

CLOUDSEC 2023

ENVISION IT

클라우드 공격 표면 위험 관리 및 네이티브 애플리케이션 보안

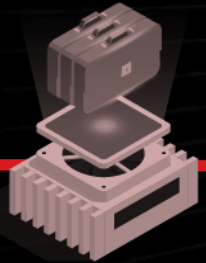
김 석 주 이사 / 트렌드마이크로

Hosted by



하이브리드 클라우드 여정

데이터센터



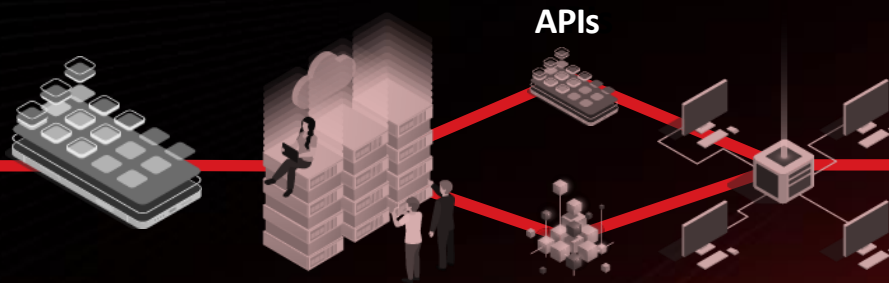
물리 서버 &
가상 서버

클라우드 환경



인스턴스 &
자동 확장

클라우드 네이티브
애플리케이션 개발



컨테이너 스토리지 3rd 라이브러리 서버리스

멀티 클라우드



보안 &
위험 관리

클라우드 여정의 보안 과제



클라우드 환경의 변화

사용자의 비즈니스 변화 전반 (데이터센터 보호, 워크로드 전환, 애플리케이션, 그리고 클라우드 네이티브 아키텍처)



하이브리드 중점

하이브리드 워크로드,
데이터센터 또는 클라우드에
적용 가능한 보안 툴



멀티 클라우드 복잡성

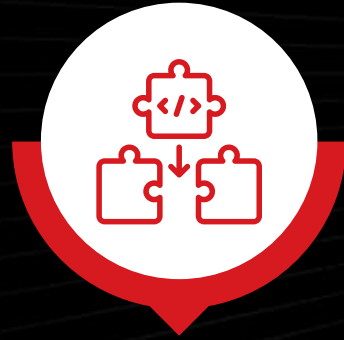
가시성과 지속적인 런타임
보호 그리고 멀티
클라우드의 보안 정책 관리



보안 사고 예방/대응

가시성 보장, 편리한 위험
우선순위, 클라우드 공격의
프로세스 인지

클라우드 보안 필요성



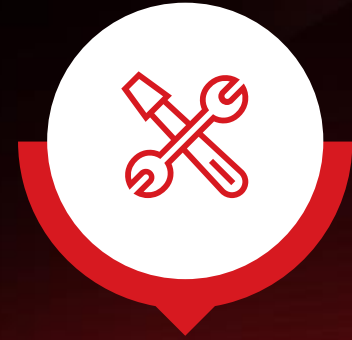
통합

보안 계층과 서비스 제공업체 전반에 걸쳐 중앙 집중화된 가시성과 관리 기능을 갖춘 통합 클라우드 보안 제어



간소화

연결된 플랫폼 워크플로우와 클라우드 자동화 및 오케스트레이션 프로세스를 통해 최적화된 사용자 경험



표준화

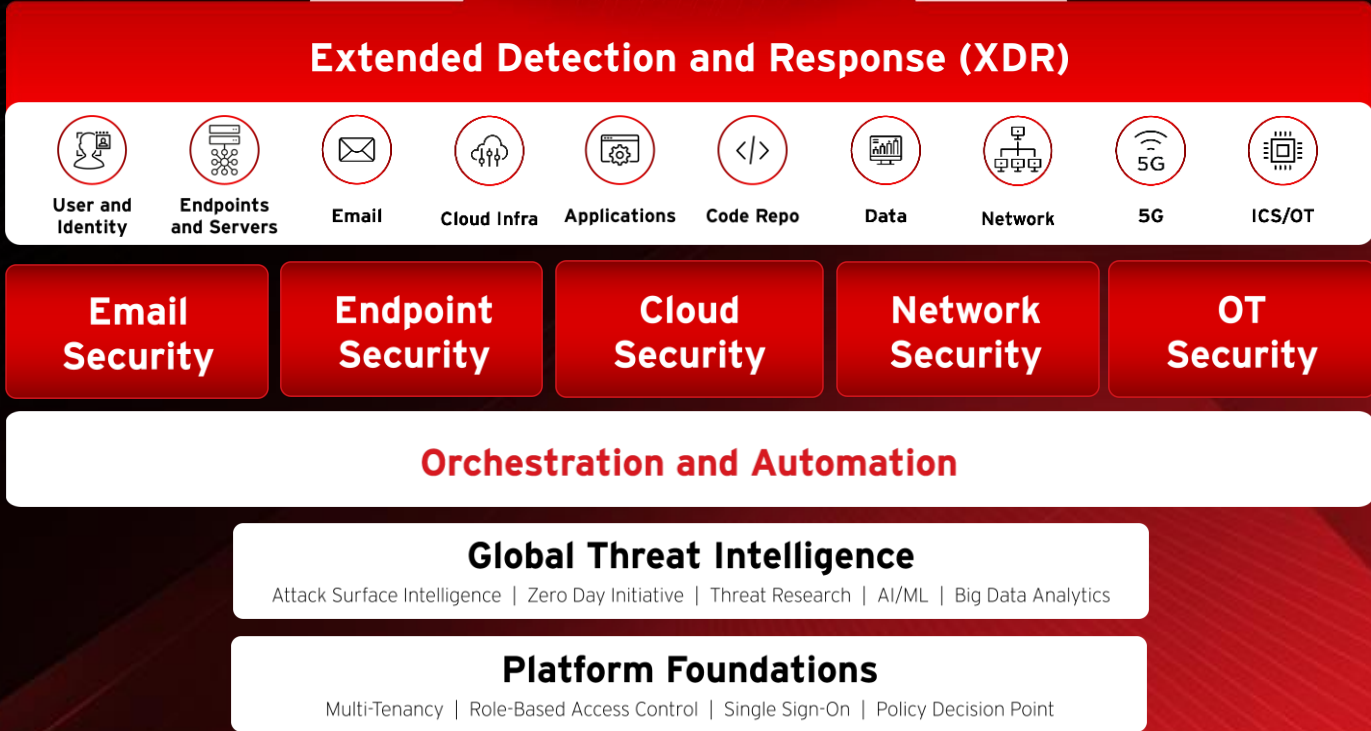
자산 검색, 보안 정책 관리, 라이선싱 등과 같은 클라우드 플랫폼 기능 전반의 일관성

