

Reel Education Site Book

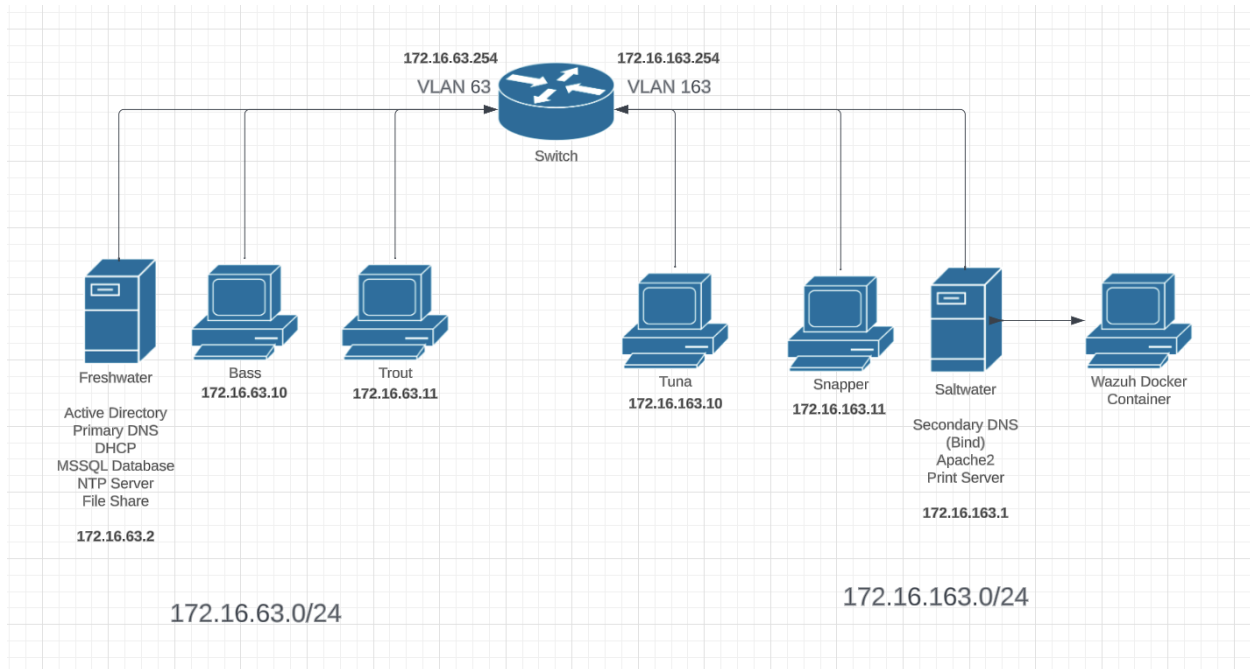


At Reel Education, our mission is to empower individuals with the knowledge and skills needed to become confident and responsible anglers. We are dedicated to providing high-quality fishing education and training that fosters a deep appreciation for aquatic ecosystems, ethical fishing practices, and conservation efforts. Our commitment is to create an inclusive learning environment where people of all ages and backgrounds can connect with nature, embrace the art of fishing, and become stewards of our precious aquatic resources. We strive to inspire a lifelong passion for angling while promoting sustainability and environmental consciousness within our community and beyond.

Table of Contents

Topology	3
Systems	3
Freshwater - Windows Server.....	3
Saltwater - Linux Server	4
Trout/Bass - Windows Clients	4
Snapper/Tuna - Linux Clients	5
Applications/Services.....	5
User Accounts.....	5
Subnet and VLAN Allocation	6
Choice of OS/Application Versions.....	6
Security Controls	7
Microsoft Windows 10 Enterprise CIS Benchmark.....	7
Ubuntu 22.04 CIS Benchmark.....	8
MDR Platform	8
MITRE ATT&CK Techniques	9
1. 5.3.7 Ensure access to the su command is restricted	9
2. 5.4.2 Ensure lockout for failed password attempts is configured	11
3. 5.2.4 Ensure SSH access is limited.....	14
4. 1.1.1 Ensure 'Enforce password history' is set to '24 or more password(s)'	16
5. 2.2.6 Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'	18
CTI Report: 30TH OCTOBER 2023 – THREAT INTELLIGENCE REPORT, Check Point Research.....	20
Akira Ransomware (Linux):	20
Data Breaches (Various Educational Institutions):	21
Vulnerabilities and Patches (Various Products):.....	21
Global Cyber Attacks Trend:	21
Check Point's Cybersecurity Predictions for 2024:.....	22
Hugging Face AI Supply Chain Attack:	22
Cactus Ransomware:	23

