

Cloud Infrastructure Security



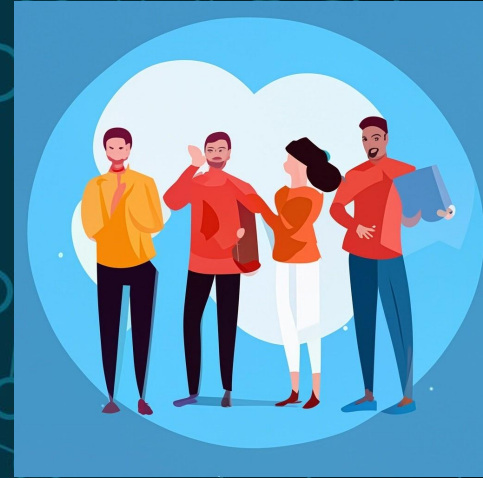
SILVERLINE
SECURITY

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

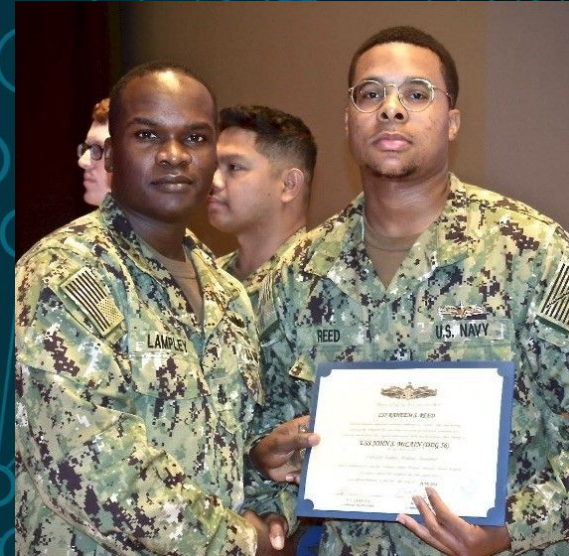
Raheem Reed

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

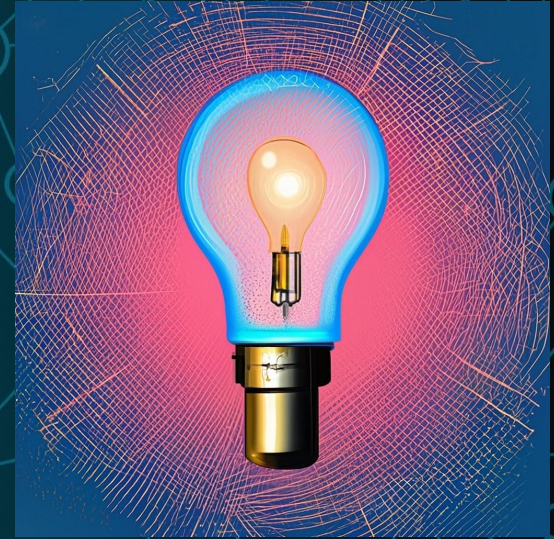
- 12 Years of experience as a Certified Financial Planner(CFP)
- 10 Years in the Army
- Unique skill set in identifying and mitigating vulnerabilities for organizations in an ever-evolving digital landscape



Problem Domain

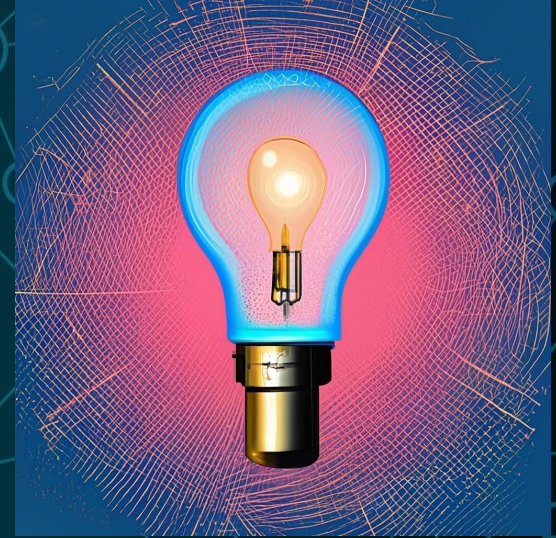
Demonstrably improve processes and systems pertaining to cybersecurity

