

Using Wazuh for Threat Prevention, Detection and Response

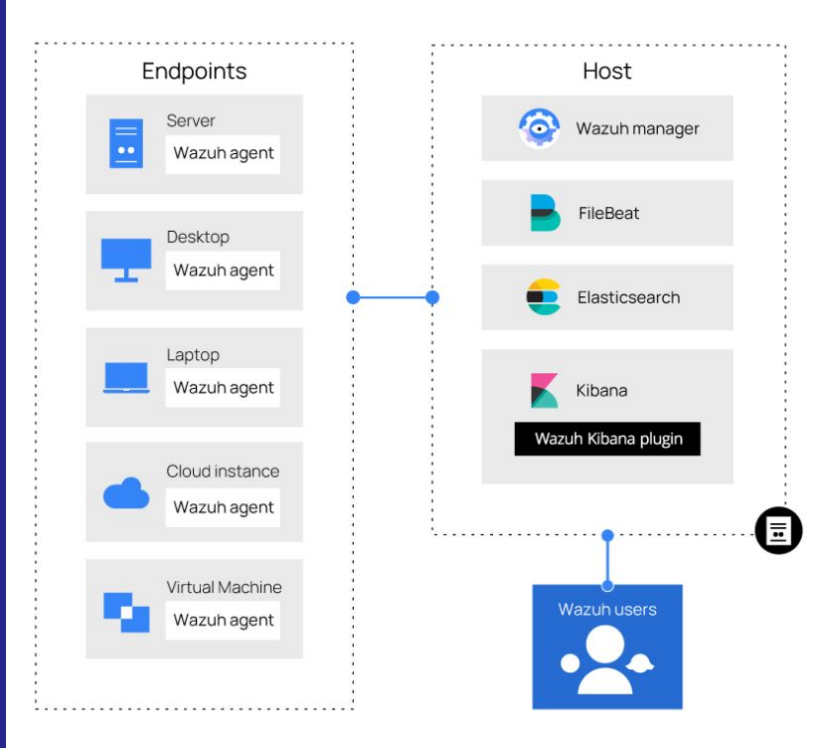


What is Wazuh?

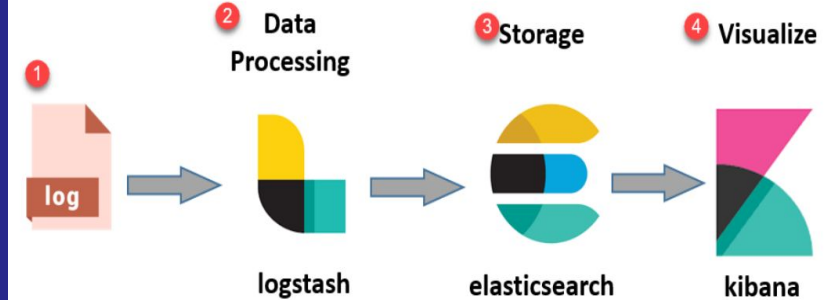


- A free open source real time and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance
- Used for collecting, indexing and analyzing security data
- Features very similar to Splunk Enterprise

How it works



Here is the simple architecture of ELK stack



Benefits of Wazuh



- Intrusion and Threat Detection
- Security Visibility
- Log Data Analysis
- Vulnerability Detection
- Incident Response
- Regulatory Compliance

Wazuh Cloud Console and Agent

← → ↻ ⚠ Not Secure | [https://172.20.10.2/app/wazuh#/overview/?_g=\(filters:\[\]\),refreshInterval:\(paused:true,value:0\),time:\(from:now-24h,to:now\)\)&_a=\(columns:\[\]\(_source\),filters:\[\]\),index:'w...](https://172.20.10.2/app/wazuh#/overview/?_g=(filters:[]),refreshInterval:(paused:true,value:0),time:(from:now-24h,to:now))&_a=(columns:[](_source),filters:[]),index:'w...) ⚙ ☆ 🏠 📄

☰ wazuh. ▾ / Modules

Total agents
2


Active agents
1

Disconnected agents
1

Pending agents
0


Never connected agents
0

SECURITY INFORMATION MANAGEMENT



Security events


Browse through your security alerts, identifying issues and threats in your environment.



Integrity monitoring


Alerts related to file changes, including permissions, content, ownership and attributes.

AUDITING AND POLICY MONITORING




Policy monitoring

Verify that your systems are configured according to your security policies baseline.



System auditing


Audit users behavior, monitoring command execution and alerting on access to critical files.