Topology



Systems

- Windows Server 2022 Standard - OS build 20348.1850
- Windows 10 Clients - OS build 15063.540
- Ubuntu Desktop 23.10.1 (Server and Clients)
- Wazuh Docker - Version 4.7.0

Freshwater - Windows Server

172.16.63.2

- Active Directory
- Primary DNS
- DHCP Scopes

- MSSQL Database
- NTP Policy
- File Share
- Security Group Policies
- User Management
- Wazuh Agent

Saltwater - Linux Server

172.16.163.1

- Secondary DNS
- Apache2 Web Server
- CUPS Print Server
- Wazuh Manager Docker Container
- Wazuh Agent

Trout/Bass - Windows Clients

172.16.63.10/11

- Connected to AD
- Uses Freshwater/Saltwater for Primary/Secondary DNS
- Gets Time from Freshwater
- RDP Remote Access via any of the 10 Accounts
- Wazuh Agent

Snapper/Tuna - Linux Clients

172.16.163.10/11

- Connected to AD
- Uses Freshwater/Saltwater for Primary/Secondary DNS
- Gets Time from Freshwater
- SSH Remote Access via any of the 10 Accounts
- Wazuh Agent

Applications/Services

- Apache2 Web Server - Apache/2.4.57 (Ubuntu)
- CUPS Print Server - 2.4.6-0ubuntu3
- BIND9 DNS Server - 1:9.18.18-0ubuntu2
- Docker - 24.0.7
- MSSQL Server - Microsoft SQL Server 2019 (MSSQLSERVER)

User Accounts

- Domain Users:
 - BigFish (Domain Admin)
 - CapAhab (Domain Admin)
 - JerWade
 - DavMoore
 - RayScott
 - MicLerner
 - TedWilliams
 - RicClunn
 - BilDance
 - AndMill

- Linux Users
 - Saltwater (Local Admin Account on Saltwater)
 - Snapper (Local Admin Account on Snapper)
 - Tuna (Local Admin Account on Tuna)

Subnet and VLAN Allocation

The subnets and VLANs were assigned to be Windows on one VLAN (63) and Linux on the other VLAN (163). This is because it made sense for us to separate the two by OS. While we understand this would not be practical in a real-world environment, we simply wanted to do this for the project.

Choice of OS/Application Versions

For our infrastructure, we picked specific OS and application/service versions based on what we were able to get our hands on. For the Windows OS versions, we did opt to go with Windows 10 instead of 11 as that is what we were more familiar with.

For the linux systems, we also chose to go with Ubuntu OS due to familiarity. We also chose to go with the latest versions of all applications and services as we believed that they would be more secure, and have the least issues with compatibility.

Security Controls

For our security controls, we mainly focused on two things: account security (strong passwords, account lockouts, etc.) and remote access control. For the Windows systems, we implemented these controls as group policy objects (GPOs) and applied them to all target hosts. For the Linux systems, the controls were implemented manually. However, we did not get to all of the controls listed under the Ubuntu benchmark below on every Ubuntu system; some (5.3.1 => 5.4.5) are ones that we would apply given more time.

