Region EC2 Modified by Previously Unseen User All AWS activities from
GuardDuty	aws:guardduty	Alert Intrusion Detection	GuardDuty Finding – common rules: Recon:EC2/Portscan UnauthorizedAccess:EC2/SSHBruteForce Trojan:EC2/DNSDataExfiltration Backdoor:EC2/C&CActivity.B!DNS CryptoCurrency:EC2/BitcoinTool.B!DNS

Use Case 3: Maintaining Compliance

내부 및 외부 통제에 대한 규정 준수 유지.

규정 위반으로 인한 데이터 위험 발생

광범위한 AWS 리소스 세트에서 규정 준수 유지 필요.



- 현재 규정을 준수하고 있습니까?
- AWS에서 규정 준수 모범 사례를 준수하고 있습니까?
- 규정 준수에서 벗어나는 즉시 알아야합니다.
- 규정을 위반하면 신속하게 문제를 해결해야합니다.





Use Case 3: Maintaining Compliance

Essential data mapping and detection rules

AWS Data Source	Source type in Add-on	CIM Model*	Detection in Splunk ES
SecurityHub	aws:securityhub*	Alert Inventory Change	SecHub Findings based on <ol style="list-style-type: none"> CIS AWS Foundations Benchmark controls – e.g. Password policies Security Groups controls PCI DSS Data Protection controls Secure network configs
CloudTrail	aws:cloudtrail	Change Authentication	S3 Bucket Exposed EC2 Instance changes Asset Ownership unspecified High Number of Hosts Unpatched
Config Rules	aws:config:rules	Alerts	ES Investigation Support

Cloud Threat Detections using Splunk ES

Leveraging security content and use cases

	Threat Category	Domain Data Model	Detection Rules in ES*
	User Activities	Authentication Change	<ul style="list-style-type: none"> • Access behavior • Login attempts analytics • Changes by User analytics
	Network & Host Activities	Endpoint Malware Network, Web	<ul style="list-style-type: none"> • High malicious network volume on host • Unrouteable activity • Container monitoring • DNS Traffic
	Compliance	Change Cloud Storage	<ul style="list-style-type: none"> • State of Cloud Resources • New open/public bucket • Storage access analytics
	Data Protection	Alerts Audit Data Loss Prevention	<ul style="list-style-type: none"> • Gaps in Data • Financial data in sensitive storage

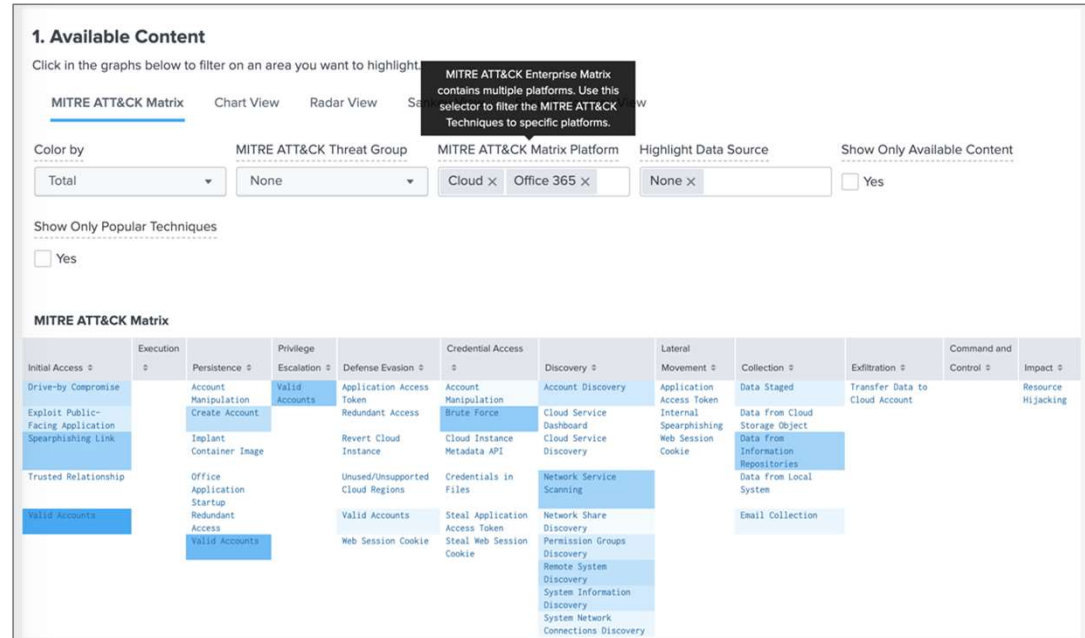
*More detections available via ES Content Update and authored via Security Essentials Apps