Security configuration assessment


Scan your assets as part of a configuration assessment audit.

THREAT DETECTION AND RESPONSE



Vulnerabilities


Discover what applications in your environment are affected by well-known vulnerabilities.



MITRE ATT&CK


Security events from the knowledge base of adversary tactics and techniques based on real-world observations

REGULATORY COMPLIANCE




PCI DSS

Global security standard for entities that process, store or transmit payment cardholder data.




NIST 800-53

National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.



TSC

Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy



GDPR

General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

Steps to Install the Wazuh OVA

1. Download the Wazuh OVA (Open Virtual Appliance) pre-built virtual machine image

2. Import the OVA into the virtualization platform. Start the machine.

Packages list

Distribution	Architecture	VM Format	Version	Package
CentOS 7	64bits	OVA	4.3.10	wazuh-4.3.10.ova (sha512)

```
user: wazuh-user
password: wazuh
```

Access the Wazuh Dashboard

3. Run `ip a` from the Wazuh OVA virtual machine to get the ip address. E.g.
10.0.0.157

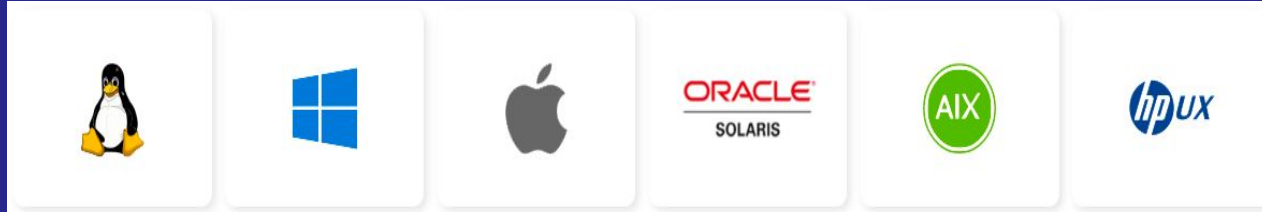
```
ip a
```

4. Open the Wazuh Cloud Console from the browser.

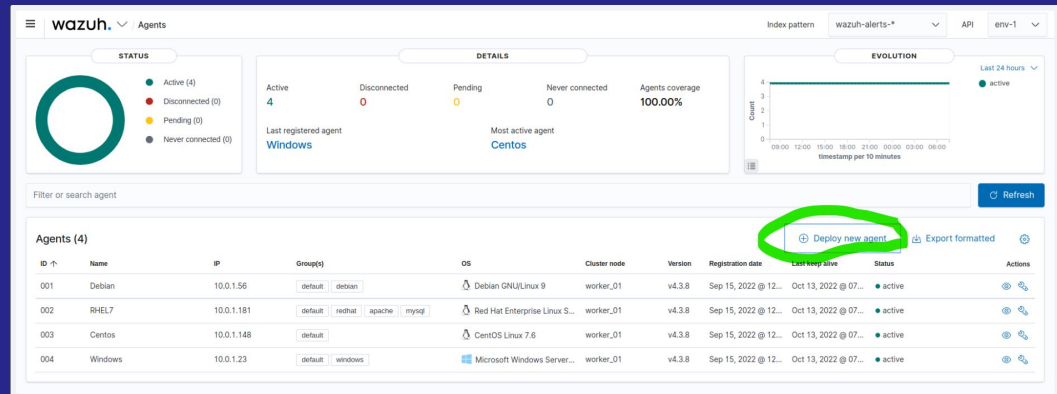
`https://10.0.0.157`

```
URL: https://<wazuh_server_ip>  
user: admin  
password: admin
```

Steps to Install the Wazuh Agent



Go to Wazuh >
Agents, and click on
Deploy new agent.



Wazuh Agents dashboard showing the following details:

- STATUS:** Active (4), Disconnected (0), Pending (0), Never connected (0).
- DETAILS:** Active: 4, Disconnected: 0, Pending: 0, Never connected: 0. Agents coverage: 100.00%. Last registered agent: Windows. Most active agent: Centos.
- EVOLUTION:** Graph showing active agents over time (Last 24 hours).
- Agents (4):** Table listing active agents.