Microsoft Windows 10 Enterprise CIS Benchmark

https://www.cisecurity.org/benchmark/microsoft_windows_desktop

- 1.1.1 Ensure 'Enforce password history' is set to '24 or more password(s)'
- 1.1.2 Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'
- 1.1.3 Ensure 'Minimum password age' is set to '1 or more day(s)'
- 1.1.4 Ensure 'Minimum password length' is set to '14 or more character(s)'
- 1.1.5 Ensure 'Password must meet complexity requirements' is set to 'Enabled'
- 1.1.6 Ensure 'Relax minimum password length limits' is set to 'Enabled'
- 1.1.7 Ensure 'Store passwords using reversible encryption' is set to 'Disabled'
- 1.2.1 Ensure 'Account lockout duration' is set to '15 or more minute(s)'
- 1.2.2 Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'
- 1.2.3 Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'
- 2.2.2 Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'
- 2.2.6 Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'
- 2.2.16 Ensure 'Deny access to this computer from the network' to include 'Guests, Local account'
- 2.2.20 Ensure 'Deny log on through Remote Desktop Services to include 'Guests, Local account'

Ubuntu 22.04 CIS Benchmark

https://www.cisecurity.org/benchmark/ubuntu_linux

- 5.2.4 Ensure SSH access is limited
- 5.2.5 Ensure SSH LogLevel is appropriate
- 5.2.6 Ensure SSH PAM is enabled
- 5.2.7 Ensure SSH root login is disabled
- 5.2.8 Ensure SSH HostbasedAuthentication is disabled
- 5.2.9 Ensure SSH PermitEmptyPasswords is disabled
- 5.2.10 Ensure SSH PermitUserEnvironment is disabled
- 5.2.11 Ensure SSH IgnoreRhosts is enabled
- 5.2.12 Ensure SSH X11 forwarding is disabled
- 5.3.1 Ensure sudo is installed
- 5.3.2 Ensure sudo commands use pty
- 5.3.3 Ensure sudo log file exists
- 5.3.4 Ensure users must provide password for privilege escalation
- 5.3.5 Ensure re-authentication for privilege escalation is not disabled globally
- 5.3.6 Ensure sudo authentication timeout is configured correctly
- 5.4.1 Ensure password creation requirements are configured
- 5.4.2 Ensure lockout for failed password attempts is configured
- 5.4.3 Ensure password reuse is limited
- 5.4.4 Ensure password hashing algorithm is up to date with the latest standards
- 5.4.5 Ensure all current passwords uses the configured hashing algorithm

MDR Platform

<https://documentation.wazuh.com/current/deployment-options/docker/wazuh-container.html>

For our Monitoring, Detection and Response (MDR) platform, we opted to go with the Wazuh Docker Container as it fulfilled the requirement for both an MDR implementation as well as an isolated Docker service. Wazuh is an open-source tool which allows for real-time monitoring of systems, intrusion detection, and incident response. It was very seamless to set up, and connecting our systems as agents to the manager was easy, as it just involved installing one piece of software to do so.

- Wazuh Manager deployed as Docker container on Saltwater (172.16.163.1)
- All hosts added as agents for real time log collection and analysis
- CIS Benchmark scans run on agents for security control recommendations

MITRE ATT&CK Techniques

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a comprehensive knowledge base that describes the actions and behaviors that adversaries may take to achieve their objectives. In this context, we'll discuss how the implementation of the CIS benchmark recommendations "5.3.7 Ensure access to the su command is restricted", "5.4.2 Ensure lockout for failed password attempts is configured", and 5.2.4 "Ensure SSH access is limited". As for our Windows Server we had chosen the two implementations of the CIS benchmark recommendations for "1.1.1 Ensure 'Enforce password history' is set to '24 or more password(s)'", and "1.1.5 Ensure 'Password must meet complexity requirements' is set to 'Enabled'".

1. 5.3.7 Ensure access to the su command is restricted

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548, T1548.000	TA0005	M1026

T1548 - Abuse Elevation Control Mechanism:

- This technique involves an adversary attempting to manipulate elevation control mechanisms to gain higher privileges on a system. By ensuring access to the su command is restricted, we are implementing a critical control to limit the ability of users to switch to the superuser or another account. This mitigation aligns with the principle of least privilege, reducing the attack surface by restricting unnecessary access. Consequently, even if an adversary gains access to a user account, the restricted su command makes it more challenging for them to escalate privileges.

