

Cloud Infrastructure Security



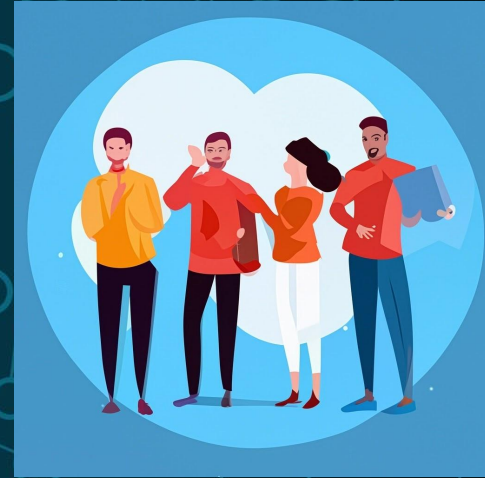
SILVERLINE
SECURITY

Agenda

1. Intro to your SilverLine Security Team
2. Problem Domain Synopsis
3. Team Process & Documentation
4. Application Demonstration
5. Q&A

Team SilverLine

1. Benjamin Hobbs
2. Raheem Reed
3. David Siebert
4. Natasha Siramarco
5. Nick Van Noort



Benjamin Hobbs

Cybersecurity Engineer

- Background:
 - Supply-Chain/Logistics
 - Real Estate Agent
- Why Cyber?:
- My Experience:
 - Military
 - Business School
 - Life

Fun fact: Trivia Enthusiast

Career Goals: To create a widely-used tool in cybersecurity



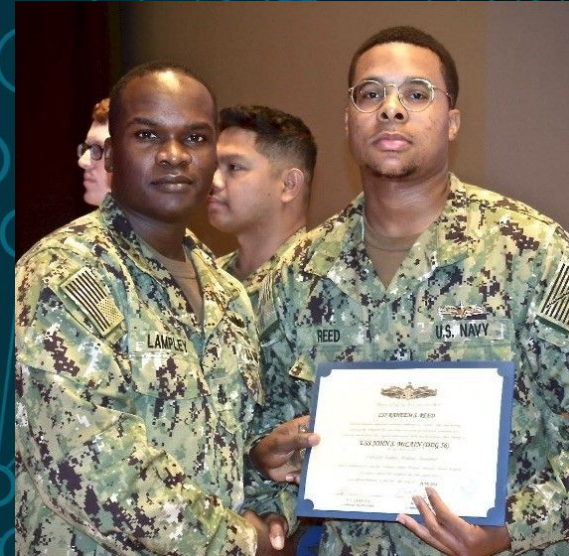
Raheem Reed

Cybersecurity Professional

Background: US Navy Veteran and Culinary arts

Why Cyber? I always wanted to help people and have a career where I can keep learning. My interest in cybersecurity has been something I wanted to pursue since I was a kid and I'm glad I'm taking this journey now.

Fun Facts: I have a love for boxing, anime, reading and chess



David Siebert

Cybersecurity Professional

Background

Retired US Army

Licensed Healthcare & Finance careers

Why Cyber?

- The ever evolving world of data protection!

Fun Fact: Automotive enthusiast.



Natasha Siramarco

CyberSecurity Professional

- Previous experience: Military
- Reason: Solving puzzles, change in career, teach others
- Interesting/fun fact:
 - I spend free time doing brain-teasers Puzzles
 - Travel and bake with my children



Nick Van Noort

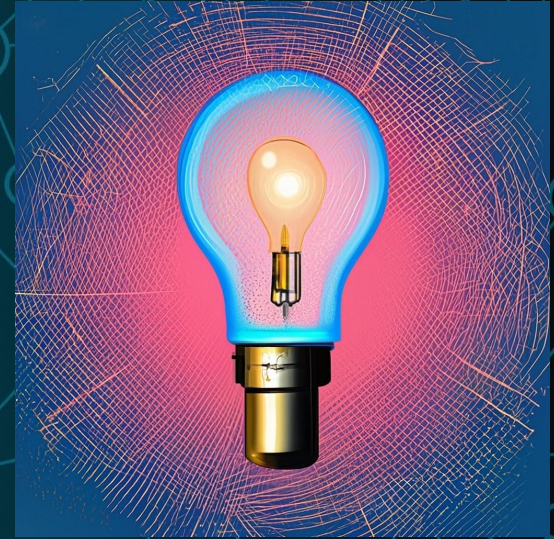
- 12 Years of experience as a Certified Financial Planner(CFP)
- 10 Years in the Army
- Unique skill set in identifying and mitigating vulnerabilities for organizations in an ever-evolving digital landscape



Problem Domain

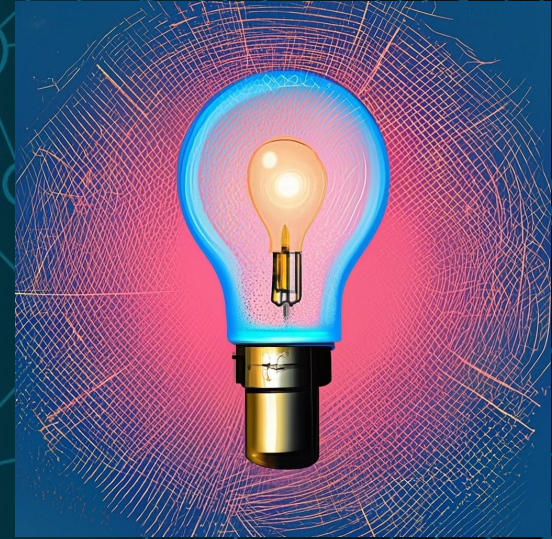
Demonstrably improve processes and systems pertaining to cybersecurity

- Stated Client Priorities include:
 - Logging
 - Access Control (IAM)
 - Monitoring
 - Visibility of Activity
 - Threat Detection and Response



Compliance requirements

- We chose the NIST 800-53 (Rev 4) to map our compliance to
 - Noteworthy Items:
 - AU (Audit & Accountability)
 - SI (System & Information Integrity)
 - AC (Access Control)

