AdminDroid

AdminDroid 365

Microsoft 365 & Active Directory Management Tool

How AdminDroid Helps Detect Storm-2949 Attacks Early In Microsoft 365

AdminDroid 365

Microsoft 365 & Active Directory Management Tool

Detecting Storm-2949 Attacks with AdminDroid

Storm-2949 can move from a single identity compromise to organization-wide impact within hours, and most of its activity blends into normal cloud usage. This guide covers the early signals admins can monitor in AdminDroid, the real-time alerts to enable for faster detection, and the hardening configurations that reduce overall exposure

STORM-2949 ATTACK OVERVIEW

WHAT ADMINDROID DETECTS

REAL-TIME ALERTS TO ENABLE

HARDENING RECOMMENDATIONS

WHERE TO START

STORM-2949 ATTACK OVERVIEW

Storm-2949 is an emerging threat campaign tracked under Microsoft's storm-naming convention. It targets Microsoft 365 and Azure environments.

What Attackers Do

A Storm-2949 intrusion typically unfolds in six phases:

1. **Compromise an identity:** abuse Self-Service Password Reset combined with social engineering to seize a user account
2. **Hijack MFA:** register attacker-controlled devices as new MFA methods, locking out the legitimate user
3. **Map the organization:** enumerate users, groups, roles, and resources via Microsoft Graph.
4. **Exfiltrate data:** bulk-download from SharePoint, OneDrive, Azure Storage, and Azure SQL
5. **Steal cloud credentials:** extract App Service publishing profiles, Azure Key Vault secrets, and managed-identity tokens
6. **Establish persistence:** add service principal secrets, backdoor VMs via the VMAccess extension, and deploy remote-access tools.

For the full 13-step attack walkthrough, see Storm-2949 Cloud Heist.

Why it's Hard to Detect

- **Identity-focused compromise:** a single account takeover can escalate to broad Microsoft 365 and Azure access
- **Legitimate-service abuse:** attackers use built-in Microsoft cloud services rather than deploying malware
- **Disk-less operation:** no local files are written, limiting antivirus and EDR detection.
- **Behavioral blending:** activities mimic legitimate Microsoft 365 user activities, masking the attack chain

Storm-2949 leaves little evidence on endpoints because it primarily abuses legitimate cloud services and identities. This shifts detection toward Microsoft 365 audit visibility rather than traditional endpoint monitoring.

Once attackers reach Key Vaults, privileged RBAC roles, or large-scale data exfiltration, the impact increases significantly. Detecting suspicious identity activity early remains the most effective way to contain the attack before it spreads.

AdminDroid centralizes these audit signals in a single console, helping admins investigate suspicious activity faster without switching between multiple Microsoft 365 portals.

WHAT ADMINDROID DETECTS

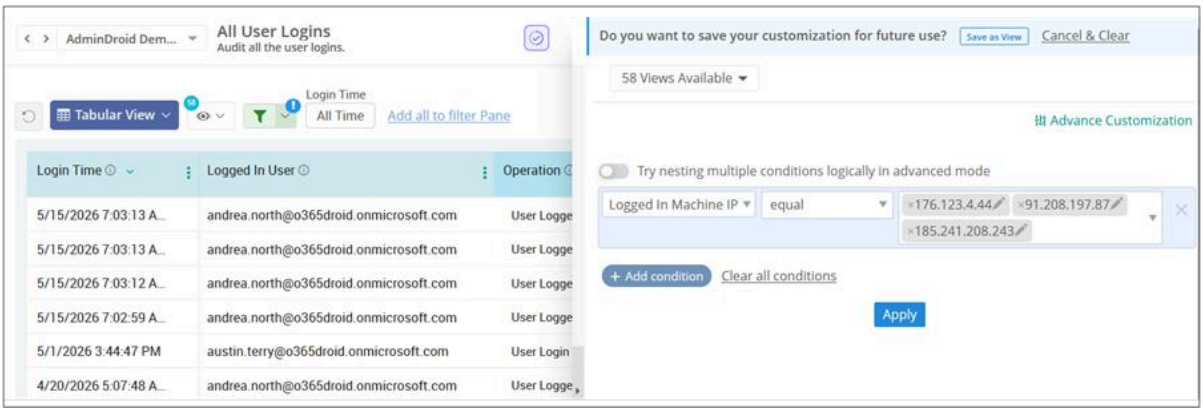
Storm-2949 can move from a single identity compromise to organization-wide impact within hours, and most of its activity blends into normal cloud usage. This guide covers the early signals admins can monitor in AdminDroid, the real-time alerts to enable for faster detection, and the hardening configurations that reduce overall exposure

Risky Sign-Ins

Sign-in analysis is the fastest entry point for Storm-2949 threat hunting. Microsoft has published three IP addresses associated with the campaign:

- 176.123.4.44
- 91.208.197.87
- 185.241.208.243

Open the All user logins report in AdminDroid and filter the Logged-In Machine IP field on these addresses. Investigate any matched accounts immediately.