T1458.000 - Disable or Modify Tools:

- Adversaries often seek to disable or modify system tools to hinder defenders' ability to detect malicious activities. By securing access to the su command, we are fortifying a fundamental tool that allows users to switch to a privileged account. This restriction helps prevent unauthorized modifications or disablement

of the su command itself. A compromised user account is less likely to be misused to manipulate the elevation control mechanisms, thereby limiting an adversary's ability to subvert the system.

Mitigation and Detection (TA0005 tactic and M1026):

- Tactic TA0005 - Defense Evasion:
 - The restriction on su command access contributes to the defense evasion tactic by limiting an attacker's ability to elevate privileges.
- Mitigation M1026 - Privileged Account Management:
 - The implementation of restricting access to the su command aligns with privileged account management principles. It ensures that privilege escalation is tightly controlled, reducing the risk associated with unauthorized access.

Prevention and Detection Mechanisms:

- Prevention
 - By enforcing the restriction on the su command as recommended by the CIS benchmark, we are proactively preventing unauthorized privilege escalation attempts, hindering adversaries from abusing elevation control mechanisms.
- Detection
 - Monitoring and logging activities related to the su command can enable the detection of suspicious or unauthorized attempts to use this command. Regularly reviewing logs for unexpected or anomalous behavior can provide insights into potential malicious activities.

Configuration, Permissions, and Baselines:

- Configuration
 - The configuration involves setting appropriate permissions on the su command, restricting its usage to authorized personnel.
- Permissions
 - User permissions are adjusted to align with the principle of least privilege. Only designated users or roles should have the ability to access the su command.
- Baselines
 - Establishing a baseline involves documenting and enforcing the standard configuration for the su command across all Ubuntu clients in the

infrastructure. This ensures consistency and aids in the detection of deviations from the established security posture.

MDR Platform Implementation:

- A Managed Detection and Response (MDR) platform can enhance the effectiveness of the prevention and detection mechanisms. It can provide real-time monitoring, alerting, and incident response capabilities, allowing security teams to promptly identify and address any suspicious activity related to the su command.

In summary, restricting access to the su command is a crucial security control that aligns with several MITRE ATT&CK techniques and contributes to the overall defense against privilege escalation and tool manipulation by adversaries. The implementation of this control, combined with effective monitoring and response measures, strengthens the security posture of Ubuntu clients in the environment.

2. 5.4.2 Ensure logout for failed password attempts is configured

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1110, T1110.001, T1110.003	TA0006	M1027

T1110 - Brute Force:

- The T1110 technique involves adversaries attempting to gain unauthorized access to accounts by systematically checking all possible passwords. Configuring lockout policies for failed password attempts is a powerful preventive measure against brute-force attacks. By limiting the number of consecutive failed attempts, the likelihood of an adversary successfully guessing the correct password is significantly reduced. Lockout mechanisms can act as a deterrent and slow down attackers attempting to compromise accounts through brute-force methods.

T1110.001 - Password Guessing:

- Similar to brute-force attacks, password guessing involves adversaries systematically attempting different passwords to gain unauthorized access. Configuring lockout policies adds an additional layer of defense against password guessing by temporarily locking out accounts after a specified number of failed attempts. This hinders the success of password guessing attacks, making it more difficult for attackers to compromise accounts through repeated trial and error.

T110.003 - Credential Stuffing:

- Credential stuffing involves the use of previously compromised username and password pairs to gain unauthorized access to other accounts. By configuring lockout policies, we can mitigate the impact of credential stuffing attempts. After a certain number of consecutive failed login attempts, the account is locked, preventing further use of stolen credentials. This restriction hampers the effectiveness of credential stuffing attacks, enhancing the security of user accounts.

Mitigation and Detection (TA0006 tactic and M1027):

- Tactic TA0006 - Credential Access:
 - The implementation of lockout policies directly aligns with the Credential Access tactic by fortifying authentication mechanisms and reducing the risk of unauthorized access.
- Mitigation M1027 - Account Use Policies:
 - Configuring lockout policies falls under the umbrella of account use policies. By defining and enforcing rules for failed password attempts, organizations can better protect user accounts and sensitive resources.