Splunk Security Essentials을 이용한 탐지



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

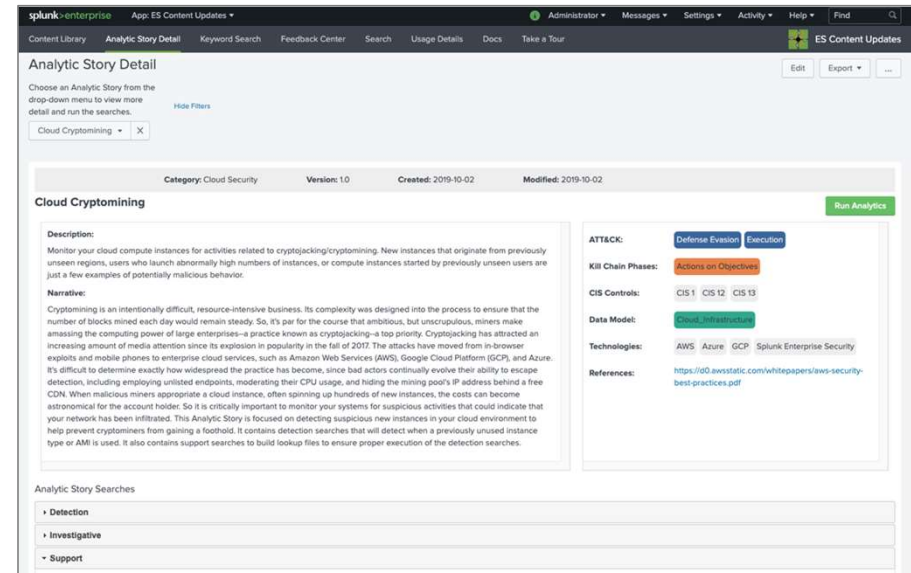
- 사용자 당 평소보다 자주 호출되는 Cloud API
- 일반적이지 않은 국가의 클라우드 프로비저닝 활동
- 일반적이지 않은 IP의 클라우드 프로비저닝 활동
- 일반적이지 않은 사용자가 만든 인스턴스
- 일반적이지 않은 사용자가 수정 한 인스턴스
- 피어 그룹당 새 Cloud API 호출
- 사용자 당 새로운 IaaS API 호출
- 퍼블릭 클라우드 스토리지 (버킷)
- 일반적이지 않은 클라우드 지역
- 일반적이지 않은 클라우드 ACL 수정 횟수



Splunk ES Content Updates를 이용한 탐지

<https://splunkbase.splunk.com/app/3449/> & <https://github.com/splunk/security-content>