IOC matching is necessary but not sufficient. Attacker infrastructure changes, so admins should continuously Monitor risky sign-in patterns such as:

- Impossible travel activities
- Password spray attempts
- Leaked credential detections
- Sign-ins from unfamiliar locations
- New browser or device combinations

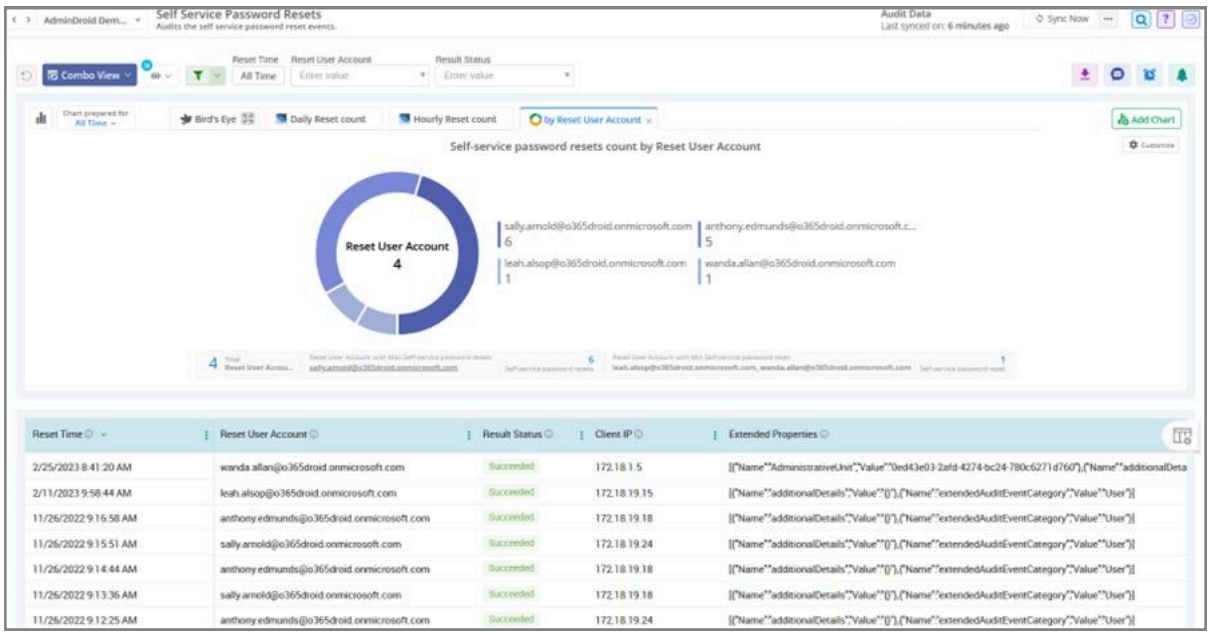
For deeper investigation of any flagged sign-in, the Detailed sign-in report adds device, browser, authentication protocol, and behavior pattern context.
Sign-in activity is the earliest visible indicator of Storm-2949. Early detection at this stage prevents the compromise from expanding across Microsoft 365.

Self-Service Password Reset (SSPR) Abuse

Storm-2949 abuses self-service password reset workflows for initial account takeover, often combined with MFA fatigue or social engineering. The signal to watch for is reset behavior that doesn't match the user's normal pattern.

Open the Self-service password reset activities report in AdminDroid and look for:

- Multiple reset attempts on the same account within a short window
- Resets from unfamiliar IPs or geographic locations
- Failed resets followed by a successful one on the same account



For any suspicious SSPR activity, cross-reference the user's sign-in history to confirm whether the attempt succeeded.
SSPR-stage detection stops the attack before valid credentials are established in the organization.

