**Responses Mixed**

**Insecure Config**

**Gemini**

Here's a breakdown of the security concerns in the provided switch configuration:

* **No Password Encryption:** The command no service password-encryption is present, which means that passwords stored in the configuration file will be visible in plain text. This is a critical security vulnerability, as anyone with access to the configuration file can easily obtain passwords.
* **Enable Password is Weak:** The configuration has both an enable secret and an enable password set. The enable password is set to "123456", which is a very weak password and poses a significant security risk. The enable secret is properly hashed, but the presence of a weak enable password undermines the security.
* **DHCP Snooping Not Configured:** The provided configuration does not include any DHCP snooping configuration. DHCP snooping is an important security feature to prevent DHCP spoofing attacks.
* The configuration lacks explicit port security configurations. Port security features, such as limiting MAC addresses per port, should be implemented to prevent MAC spoofing and other port-based attacks.
* **SSH/Telnet:** The configuration shows password protection for VTY lines (telnet/SSH access) but doesn't include access control lists (ACLs) to restrict which hosts can connect to these services. This means any device that can reach the switch could attempt to establish a Telnet or SSH session.
* The configuration does not show any ports being shut down. It's crucial to ensure that all unused ports are administratively shut down to minimize potential attack vectors.
* **HTTP Services Not Disabled:** The configuration does not explicitly disable the HTTP server or secure HTTP server. Leaving these services enabled can expose the switch to potential vulnerabilities.
* **Self-Signed Certificate:** The configuration includes a self-signed certificate. While self-signed certificates provide encryption, they are not trusted by default and can lead to man-in-the-middle attacks if not handled carefully. Consider using certificates issued by a trusted Certificate Authority (CA) for production environments.

**ChatGPT**

Thanks for sharing the switch configuration. Here’s a security review of the provided configuration, with highlights of potential vulnerabilities and recommended best practices:

🔐 Security Issues Identified Plaintext Passwords

enable password 123456 – This is stored in plaintext, which is a major security risk.

VTY line passwords are obfuscated but not secure (password 1kWY9UYyopV3rp0iV3c7Ow==). This uses type 7 encryption, which is easily reversible.

Fix:

plaintext Copy Edit no enable password service password-encryption Use only enable secret for secure password storage.

no aaa new-model

AAA (Authentication, Authorization, Accounting) is disabled. This leaves the switch with very basic and insecure authentication methods.

Fix:

plaintext Copy Edit aaa new-model Password Encryption Not Enabled

no service password-encryption is set, so all local passwords are stored in cleartext unless specifically hashed (type 5 or 9). This allows for potential credential compromise if the config is exposed.

Fix:

plaintext Copy Edit service password-encryption Unused Ports Not Disabled

Interfaces FastEthernet0/13 to 0/23, and both GigabitEthernet0/1 and 0/2 are not in use but are left administratively up by default.

Fix:

plaintext Copy Edit interface range Fa0/13 - 23 , Gi0/1 - 2 shutdown switchport mode access switchport access vlan 999 description **Unused Port** No Port Security on Access Ports

Access ports on VLANs 2 and 3 have no port security configured. This leaves them vulnerable to MAC flooding and rogue devices.

Fix:

plaintext Copy Edit interface range Fa0/1 - 12 switchport port-security switchport port-security maximum 1 switchport port-security violation restrict switchport port-security mac-address sticky No Logging or Syslog Server Defined

No syslog or logging destination is configured. This limits monitoring and incident response capability.

Fix (example):

plaintext Copy Edit logging 192.168.1.100 logging trap warnings No NTP Configuration

Lack of NTP results in inaccurate timestamps in logs, making event correlation harder.

Fix:

plaintext Copy Edit ntp server 192.168.1.1 Trunk Port Open Without Filtering

FastEthernet0/24 is configured as a trunk with no VLAN filtering or allowed VLANs.

Fix:

plaintext Copy Edit switchport trunk allowed vlan 2,3 ✅ Good Practices Present enable secret is present and hashed (type 5).

no ip http server and no ip http secure-server – disables the web UI, which is good for security.