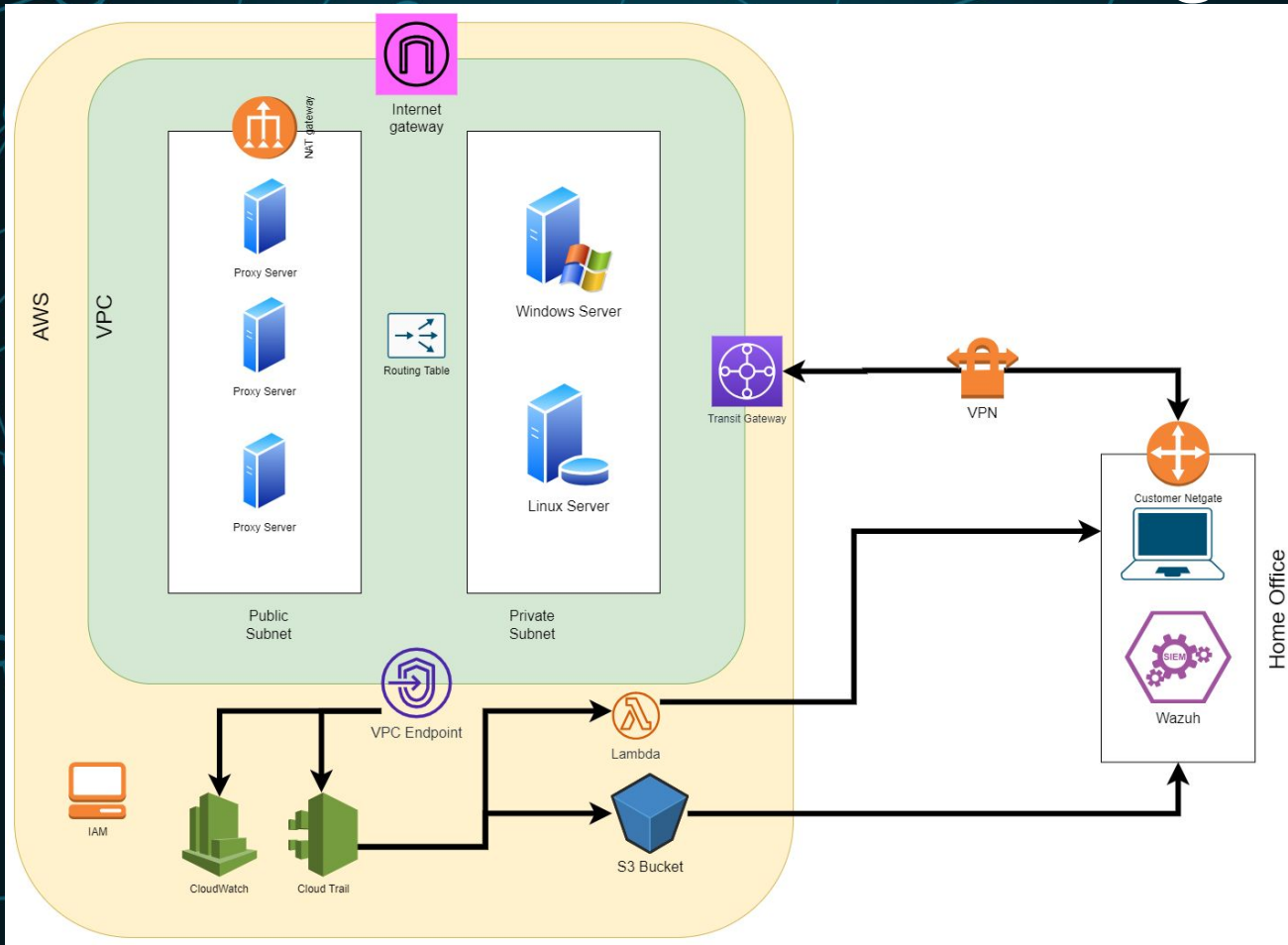




Solutions

- Apply IAM best practices
- Minimize Attack Surface
 - Server Hardening
 - Data Encryption
 - Reverse Proxy
- Log Aggregation (and Alerts)
 - Sysmon
 - CloudWatch/CloudTrail
 - VPC Flow Logs
 - Lambda Function Creation
 - SIEM implementation

Cloud Infrastructure Design



The background of the slide is a dark blue color with a complex network diagram. The diagram consists of numerous light blue circles of varying sizes, representing nodes, which are interconnected by thin, light blue lines, representing edges. The connections form a dense, web-like structure that fills the entire background.

Demo- Raheem

Identity Access Management (IAM)

Best Practices

IAM Best Practices

Identity and Access Management (IAM)

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

IAM > Roles > SilverLineSecurityRoles

SilverLineSecurityRoles

Allows EC2 instances to call AWS services on your behalf.

Delete

Edit

Summary

Creation date

August 07, 2023, 10:34 (UTC-07:00)

Last activity

None

ARN

[arn:aws:iam::319232243474:role/SilverLineSecurityRoles](#)

Instance profile ARN

[arn:aws:iam::319232243474:instance-profile/SilverLineSecurityRoles](#)

Maximum session duration

1 hour

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

Identity and Access Management (IAM)

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

IAM > Users

Users (4) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

< 1 >

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password a...	Activ
<input type="checkbox"/>	BenjaminHobbs	SilverLineSecurity	1 hour ago	Virtual	1 hour ago	-
<input type="checkbox"/>	DavidSiebert	SilverLineSecurity	1 hour ago	Virtual	1 hour ago	-
<input type="checkbox"/>	NatashaSiramarco	SilverLineSecurity	Never	Virtual	1 hour ago	-
<input type="checkbox"/>	NicholasVanNort	SilverLineSecurity	Never	Virtual	1 hour ago	-

IAM Best Practices

Identity and Access Management (IAM)

Dashboard

▼ Access management

User Groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analysers

Settings

New: IAM Access Analyzer makes it easier to implement least privilege permissions by generating IAM policies based on access activity.