ID	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last seen	Status	Actions
001	Debian	10.0.1.56	default debian	Debian GNU/Linux 9	worker_01	v4.3.8	Sep 15, 2022 @ 12...	Oct 13, 2022 @ 07...	active	
002	RHEL7	10.0.1.181	default redhat apache mylog	Red Hat Enterprise Linux S...	worker_01	v4.3.8	Sep 15, 2022 @ 12...	Oct 13, 2022 @ 07...	active	
003	Centos	10.0.1.148	default	CentOS Linux 7.6	worker_01	v4.3.8	Sep 15, 2022 @ 12...	Oct 13, 2022 @ 07...	active	
004	Windows	10.0.1.23	default windows	Microsoft Windows Server...	worker_01	v4.3.8	Sep 15, 2022 @ 12...	Oct 13, 2022 @ 07...	active	

Steps to Install the Wazuh Agent

- Enter the IP address of the Wazuh server
- Assign the agent to a DEFAULT group
- Install and enroll the agent by running the command
- Start the agent

Deploy a new agent

Close

1

Choose the Operating system

Red Hat / CentOSDebian / UbuntuWindowsMacOS

2

Wazuh server address

This is the address the agent uses to communicate with the Wazuh server. It can be an IP address or a fully qualified domain name (FQDN).

10.0.0.198

3

Assign the agent to a group

Select one or more existing groups

Windows X

4

Install and enroll the agent

You can use this command to install and enroll the Wazuh agent in one or more hosts.

If the installer finds another Wazuh agent in the system, it will upgrade it preserving the configuration.

Requirements

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

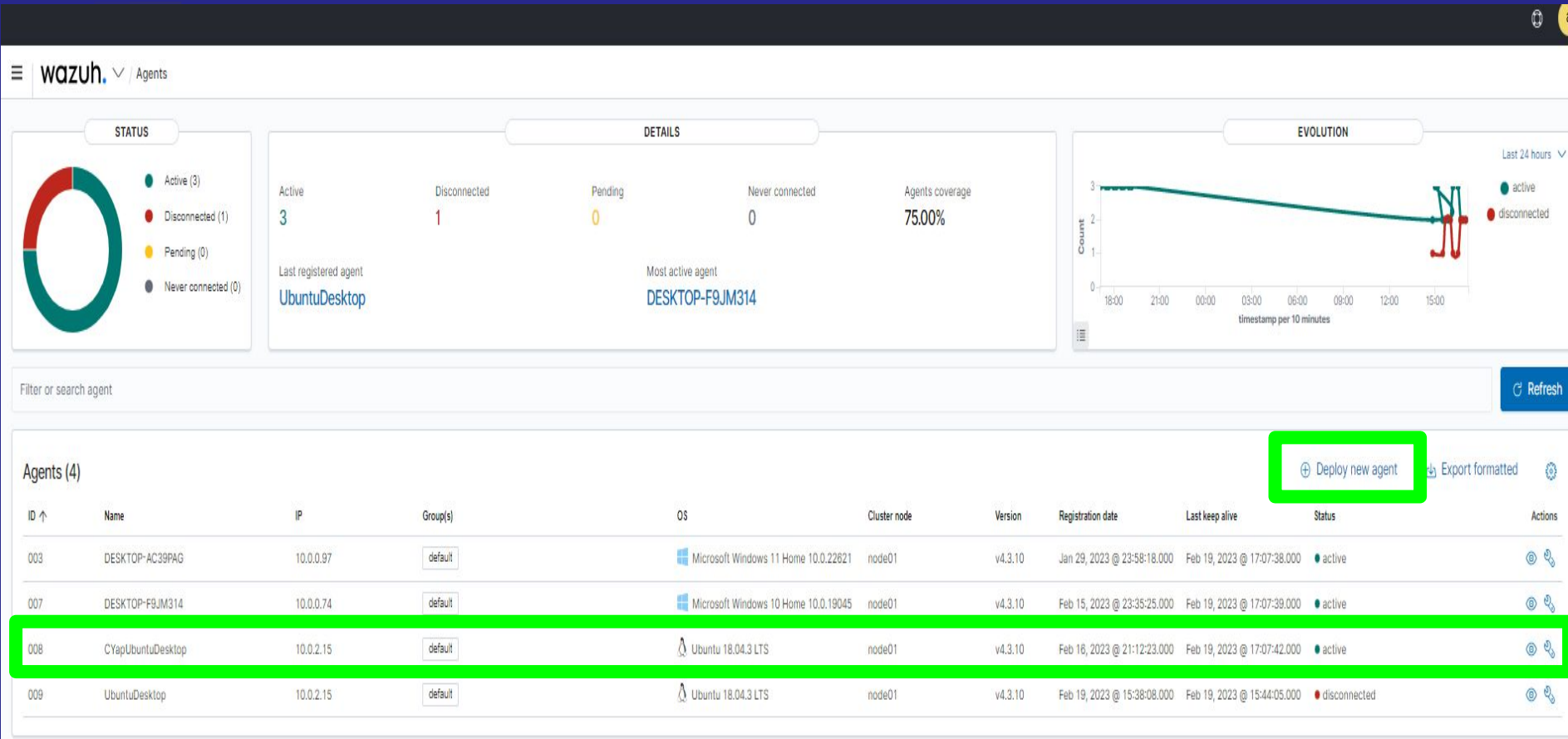
```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.9-1.msi -OutFile $(env:tmp)\wazuh-agent-4.3.9.msi; msexec.exe /i $(env:tmp)\wazuh-agent-4.3.9.msi /q WAZUH_MANAGER="10.0.0.198" WAZUH_REGISTRATION_SERVER="10.0.0.198" WAZUH_AGENT_GROUP="windows"
```