Prevention and Detection Mechanisms:

- Prevention
 - Lockout policies prevent adversaries from gaining unauthorized access through brute-force, password guessing, or credential stuffing attempts. Temporary lockouts act as a deterrent, making these techniques less practical for attackers.
- Detection
 - Monitoring and logging failed password attempts can provide early indications of potential malicious activity. Security teams can analyze

these logs to identify patterns or anomalies that may indicate an ongoing brute-force, password guessing, or credential stuffing attack.

Configuration, Permissions, and Baselines:

- Configuration
 - The configuration involves setting lockout thresholds and durations for failed password attempts. This should be implemented consistently across all user accounts and systems.
- Permissions
 - Appropriate permissions should be assigned to ensure that the lockout configuration is enforced uniformly. This may involve adjusting settings in the security policy or access control mechanisms.
- Baselines
 - Establishing a baseline involves documenting and enforcing the standard lockout configuration for failed password attempts across all systems. Regular audits can ensure that deviations from the baseline are promptly identified and addressed.

MDR Platform Implementation:

- An MDR platform can enhance the detection capabilities by providing real-time analysis of login attempts and failed password events. It can generate alerts for security teams to investigate potential malicious activities and respond to incidents promptly.

In conclusion, configuring lockout policies for failed password attempts is a fundamental security control that directly addresses multiple MITRE ATT&CK techniques associated with unauthorized credential access. By aligning with best practices and mitigation strategies, organizations can significantly enhance the security of their systems and mitigate the risks posed by various credential-based attack techniques.

3. 5.2.4 Ensure SSH access is limited

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021, T1021.004	TA0008	M1018

T1021 - Remote Services:

- T1021 involves adversaries leveraging remote services to establish or maintain control over a system. By limiting SSH access as per the CIS benchmark recommendation, organizations can reduce the attack surface exposed to potential adversaries. Restricting SSH access to only authorized users and systems helps prevent unauthorized remote access attempts, making it more difficult for adversaries to exploit this avenue for gaining control over the system.

T1021.004 - Remote System Discovery:

- Remote System Discovery (T1021.004) involves adversaries identifying and enumerating remote systems on a network to gather information for potential exploitation. Limiting SSH access contributes to the prevention of this technique by restricting the ability of adversaries to connect to systems remotely and perform reconnaissance activities. This control is particularly relevant as SSH is a common protocol used for remote system administration and should be tightly controlled to prevent unauthorized discovery.

Mitigation and Detection (TA0008 tactic and M1018):

- Tactic TA0008 - Exfiltration Over Physical Medium:
 - While limiting SSH access primarily focuses on prevention, it indirectly contributes to the Exfiltration Over Physical Medium tactic by reducing the risk of unauthorized access, which could lead to data exfiltration. By controlling remote access, organizations mitigate the potential for adversaries to establish a foothold for later exfiltration.
- Mitigation M1018 - Network Segmentation:
 - The limited SSH access aligns with network segmentation principles, as it helps create boundaries and restricts the potential lateral movement of

adversaries within the network. Network segmentation enhances security by containing and isolating potential threats.

Prevention and Detection Mechanisms:

- Prevention
 - Limiting SSH access prevents adversaries from exploiting this remote service for unauthorized access. This is achieved by defining and enforcing strict rules regarding who can access systems via SSH, reducing the risk of compromise.
- Detection
 - Monitoring and logging SSH access attempts can aid in the detection of potential unauthorized activities. Anomalies such as multiple failed login attempts or unexpected connections can be indicators of malicious intent, prompting further investigation.