- 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
 -

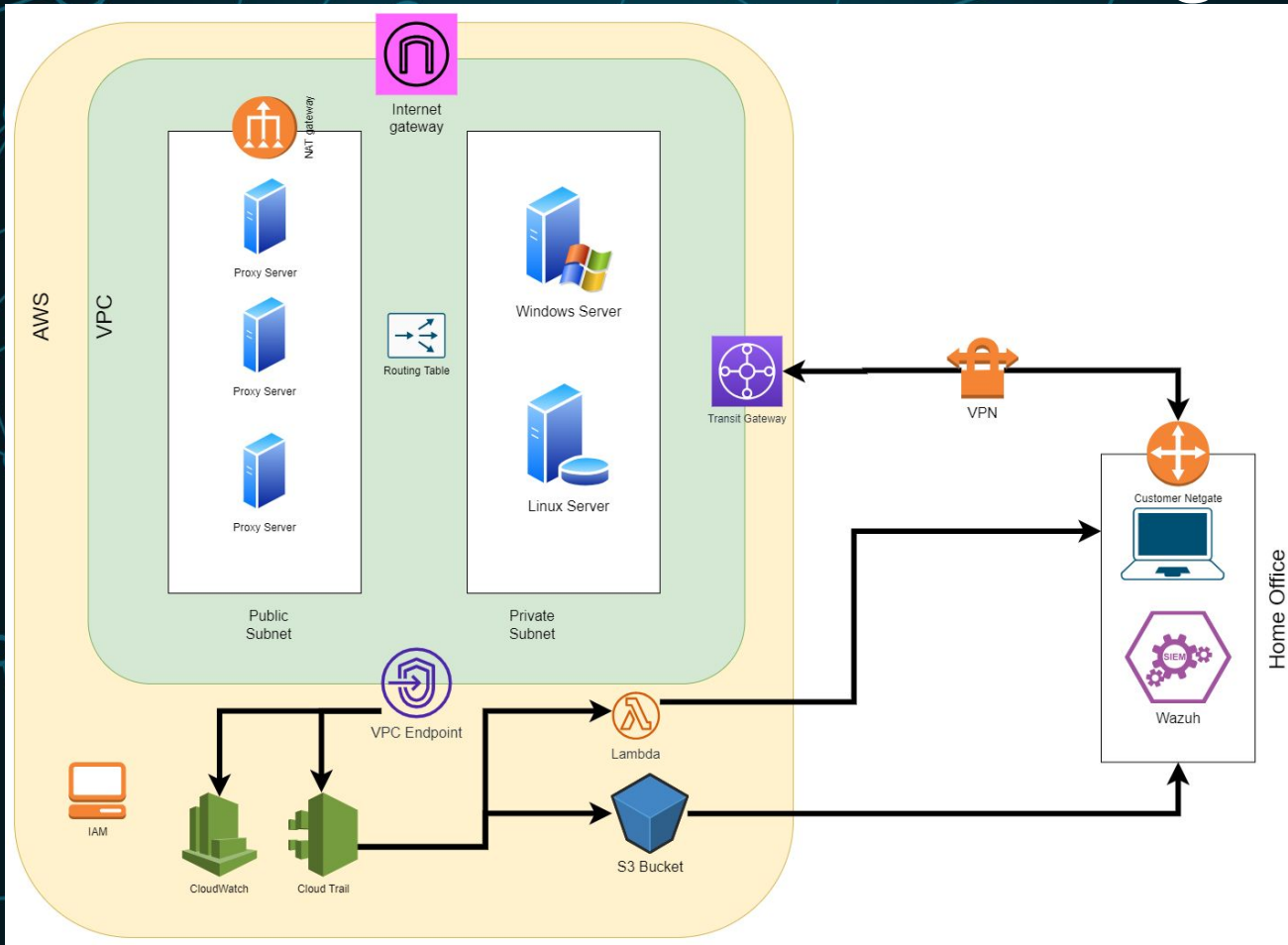




Solutions

- 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



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, creating a web-like structure that fills the entire frame.

Demo- Raheem

Identity Access Management (IAM)