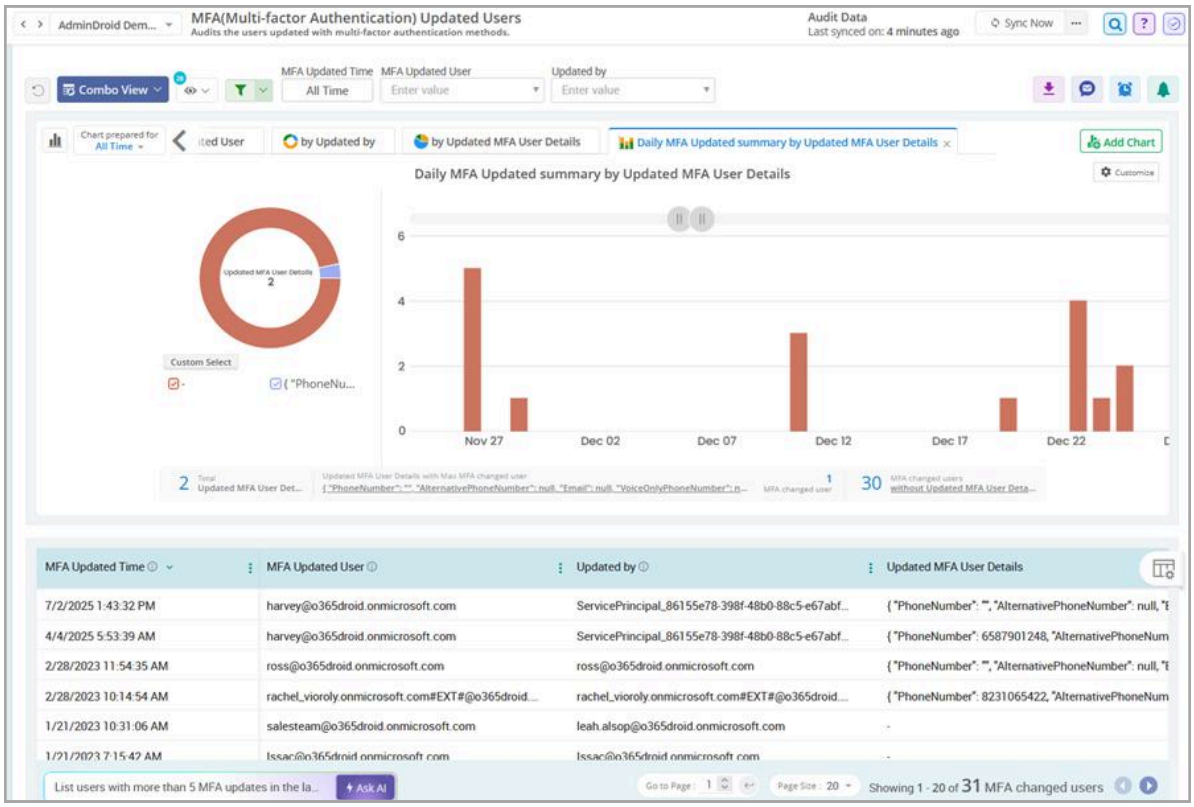
MFA Tampering

After gaining valid credentials, Storm-2949 registers attacker-controlled MFA methods to lock out the legitimate user. A risky sign-in followed shortly by an MFA configuration change for the same user is the highest-confidence account takeover signal AdminDroid surfaces.

Open the MFA updated users report in AdminDroid and watch for:

- New MFA method registrations
- MFA method removals
- Microsoft Authenticator re-registrations
- Phone-number modifications

For any flagged MFA change, open the All user logins report for the same user and time window. A risky sign-in within the prior hour materially raises confidence that the change is an attacker action.