IAM > Access Analyzer

Access Analyzer [Info](#)

Last scan: a few seconds ago

Analyzer

ConsoleAnalyzer-ad502212-4b1f-45c3-a39e-dfa54a026c83

Zone of trust: Current account (319232243474)

Active

Archived

Resolved

All

Active findings

Account ID 319232243474

Actions

< 1 >

Finding ID	Resource	External p...	Condition	Shared thr...	Access level	Upd.
------------	----------	---------------	-----------	---------------	--------------	------

Identity and Access Management (IAM)

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

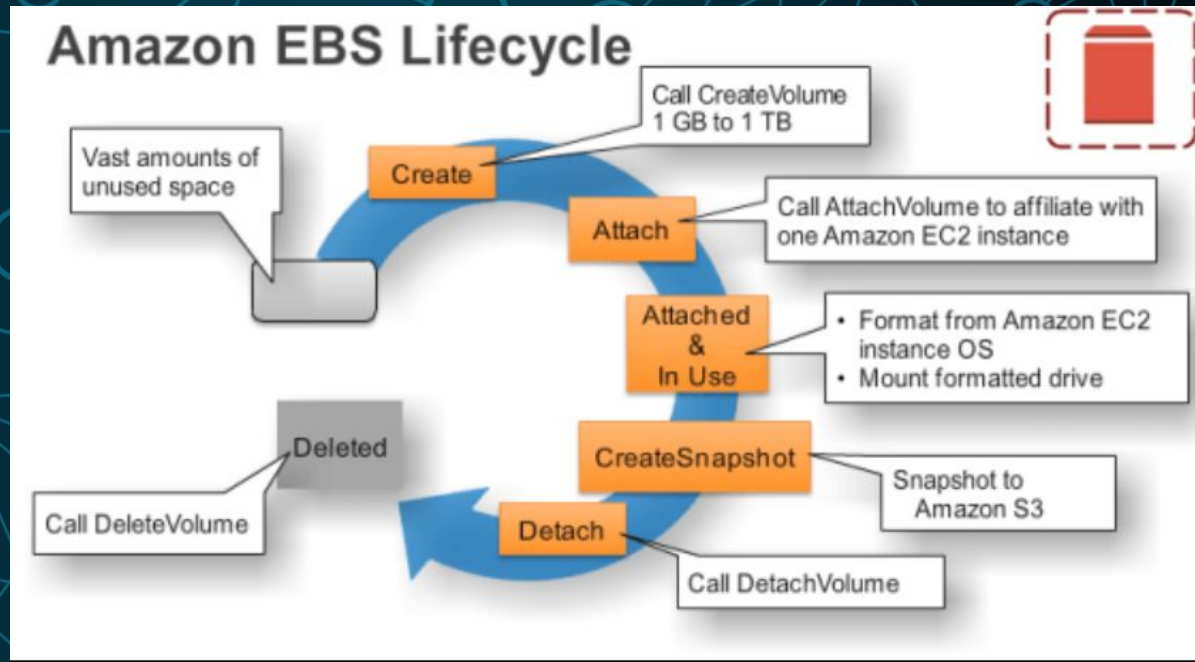
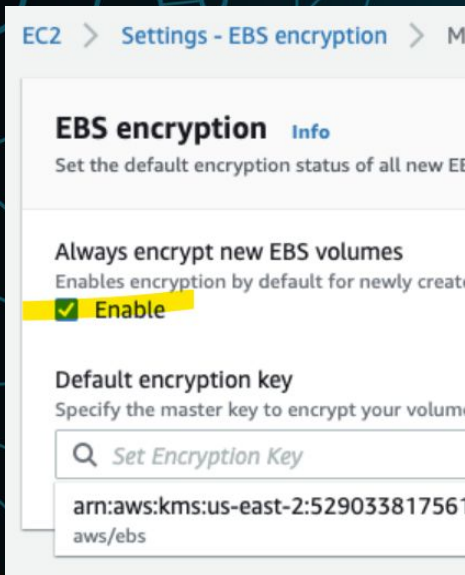
▼ Access reports

	Policy name	Type	Description
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	Provides full access to AWS services and reso...
<input type="checkbox"/>	AWSCloudFormationReadOnlyAcc...	AWS managed	Provides access to AWS CloudFormation via t...
<input type="checkbox"/>	CloudFrontFullAccess	AWS managed	Provides full access to the CloudFront console...
<input type="checkbox"/>	AWSCloudHSMFullAccess	AWS managed	Provides full access to all CloudHSM resources.
<input type="checkbox"/>	CloudFrontReadOnlyAccess	AWS managed	Provides access to CloudFront distribution co...
<input type="checkbox"/>	CloudSearchFullAccess	AWS managed	Provides full access to the Amazon CloudSear...
<input type="checkbox"/>	CloudWatchFullAccess	AWS managed	Provides full access to CloudWatch.
<input type="checkbox"/>	CloudWatchLogsFullAccess	AWS managed	Provides full access to CloudWatch Logs
<input type="checkbox"/>	AWSDirectConnectFullAccess	AWS managed	Provides full access to AWS Direct Connect vi...
<input type="checkbox"/>	AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via the A...

Data Protection & Hardening

Server

CIS compliance = EBS (Full Disk Encryption)