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

Filter active findings

Actions

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

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

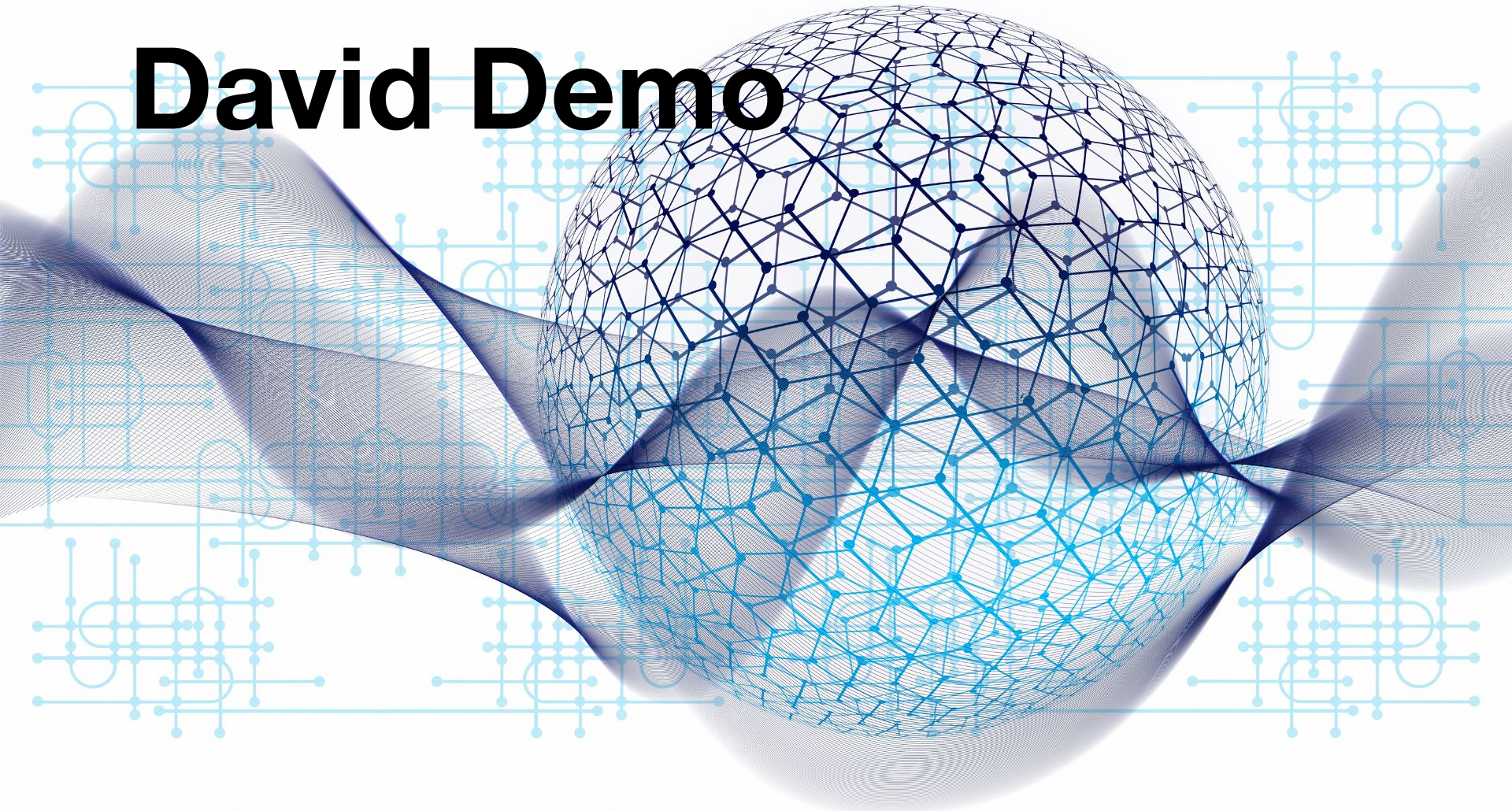
▼ Access reports