VLAN interfaces are configured correctly for routing.

Would you like me to create a hardened version of this config for you?

**Grok 3**

Reviewing the provided Cisco switch configuration, several security issues stand out that could expose the network to risks. Below is a detailed analysis of the potential security errors and recommendations for mitigation:

Plaintext Passwords:

Issue: The configuration includes an enable password set as 123456, which is stored in plaintext (enable password 123456). Additionally, the line vty passwords are also visible in the configuration, though they appear to be encoded, the encoding method is not specified and could be weak.

Risk: Plaintext passwords are easily readable by anyone with access to the configuration file, increasing the risk of unauthorized access. Weak passwords like 123456 are especially vulnerable to brute-force attacks.

Recommendation:

Replace enable password with enable secret, which uses stronger hashing (e.g., MD5 in this case, as seen with enable secret 5 ...). For example:

no enable password

enable secret <strong-password>

Ensure all passwords are complex, using a mix of letters, numbers, and symbols, and at least 12 characters long.

For VTY lines, use password with a strong value and consider enabling service password-encryption to encrypt passwords in the configuration:

service password-encryption

Lack of AAA (Authentication, Authorization, Accounting):

Issue: The configuration explicitly disables AAA with no aaa new-model.

Risk: Without AAA, the switch relies on local passwords, which are less secure and harder to manage for multiple users. There’s no centralized authentication or logging of access attempts.

Recommendation:

Enable AAA for centralized authentication, preferably using a protocol like TACACS+ or RADIUS. Example:

aaa new-model

aaa authentication login default group tacacs+ local

aaa authorization exec default group tacacs+ local

tacacs-server host <server-ip>

tacacs-server key <key>

If AAA isn’t feasible, configure local usernames with strong passwords:

username admin privilege 15 secret <strong-password>

Insecure VTY Access:

Issue: The VTY lines (line vty 0 4 and line vty 5 15) allow remote access via Telnet, as no transport input restriction is specified, and SSH isn’t explicitly enforced. The password for VTY access appears encoded but may use a weak method.

Risk: Telnet sends credentials in plaintext, making them vulnerable to interception. Open VTY lines without access restrictions could allow unauthorized access attempts.

Recommendation:

Disable Telnet and enforce SSH:

line vty 0 15

transport input ssh

login local

Generate an RSA key for SSH if not already present:

crypto key generate rsa

Choose a key length of at least 2048 bits for better security.

Restrict VTY access with an access list:

access-list 10 permit 192.168.8.0 0.0.0.255

line vty 0 15

access-class 10 in

HTTP Server Enabled with Self-Signed Certificate:

Issue: The configuration includes a self-signed certificate for HTTPS (crypto pki trustpoint), but no ip http server and no ip http secure-server are present, suggesting the HTTP/HTTPS servers are disabled. However, the presence of the certificate without clear usage raises questions about prior configurations.

Risk: If the HTTP server was previously enabled, it could have been a vector for attacks, especially with a self-signed certificate, which is less trusted and easier to spoof.

Recommendation:

Confirm that HTTP and HTTPS servers remain disabled unless absolutely needed. If web management is required, use HTTPS with a trusted certificate and restrict access:

ip http secure-server

ip http authentication local

ip http access-class 10

If web management isn’t needed, remove unused crypto configurations to reduce attack surface:

no crypto pki trustpoint TP-self-signed-2135278336

No VLAN 1 Security:

Issue: VLAN 1 is shut down (interface Vlan1 ... shutdown), which is good, but there’s no explicit configuration to secure it further or prevent its use on access ports.

Risk: VLAN 1 is the default VLAN and often targeted by attackers. If accidentally enabled, it could be exploited.