Reverse Proxy



Client



Internet



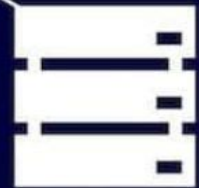
Reverse Proxy



Origin Server



Client

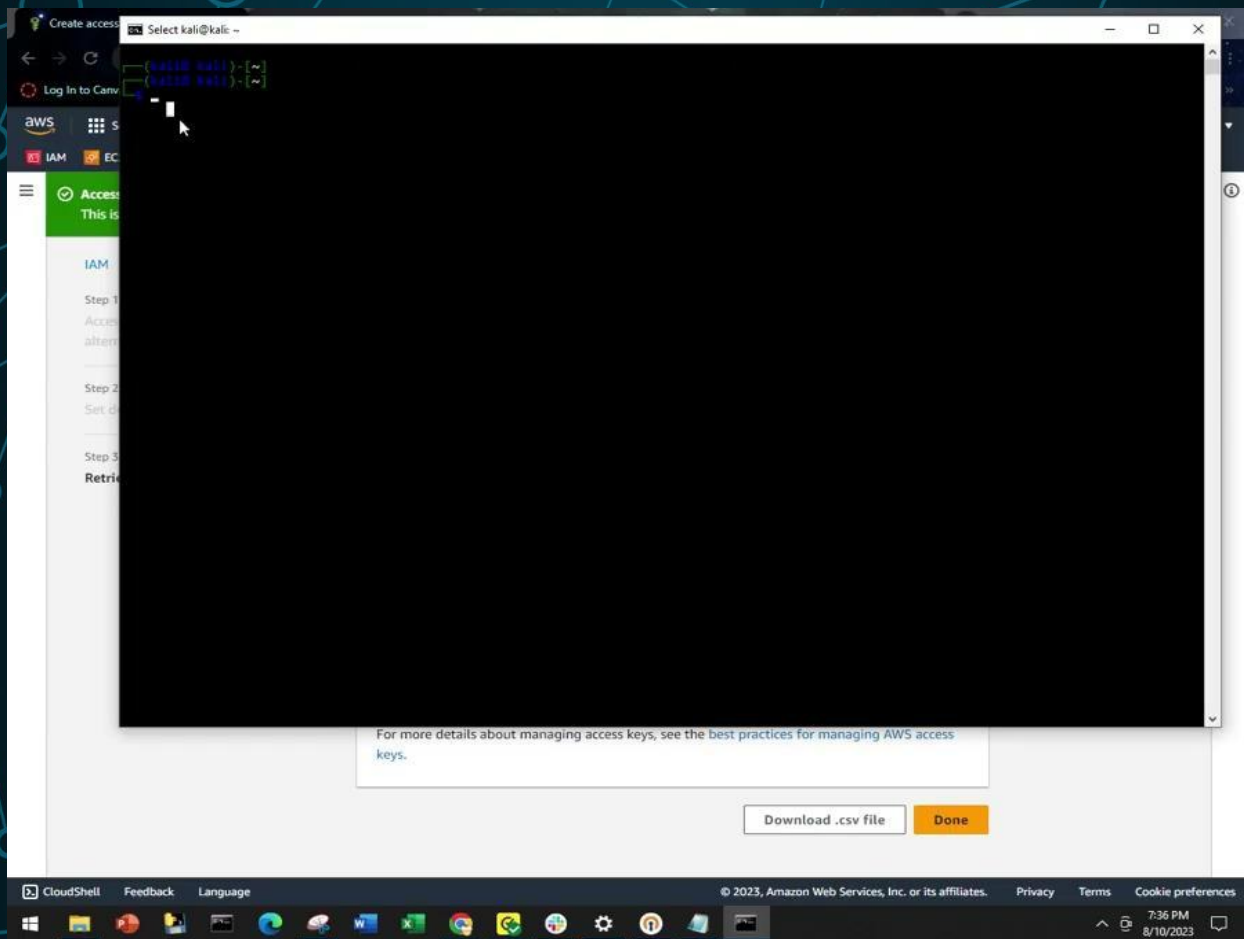


Origin Server

A dark blue background featuring a complex network diagram. The diagram consists of numerous light blue circles of varying sizes, representing nodes, which are interconnected by thin, light blue lines representing edges. The connections form a dense, web-like structure across the entire frame.

Demo- Natasha

Red Team



—(kali@kali)-[~]