| | 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... |

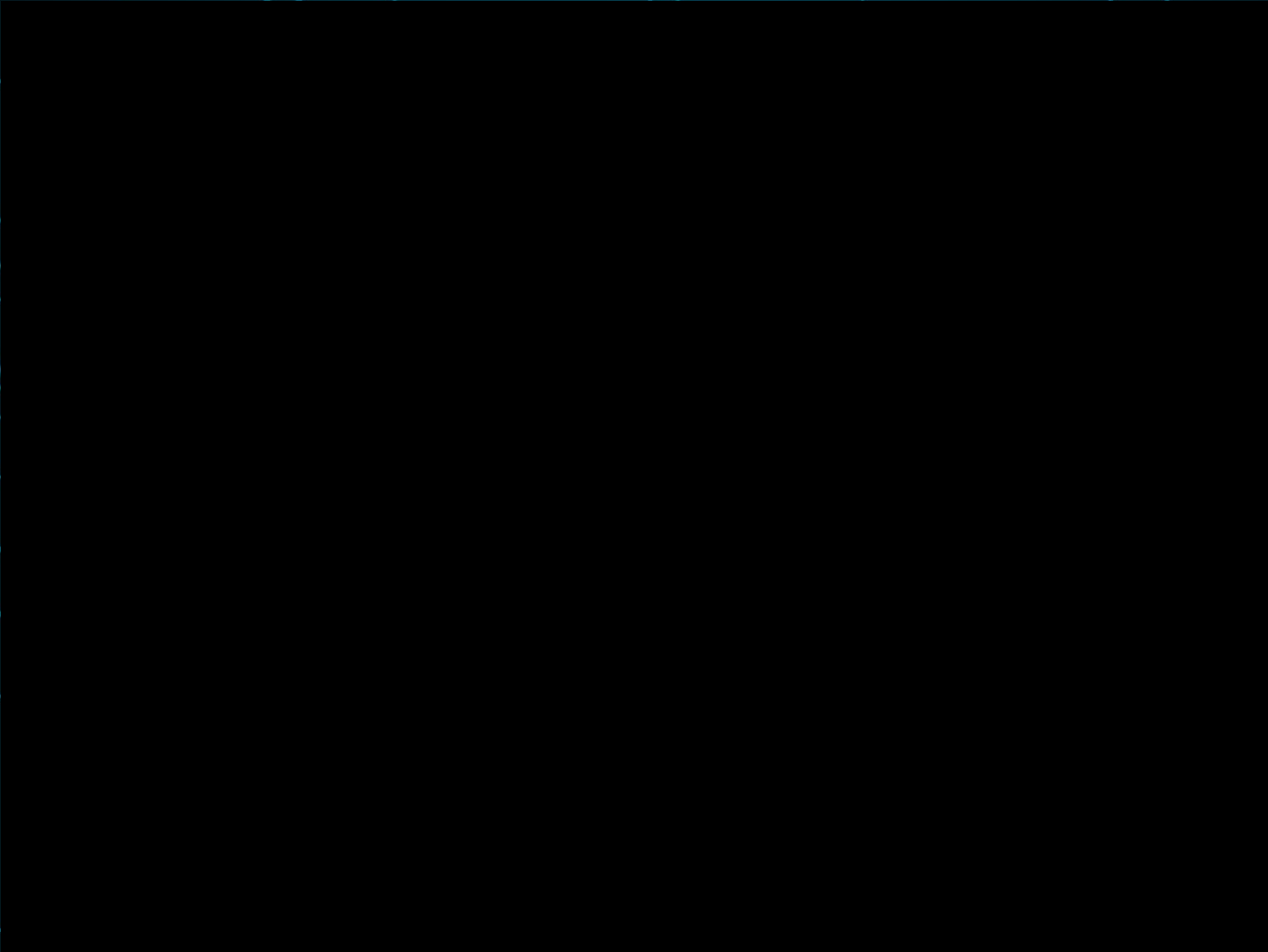
Data Protection & Hardening

Server

David Demo



Demo David



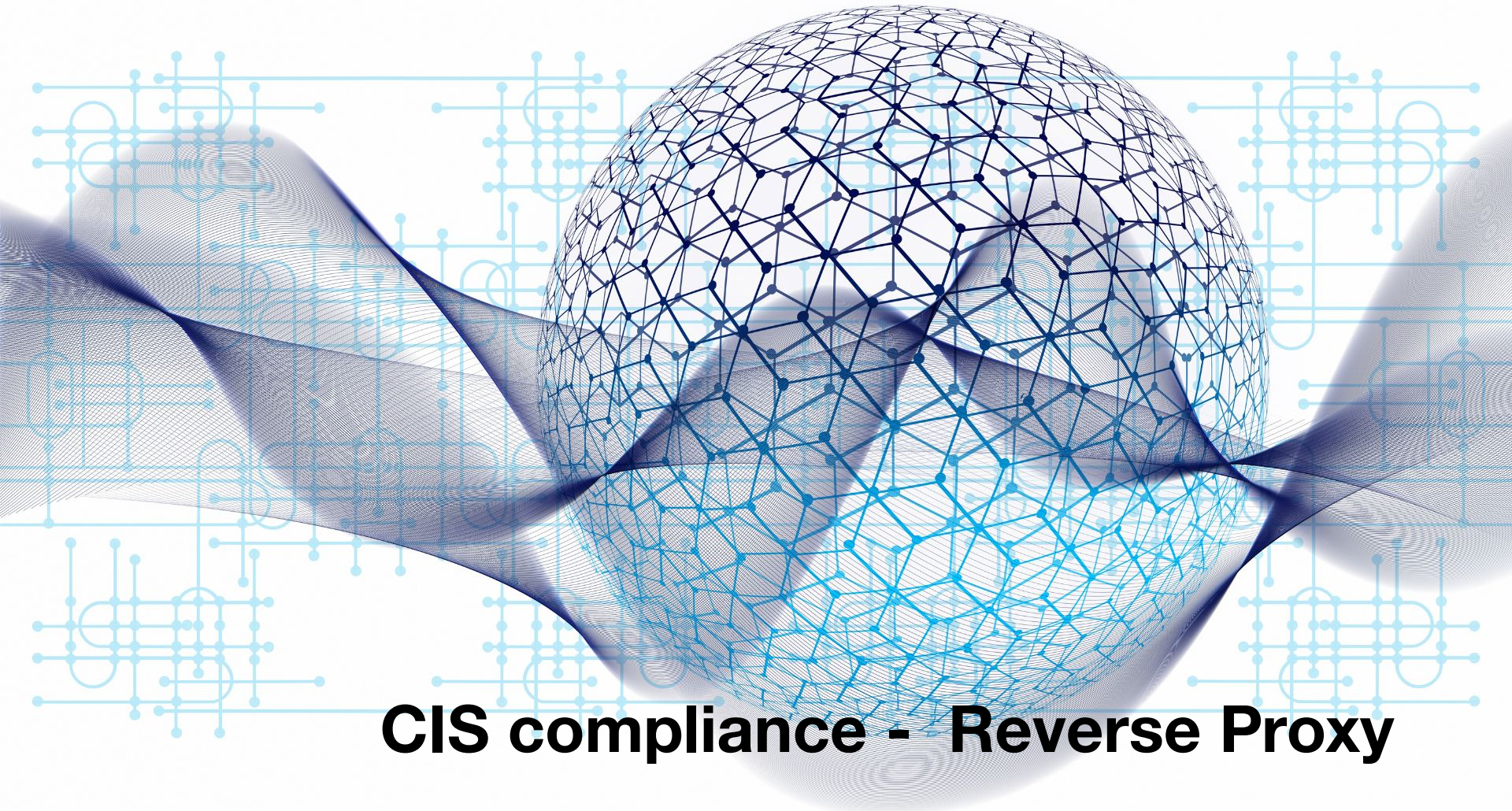
CIS compliance = EBS (Full Disk Encryption)