보안 틀에서 사이버 보안 플랫폼으로 전환

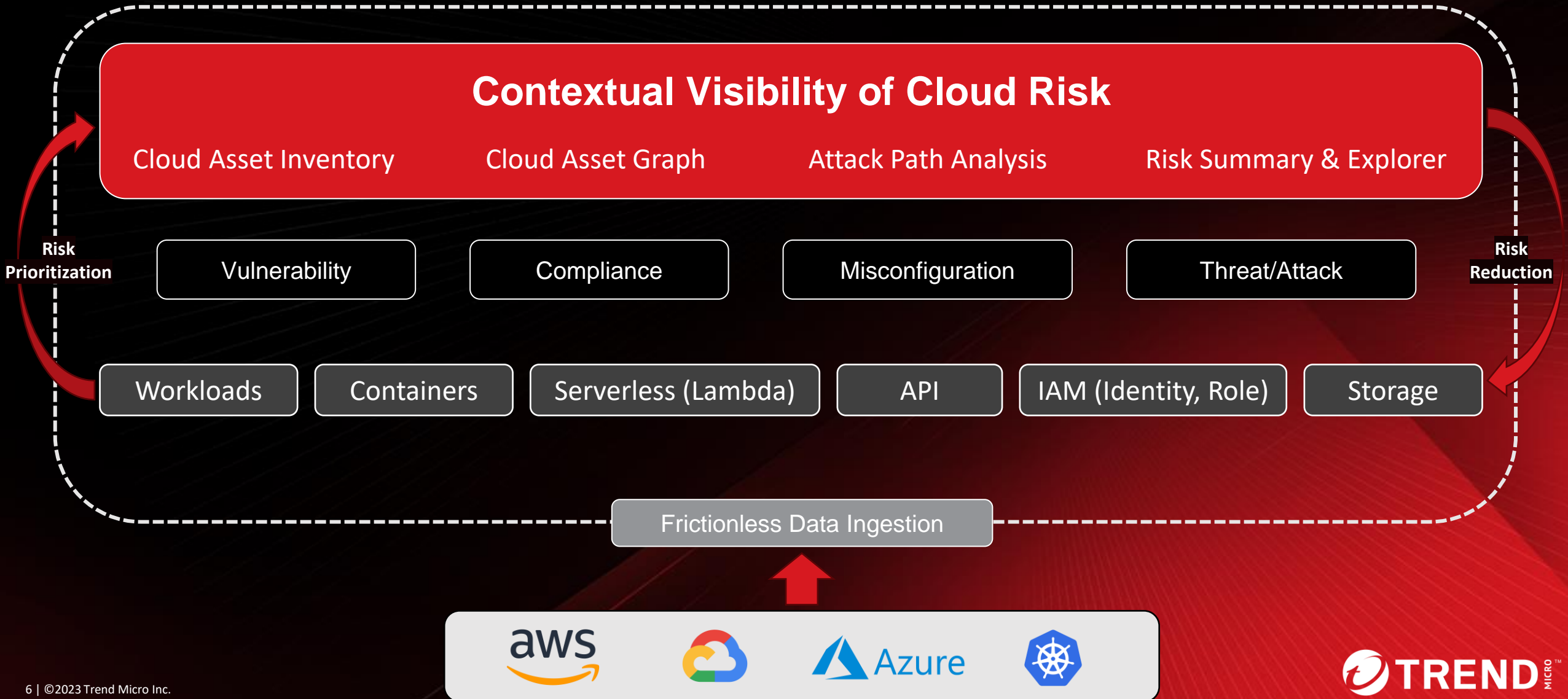


Managed Services

Ecosystem Integration



클라우드 공격 표면 위험 관리



Trend Vision One™ – 클라우드 보안

조직이 하이브리드 클라우드 환경 전반에서 위협을 신속하게 식별하고 침해 노출을 줄이며 보안 위협에 대응할 수 있도록 지원

HYBRID CLOUD STRATEGY

On-premise + Multi Cloud – AWS, Azure, GCP, and Others



ASRM for Cloud

(Attack Surface Risk Management)

하이브리드 클라우드 중심의 내부 및 외부 공격 표면 발견, 위험 우선순위 지정 및 해결



XDR for Cloud

(Cloud Detection & Response)