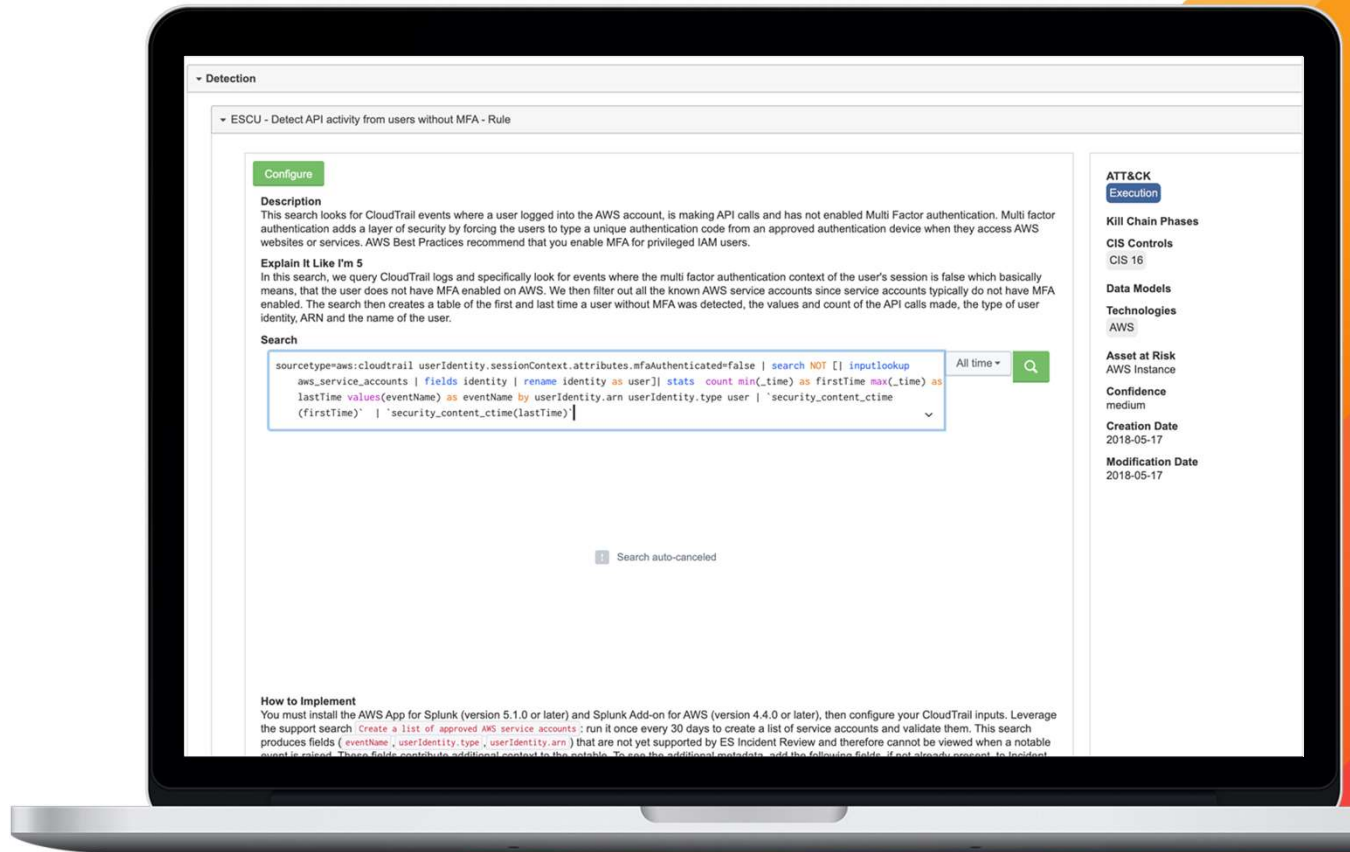
- 클라우드 크립토마이닝
- Container Implantation Monitoring & Investigation
- Kubernetes 스캐닝 활동
- Kubernetes 민감한 개체 액세스 활동
- Kubernetes 민감한 역할 활동
- 이전에 보지 못한 사용자가 만든 클라우드 컴퓨팅 인스턴스
- 이전에 보지 못한 이미지로 생성 된 클라우드 컴퓨팅 인스턴스
- 이전에 사용되지 않은 리전에서 시작된 클라우드 컴퓨팅 인스턴스
- 클라우드 컴퓨팅 인스턴스 활동 조사
- 모든 클라우드 지역의 사용자 활동 조사



The screenshot displays the 'Analytic Story Detail' page for 'Cloud Cryptomining' in the Splunk ES Content Updates application. The interface includes a navigation bar with 'App: ES Content Updates', user roles, and search options. The main content area shows the story's title, category (Cloud Security), version (1.0), and creation/modification dates (2019-10-02). A 'Run Analytics' button is visible. The 'Description' section provides a summary of the story's purpose: monitoring cloud compute instances for cryptojacking/cryptomining activities. The 'Narrative' section offers a detailed background on the complexity of cryptomining and the challenges of detection. On the right, there are sections for 'ATTACK' (Defense, Evasion, Execution), 'Kill Chain Phases' (Actions on Objectives), 'CIS Controls' (CIS 1, CIS 12, CIS 13), 'Data Model' (cloud_infrastructure), 'Technologies' (AWS, Azure, GCP, Splunk Enterprise Security), and 'References' (a link to an AWS whitepaper). At the bottom, there is a section for 'Analytic Story Searches' with expandable categories: Detection, Investigative, and Support.