Demo David

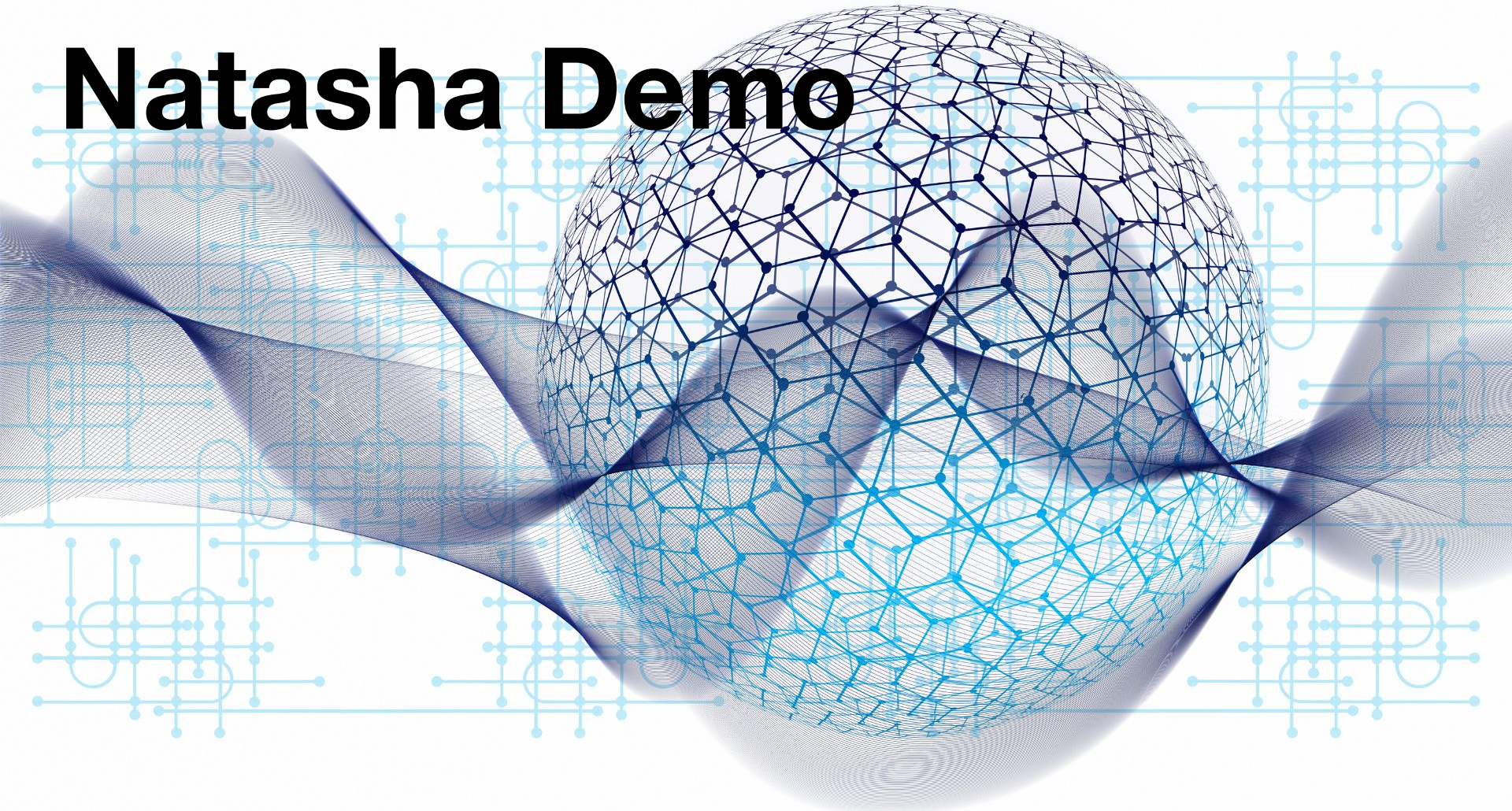
Reverse Proxy

vpn tunnel- data in transit protection.