빠른 감지 및 대응을 위한 맞춤형 하이브리드 클라우드 원격 상관 관계 분석

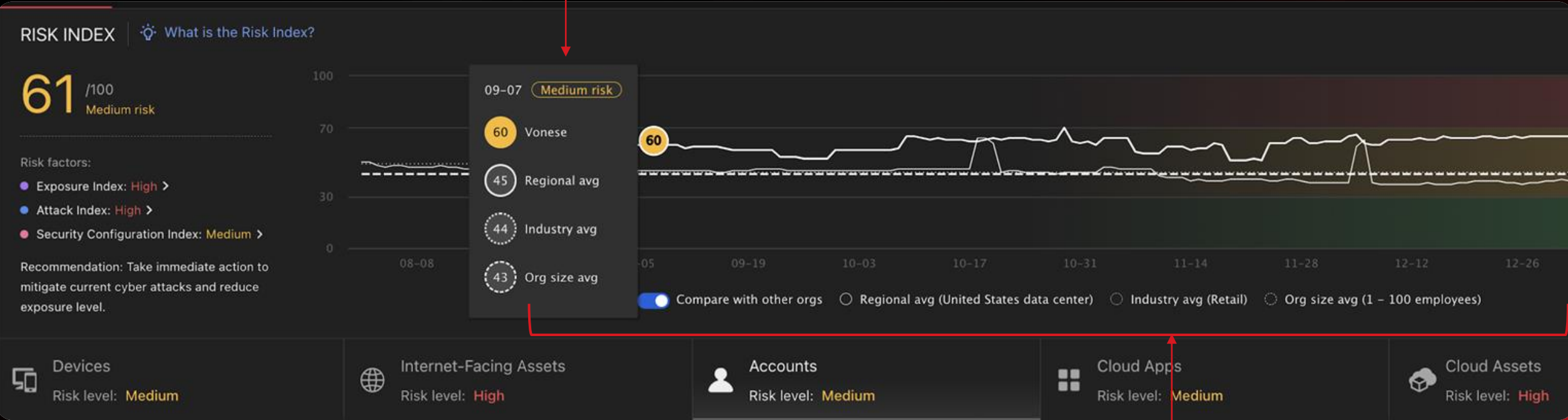


Protection

하이브리드 클라우드를 위한 주문형 및 런타임 보호. 서버, 가상 머신, 컨테이너, 스토리지 등 모든 워크로드에서 취약점과 멀웨어를 발견하고 차단

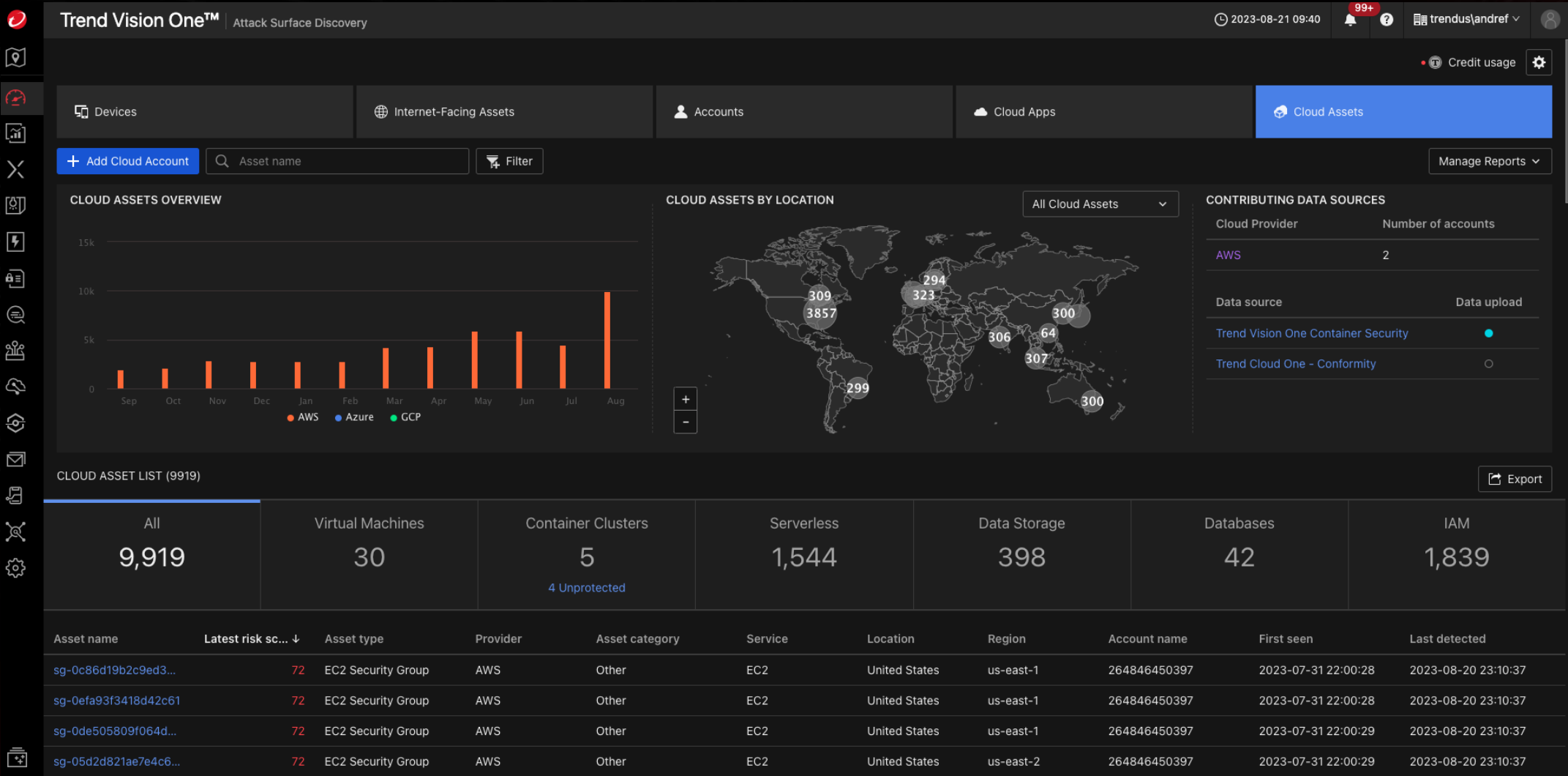
중앙 집중식 위험 가시성 및 벤치마킹

기준별 비교 분석



시간대별 위험 레벨

클라우드 자산 시각화와 위험 관리



대응 가이드가 포함된 보안 취약한 구성 가시성

Trend Vision One™ Operations Dashboard > System Configuration > Cloud Asset Compliance Violations 2023-06-16 12:30

< Back

172 rules PCI DSS(v4) 176 rules System and Organization Controls 2 (SOC 2) 114 rules AWS Well-Architected Framework

CLOUD ASSET COMPLIANCE VIOLATIONS Last assess

Standard/Framework: All Severity: All Provider: All

<input type="checkbox"/>	Rule	Severity ↓	Events	Selected standards/frameworks	Provider	Service	Asset type
<input type="checkbox"/>	Check for Unrestricted Memcached Access	High	1	AWS Well-Architected Framework, PCI ...	AWS	EC2	EC2 Security Group
	Remediation: Ensure that no security group allows unrestricted inbound access on TCP/UDP port 11211 (Memcached) View more						
<input type="checkbox"/>	> VPC Access for AWS Lambda Functions	Medium	405	AWS Well-Architected Framework			Lambda Function
<input type="checkbox"/>	> Enable Encryption at Rest for Environment Variables using Cust...	Medium	398	AWS Well-Architected Framework, PCI ...	AWS	Lambda	Lambda Function
<input type="checkbox"/>	> SQS Encrypted With KMS Customer Master Keys	Medium	85	AWS Well-Architected Framework, PCI ...	AWS	SQS	SQS Queue
	Remediation: Ensure SQS queues are encrypted with KMS CMKs to gain full control over data encryption and decryption View more						
<input type="checkbox"/>	> Enable VPC Flow Logs for VPC Subnets	Medium	76	PCI DSS(v4), System and Organization ...	GCP	CloudVPC	CloudVPC Subnet
<input type="checkbox"/>	> CloudFormation Stack Notification	Medium	52	AWS Well-Architected Framework, PCI ...	AWS	CloudFormation	CloudFormation Stack
<input type="checkbox"/>	> CloudFormation Stack Policy	Medium	52	AWS Well-Architected Framework, PCI ...	AWS	CloudFormation	CloudFormation Stack
<input type="checkbox"/>	> CloudFormation Stack Termination Protection	Medium	52	AWS Well-Architected Framework, PCI ...	AWS	CloudFormation	CloudFormation Stack
<input type="checkbox"/>	> S3 Bucket MFA Delete Enabled	Medium	44	AWS Well-Architected Framework, PCI ...	AWS	S3	S3 Bucket
	Remediation: Ensure S3 buckets have an MFA-Delete policy to prevent deletion of files without an MFA token View more						
<input type="checkbox"/>	> S3 Object Lock	Medium	44	AWS Well-Architected Framework, Syst...	AWS	S3	S3 Bucket

확인 및 해결을 위한 단계별 지침이 포함된 기술 자료 링크

컨테이너 취약점 우선순위 가시성

Trend Vision One™ Operations Dashboard > Vulnerabilities 2023-08-29 11:44 99+ trend

VULNERABILITY MANAGEMENT METRICS

Patch Management (MTTP & AUT)

- days on average to patch highly exploitable CVEs >
- 46.2 days on average that highly exploitable CVEs remain unpatched >

Highly Exploitable CVEs

- 10.5% of your internal assets contain highly exploitable CVEs >
- 0% of your hosts contain highly exploitable CVEs >
- 100% of your container clusters contain highly exploitable CVEs >
- 11 highly exploitable CVEs per internal asset on average >
- 0 highly exploitable CVEs per host on average >

Legacy Operating Systems

- 0 devices with legacy Windows systems >

HIGHLY EXPLOITABLE UNIQUE CVEs | Powered by Zero Day Initiative ⓘ

Internal Assets | Internet-facing Assets | **Containers** Last assessment: 2023-08-29