Example

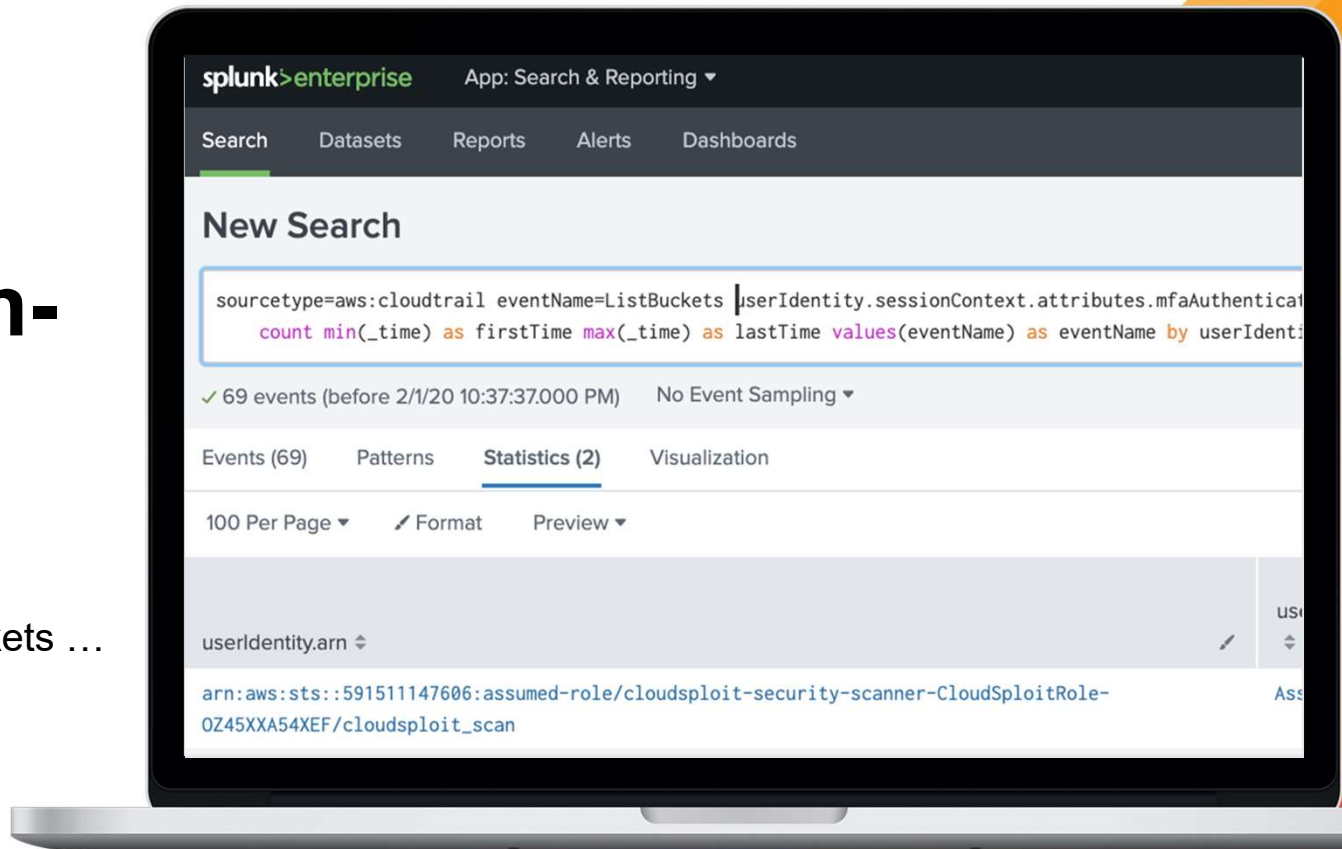
Simple detection of users activity without MFA



Detection of Activity by Non-MFA Enabled Accounts



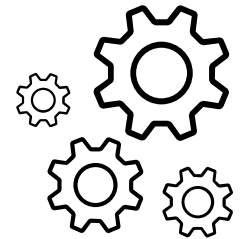
Non MFA enabled user listing buckets ...



