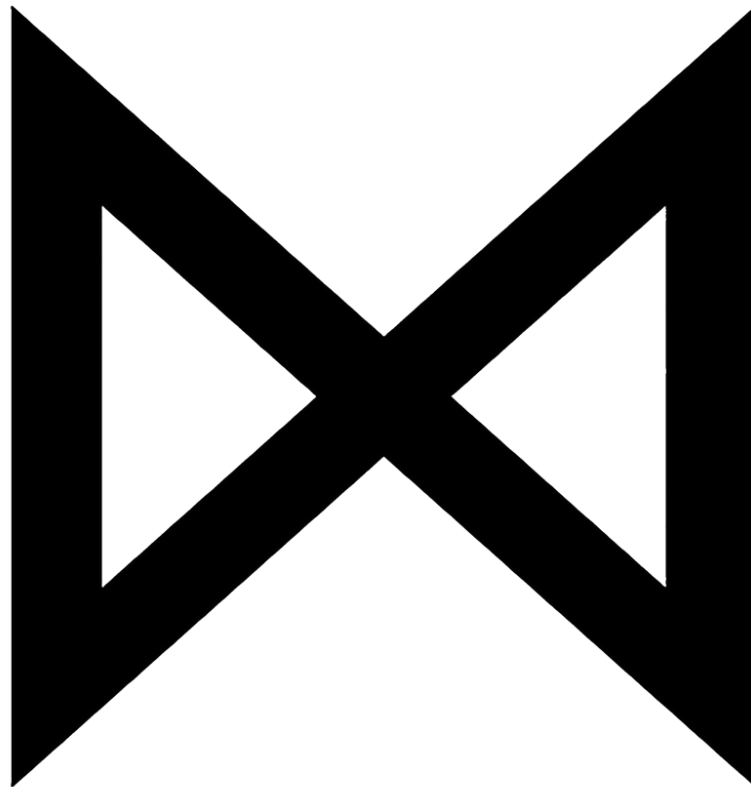


OPERATION TITAN SHIELD



MONARCH

Discovery and Defense in a Time of Monsters



SCENARIO

Monarch is a global scientific organization tasked with studying and protecting the ancient and powerful creatures known as massive unidentified terrestrial organisms, also referred to as "Titans." Founded as a joint Japanese-American task force in 1946, Monarch's mission has evolved over the years from simple investigation to the discovery and observance of Titans, which it believes are essential to the preservation of life on Earth. With at least 67 outposts around the world and a military branch known as the G-Team, Monarch is dedicated to protecting humanity from the dangers posed by these massive creatures while unlocking the secrets of their biology and behavior.

As the newly hired incident response team for Monarch, your primary responsibility is to ensure that the organization's critical services remain available in the face of cyber threats. You work alongside Monarch's IT team and G-Team to implement security measures that protect Monarch's networks, systems, and data from cyber-attacks.

Your team has received a warning from Monarch's IT team that attackers are attempting to breach Monarch's network. The intent is unclear, but their actions suggest that they are attempting to disrupt Monarch's critical services. If the network takes significant damage and the critical services are unable to function properly Monarch may lose control over the titans and set forth a worldwide event that can only be described as apocalyptic.

Monarch is constantly evolving and improving to stay on the cutting edge of Titan research. To ensure this, Monarch is committed to constantly upgrading, improving, and adding network services. To uphold this standard, your team will be required to complete various technical tasks throughout the night known as "injects."

The system administration team for Monarch has identified a number of vulnerabilities in Monarch's systems that must be addressed immediately to protect against cyber attacks. To incentivize the remediation of these vulnerabilities, Monarch has implemented a rewards program that recognizes and celebrates the hard work and dedication of its incident response team. This rewards system has been affectionately named "Aeacus" and will be available on some of the systems in the network.

Tonight's events will underscore the importance of protecting Monarch's mission of studying and protecting the Titans while also highlighting the critical nature of the incident response team's role in shielding Monarch's networks and systems from cyber threats. Thus, tonight's operation will be named TITAN SHIELD.