Recommendation:

Ensure VLAN 1 is not used for any access ports and explicitly configure unused ports to a dummy VLAN:

vlan 999

name DUMMY

interface range FastEthernet0/13 - 23

switchport mode access

switchport access vlan 999

shutdown

PortFast on Access Ports Without BPDU Guard:

Issue: Access ports (e.g., FastEthernet0/1 to 0/12) have spanning-tree portfast enabled, but there’s no spanning-tree bpduguard enable configured globally or per port.

Risk: PortFast allows immediate transition to forwarding, which is fine for end devices but dangerous if a switch is connected, potentially causing loops. Without BPDU guard, a rogue switch could disrupt the spanning-tree topology.

Recommendation:

Enable BPDU guard globally or per port:

spanning-tree portfast bpduguard default

Or per port:

interface FastEthernet0/1

spanning-tree bpduguard enable

Unused Ports Not Disabled:

Issue: Ports FastEthernet0/13 to 0/23 have no configuration, meaning they’re active and in the default VLAN (typically VLAN 1).

Risk: Unused ports can be exploited by unauthorized devices to gain network access.

Recommendation:

Disable unused ports and place them in a dummy VLAN:

interface range FastEthernet0/13 - 23

switchport mode access

switchport access vlan 999

shutdown

No Logging for Security Events:

Issue: While service timestamps log datetime msec is enabled, there’s no configuration for centralized logging (e.g., to a syslog server) or specific logging levels for security events.

Risk: Without proper logging, unauthorized access attempts or configuration changes may go unnoticed.

Recommendation:

Configure a syslog server and enable logging for security events:

logging host <syslog-server-ip>

logging trap warnings

logging on

No DHCP Snooping or IP Source Guard:

Issue: The switch uses DHCP pools for VLANs 2 and 3, but there’s no DHCP snooping or IP Source Guard configured.

Risk: Rogue DHCP servers could assign malicious IP addresses, and devices could spoof IP addresses, leading to man-in-the-middle attacks.

Recommendation:

Enable DHCP snooping and IP Source Guard:

ip dhcp snooping

ip dhcp snooping vlan 2,3

interface FastEthernet0/1

ip verify source

Weak Self-Signed Certificate:

Issue: The self-signed certificate uses a 1024-bit RSA key (rsakeypair TP-self-signed-2135278336), which is considered weak by modern standards.

Risk: Weak keys are vulnerable to cryptographic attacks, compromising SSH or HTTPS sessions if used.

Recommendation:

Regenerate the RSA key with at least 2048 bits:

crypto key generate rsa general-keys modulus 2048

Summary of Key Actions

Replace enable password with enable secret and use strong passwords.

Enable AAA or local usernames for authentication.

Enforce SSH, disable Telnet, and restrict VTY access.

Disable unused ports and secure VLAN 1.

Enable BPDU guard with PortFast.

Configure DHCP snooping and IP Source Guard.

Set up centralized logging for security events.

If HTTPS is needed, use a stronger certificate; otherwise, remove unused crypto configs.

Implementing these changes will significantly improve the switch’s security posture. Let me know if you’d like a step-by-step guide for any of these recommendations or further analysis!

**Copilot**

Copilot I've reviewed the switch configuration file Catalyst2960\_Switch\_Insecure.txt. Here are some security concerns and recommendations:

Enable Secret and Passwords:

The configuration uses both enable secret and enable password. The enable password is stored in plain text, which is insecure. It's recommended to use only enable secret as it is encrypted. Example:

Service Password-Encryption:

The command no service password-encryption is present, which means passwords are not encrypted in the configuration file. Enabling password encryption is recommended. Recommended command:

AAA New-Model:

The configuration has no aaa new-model, which disables the AAA (Authentication, Authorization, and Accounting) framework. Enabling AAA is recommended for better security management. Recommended command:

Line VTY Passwords:

The VTY lines use a base64 encoded password, which is not secure. It's better to use login local with a properly configured local user database or use AAA. Example:

HTTP Server:

The configuration disables both ip http server and ip http secure-server, which is good practice if HTTP/HTTPS services are not needed. Example:

Spanning Tree Protocol (STP):

The configuration uses spanning-tree mode pvst and spanning-tree extend system-id. Ensure that STP is configured correctly to prevent loops and enhance network stability. Unused Interfaces:

Unused interfaces should be administratively shut down to prevent unauthorized access. Example:

VLAN Configuration:

Ensure that VLANs are properly segmented and that sensitive data is isolated. By addressing these security concerns, you can enhance the overall security of your switch configuration. If you need further assistance or have any specific questions, feel free to ask!