5

Start the agent

NET START WazuhSvc

Steps to Install the Wazuh Agent



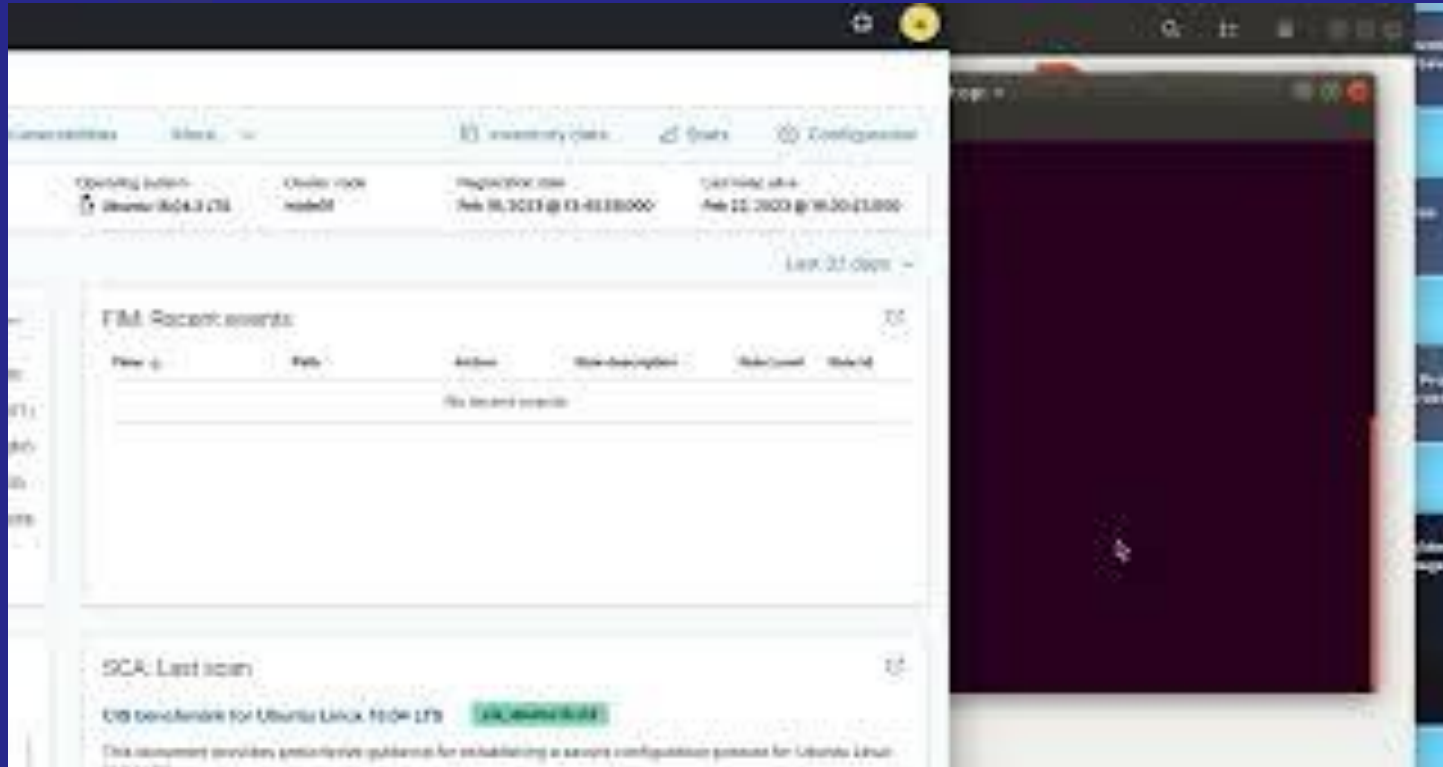
End Goal or Vulnerability Being Exploited