Configuration, Permissions, and Baselines:






- Configuration
 - The configuration involves defining and enforcing rules for SSH access, specifying which users or groups are allowed remote access and from which IP addresses. This configuration should be consistent across all systems.
- Permissions
 - Proper permissions must be assigned to enforce the limited SSH access configuration. This may involve adjusting settings in the SSH server configuration and access control mechanisms.
- Baselines
 - Establishing a baseline involves documenting and enforcing the standard SSH access configuration across all systems. Regular audits can ensure that deviations from the baseline are promptly identified and addressed.

MDR Platform Implementation:

- An MDR platform can enhance detection capabilities by monitoring SSH access logs in real-time. It can generate alerts for security teams to investigate suspicious activities, such as unusual login patterns or multiple failed login attempts, and respond to potential security incidents promptly.

In conclusion, ensuring limited SSH access is a critical security control that directly addresses multiple MITRE ATT&CK techniques associated with remote services and system discovery. By aligning with best practices and mitigation strategies, organizations can significantly enhance the security of their systems and reduce the risk of unauthorized access and reconnaissance activities.

4. 1.1.1 Ensure 'Enforce password history' is set to '24 or more password(s)'

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

T1110 - Brute Force:

- Brute force attacks involve adversaries systematically attempting different passwords to gain unauthorized access. By enforcing a password history policy requiring '24 or more password(s),' the organization mitigates the risk of successful brute force attacks. Attackers are restricted from cycling through a limited set of passwords, making it significantly more challenging to guess the correct password and gain unauthorized access.

T1201 - Password Policy Discovery:

- Password policy discovery involves adversaries attempting to understand the password requirements and constraints of a target system. Enforcing a specific password history setting (e.g., '24 or more password(s)') complicates the adversary's efforts to discern the organization's password policy. This enhances the security of the environment by reducing the likelihood of attackers exploiting weaknesses in password policies.

Mitigation and Detection (TA0006 tactic and M1027):

- Tactic TA0006 - Credential Access:
 - Enforcing a robust password history policy contributes to the Credential Access tactic by making it more challenging for adversaries to gain unauthorized access to accounts through password-related tactics, such as brute force attacks.
- Mitigation M1027 - Account Use Policies:
 - The implementation of the password history policy aligns with account use policies, specifically enhancing password-related controls. It ensures that users adhere to a secure practice of not reusing passwords within a specified history, reducing the risk of compromised credentials.

Prevention and Detection Mechanisms:

- Prevention
 - By enforcing the '24 or more password(s)' requirement, the organization proactively prevents brute force attacks that rely on the reuse of passwords. Attackers attempting to guess passwords are limited in their effectiveness due to the requirement for a large and non-repeating set of passwords.
- Detection
 - Monitoring and logging password change events can aid in the detection of potential anomalies or malicious activities. Sudden and unexpected changes in password patterns, such as multiple password changes in a short period, can trigger alerts for investigation.

Configuration, Permissions, and Baselines:

- Configuration
 - The configuration involves setting the 'Enforce password history' policy to '24 or more password(s)' in line with the CIS benchmark. This is applied consistently across all user accounts in the environment.
- Permissions
 - Permissions are adjusted to ensure that the password history policy is uniformly enforced. Appropriate access controls are configured to prevent unauthorized changes to the password policy settings.
- Baselines

- Establishing a baseline involves documenting and enforcing the standard password history configuration across all systems. Regular audits can help identify and rectify any deviations from the established baseline.

MDR Platform Implementation:

- A Managed Detection and Response (MDR) platform can enhance the detection capabilities by providing real-time analysis of password change events and related activities. It can generate alerts for security teams to investigate potential malicious activities and respond to incidents promptly.

In summary, enforcing the 'Enforce password history' policy with '24 or more password(s)' is a critical security control that aligns with various MITRE ATT&CK techniques and contributes to the prevention of brute force attacks and unauthorized credential access. The implementation of this control, along with effective monitoring and response measures, strengthens the security posture of the environment.

5. 2.2.6 Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

T1021 - Remote Services:

- The configuration of "Allow log on through Remote Desktop Services" directly impacts the Remote Services tactic (T1021) by restricting access to specified user groups. This helps prevent unauthorized remote access to systems, limiting the attack surface for adversaries attempting to leverage remote services for lateral movement.