**Sign-in Log Analysis**

**Gemini**

Here's a breakdown of the security concerns in the provided sign-in logs:

* **Inconsistent Authentication Factors:** The logs show a mix of single-factor and multi-factor authentication for the user "Daniel P Yoder". This inconsistency is a security risk, as single-factor authentication is less secure and can be more easily compromised.
* **Location Anomalies:** There are sign-in attempts from various locations, including Youngstown, Canfield, Sarasota, Los Angeles, New York, Hubbard, and Warren. This could indicate that the user's account is being accessed from multiple, potentially unauthorized locations.
* **Failed Authentication Attempts:** There are instances of "Failure" status for authentication, specifically for Office 365 Exchange Online and OfficeHome, both from Sarasota. This could indicate attempts to gain unauthorized access to the account.
* **Single-Factor Authentication:** There are several instances where the user successfully signs in using only single-factor authentication, which is a security vulnerability.

The switch configurations also present several security concerns:

* **Password Encryption:** "Catalyst2960\_Switch\_Insecure.txt" has the no service password-encryption command, meaning passwords are in plain text, a critical vulnerability. "Catalyst2960\_Switch\_clean1.txt" has service password-encryption, which is more secure.
* **Enable Password:** Both configurations have a weak enable password ("123456"), posing a security risk.
* **DHCP Snooping:** "Catalyst2960\_Switch\_clean1.txt" has DHCP snooping enabled, which is a positive security measure. "Catalyst2960\_Switch\_Insecure.txt" does not have DHCP snooping configured.
* **Unused Ports:** "Catalyst2960\_Switch\_clean1.txt" has several interfaces shut down, which is good security practice. "Catalyst2960\_Switch\_Insecure.txt" does not show ports being shut down.

**ChatGPT**

It seems like I can’t do more advanced data analysis right now. Please try again later.

If you'd like, I can guide you on how to analyze the sign-in logs manually or help you extract suspicious patterns using Excel filters. Just let me know how you'd like to proceed!

**Grok 3**

Analyzing the provided sign-in logs for the user Daniel P. Yoder ([dpyoder@ysu.edu](mailto:dpyoder@ysu.edu)), several potential threat patterns and anomalies emerge that warrant further investigation. Below is a detailed review of the logs, focusing on patterns that could indicate security risks, followed by recommendations for mitigation.