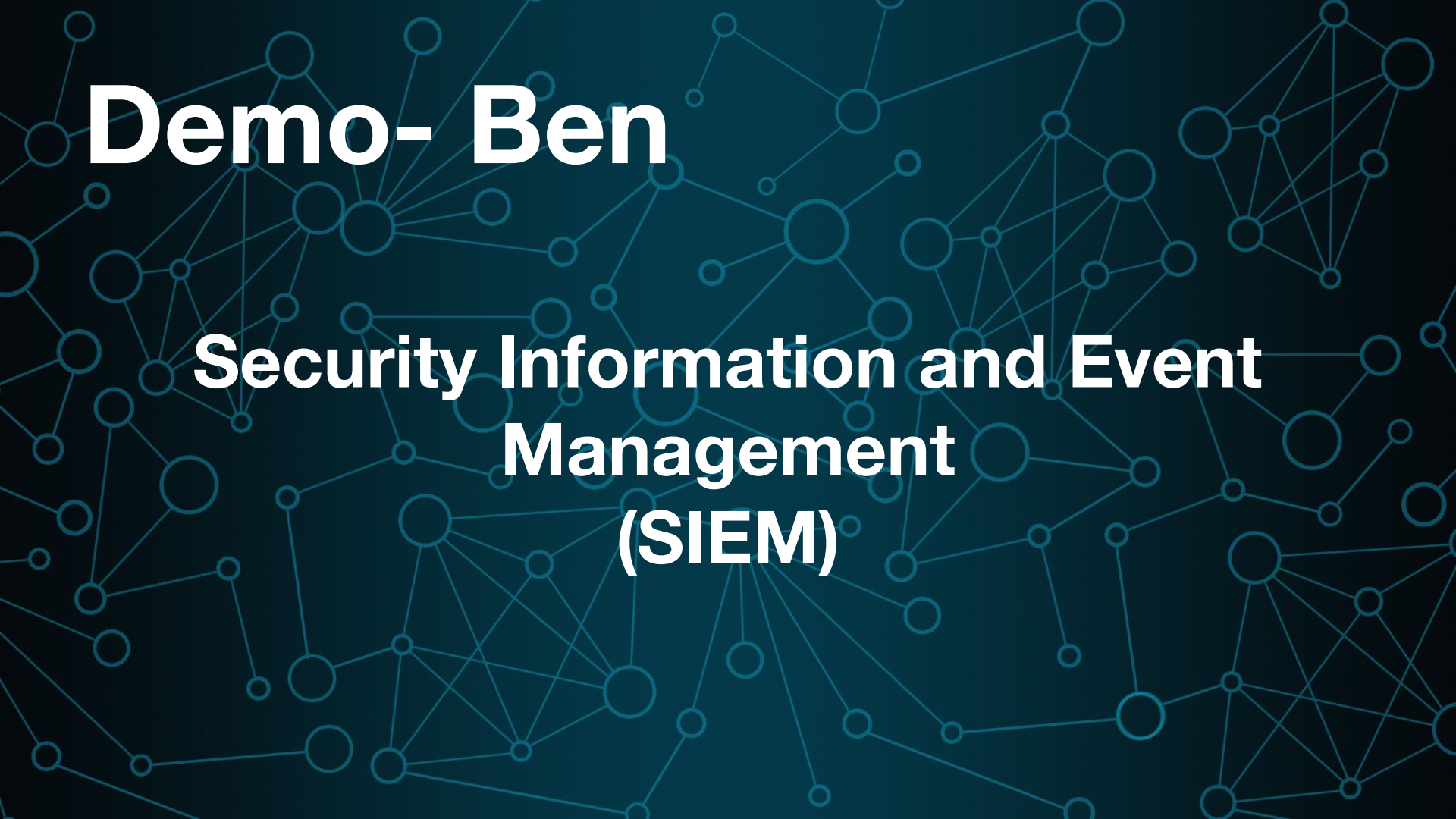
—\$ ssh -i /usr/share/python3/SLSecKey.pem ubuntu@52.88.45.109 "python3 describeInstances.py"

```
{'Reservations': [{'Groups': [], 'Instances': [{'AmiLaunchIndex': 0, 'ImageId': 'ami-0c65adc9a5c1b5d7c', 'InstanceId': 'i-024bdf23631a40305', 'InstanceType': 't2.micro', 'KeyName': 'SLSecKey', 'LaunchTime': datetime.datetime(2023, 8, 10, 4, 58, 16, tzinfo=tzlocal()), 'Monitoring': {'State': 'enabled'}, 'Placement': {'AvailabilityZone': 'us-west-2c', 'Group': 'us-west-2c', 'GroupPlaceholder': 'default', 'PrivateDnsName': 'ip-172-31-2-151.us-west-2.compute.internal', 'PrivateIpAddress': '172.31.2.151', 'ProductCodes': [], 'PublicDnsName': 'ec2-52-88-45-109.us-west-2.compute.amazonaws.com', 'PublicIpAddress': '52.88.45.109', 'State': {'Code': 16, 'Name': 'running'}, 'StateTransitionReason': '', 'SubnetId': 'subnet-06ef193843ec12809', 'VpcId': 'vpc-064db35c71b2b7c9e', 'Architecture': 'x86_64', 'BlockDeviceMappings': [{'DeviceName': '/dev/sda1', 'Ebs': {'AttachTime': datetime.datetime(2023, 8, 8, 23, 31, 33, tzinfo=tzlocal()), 'DeleteOnTermination': True, 'Status': 'attached', 'VolumeId': 'vol-03c6610ea27472df7'}]}, 'ClientToken': 'e920cf55-245d-470e-a665-b475bf75622d', 'EbsOptimized': False, 'EnaSupport': True, 'Hypervisor': 'xen', 'NetworkInterfaces': [{'Association': {'IpOwnerId': '319232243474', 'PublicDnsName': 'ec2-52-88-45-109.us-west-2.compute.amazonaws.com', 'PublicIp': '52.88.45.109'}, 'Attachment': {'AttachTime': datetime.datetime(2023, 8, 8, 23, 31, 32, tzinfo=tzlocal()), 'AttachmentId': 'eni-attach-0309f18db16d320af', 'DeleteOnTermination': True, 'DeviceIndex': 0, 'Status': 'attached', 'NetworkCardIndex': 0, 'Description': '', 'Groups': [{'GroupName': 'RevProxy-SG', 'GroupId': 'sg-0d0ccf5b42d3f2ef3'}], 'Ipv6Addresses': [], 'MacAddress': '0a:4b:e2:67:e9:af', 'NetworkInterfaceId': 'eni-03566e334942a6cd8', 'OwnerId': '319232243474', 'PrivateDnsName': 'ip-172-31-2-151.us-west-2.compute.internal', 'PrivateIpAddress': '172.31.2.151', 'PrivateIpAddresses': [{'Association': {'IpOwnerId': '319232243474', 'PublicDnsName': 'ec2-52-88-45-109.us-west-2.compute.amazonaws.com', 'PublicIp': '52.88.45.109'}, 'Primary': True, 'PrivateDnsName': 'ip-172-31-2-151.us-west-2.compute.internal', 'PrivateIpAddress': '172.31.2.151'}], 'SourceDestCheck': True, 'Status': 'in-use', 'SubnetId': 'subnet-06ef193843ec12809', 'VpcId': 'vpc-064db35c71b2b7c9e', 'InterfaceType': 'interface'}], 'RootDeviceName': '/dev/sda1', 'RootDeviceType': 'ebs', 'SecurityGroups': [{'GroupName': 'RevProxy-SG', 'GroupId': 'sg-0d0ccf5b42d3f2ef3'}], 'SourceDestCheck': True, 'Tags': [{'Key': 'Name', 'Value': 'SLSec-UbuntuSrv20-RevProxy1'}], 'VirtualizationType': 'hvm', 'CpuOptions': {'CoreCount': 1, 'ThreadsPerCore': 1}, 'CapacityReservationSpecification': {'CapacityReservationPreference': 'open'}, 'HibernationOptions': {'Configured': False}, 'MetadataOptions': {'State': 'applied', 'HttpTokens': 'optional', 'HttpPutResponseHopLimit': 1, 'HttpEndpoint': 'enabled', 'HttpProtocolIpv6': 'disabled', 'InstanceMetadataTags': 'disabled', 'EnclaveOptions': {'Enabled': False}, 'PlatformDetails': 'Linux/UNIX', 'UsageOperation': 'RunInstances', 'UsageOperationUpdateTime': datetime.datetime(2023, 8, 8, 23, 31, 32, tzinfo=tzlocal()), 'PrivateDnsNameOptions': {'HostnameType': 'ip-name', 'EnableResourceNameDnsARecord': False, 'EnableResourceNameDnsAAAARecord': False}, 'MaintenanceOptions': {'AutoRecovery': 'default'}], 'CurrentInstanceBootMode': 'legacy-bios'}, {'OwnerId': '319232243474', 'ReservationId': 'r-071851397e894756e'}], 'ResponseMetadata': {'RequestId': 'cda99939-a545-4e50-9016-5959ef39d51b', 'HTTPStatusCode': 200, 'HTTPHeaders': {'x-amzn-requestid': 'cda99939-a545-4e50-9016-5959ef39d51b', 'cache-control': 'no-cache, no-store', 'strict-transport-security': 'max-age=31536000; includeSubDomains', 'vary': 'accept-encoding', 'content-type': 'text/xml; charset=UTF-8', 'transfer-encoding': 'chunked', 'date': 'Thu, 10 Aug 2023 23:16:40 GMT', 'server': 'AmazonEC2'}, 'RetryAttempts': 0}]}
```


The background of the slide is a dark teal color with a complex network diagram. It consists of numerous light blue circles of varying sizes, representing nodes, which are interconnected by thin, light blue lines, representing connections or data flow. The network is dense and spans the entire width and height of the slide.