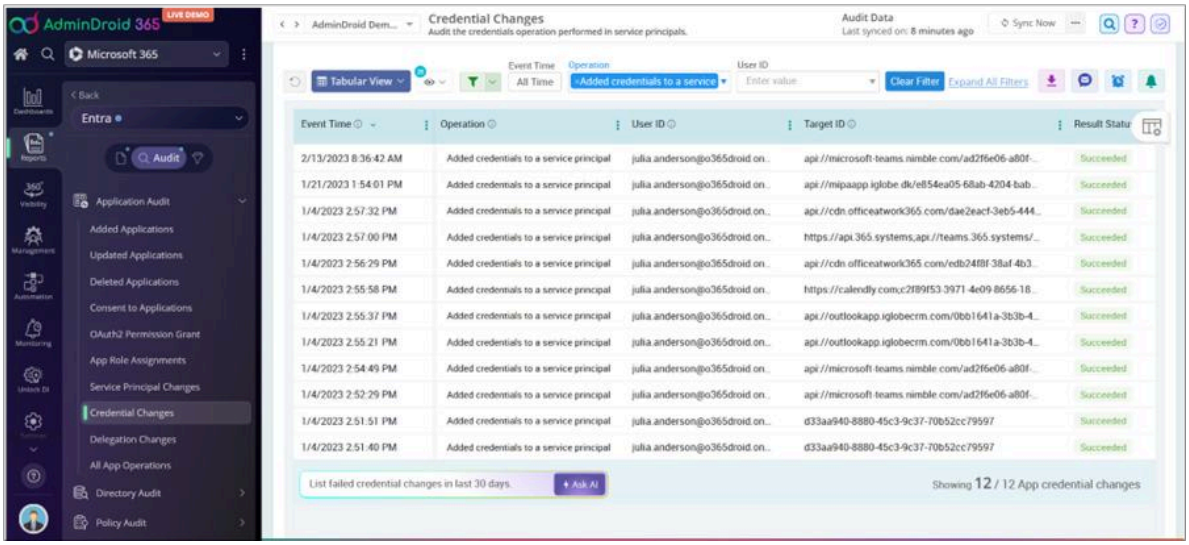
MFA tampering shifts an account from potentially compromised to actively under attacker control.

Service Principal Credential Changes

Adding credentials to a service principal is one of Storm-2949's key persistence mechanisms. Service principals retain access even after passwords are reset or sessions revoked, so a single successful client secret or certificate addition can give attackers long-term background access for weeks. In Microsoft's documented case, the credential addition attempt failed due to insufficient permissions. However, failed attempts remain valuable signals because the audit events remain available for investigation.

Open the Credential changes report in AdminDroid and watch for:

- New client secret additions
- Certificate additions



For broader service principal coverage, AdminDroid also surfaces:

- Service principal property changes
- Delegation changes
- Ownership modifications

For any flagged change, validate the actor against known tickets or approved tasks. Investigate failed attempts as carefully as successful ones. They still reveal attacker activity in the organization.

Service principal monitoring closes the persistence loop. Without it, password resets alone won't remediate the attack.

SharePoint and OneDrive Data Exfiltration

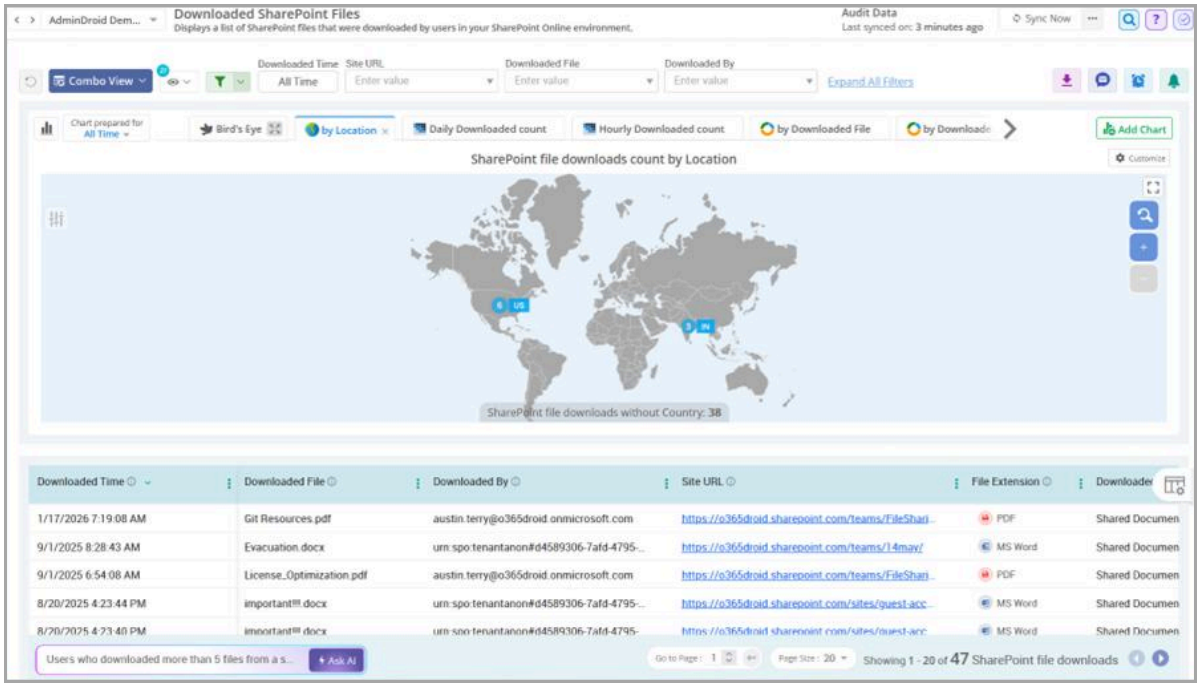
Once attackers have reconnaissance and access, Storm-2949 shifts to SharePoint and OneDrive data exfiltration. The campaign has specifically targeted IT documentation such as VPN configurations and remote-access procedures.