Status: New

<input type="checkbox"/>	Vulnerability ID	CVE impact score ⓘ ↓	Impacted clusters	Impacted images	Prevention rule	First seen time
<input type="checkbox"/>	> CVE-2017-5638	70	1	1	14	2023-08-23
<input type="checkbox"/>	> CVE-2017-9791	70	1	1	10	2023-08-23
<input type="checkbox"/>	> CVE-2020-17530	70	1	1	8	2023-08-23
<input type="checkbox"/>	> CVE-2013-2251	69	1	1	9	2023-08-23
<input type="checkbox"/>	> CVE-2022-22965	69	1	1	14	2023-08-23
<input type="checkbox"/>	> CVE-2018-11776	64	1	1	9	2023-08-23
<input type="checkbox"/>	> CVE-2021-39144	64	1	1	4	2023-08-23
<input type="checkbox"/>	> CVE-2017-9805	63	1	1	11	2023-08-23
<input type="checkbox"/>	> CVE-2006-1547	62	1	1	0	2023-08-23
<input type="checkbox"/>	> CVE-2013-7285	60	1	1	0	2023-08-23
<input type="checkbox"/>	> CVE-2022-37434	60	1	2	0	2023-08-23

Trend Vision One™ – 클라우드 보안

조직이 하이브리드 클라우드 환경 전반에서 위협을 신속하게 식별하고 침해 노출을 줄이며 보안 위협에 대응할 수 있도록 지원

HYBRID CLOUD STRATEGY

On-premise + Multi Cloud – AWS, Azure, GCP, and Others



ASRM for Cloud

(Attack Surface Risk Management)

하이브리드 클라우드 중심의 내부 및 외부 공격 표면 발견, 위험 우선순위 지정 및 해결



XDR for Cloud

(Cloud Detection & Response)

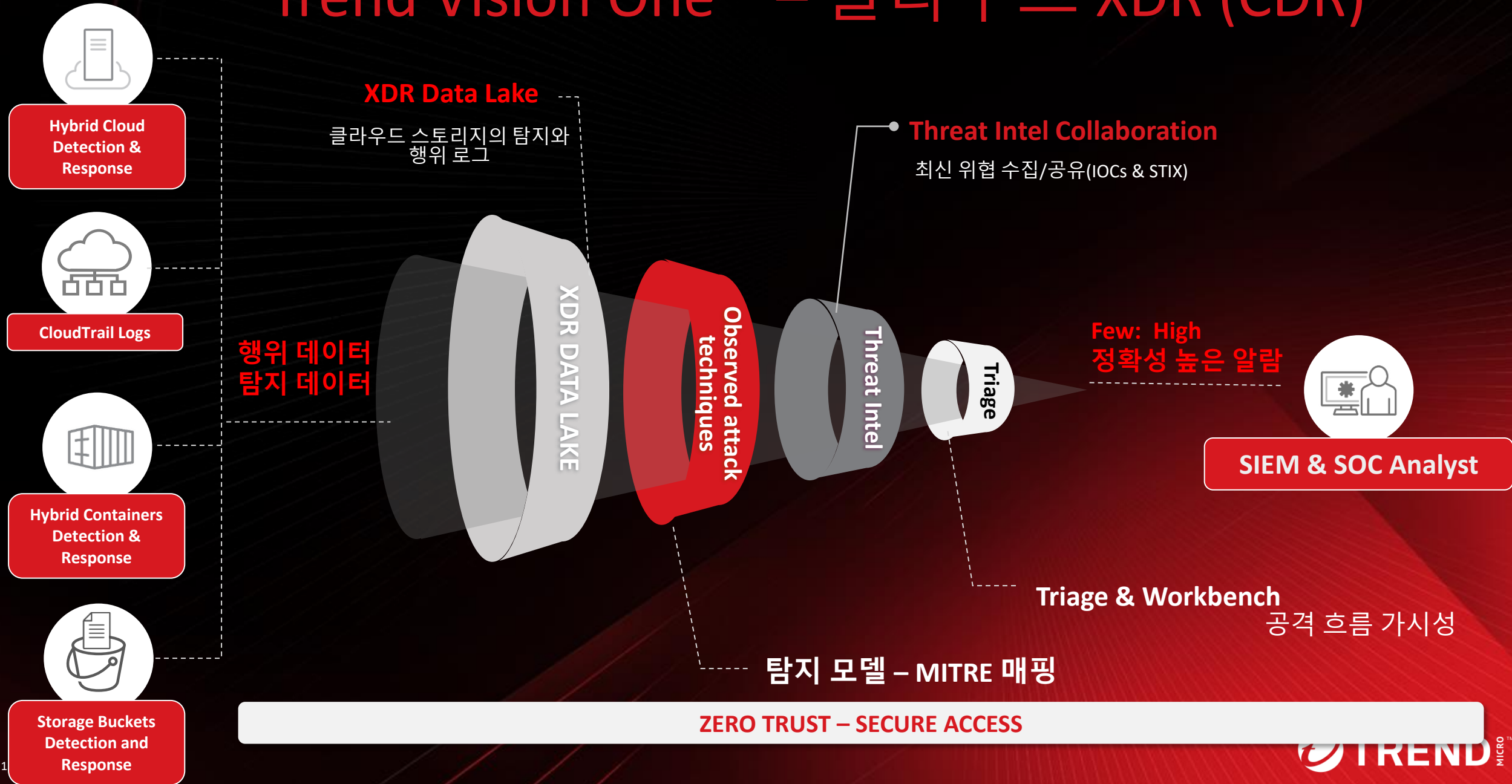
빠른 감지 및 대응을 위한 맞춤형 하이브리드 클라우드 원격 상관 관계 분석



Protection

하이브리드 클라우드를 위한 주문형 및 런타임 보호. 서버, 가상 머신, 컨테이너, 스토리지 등 모든 워크로드에서 취약점과 멀웨어를 발견하고 차단

Trend Vision One™ – 클라우드 XDR (CDR)



Trend Vision One™ – 클라우드 XDR (CDR)

탐지 모델



- 700 개 이상 탐지 모델
- 순도 높은 경고 알람
- 위협 인텔리전스 기반 데이터 레이크 로그

하이브리드 클라우드 통합 XDR



- SOC 팀을 위한 폭넓은 가시성을 위한 하이브리드 워크로드의 텔레메트리 수집
- 하이브리드 서버, 인스턴스, 컨테이너를 위한 특징적 XDR
- 클라우드 사업자의 모니터링 리소스와 연동하여 가시성 확대

사용자 정의 탐지 모델



- 정책의 유연한 생성
- 독립적, 관계적 사용자 정의 정책 생성 가능
- 행위 데이터를 수집하는 정책의 실행 빈도를 스케줄로 지정

XDR for Cloud – AWS Cloud Trail 연동

워크로드, 컨테이너 및 추가 클라우드 리소스에 대한 XDR을 포함하여 빠른 감지 및 대응을 위한 클라우드 보안 상관 관계

Trend Vision One™ | Workbook 2023-07-13 01:23

Summary

-AWS IAM Policy Attached To User Or Role Or Group
An attachment of an AWS IAM policy to user or group or role was detected.

Score: 26
Impact scope: 1 1
Created: 2023-03-19 11:47:56
Owner: None [Assign owner](#)

Highlights

AWS IAM Policy Attached To A Role
Technique: T1078 - Valid Accounts
Data source / processor: Trend Cloud One - AWS CloudTrail Integration

2023-03-19 11:41:34 | [View event](#)
(userIdentity.arn) arn:aws:sts::780477232234:assumed-role/aw...
(sourceIPAddress) 13.236.119.180
(requestParameters.policyArn) arn:aws:iam::...
(eventName) AttachRolePolicy
(arn:aws:sts::780477232234:assumed-role/a...
(arn:aws:lambda:*:780477232234:function:a...

arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
arn:aws:sts::780477232234:assumed-role/AWS-QuickSetup-HostMgmtRole-ap-...
arn:aws:sts::780477232234:assumed-role/aw...
arn:aws:sts::780477232234:assumed-role/aw...