Demo- Nick

Cloud Monitoring Solutions

The background of the slide is a dark blue field filled with a complex network diagram. It consists of numerous light blue circles of varying sizes, representing nodes, which are interconnected by thin, light blue lines, representing edges. The connections form a dense, web-like structure that covers the entire background.

Demo- Ben

Security Information and Event Management (SIEM)



wazuh. ▾

Agents

a



STATUS

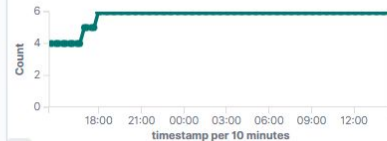


- Active (6)
- Disconnected (0)
- Pending (0)
- Never connected (0)

DETAILS

Active
6Disconnected
0Pending
0Never connected
0Agents coverage
100.00%Last registered agent
EC2AMAZ-5L6GIELMost active agent
EC2AMAZ-5L6GIEL

EVOLUTION



Last 24 hours ▾

● active

Filter or search agent

Refresh

Agents (6)

⊕ Deploy new agent

📄 Export formatted



ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	labPC	172.31.88.24	SilverLine	🐧 Ubuntu 22.04.3 LTS	node01	v4.4.5	● active	👁️ 🔗
002	SLUbuntuProx2	172.31.12.226	SilverLine	🐧 Ubuntu 20.04.6 LTS	node01	v4.4.5	● active	👁️ 🔗
003	ip-172-31-2-151	172.31.2.151	SilverLine	🐧 Ubuntu 20.04.6 LTS	node01	v4.4.5	● active	👁️ 🔗
004	EC2AMAZ-M6C310I	172.31.5.63	SilverLine	🪟 Microsoft Windows Server 2019 Datacenter 10.0.17763.4645	node01	v4.4.5	● active	👁️ 🔗
005	ubuntuhard	172.31.54.119	SilverLine	🐧 Ubuntu 22.04.3 LTS	node01	v4.5.0	● active	👁️ 🔗
006	EC2AMAZ-5L6GIEL	172.31.26.31	default	🪟 Microsoft Windows Server 2022 Datacenter 10.0.20348.1850	node01	v4.4.5	● active	👁️ 🔗

 Configuration

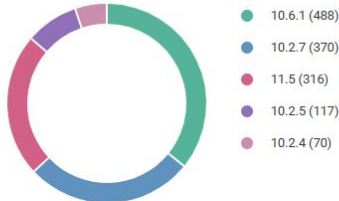
Last keep alive
Aug 11, 2023 @ 14:36:06.000