### **Observations and Potential Threat Patterns**

1. **Geographical Anomalies and Rapid Location Changes**:
   1. **Details**:
      1. On 3/28/2025, within a 26-second window (9:15:23 AM to 9:15:49 AM), the user successfully signed in from three different locations: Sarasota, Florida (9:15:23 AM, Windows Sign In), Canfield, Ohio (9:15:26 AM, M365ChatClient), and Youngstown, Ohio (multiple sign-ins starting 9:15:32 AM).
      2. On 3/27/2025, sign-ins occurred from Los Angeles, California (9:12:56 AM, failed), New York, New York (8:14:25 AM, success), and Youngstown, Ohio (multiple times throughout the day).
   2. **Risk**:
      1. Rapid changes in location within short timeframes (e.g., Florida to Ohio in seconds) are physically implausible, suggesting possible account compromise, session hijacking, or VPN/proxy usage to mask the true location.
      2. The failed attempt from Los Angeles and successful sign-in from New York on 3/27/2025 could indicate brute-force attempts or unauthorized access from unfamiliar locations.
   3. **Analysis**:
      1. The Sarasota to Ohio jump on 3/28/2025 is particularly suspicious, as it occurs across multiple applications in under 30 seconds.
      2. New York and Los Angeles are outliers compared to the user’s typical locations (Youngstown, Warren, Hubbard, Canfield—all in Ohio).
      3. The lack of IP addresses in the logs makes it harder to confirm if these are distinct devices or sessions, but the location data alone raises red flags.
2. **Single-Factor Authentication Usage**:
   1. **Details**:
      1. Several successful sign-ins used single-factor authentication (SFA):
         1. 3/28/2025, 9:15:23 AM (Sarasota, Florida, Windows Sign In).
         2. 3/27/2025, 9:14:57 AM (Youngstown, Ohio, Windows Sign In).
         3. 3/27/2025, 8:14:25 AM (New York, New York, Windows Sign In).
         4. 3/26/2025, 3:14:54 PM (Youngstown, Ohio, Windows Sign In).
   2. **Risk**:
      1. SFA is less secure than multifactor authentication (MFA), which is used in most other sign-ins. Successful SFA from unusual locations (Sarasota, New York) could indicate a bypass of stronger security controls, possibly due to misconfigured conditional access policies or legacy authentication methods.
      2. Attackers often exploit SFA-enabled accounts for initial access.
   3. **Analysis**:
      1. The use of SFA for Windows Sign In, especially from Sarasota and New York, contrasts with MFA for cloud-based services like Exchange and SharePoint, suggesting inconsistent application of security policies.
      2. The conditional access status is marked as “Success” even for SFA sign-ins, which may indicate a policy allowing SFA under certain conditions (e.g., trusted locations or devices), but this is risky for remote locations.
3. **Failed Sign-In Attempts**:
   1. **Details**:
      1. Two failed sign-ins were recorded:
         1. 3/27/2025, 9:12:56 AM (Los Angeles, California, Office 365 Exchange Online, MFA).
         2. 3/25/2025, 9:14:45 AM (Sarasota, Florida, OfficeHome, MFA).
   2. **Risk**:
      1. Failed attempts from unusual locations (Los Angeles, Sarasota) could indicate unauthorized access attempts, such as password guessing or credential stuffing.
      2. The Los Angeles failure followed by a successful New York sign-in (8:14:25 AM, ~1 hour earlier) on the same day suggests potential probing from multiple locations.
   3. **Analysis**:
      1. Both failures required MFA, suggesting the attacker may have had partial credentials but failed the second factor. This could indicate a targeted attack on the user’s account.
      2. The absence of IP addresses limits correlation with other sign-ins, but the geographical outliers align with suspicious patterns.
4. **High-Frequency Sign-Ins Within Short Timeframes**:
   1. **Details**:
      1. On 3/28/2025, between 9:15:23 AM and 9:15:49 AM, there were seven successful sign-ins across multiple applications (Exchange, M365ChatClient, SharePoint, Shell WCSS-Client) in 26 seconds.
      2. Similar patterns appear on other days, such as 3/27/2025 and 3/26/2025, with multiple Exchange sign-ins in close succession.
   2. **Risk**:
      1. Rapid, automated sign-ins across multiple services could indicate scripted activity, possibly from a compromised account or bot-like behavior.
      2. Alternatively, this could reflect legitimate single sign-on (SSO) behavior, but the frequency and location anomalies (e.g., 3/28/2025) raise concerns.
   3. **Analysis**:
      1. The 3/28/2025 burst includes a location change (Sarasota to Canfield to Youngstown), making automated or malicious activity more likely than normal SSO.
      2. Without device or session IDs, it’s unclear if these are from the same device, but the pattern warrants scrutiny.
5. **Inconsistent Application Usage**:
   1. **Details**:
      1. The logs show access to a variety of applications (Exchange, SharePoint, M365ChatClient, Bing, OfficeHome, Windows Sign In, etc.), with some less common ones like “Office365 Shell WCSS-Client” and “SharePoint Online Web Client Extensibility.”
      2. The Bing sign-in on 3/27/2025 (1:15:20 PM) stands out as unusual compared to the predominantly Office 365-focused activity.
   2. **Risk**:
      1. Access to unexpected applications (e.g., Bing, Shell WCSS-Client) could indicate unauthorized exploration of services available to the account, a common tactic post-compromise.
      2. Shell WCSS-Client suggests possible administrative or PowerShell activity, which is high-risk if unauthorized.
   3. **Analysis**:
      1. The Bing sign-in may be benign (e.g., browser integration), but its singularity in the logs is notable.
      2. Shell WCSS-Client access (3/28/2025, 9:15:34 AM) from Youngstown is less concerning given MFA, but should be verified as legitimate, especially given the rapid sign-in burst.