CIS compliance - Reverse Proxy

Natasha Demo



Create access key

Select kali@kali: ~

```
kali@kali:~$ aws iam create-access-key
```

Log in to Cam...

aws IAM EC2

Access key
This is...

IAM

Step 1
Access
attent...

Step 2
Set d...

Step 3
Retri...

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

Download .csv file Done

CloudShell Feedback Language

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

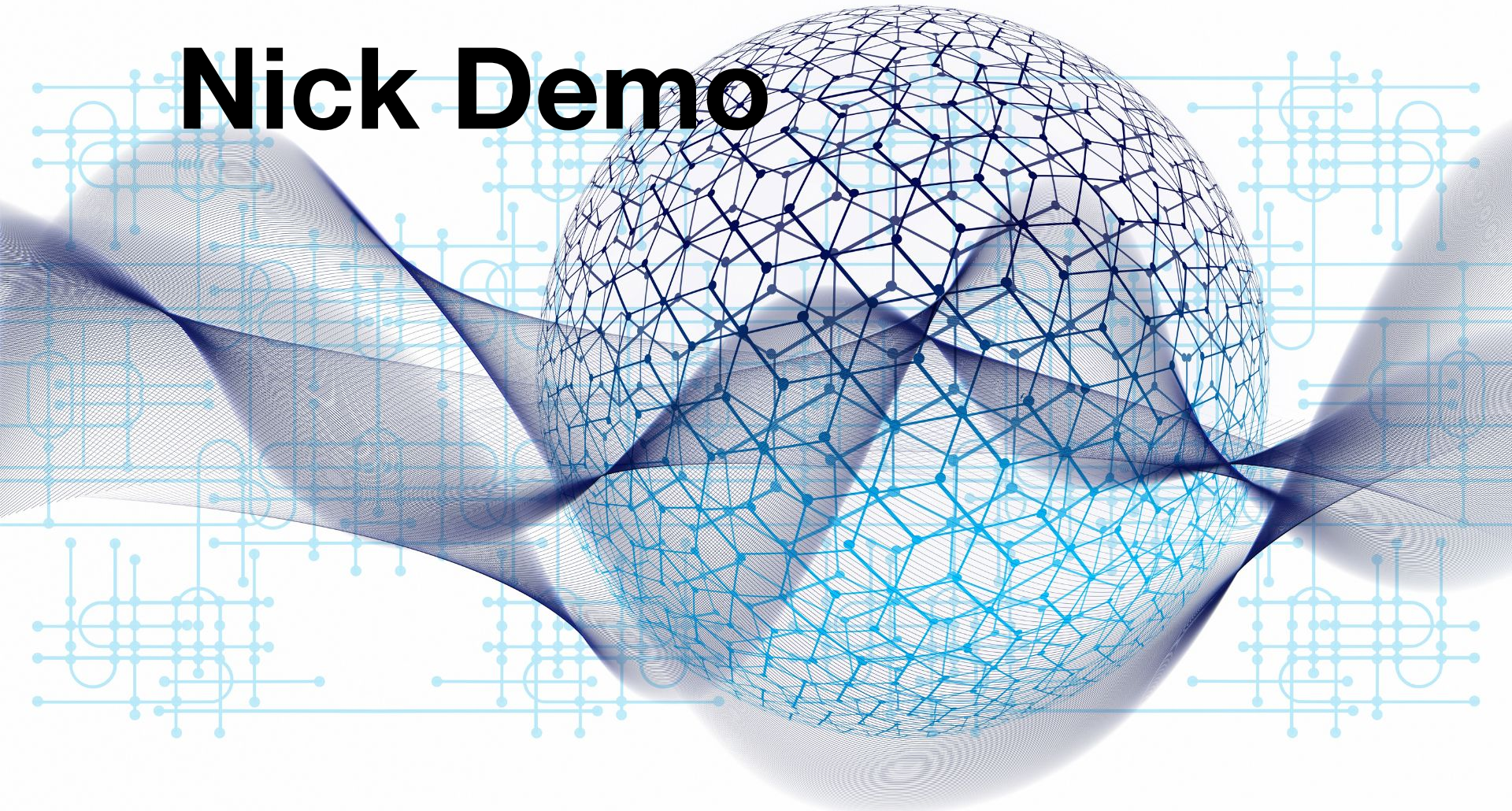
7:36 PM
8/10/2023

—(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}]}