Last 24 hours ▾

Persistence

91

PCI DSS

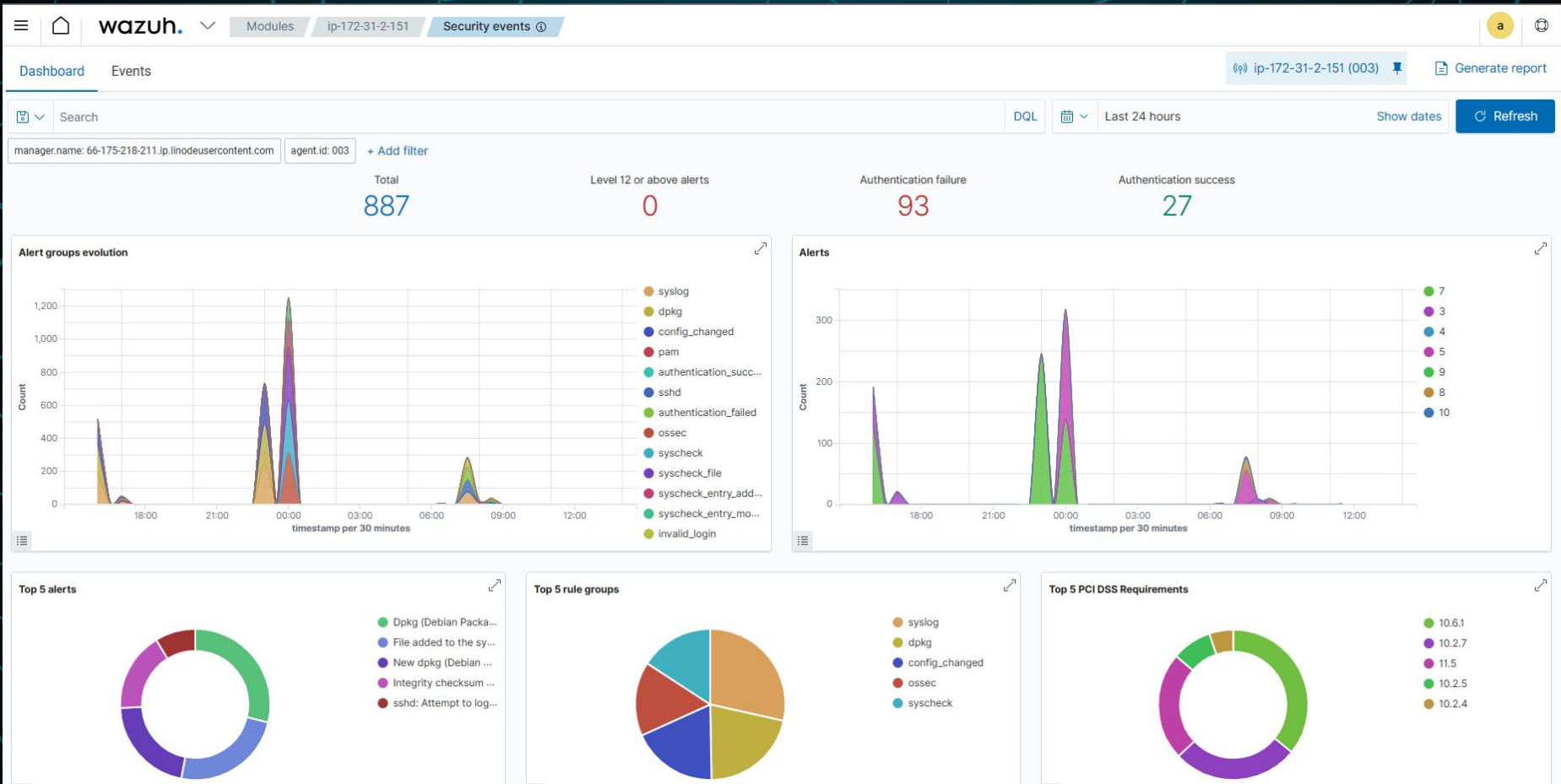


Time ↓	Path	Action	Rule description	Rule Level	Rule Id
Aug 11, 2023 @ 00:18:57.122	/etc/ssl/certs/Staat_der_Nederlande...	deleted	File deleted.	7	553
Aug 11, 2023 @ 00:18:57.117	/etc/ssl/certs/Hellenic_Academic_a...	deleted	File deleted.	7	553
Aug 11, 2023 @ 00:18:57.117	/etc/ssl/certs/GlobalSign_Root_CA_-...	deleted	File deleted.	7	553
Aug 11, 2023 @ 00:18:57.117	/etc/ssl/certs/Network_Solutions_C...	deleted	File deleted.	7	553
Aug 11, 2023 @ 00:18:57.111	/etc/ssl/certs/76cb8f92.0	deleted	File deleted.	7	553

The line plot displays the frequency of word counts. The x-axis represents the count of words, and the y-axis represents the count of words. The plot shows a sharp increase in count for words with a count of 300, followed by a sharp decrease for words with a count of 350.

cis_ubuntu20-04

Policy	End scan	Passed	Failed	Not applic...	Score
CIS Ubuntu Linux 20.04 LTS Benchmark v1.1.0	Aug 11, 2023 @ 12:18:44.000	75	117	3	39%



wazuh. Modules ip-172-31-2-151 Security events						
Security Alerts						
Time ↓	Technique(s)			Tactic(s)	Description	Level
> Aug 11, 2023 @ 11:52:53.421					sshd: connection reset by peer	4
> Aug 11, 2023 @ 09:58:40.480					sshd: connection reset	4
> Aug 11, 2023 @ 08:37:43.609	T1110.001	T1021.004	T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5
> Aug 11, 2023 @ 08:37:39.673	T1110.001	T1021.004	T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5
> Aug 11, 2023 @ 08:37:39.605	T1110			Credential Access	Maximum authentication attempts exceeded.	8
> Aug 11, 2023 @ 08:37:27.619	T1110.001	T1021.004	T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5
> Aug 11, 2023 @ 08:37:19.649	T1110.001	T1021.004	T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5
> Aug 11, 2023 @ 08:37:19.585	T1110			Credential Access	Maximum authentication attempts exceeded.	8
> Aug 11, 2023 @ 08:37:07.599	T1110.001	T1021.004	T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5
> Aug 11, 2023 @ 08:36:59.633	T1110.001	T1021.004	T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5
> Aug 11, 2023 @ 08:36:59.566	T1110			Credential Access	Maximum authentication attempts exceeded.	8
> Aug 11, 2023 @ 08:36:47.553	T1110.001	T1021.004	T1078	Credential Access, Lateral Movement, Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: Attempt to login using a non-existent user	5

Search

DQL

📅

Last 24 hours

Show dates

Refresh

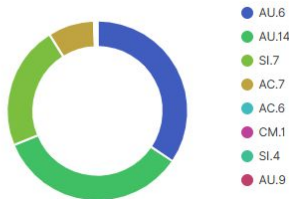
manager.name: 66-175-218-211.ip.linodeusercontent.com
 rule.nist_800_53: exists
 agent.id: 003
 + Add filter