Summary

AWS S3 Bucket Data Exfiltration
A possible data exfiltration from AWS S3 bucket that may result to stolen confidential data was identified.

Score: 43
Impact scope: 1
Created: 2023-05-12 19:33:38
Owner: None [Assign owner](#)

Highlights

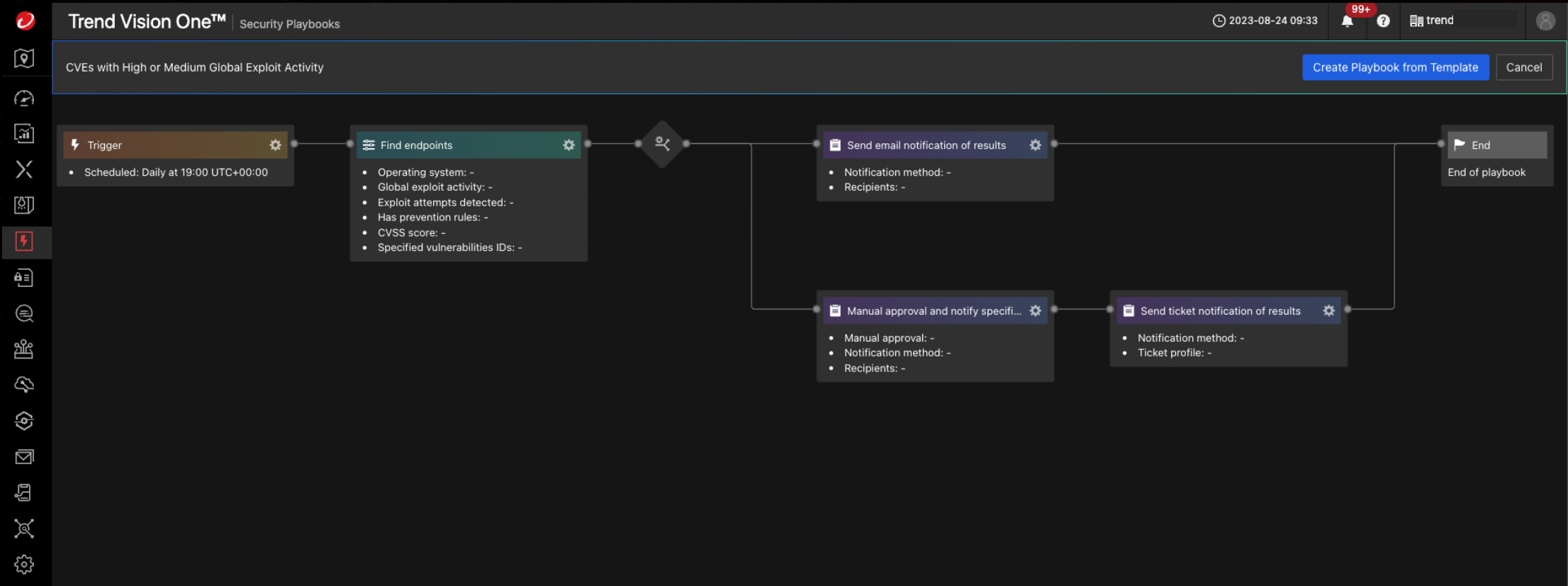
AWS S3 Bucket Listing
Technique: T1580 - Cloud Infrastructure Discovery
Data source / processor: Trend Cloud One - AWS CloudTrail Integration

2023-05-12 19:28:01 | [View event](#)
(userIdentity.accessKeyId) AKIATFTUGKBG...
(userIdentity.arn) arn:aws:iam::2182132736...
(sourceIPAddress) 47.161.29.12
(eventName) ListBuckets
(arn:aws:iam::218213273676:user/not-attac...

AWS S3 Object Sync
Technique: T1530 - Data from Cloud Storage
Data source / processor: Trend Cloud One - AWS CloudTrail Integration

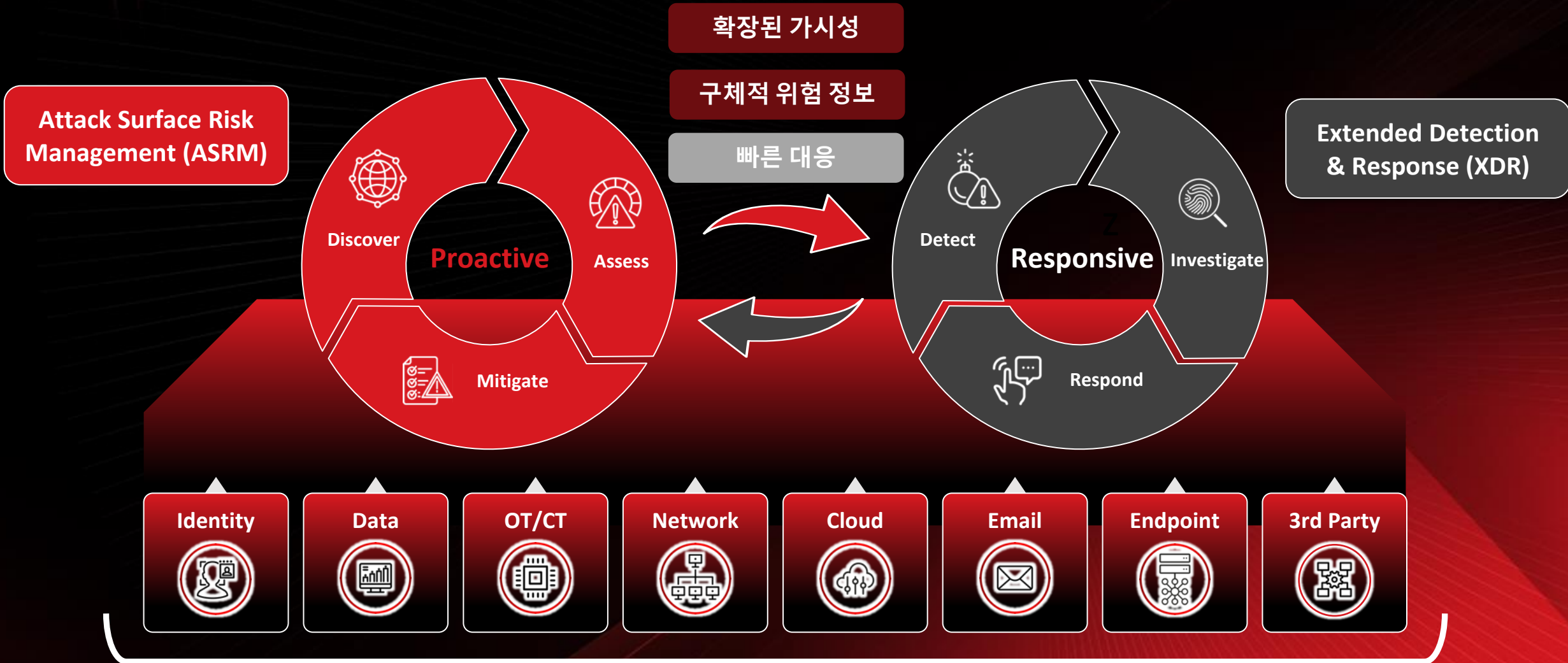
arn:aws:iam::218213273676:user/not-attacker
arn:aws:iam::218213273676:user/not-attacker
AKIATFTUGKBGDRJO4AR5
AKIATFTUGKBGDRJO4AR5
47.161.29.12