OPERATION BRIEFING INDEX

1-NETWORK [monarch.lan]

2-USER ADMINISTRATION

3-OPERATIONS



NETWORK [monarch.lan]

Hostname	External IP	OS	Role	Description
bravo	172.16.x.3	WS2016	DC DNS RDP SSH	Domain Controller and primary DNS server for Monarch's network. Monarch's domain controller manages access to the organization's resources and data. RDP and SSH are required for remote access.
skullisland	172.16.x.4	WS2019	FTP HTTP RDP	Server located at the Skull Island research outpost. On-site researchers report findings through a Wiki. File sharing server shares documents/media relating to Kong. RDP is required for remote access.
atoll	172.16.x.5	WS2019	SQL HTTP RDP	SQL server for Monarch Systems. Hosts an e-commerce website selling Monarch merchandise. RDP is required for remote access.
hollowdark	172.16.x.6	W10	RDP	Workstation machine located in the Hollow Dark research center. Often used by the IT team to remotely manage other Monarch servers.
sedona	172.16.x.7	U22	HTTP SSH	Server located in Monarch's Sedona outpost where the MUTO known as Scylla is being studied. The blog website is recording research data. SSH is required for remote access.
janjira	172.16.x.8	U20	SQL SSH	SQL server for Monarch Systems built upon the ruins of the Janjira Nuclear Power Plant. SSH is required for remote access.
yunnan	172.16.x.9	F36	SMTP HTTP SSH	Monarch internal mail server, also hosts a webmail interface. SSH is required for remote access.

KEY:

WS	Windows Server
W	Windows Desktop [Professional]
U	Ubuntu Desktop
F	Fedora Desktop



USER ADMINISTRATION

For Monarch, the importance of ensuring user accounts are configured correctly cannot be overstated. Misconfigured accounts can lead to unauthorized access to Monarch's systems and sensitive data, putting the organization's mission at risk. By carefully configuring user accounts and access permissions, Monarch can reduce the risk of these types of attacks and help to ensure that its critical services remain secure. As the incident response team for Monarch, it is imperative that you prioritize the identification and remediation of any misconfigured accounts to prevent unauthorized access and maintain the security of the organization's systems and networks.

Standard account configuration

Administrators:

```
madmin (you)
  - Password: Password1!
iserizawa
  - Password: Password1!
vgraham
  - Password: Password1!
ichen
  - Password: Password1!
```

Users:

```
branda
hbrooks
lsan
jconrad
abrooks
wriccio
singh
erussell
mrussell
scoleman
rstanton
nlind
iandrews
```



Recovered Credentials

The list of credentials provided in this report represents only what was able to be recovered and may not be a comprehensive representation of all credentials.

Prestashop:

madmin@monarch.co:Password1!

Atoll SQL:

root:root

Janjira SQL:

root:<blank>

Found issues

During testing we have found that the Prestashop instance is not accessible internally. If you need to manage the e-commerce site, please access it externally at <http://172.16.x.5>.

Attackers have changed passwords to the users on the `sedona` system. Users vgraham, iserizawa, and ichen have the password ffa35gBB1!



OPERATIONS

Network Access

To access Monarch's critical services and systems, employees and authorized personnel must first establish a Virtual Private Network (VPN) connection. This VPN connection is established using secure authentication methods and encryption protocols to ensure the confidentiality and integrity of data transmitted over the network. Once the VPN connection is established, employees and authorized personnel can access Monarch's network and various dashboards that provide real-time visibility into the security posture of Monarch's systems and networks.

VPN Instructions	VPN Instructions [LINK]
------------------	---

Dashboards

As the incident response team for Monarch, your role is to ensure the security and integrity of the organization's critical services. To achieve this, you need to be able to quickly identify and respond to potential threats and vulnerabilities. One effective tool for achieving this is the use of security dashboards that provide real-time visibility into the security posture of Monarch's systems and networks. These dashboards can help your team to identify potential threats, track the status of ongoing security incidents, and prioritize remediation efforts. To assist you in this mission, we have compiled a list of various dashboards and services that can help you to manage Monarch's security operations more effectively.

Critical service status	http://172.16.10.24
Rewards system status	https://scoring.cyberaegis.tech

Machine Access



The Proxmox Hypervisor is a virtualization platform that allows Monarch's security team to access and manage the organization's virtual machines and containers.

Proxmox Hypervisor	https://172.16.10.10:8006
--------------------	---



Critical Service Status Dashboard (Details)

The Critical Service Status Dashboard provides a visual representation of the status of Monarch's critical services. **Green** indicates that the service is up and running without any issues, while **Red** indicates that the service is currently down or experiencing significant issues. **Grey** indicates that the status of the service is currently unknown or pending further investigation.

Service Status: Functional	
Service Status: Down	
Service Status: Pending	