T1021.004 - Remote Desktop Protocol (RDP):

- By defining the allowed user groups for Remote Desktop Services, the organization can prevent adversaries from exploiting RDP to gain unauthorized

access. This configuration aligns with the broader defense against T1021.004, reducing the risk associated with unauthorized RDP access.

Mitigation and Detection (TA0008 tactic and M1018):

- **Tactic TA0008 - Discovery:**
 - The mitigation aligns with the broader discovery tactic (TA0008) by limiting the visibility of remote systems to unauthorized entities. Adversaries seeking to discover and enumerate systems may find it challenging to gather information through RDP due to the configured access restrictions.
- **Mitigation M1018 - Remote System Discovery:**
 - Configuring "Allow log on through Remote Desktop Services" to specific user groups contributes to the mitigation of remote system discovery (M1018). Adversaries looking to discover and enumerate remote systems may encounter restrictions, hindering their ability to identify potential targets through RDP.

Prevention and Detection Mechanisms:

- **Prevention**
 - By setting "Allow log on through Remote Desktop Services" to 'Administrators, Remote Desktop Users,' the organization proactively prevents unauthorized users from accessing systems through RDP. This limits the exposure of systems to potential adversaries attempting to leverage RDP for unauthorized access or lateral movement.
- **Detection**
 - Monitoring and logging RDP login attempts can aid in the detection of potential anomalies or malicious activities related to Remote Desktop Services. Unusual login patterns, repeated failed login attempts, or login attempts from unauthorized users can trigger alerts for investigation.

Configuration, Permissions, and Baselines:

- **Configuration**
 - The configuration involves setting the "Allow log on through Remote Desktop Services" policy to 'Administrators, Remote Desktop Users' in accordance with the CIS benchmark. This ensures that only authorized users can log in remotely through RDP.
- **Permissions**

- Permissions are adjusted to ensure the uniform enforcement of RDP access restrictions. Access controls are configured to prevent unauthorized changes to the Remote Desktop Services policy settings.
- **Baselines**
 - Establishing a baseline involves documenting and enforcing the standard Remote Desktop Services configuration across all systems. Regular audits can help identify and rectify any deviations from the established baseline.

MDR Platform Implementation:

- A Managed Detection and Response (MDR) platform can enhance detection capabilities by providing real-time analysis of RDP login attempts and related activities. It can generate alerts for security teams to investigate potential malicious activities and respond to incidents promptly, especially in cases where adversaries attempt to manipulate RDP access settings.

In conclusion, configuring "Allow log on through Remote Desktop Services" to 'Administrators, Remote Desktop Users' is a critical security control that aligns with various MITRE ATT&CK techniques. It contributes to the prevention of unauthorized RDP access, mitigates the risk associated with remote system discovery, and enhances the overall security posture of the environment. The implementation of this control, along with effective monitoring and response measures, strengthens the organization's resilience against potential threats leveraging RDP.

CTI Report: 30TH OCTOBER 2023 – THREAT INTELLIGENCE REPORT, Check Point Research

Lorenf. "30th October – Threat Intelligence Report." Check Point Research, 30 Oct. 2023, research.checkpoint.com/2023/30th-october-threat-intelligence-report/.

Akira Ransomware (Linux):

Mitigations:

- Implement regular backups of critical data to ensure quick recovery in case of a ransomware attack.
- Utilize endpoint protection solutions like Check Point Harmony End Point to detect and mitigate ransomware threats.

Threats to Reel Education:

- Possible exposure of sensitive educational data.
- Disruption of services and operations due to encrypted files.

Current Security Capability:

- Backups are not implemented, so recovery would be a challenge in the case of a ransomware attack.
- MDR has been implemented through use of Wazuh, so the team would be able to detect possible ransomware threats and work to mitigate them as fast as possible.

Data Breaches (Various Educational Institutions):

Mitigations:

- Strengthen network segmentation to limit lateral movement in case of unauthorized access.
- Regularly audit and update security policies to ensure access controls are robust.
- Implement strong email security measures to prevent phishing attacks.