보안 플레이북



자동화 | 통합 보안 Playbook을 통해 수동 대응에서 자동화된 워크플로 및 SI 지원 대응으로 전환

Cloud: CDR/XDR + ASRM



글로벌 마켓에서 가장 광범위한 센서 범위

Trend Vision One™ – 클라우드 보안

조직이 하이브리드 클라우드 환경 전반에서 위협을 신속하게 식별하고 침해 노출을 줄이며 보안 위협에 대응할 수 있도록 지원

HYBRID CLOUD STRATEGY

On-premise + Multi Cloud – AWS, Azure, GCP, and Others



ASRM for Cloud

(Attack Surface Risk Management)

하이브리드 클라우드 중심의 내부 및 외부 공격 표면 발견, 위험 우선순위 지정 및 해결



XDR for Cloud

(Cloud Detection & Response)

빠른 감지 및 대응을 위한 맞춤형 하이브리드 클라우드 원격 상관 관계 분석

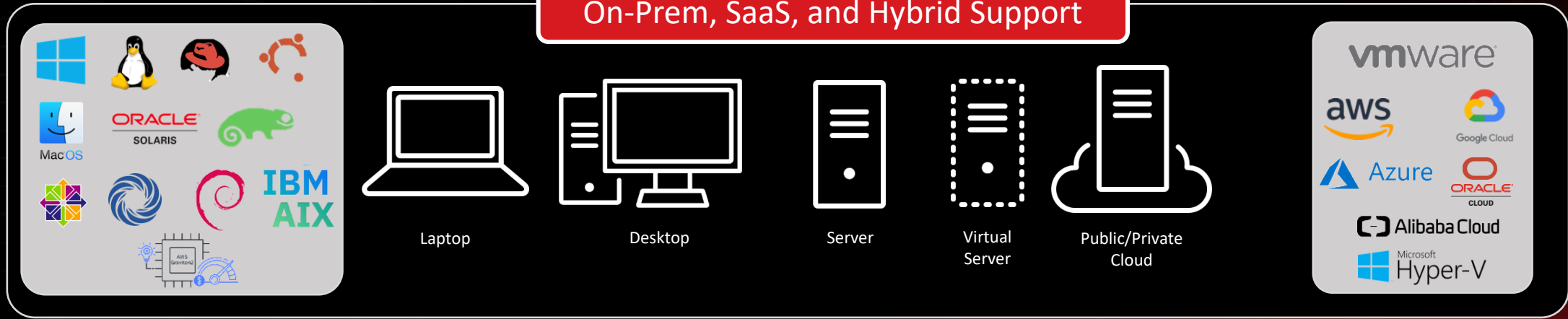


Protection

하이브리드 클라우드를 위한 주문형 및 런타임 보호. 서버, 가상 머신, 컨테이너, 스토리지 등 모든 워크로드에서 취약점과 멀웨어를 발견하고 차단

Trend Vision One™ – 서버 & 워크로드 보안

On-Prem, SaaS, and Hybrid Support



중앙 집중식 가시성 & 관리

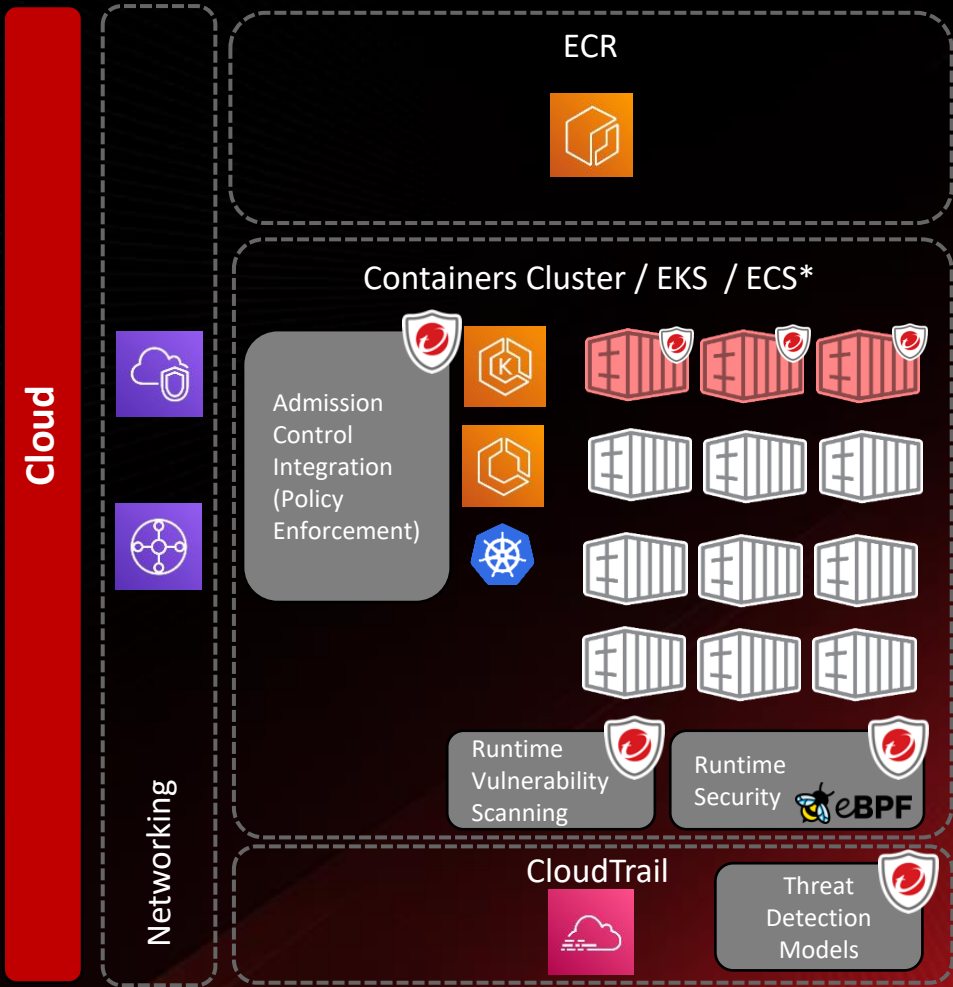
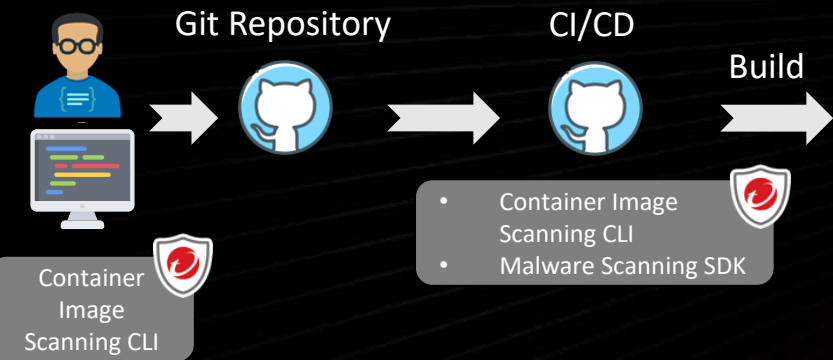
EPP & EDR/XDR을 위한 통합 플랫폼