Stats

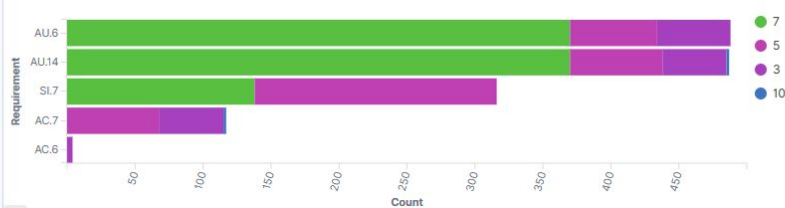
860
Total alerts

10
Max rule level

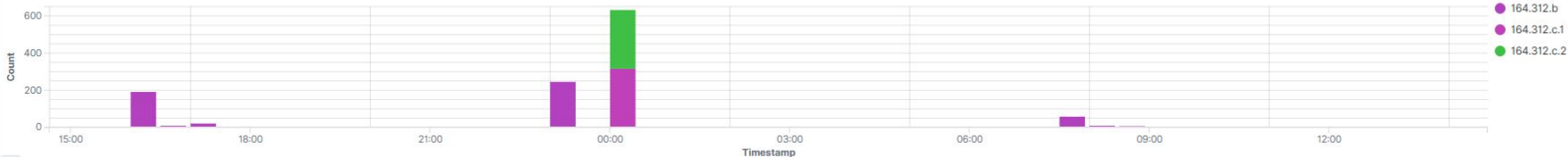
Top 10 requirements



Requirements distributed by level



Requirements over time



manager.name: 66-175-218-211.ip.linodeusercontent.com

rule.mitre.id: exists

agent.id: 003

+ Add filter

wazuh-alerts-*

Search field names

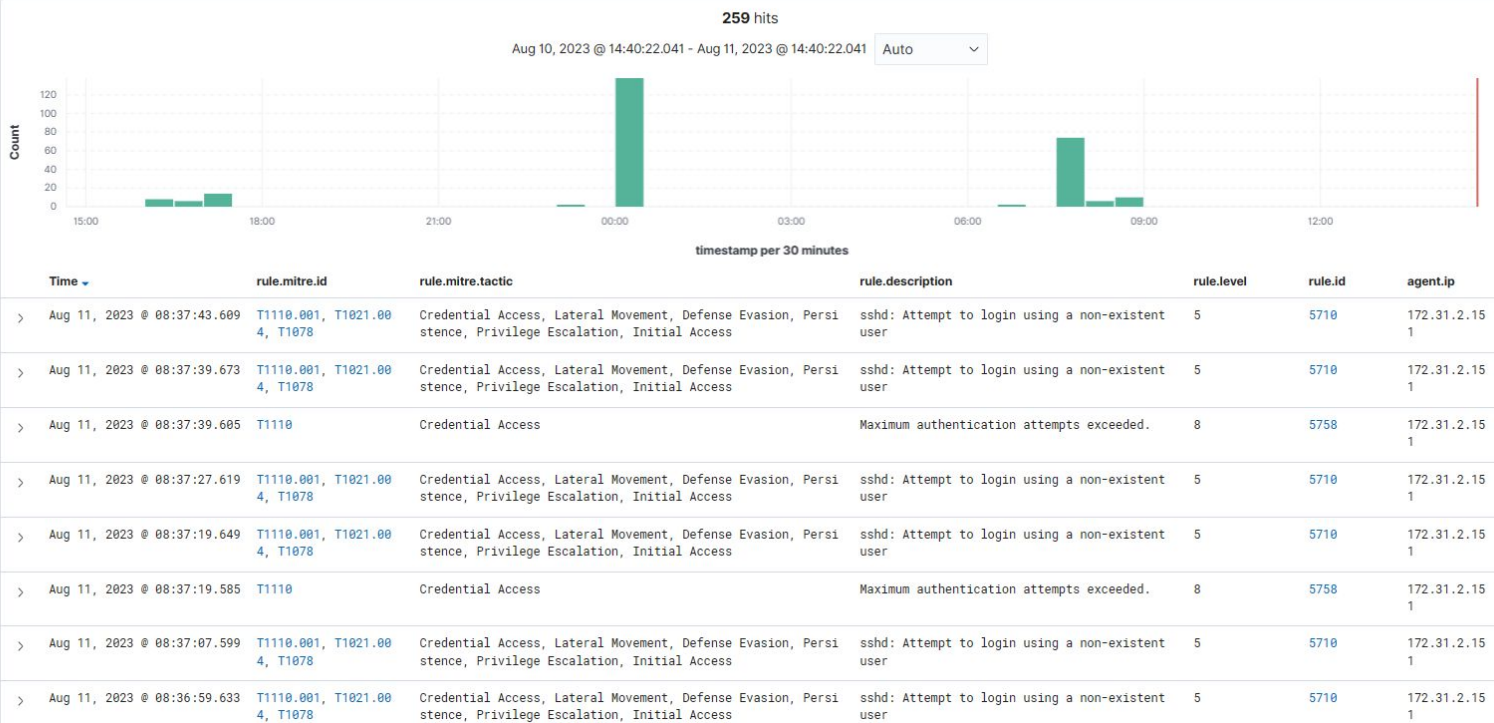
Filter by type

Selected fields

- agent.ip
- rule.description
- rule.id
- rule.level
- rule.mitre.id
- rule.mitre.tactic

Available fields

- agent.id
- agent.name
- data.command
- data.dstuser
- data.pwd
- data.scrip
- data.srcport
- data.srcuser
- data.tty
- data.uid
- decoder.ftscomment
- decoder.name
- decoder.parent
- full_log
- GeoLocation.city_name



ID

T1078

Name _____

Valid Accounts

Created Time

May 31, 2017 @ 14:31:00.645

Modified Time

May 4, 2022 @ 21:55:21.981

Version

2.4

Description

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access and remote desktop. Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account. (Citation: CISA MFA PrintNightmare)

The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise. (Citation: TechNet Credential Theft)

Groups

ID

Name ↓

Description

G0045

menuPass

[menuPass](#) is a threat group that has been active since at least 2006. Individual members of [menuPass](#) are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company. (Citation: DOJ APT10 Dec 2018) (Citation: District Court of NY APT10 Indictment December 2018)

menuPass has targeted health care, defense, aerospace, finance, maritime, biotechnology, energy, and government sectors globally, with an emphasis on Japanese organizations. In 2016 and 2017, the group is known to have targeted managed IT service providers (MSPs), manufacturing and mining companies, and a university.(Citation: Palo Alto menuPass Feb 2017) (Citation: Crowdstrike CrowdCast Oct 2017)(Citation: FireEye Poison Ivy)(Citation: PWC Cloud Hopper April 2017)(Citation: FireEye APT10 April 2017)(Citation: DOJ APT10 Dec 2018)(Citation: District Court of NY APT10 Indictment December 2018)

G0102

Wizard Spider

Wizard Spider is a Russia-based financially motivated threat group originally known for the creation and deployment of **TrickBot** since at least 2016. **Wizard Spider** possesses a diverse arsenal of tools and has conducted ransomware campaigns against a variety of organizations, ranging from major corporations to hospitals. (Citation: CrowdStrike Ryuk January 2019) (Citation: DHS/CISA Ransomware Targeting Healthcare October 2020) (Citation: CrowdStrike Wizard Spider October 2020)

G0118

UNC2452

UNC2452 is a suspected Russian state-sponsored threat group responsible for the 2020 SolarWinds software supply chain intrusion.(Citation: FireEye SUNBURST Backdoor December 2020) Victims of this campaign include government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East.(Citation: FireEye SUNBURST Backdoor December 2020) The group also compromised at least one think tank by late 2019.(Citation: Volexity SolarWinds)

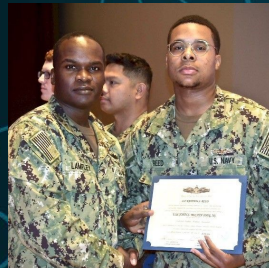
Resources & Thanks



Natasha
Siramarco



Raheem
Reed



Nick Van
Noort



Benjamin
Hobbs



David
Siebert





Questions?