FORUM 2020

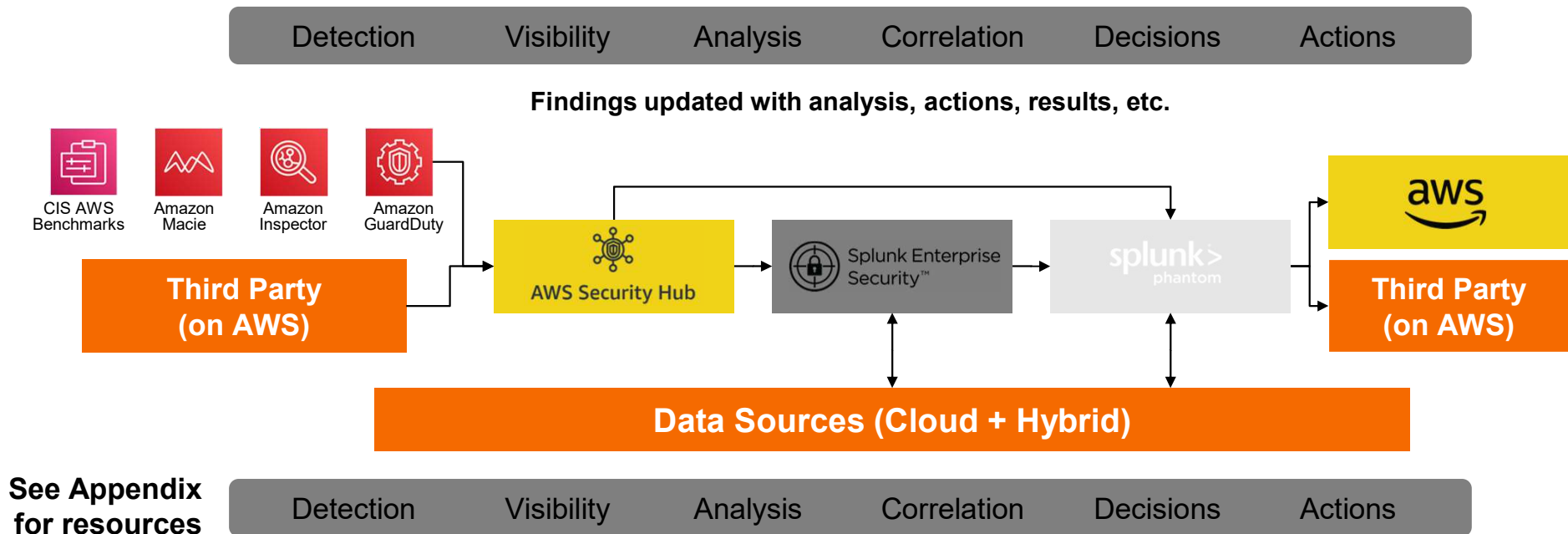
Automated Threat Mitigation

Automated decision making and response with AWS and Splunk



Automated Cloud Security Incident Response

End-to-End SecOps By Combining AWS Services with Splunk ES/SIEM and Phantom/SOAR



See Appendix for resources

Cloud SOAR Use Case 1

Automated Response in Splunk Phantom to a SecurityHub finding

Observe

1

AWS SecurityHub

- SecurityHub는 노출된 EC2 인스턴스의 잠재적 위협을 감지합니다.
- SecurityHub는 결과를 CloudWatch 이벤트로 트리거합니다.
- Cloudwatch 이벤트 규칙은 결과를 SQS Queue에 전달합니다.
- Phantom App for SecurityHub SQS

Decide

2

Playbook: EC2 Instance Investigation

- 수집을 위해 자동화된 단계:
 - 위험 레벨과 세부 정보 찾기
 - EC2 인스턴스 구성
 - 호스트 활동
- 연결된 인스턴스 정보 가져오기
 - IP 평판 확인
 - 위치 정보 확인
- service ticket 생성
- Slack message 보안팀에 전송

Act

3

Playbook: Instance Isolation

- 자동화된 스텝:
- 격리된 security group 에 인스턴스 이동

FORUM 2020

splunk>

Automated Threat Mitigation Demo

Detect & remediate compromised VM instance



- Compute Engine
- VM instances
- Instance groups
- Instance templates
- Sole-tenant nodes
- Machine images
- Disks
- Snapshots
- Images
- TPUs
- Migrate for Compute Engine
- Committed use discounts
- Metadata
- Health checks
- Zones
- Network endpoint groups
- Operations
- Security scans
- OS patch management
- Settings

splunk-es-ig

CPU platform
Intel Broadwell

Display device
Turn on a display device if you want to use screen capturing and recording tools.
 Turn on display device