Open SharePoint and OneDrive activity reports in AdminDroid and watch for:

- Large-volume file downloads from a single account
- Mass sharing events across many documents
- External sharing policy changes
- Guest access additions to sensitive sites

Open SharePoint and OneDrive activity reports in AdminDroid and watch for:

- Large-volume file downloads from a single account
- Mass sharing events across many documents
- External sharing policy changes
- Guest access additions to sensitive sites



For any flagged signal, identify the document scope and destination before scoping the response. Detection at this stage limits further data loss and triggers containment.

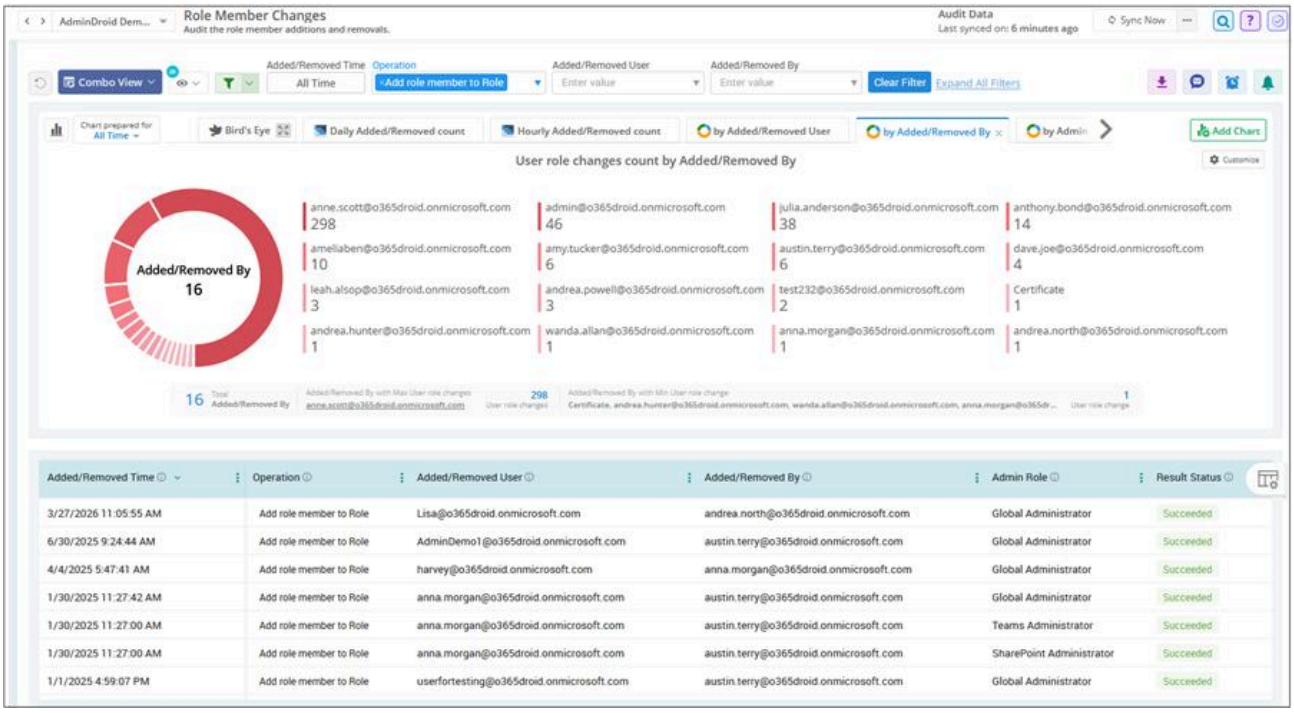
Privilege Escalation

Privilege escalation is the point where Storm-2949 moves from individual account compromise to broader cloud control.

While attackers may attempt broader Azure RBAC abuse, privileged Microsoft 365 administrative role changes are also critical indicators of escalation activity and should be continuously monitored.