Today's demo will illustrate the following functionalities:

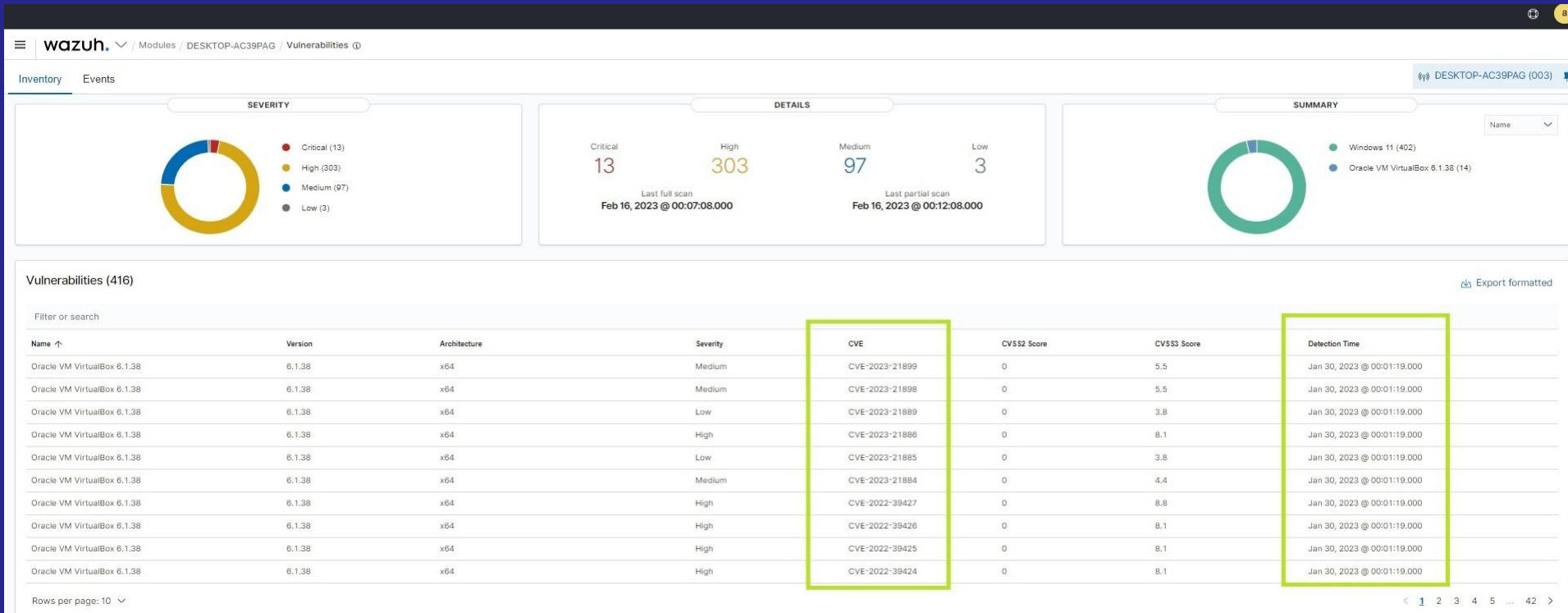
- Brute Force Attacks
- Common Vulnerabilities and Exposures (CVEs)



Brute Force Attack Simulation Demo

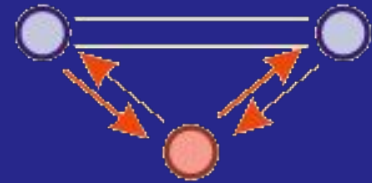


Detecting Unpatched CVEs



Mitigations

- Close all ports on your personal computer
- Firewalls should be up-to-date
- Aging firewalls present a security risk for your environment
- Make sure IPS is updated



Mitigations

- Proper Security training on multi-factor authentication
- Don't use your personal information for your passwords and never recycle passwords for your accounts.
- Patching Vulnerabilities.
- Bi-weekly In house Pentesting: can proactively prevent incidents from happening.
- Hardening systems against high CVEs higher than 6

We hope to see you guys again soon!