Zone
us-west1-b

Labels
None

Creation time
Oct 3, 2020, 9:29:46 AM

Network interfaces

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP	Network Tier	IP forwarding	Network details
nic0	default	default	10.138.0.17	—	None		Off	View details

Firewalls
 Allow HTTP traffic
 Allow HTTPS traffic

Network tags
http-server, https-server, splunk

Deletion protection
 Enable deletion protection
When deletion protection is enabled, instance cannot be deleted. [Learn more](#)

Confidential VM service
Disabled

Boot disk

Name	Image	Size (GB)	Device name	Type	Encryption	Mode
wissam-demo-compromised-vm	ubuntu-1604-xenial-v20200923	50	wissam-demo-compromised-vm	Standard persistent disk	Google managed	Boot, read/write

Additional disks

SOAR Use Case 1 Demo

Detect & remediate compromised VM instance

Cloud SOAR Use Case for Multicloud



AWS EC2 Publisher: Splunk Version: 1.0.7 [Documentation](#)

This app integrates with AWS Elastic Compute Cloud (EC2) to perform virtualization actions

▼ 20 supported actions

- **list autoscaling groups** - Display autoscaling groups
- **list network interfaces** - Display network interfaces
- **create vpc** - Create a VPC with the specified IPv4 CIDR block
- **remove instance** - Removes an EC2 instance from a security group
- **assign instance** - Assign an instance to a security group
- **list security groups** - Display security groups
- **remove acl** - Remove ACL from an instance. The default network ACL and ACLs associated with any subnets
- **add acl** - Add ACL to an instance
- **get acls** - Get one or more network ACLs
- **remove tag** - Remove specified tag from an instance
- **add tag** - Add tag to an instance
- **get tag** - Get the value of a tag for the given instance ID
- **snapshot instance** - Snapshot AWS instance that has the given IP address or instance ID
- **deregister instance** - Deregister an instance from AWS Elastic Load Balance
- **attach instance** - Attach an instance to an autoscaling group
- **detach instance** - Detach an instance from an autoscaling group
- **describe instance** - Describe one or more instances
- **stop instance** - Stop one or more instances
- **start instance** - Start one or more instances
- **test connectivity** - Validate the asset configuration for connectivity using supplied configuration



Microsoft Azure Compute Publisher: Splunk Version: 1.0.10 [Documentation](#)

This app implements virtualization actions for Microsoft Azure Virtual Machines

▼ 22 supported actions

- **run command** - Run a command on the virtual machine
- **redeploy vm** - Redeploy a virtual machine
- **generalize vm** - Set the state of the virtual machine to be generalized
- **get ip availability** - Check if a private IP address is available for use
- **list subnets** - Get the list of subnets
- **list virtual networks** - Get the list of virtual networks
- **add application group** - Add an application security groups in a resource group
- **add network group** - Add a network security group in a resource group
- **list security groups** - Get the list of all security groups in a resource group
- **list snapshots** - Get the list of snapshots under the subscription
- **list resource groups** - Get the list of resource groups for the subscription
- **create tag** - Create or update a tag
- **list tags** - Get the names and values of all resource tags that are defined in the subscription
- **deallocate vm** - Shut down the virtual machine and release the compute resources. You are not billed
- **delete vm** - Delete a VM
- **stop vm** - Stop a VM
- **start vm** - Start a stopped or suspended VM
- **snapshot vm** - Take a snapshot of the VM
- **list vms** - Get the list of registered VMs
- **get system info** - Get information about a VM
- **generate token** - Generates a token
- **test connectivity** - Validate the asset configuration for connectivity using supplied configuration



Google Cloud Compute Engine Publisher: FDSE Version: 1.0.0 [Documentation](#)

This app integrates with Google Cloud Compute Engine

▼ 5 supported actions

- **start instance** - Starts an instance that was previously stopped
- **stop instance** - Stops an instance
- **describe instance** - Get instance information
- **tag instance** - Modify tags on instance
- **test connectivity** - Validate the asset configuration for connectivity using supplied configuration

Customers

RAYMOND JAMES

Splunk 클라우드를 통한 빠른 가치 실현

\$790B

in Client assets

Moved

on-premises SIEM to
Splunk Cloud

2-person team

onboarded 1.5 TB
in a weekend

No infrastructure

Avg. security search from
48 hours to under 15 mins

Expanded use: from security to IT Ops,
DevOps, and IT support/ Help Desk



FINRA®

© 2017 SPLUNK INC.