### **Potential Threat Scenarios**

Based on the patterns, the following scenarios are possible:

* **Account Compromise**: The geographical anomalies (Sarasota, New York, Los Angeles) and failed sign-ins suggest an attacker may have partial credentials and is attempting access from various locations, possibly using stolen passwords or session tokens.
* **Policy Misconfiguration**: The use of SFA from unusual locations (Sarasota, New York) indicates potential gaps in conditional access policies, allowing weaker authentication methods for certain scenarios (e.g., Windows Sign In).
* **Automated Attack**: The rapid sign-in burst on 3/28/2025, combined with location changes, could reflect automated scripts testing credentials or exploiting SSO sessions.
* **Legitimate but Risky Behavior**: The user may be traveling (e.g., Sarasota) or using a VPN, but the lack of IP correlation and SFA usage still poses risks if not tightly controlled.

### **Recommendations**

1. **Investigate Suspicious Sign-Ins**:
   1. **Action**: Review detailed logs (including IP addresses, device IDs, and user agents) for the following:
      1. 3/28/2025, 9:15:23 AM (Sarasota), 9:15:26 AM (Canfield), and 9:15:32–9:15:49 AM (Youngstown) to confirm if these are from the same device or session.
      2. 3/27/2025, 8:14:25 AM (New York) and 9:12:56 AM (Los Angeles, failed) to check for signs of compromise.
      3. 3/25/2025, 9:14:45 AM (Sarasota, failed) for correlation with the 3/28/2025 Sarasota sign-in.
   2. **Tool**: Use Microsoft Entra ID Sign-In Logs or a SIEM system to correlate events.
   3. **Contact User**: Verify with Daniel P. Yoder whether they were physically in Sarasota, New York, or Los Angeles, or using a VPN during these times.
2. **Enforce Consistent MFA**:
   1. **Action**: Update conditional access policies to require MFA for all sign-ins, especially for Windows Sign In and external locations. Example policy in Entra ID:
      1. Condition: All locations, exclude trusted IPs (if applicable).
      2. Grant: Require MFA.
   2. **Action**: Disable legacy authentication protocols (e.g., POP3, IMAP) that may bypass MFA:

plaintext

CollapseWrapCopy

Set Entra ID Security Defaults to block legacy authentication.

* 1. **Verify**: Ensure “Conditional Access applied? Success” for SFA sign-ins isn’t a policy loophole.