```

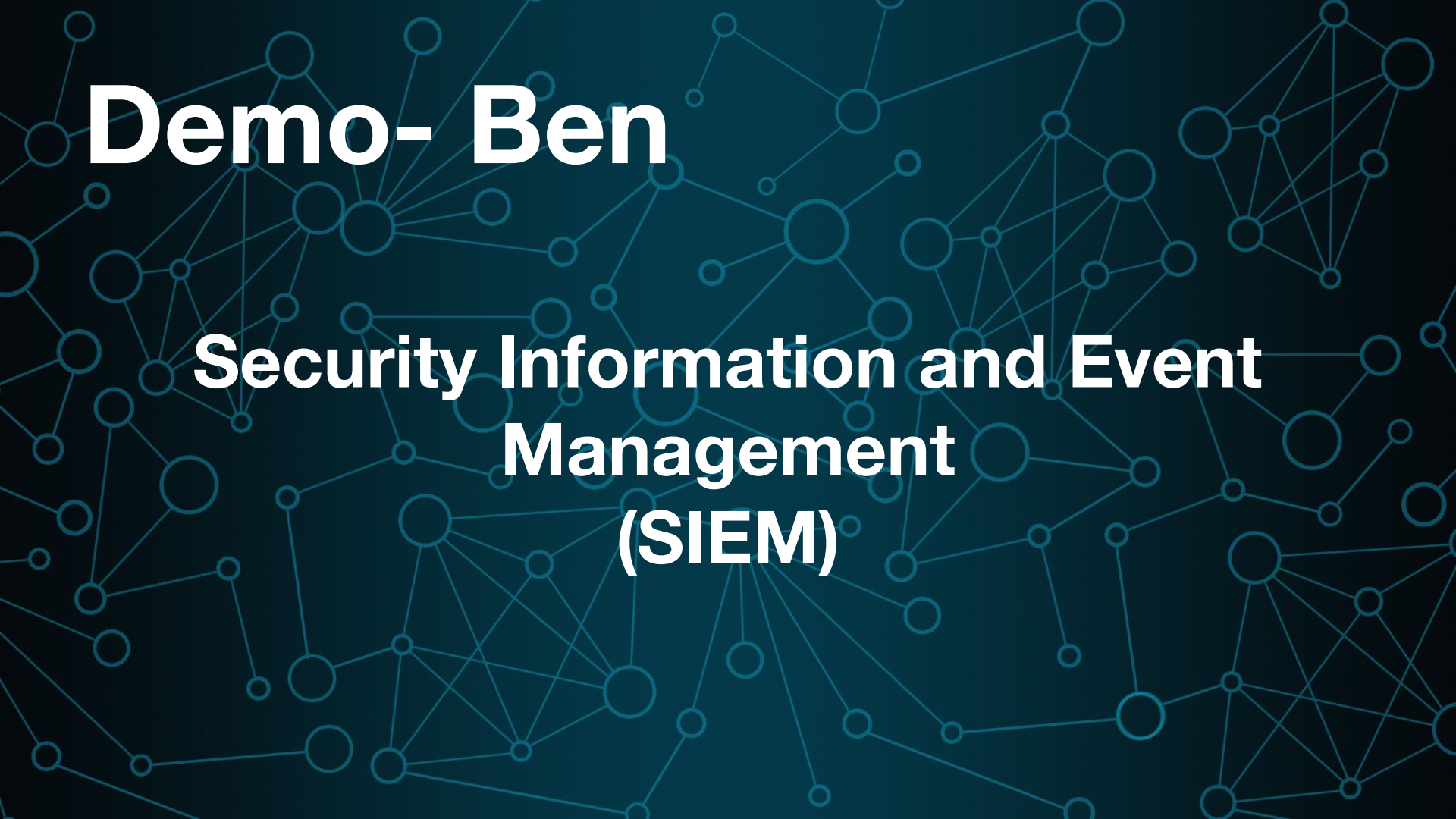

Nick Demo



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 are dense and form a web-like structure across the entire background.

Demo- Ben

Security Information and Event Management (SIEM)



wazuh.



Modules

ip-172-31-2-151

Security events ①

a



Dashboard

Events

ip-172-31-2-151 (003)

Generate report



Search

DQL



Last 24 hours

Show dates



Refresh

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