FINANCIAL SERVICES – CLOUD SOLUTIONS, SECURITY

FINRA: Security in the Cloud

“Splunk Cloud gives you applications that let you get huge amounts of value from your data.”

– *Sr. Director, Information Security*

- ▶ Transforms third-party threat intelligence information into security alerts
- ▶ Leverages Splunk App for AWS for log centralization and correlation
- ▶ Compliance/Governance dashboards (ensure adherence to FINRA standards)



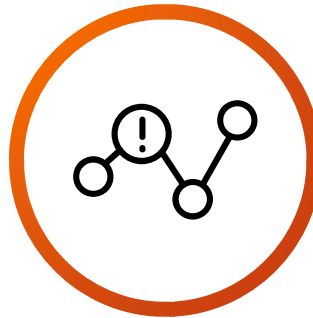
Security For the Cloud

Cloud Security Posture Management (Important for unified cloud management)



- 접근 제한
- 데이터 보호
- 감사 및 검증
- 로깅 및 모니터링
- 사용자 액세스 — 응용 프로그램
- 워크로드 구성 및 취약성 관리
- 네트워크 세분화 — 트래픽 가시성
- 컨트롤 관리
- 사고 예방

Challenges



- 다중 클라우드 환경 — 서로 다른 데이터 소스
- 가시성 부족과 데이터 제어 및 관리
- 데이터 정규화
- 규정 준수의 복잡성
- 기술 취약성
- 클라우드 남용
- 데이터 손실
- 안전하지 않은 액세스 포인트
- 알림 및 경고

Splunk Benefits (Across various cloud services)



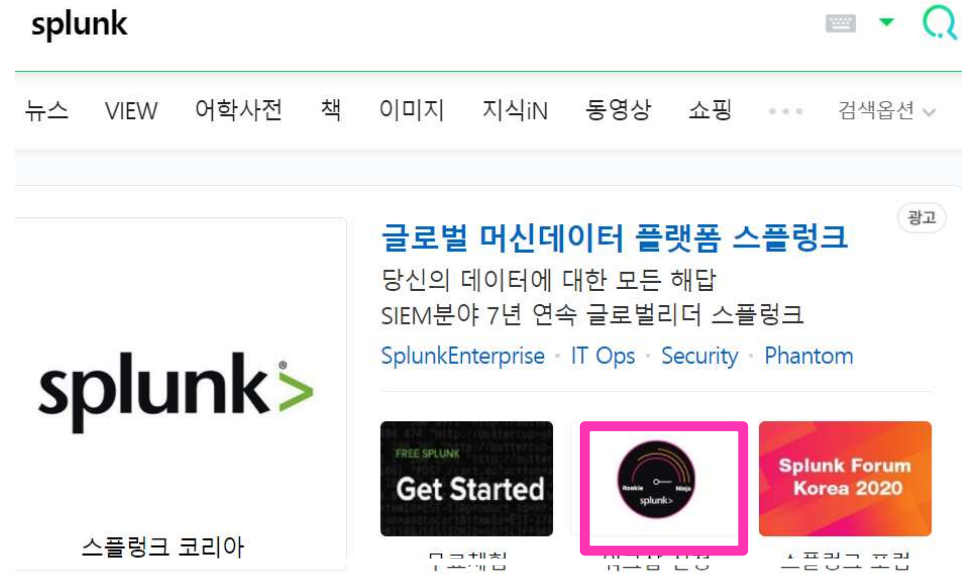
- 중요한 데이터를 정규화 및 관리하고 잘못된 구성을 방지하며 사전 경고
- 분석가에게 AWS, GCP, Azure 보안 태세에 대한 포괄적인 비전 제공
- 클라우드 환경의 취약점 모니터링, 조사 및 감지
- 다중 클라우드 위협 표면 및 취약성을 시각화하고 분석
- 여러 클라우드 제공 업체에서 클라우드 감사를 위한 항상 도구 설정

Splunk 4 Rookies 핸드온 워크샵



실습 + 무료 + 다양한 주제 + 반복

매 분기마다 Splunk Korea 에서는 정기 핸드온 워크샵을 제공합니다. 스플링크 엔지니어와 직접 Splunk의 여러 기능을 만져볼 수 있는 기회입니다!



네이버에서 스플링크를 검색, 워크샵을 신청하세요.

감사합니다!