Threats to Reel Education:

- Potential exposure of student and employee personal information.
- Risk of unauthorized access to servers and systems.

Current Security Capability:

- Lateral movement is limited in the infrastructure through usage of strong security controls involving remote access to systems.
- Reel Education currently does not have email accounts, so the susceptibility to phishing attacks is low.

Vulnerabilities and Patches (Various Products):

Mitigations:

- Establish a robust patch management process to promptly apply security updates.
- Regularly assess and update third-party plugins and applications.
- Employ network-based security solutions to detect and block exploitation attempts.

Threats to Reel Education:

- Exploitation of unpatched vulnerabilities could lead to unauthorized access.
- Possible compromise of systems and data due to exploitation of known vulnerabilities.

Current Security Capability:

- Reel Education does manual installations of security updates and patches to all of our software products. This could leave the company open to vulnerabilities if we are not meticulous with checking for updates.

- ReelEducation would be wise to implement an automated solution to check for updates periodically and install them if needed.

Global Cyber Attacks Trend:

Mitigations:

- Enhance security awareness training for staff to recognize and avoid phishing attacks.
- Monitor network traffic and logs for signs of unusual activity.
- Regularly update and test incident response plans.

Threats to Reel Education:

- Increased likelihood of phishing attempts and ransomware attacks.
- Potential compromise of educational data and disruption of services.

Current Security Capability:

- There is currently no security awareness training within Reel Education's organization for its employees which will make it harder for staff to recognize and avoid phishing attacks however, Reel Education does not have email accounts so our susceptibility to phishing attacks is low.
- MDR has been implemented through the use of Wazuh, so network traffic and logs are able to be monitored for anomalous activity.
- Reel Education currently has no incident response plans in place so the company will need to work on creating them and updating them based on current events as well as infrastructure.

Check Point's Cybersecurity Predictions for 2024:

Mitigations:

- Stay informed about emerging cybersecurity threats and trends.
- Invest in advanced threat detection and response capabilities.
- Collaborate with industry partners and organizations for threat intelligence.

Threats to Reel Education:

- Potential targeted attacks on educational institutions.
- Increased sophistication and diversity of cyber threats.

Current Security Capability:

- Reel Education does not currently utilize CTI in order to make informed cyber decisions. This is something that will be implemented in the future.
- Reel Education utilizes Wazuh in order to monitor network and endpoint traffic and logs which will help with threat detection and response capabilities.
- Reel Education does not collaborate with industry partners and organizations for threat intelligence. This will be considered for the future of the company.

Hugging Face AI Supply Chain Attack:

Mitigations:

- Monitor and control access to AI development platforms.
- Regularly review and verify the integrity of AI models and datasets.
- Implement secure coding practices for AI applications.

Threats to Reel Education:

- Potential compromise of future AI models and datasets used in educational applications.
- Risk of malicious code execution and unauthorized access.

Current Security Capability:

- Reel Education currently does not use any AI software, so the organization is not prone to this attack.
- In the future, if the organization did venture into the usage of AI, the mitigations listed above would have to be implemented.

Cactus Ransomware:

Mitigations:

- Enhance email security to prevent phishing attacks that may deliver ransomware.
- Implement behavior-based detection mechanisms to identify unusual activities.
- Regularly update and patch software to address known vulnerabilities.

Threats to Reel Education:

- Risk of ransomware infection and encryption of critical educational data.
- Potential disruption of operations and services.

Current Security Capability:

- Reel Education currently uses up-to-date software versions, so we are not prone to any known vulnerabilities at the moment.
- Reel Education does not use email technology, so we are protected against phishing attacks.
- Reel Education has an MDR platform and given the time, would be able to implement behavior-based detection using things such as Sigma rules.

By adopting these mitigations, Reel Education can better protect its computer infrastructure against a range of cyber threats and vulnerabilities, ensuring the confidentiality and integrity of sensitive educational information. Regular monitoring, training, and collaboration with cybersecurity experts can further enhance the institution's overall security posture.