agent.id: 003

+ Add filter

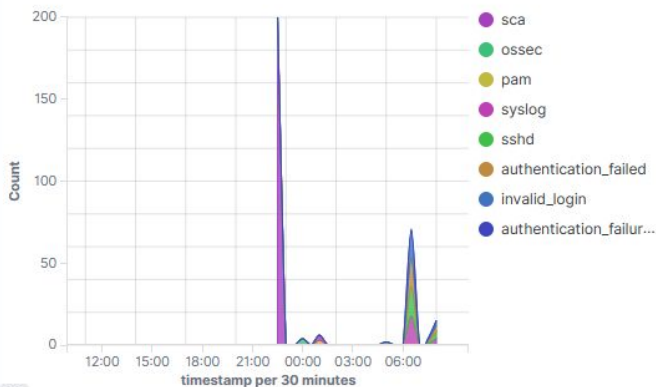
Total
231

Level 12 or above alerts
0

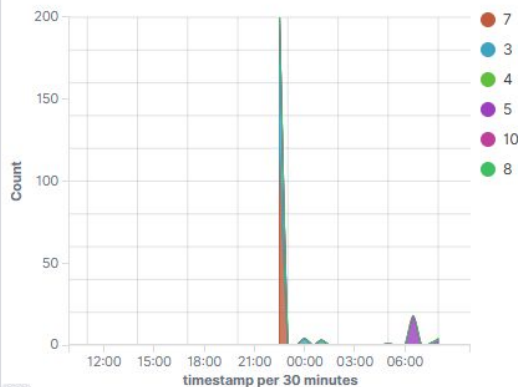
Authentication failure
23

Authentication success
0

Alert groups evolution



Alerts



Top 5 alerts

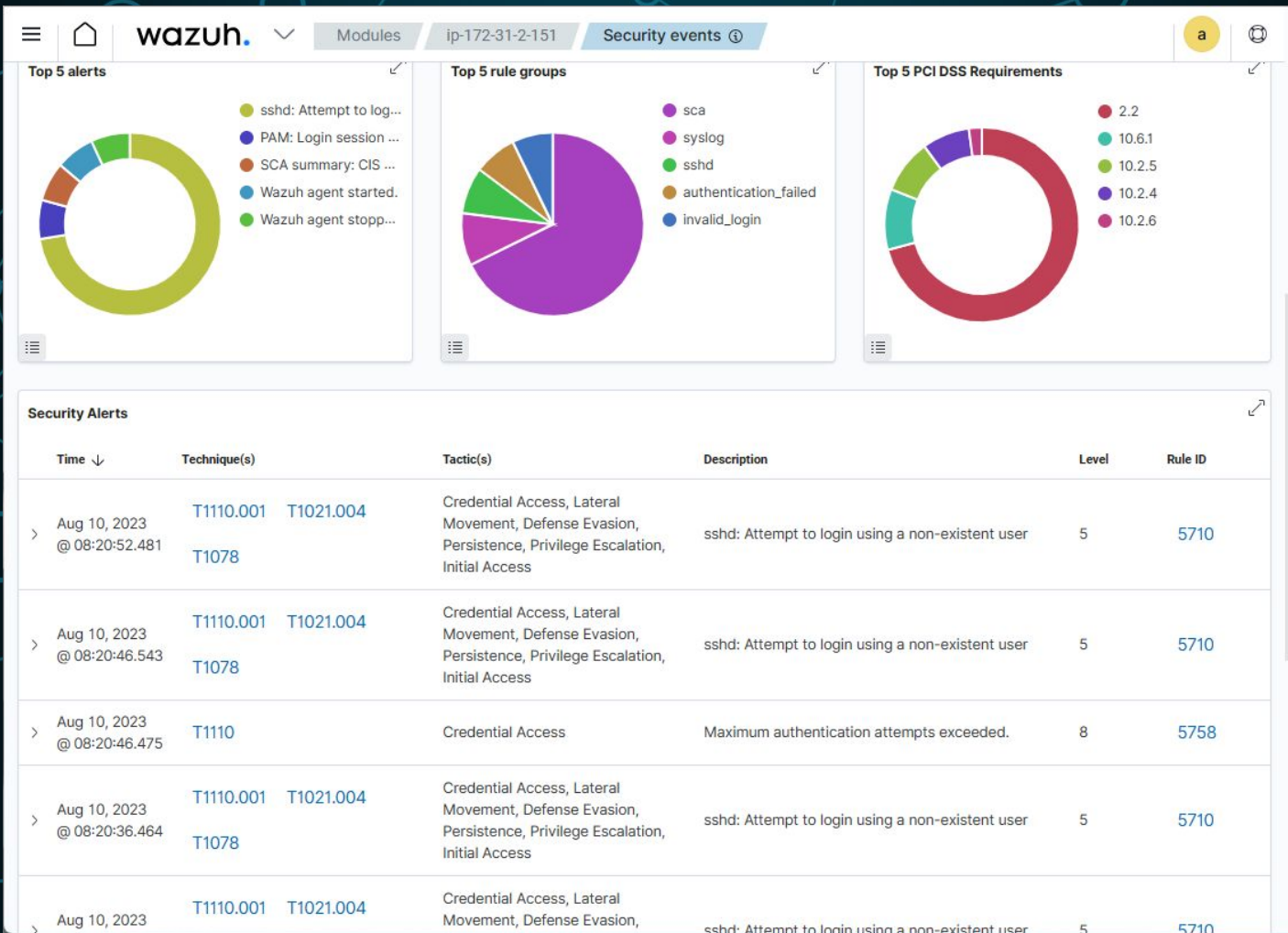


Top 5 rule groups



Top 5 PCI DSS Requirements





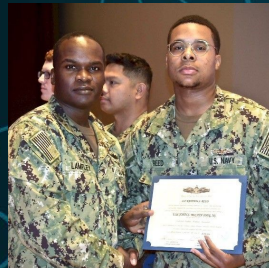
Resources & Thanks



Natasha
Siramarco



Raheem
Reed



Nick Van
Noort



Benjamin
Hobbs



David
Siebert





Questions?