1. **Implement Location-Based Restrictions**:
   1. **Action**: Configure a conditional access policy to block or challenge sign-ins from unusual locations (e.g., outside Ohio, unless verified as legitimate travel). Example:
      1. Condition: Locations exclude Ohio.
      2. Grant: Block or require MFA + device compliance.
   2. **Action**: Monitor for VPN usage and ensure it aligns with organizational policy.
2. **Analyze Failed Sign-In Root Causes**:
   1. **Action**: Check Entra ID logs for the failure reasons (e.g., incorrect password, MFA failure) for 3/27/2025 (Los Angeles) and 3/25/2025 (Sarasota).
   2. **Action**: Enable alerts for multiple failed sign-ins within a short timeframe to detect brute-force attempts.
3. **Review Application Access**:
   1. **Action**: Verify the legitimacy of access to “Office365 Shell WCSS-Client” (3/28/2025) and “Bing” (3/27/2025). Confirm if the user has a role requiring PowerShell or if Bing access is expected.
   2. **Action**: Restrict high-risk applications (e.g., PowerShell) to specific roles or devices via conditional access.
4. **Enhance Monitoring and Alerts**:
   1. **Action**: Set up real-time alerts in Entra ID or a SIEM for:
      1. Sign-ins from multiple locations within a short timeframe (e.g., <5 minutes).
      2. Successful SFA from non-trusted locations.
      3. Failed sign-ins followed by successful sign-ins from different locations.
   2. **Action**: Enable Impossible Travel alerts in Microsoft Defender for Identity or Entra ID Identity Protection.
5. **User Education**:
   1. **Action**: Train the user on recognizing phishing attempts and securing their account, especially given the failed sign-ins and SFA usage.
   2. **Action**: Advise against using unverified devices or networks for sign-ins, particularly in unusual locations.

### **Additional Notes**

* **Missing IP Addresses**: The absence of IP addresses in the logs limits deeper analysis (e.g., correlating sessions or detecting proxies). Ensure logs capture IPs, device IDs, and user agents for future investigations.
* **Context with Switch Configuration**: Since you previously shared a switch configuration, I assume this is part of a broader network review. The switch’s security issues (e.g., plaintext passwords, lack of DHCP snooping) could indirectly contribute to risks if credentials are intercepted locally, but the logs here point more to cloud-based threats (e.g., credential theft or policy gaps).

### **Conclusion**

The logs show concerning patterns, particularly the rapid location changes on 3/28/2025, SFA usage from unusual locations (Sarasota, New York), and failed sign-ins from Los Angeles and Sarasota. These suggest potential account compromise or policy misconfigurations. Immediate actions should include investigating the suspicious sign-ins, enforcing MFA universally, and tightening conditional access policies. Monitoring and user verification will be critical to confirm whether this is malicious activity or legitimate but risky behavior.

If you have additional logs (e.g., with IPs or failure details) or want guidance on implementing specific Entra ID policies, let me know!

**Copilot**

I've reviewed the sign-in logs from the file Sign-in\_Logs\_Suspect.xlsx. Here are some observations and potential threat patterns:

Multiple Locations in a Short Time Frame:

On 3/28/2025, there are sign-ins from Youngstown, Ohio, Canfield, Ohio, and Sarasota, Florida within a very short time frame. This could indicate a potential account compromise or the use of a VPN. Example: 9:15:26 AM from Canfield, Ohio 9:15:23 AM from Sarasota, Florida 9:15:49 AM from Youngstown, Ohio Failed Sign-In Attempts:

There are failed sign-in attempts from locations that are not consistent with the usual sign-in locations. Example: 3/27/2025, 9:12:56 AM from Los Angeles, California (Failure) 3/25/2025, 9:14:45 AM from Sarasota, Florida (Failure) Single-Factor Authentication:

Some sign-ins are using single-factor authentication, which is less secure compared to multifactor authentication. Example: 3/28/2025, 9:15:23 AM from Sarasota, Florida (Single-factor authentication) 3/27/2025, 9:14:57 AM from Youngstown, Ohio (Single-factor authentication) 3/27/2025, 8:14:25 AM from New York, New York (Single-factor authentication) Unusual Locations:

Sign-ins from locations that are not typical for the user, such as New York, New York, and Los Angeles, California. Example: 3/27/2025, 8:14:25 AM from New York, New York 3/27/2025, 9:12:56 AM from Los Angeles, California Recommendations: Investigate the unusual sign-ins from different locations within a short time frame to determine if they are legitimate or if the account has been compromised. Review the failed sign-in attempts to ensure they are not part of a brute force attack or unauthorized access attempts. Enforce multifactor authentication for all sign-ins to enhance security. Monitor for any further unusual activity and consider implementing additional security measures such as IP whitelisting or geofencing. If you need further assistance or have any specific questions, feel free to ask!