하이브리드 워크로드의 전체 통합 보안 적용

보안 규정 준수를 지킬 수 있는 보안 범위

더 나은 분석 및 해결을 위해 보안 정보를 집계하는 데 도움이 되는 유연한 3rd Party 통합

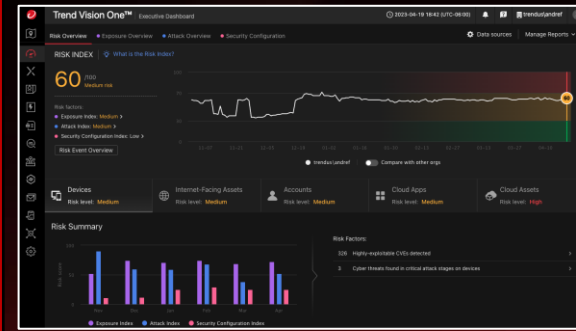
Trend Vision One™ – 컨테이너 보안



Cloud Attack Surface Risk Management
+
Cloud Detection & Response

Trend Vision One™ – Container Security

Cloud Attack Surface Risk Management



Cloud XDR + Runtime Protection

Status	Score	Workbench ID	Model name	Model severity	Impact scope	Data source / processor
71	71	WB-12287-20220507-00001	Remote Code Execution via HTTP	High	2	Trend Micro Deep Discovery Inspector
69	69	WB-12287-20220506-00000	Replicat Rootkit Entry	High	1	Endpoint Sensor
66	66	WB-12287-20220505-00000	Replicat Rootkit Entry	High	1	Endpoint Sensor
61	61	WB-12287-20220531-00007	Possible Container Escape	High	1	Trend Cloud One - Container Security
61	61	WB-12287-20220531-00004	Possible Container Escape	High	1	Trend Cloud One - Container Security
61	61	WB-12287-20220531-00003	Possible Container Escape	High	1	Trend Cloud One - Container Security



클러스터 인벤토리 시각화

클러스터 인벤토리에 대한
명확하고 체계적인 개요를
확보하여 리소스를
효과적으로 관리하고
추적하기 쉬움

클러스터, 노드, 파드!

The screenshot displays the Trend Vision One™ Container Inventory interface. The left sidebar shows a navigation tree with 'Kubernetes' expanded to 'SecinCloud'. The main panel shows details for the 'SecinCloud' cluster, including its name, description, protection status, policy, and runtime security/scanning settings. A table below lists the pods in the cluster, with columns for Pod name, Protection status, Last Evaluation, Created time, Status, and Namespace.

Pod	Protection	Last Evaluation	Created	Status	Namespace
aws-node-6t6mf	●	2023-08-29 11:45:31	2023-08-15 13:38:26	Running	kube-system
aws-node-8q72g	●	2023-08-29 11:45:31	2023-08-15 13:38:28	Running	kube-system
calico-kube-controllers-78d8c9df64-t6w29	●	2023-08-29 11:45:31	2023-08-15 13:48:57	Running	calico-system
calico-node-8rg2n	●	2023-08-29 11:45:31	2023-08-15 13:48:57	Running	calico-system
calico-node-fq7h7	●	2023-08-29 11:45:31	2023-08-15 13:48:57	Running	calico-system
calico-typha-646bb8d9bd-bzvdv	●	2023-08-29 11:45:31	2023-08-15 13:48:56	Running	calico-system
coredns-79df7ff65-p79b8	●	2023-08-29 11:45:31	2023-08-15 13:30:16	Running	kube-system
coredns-79df7ff65-rpk9k	●	2023-08-29 11:45:31	2023-08-15 13:30:16	Running	kube-system

정책 관리 & 이벤트 시각화

Trend Vision One
콘솔에서 정책, 규칙,
이벤트를 모두
원활하게 관리하고
모니터링하여 보안
운영 및 워크플로를
간소화

The screenshot displays the 'Policy Definitions' configuration page in Trend Vision One. It features a sidebar with navigation options like '+ New' and '+ Duplicate'. The main content area is divided into sections for 'Pod properties', 'Container properties', and 'Image properties'. Each section contains a list of rules with checkboxes and dropdown menus for configuration. For example, under 'Pod properties', there are rules for containers running as root, in the host network, or in the host IPC namespace. A warning banner at the top indicates that this is a 'Pre-release' feature.

This screenshot shows the 'Rulesets' configuration page. It includes a table of existing rulesets with columns for 'Mitigation', 'Rule ID', and 'Name'. The 'Mitigation' column has dropdown menus for actions like 'Log', 'Isolate', and 'Terminate'. The 'Rule ID' column contains identifiers like 'TM-00000001'. The 'Name' column lists specific rules such as '(T1546.004)Modify Shell Configuration File'. A '+ Add Rule' button is visible at the top right of the table.

Mitigation	Rule ID	Name
Log	TM-00000001	(T1546.004)Modify Shell Configuration File
Log	TM-00000002	(T1059.004)Update Package Repository
Log	TM-00000003	(T1082)Read ssh information
Log	TM-00000004	(T1003.008)Read sensitive file trusted after startup
Log	TM-00000005	(T1021.004)System user interactive
Log	TM-00000006	(T1059.004)Terminal shell in container
Log	TM-00000007	(T1020)System procs network activity
Isolate	TM-00000008	(T1613)Contact EC2 Instance Metadata Service From Container
Terminate	TM-00000009	(T1613)Contact K8S API Server From Container
Log	TM-00000010	(T1543)Launch Package Management Process in Container
Log	TM-00000011	(T1059.004)Netcat Remote Code Execution in Container
Log	TM-00000012	(T1070.002)Clear Log Activities
Log	TM-00000013	(T1059.004)Create Symlink Over Sensitive Files
Log	TM-00000014	(T1068)Packet socket created in container

보안 취약점 검사 & 시각화

Kubernetes 외에도 Amazon ECS를 지원하도록 확장된 취약성 검사를 통해 고객은 컨테이너 환경을 보호하기 위한 사전 조치 가능

Trend Vision One™ Container Protection 2023-08-29 11:49

Important: This is a "Pre-release" feature and is not considered an official release. Please review the [Pre-release Disclaimer](#) before using the feature. This feature will require credits for continued usage if officially released.

Policies Rulesets **Vulnerability** Events Artifact Scanner

Filter By: None Severity: None

Kubernetes ECS

CVE	Severity	Image	Package Name	Package Version	Fix Available
CVE-2022-23943	Critical	dvwa	apache2	2.4.25-3+deb9u5	2.4.25-3+deb9u13
CVE-2019-11039	Critical	dvwa	php7.0-opcache	7.0.30-0+deb9u1	7.0.33-0+deb9u5

Description:
Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

Vulnerability Information:

CVE	CVE-2022-23943	Package Version	2.4.25-3+deb9u5
Severity	Critical	Fix Available	2.4.25-3+deb9u13
Package Name	apache2		

Image Information:

Image	662446947455.dkr.ecr.us-east-2.amazonaws.com/dvwa:sha256:dc1421bb19a65aeb07d8eb4aff03d155c2d509ce1deca35b3d57cfdad1620c9
Registry	662446947455.dkr.ecr.us-east-2.amazonaws.com
Digest	sha256:dc1421bb19a65aeb07d8eb4aff03d155c2d509ce1deca35b3d57cfdad1620c9

Detection Information:

Container	AWS Account	Task Defini
dvwa	662446947455	arn:aws:ecr:lab:1

Trend Vision One™ Container Protection 2023-08-29 11:49

Important: This is a "Pre-release" feature and is not considered an official release. Please review the [Pre-release Disclaimer](#) before using the feature. This feature will require credits for continued usage if officially released.

Policies Rulesets **Vulnerability** Events Artifact Scanner

Filter By: None Severity: None

Kubernetes ECS

CVE	Severity	Image	Cluster	Package Name	Package Version	Fix Available
GHSA-xpfp-f569-q3p2	Critical	trendworkshopdevcecp	SecinCloud	Django	3.1.12	3.1.13
CVE-2023-38408	Critical	trendworkshopdevcecp	SecinCloud	openssh-client	1:9.2p1-2	N/A
CVE-2023-28531	Critical	trendworkshopdevcecp	SecinCloud	openssh-client	1:9.2p1-2	N/A
CVE-2019-1010022	Critical	calico/node	SecinCloud	glibc-common	2.28-211.e18	N/A
CVE-2019-1010022	Critical	calico/node	SecinCloud	glibc	2.28-211.e18	N/A
CVE-2019-1010022	Critical	calico/node	SecinCloud	glibc-minimal-langpack	2.28-211.e18	N/A
GHSA-r48q-9g5r-8q2h	Critical	calico/apiserver	Test_demo	github.com/iemickle/go-restful	v2.11.2-0.20200112161605-a7c079c43d51+incompatible	2.16.0
GHSA-r48q-9g5r-8q2h	Critical	calico/kube-controllers	Test_demo	github.com/iemickle/go-restful	v2.11.2-0.20200112161605-a7c079c43d51+incompatible	2.16.0
CVE-2019-1010022	Critical	calico/node	Test_demo	glibc-minimal-langpack	2.28-189.5.e18_6	N/A

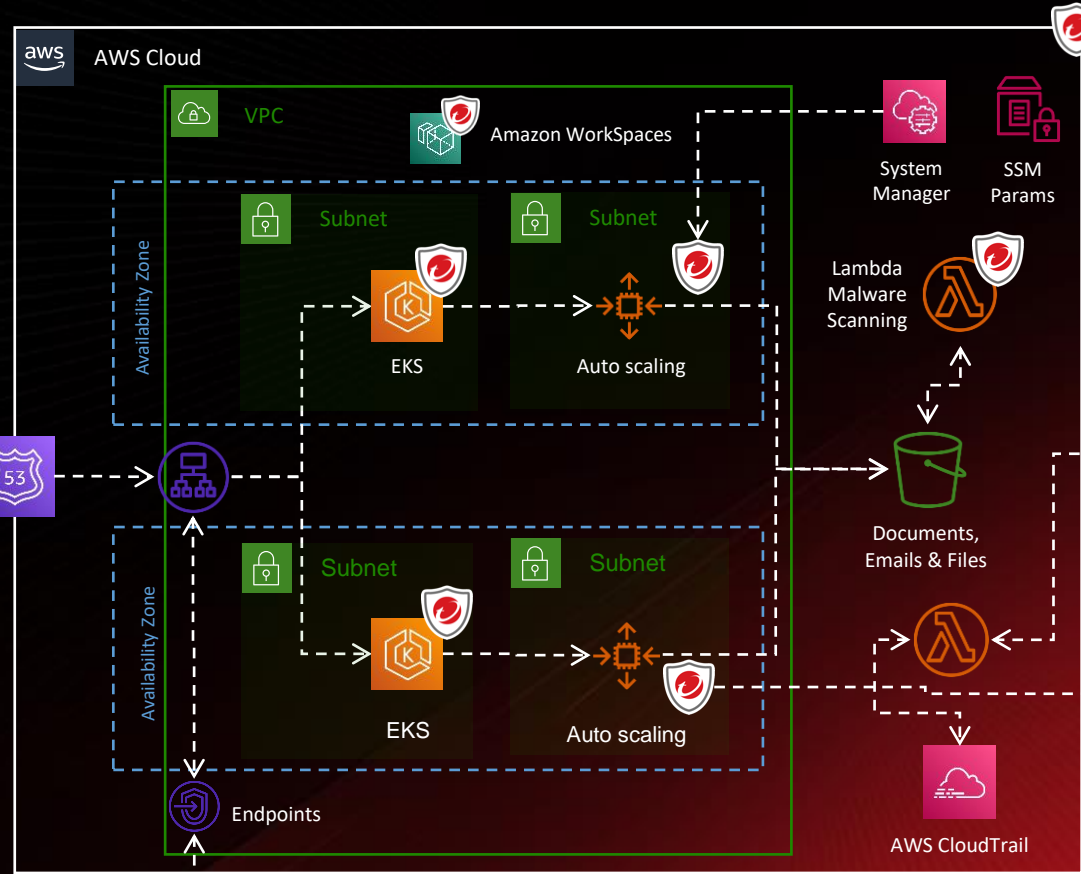
Description:
ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9.

Vulnerability Information:

CVE	CVE-2023-28531	Package Version	1:9.2p1-2
Severity	Critical	Fix Available	N/A
Package Name	openssh-client		

클라우드 고객을 위한 상호 보완적 보안(AWS Case)

- 컨테이너 런타임 보호
- 자동화된 EDR 에이전트 배포
- 보안 규정 준수 목표를 위한 넓은 보안 범위
- 클라우드 보안 취약 구성 & 컴플라이언스 규칙 매핑
- 서버리스 클라우드 네트워크 IDS/IPS
- Amazon S3를 위한 클라우드 네이티브 멀웨어 검사
- 기업의 보안적 위험 감사를 위한 통합적 XDR 연계

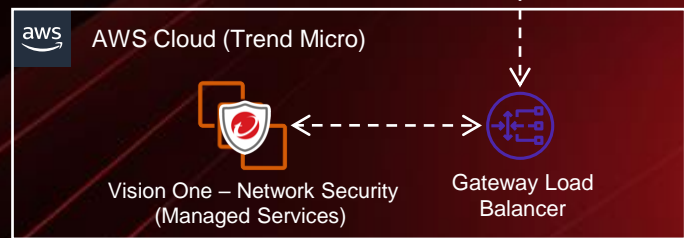


AWS Well-Architected



Trend Vision One XDR Platform

- Antimalware + Web reputation
- Firewall
- Device control
- App control
- IPS (Desktop OS)
- EDR/XDR
- IPS (Server applications)
- Integrity monitoring / Log inspection
- Container protection
- SAP scanner (add-on)





김석주 이사

Anthony_kim@trendmicro.com

트렌드마이크로