Open the User added to admin role report and the PIM role activation report in AdminDroid and watch for:

- New Global Administrator assignments
- Assignments to other highly-privileged roles (Privileged Role Administrator, Security Administrator, User Administrator)
- Unexpected PIM role activations
- Sudden role assignments outside approved change windows



For any new privileged role assignment, validate it against an approval or change ticket. Unexplained escalation at this stage almost always indicates compromise.

Privilege escalation expands the compromise from one account to the organization. Early detection limits how far the compromise can spread.

REAL-TIME ALERTS TO ENABLE

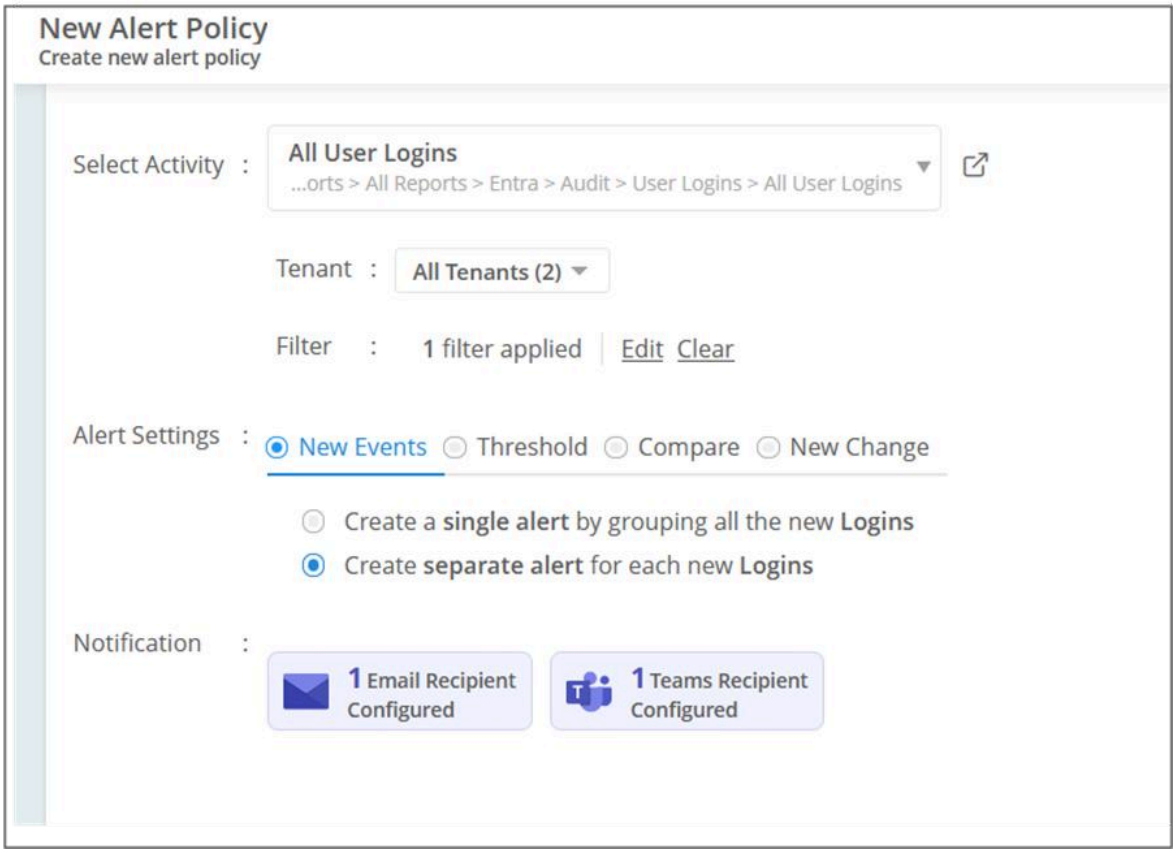
Detecting Storm-2949 through reports is important, but real-time alerting enables security teams to respond before the attack progresses further. The following AdminDroid alert policies help organizations provide continuous monitoring for high-risk Storm-2949 activities.

Sign-ins from Storm-2949 IOC IP Addresses

Create an alert policy on the All user sign-in report to fire when any user signs in from a Storm-2949 IOC IP address.

Configure:

1. Navigate to **Monitoring → Alerts → Policies** and click **Add New alert policy.**
2. Select the All user logins report as the source report.
3. Click **Filter** to filter by property value, choose the Logged-In Machine IP field, and add the three IOC addresses: 176.123.4.44, 91.208.197.87, and 185.241.208.243.
4. Under **Alert Settings,** choose New Events and select Create separate alert for each new Logins.
5. Assign notification recipients and save the policy.



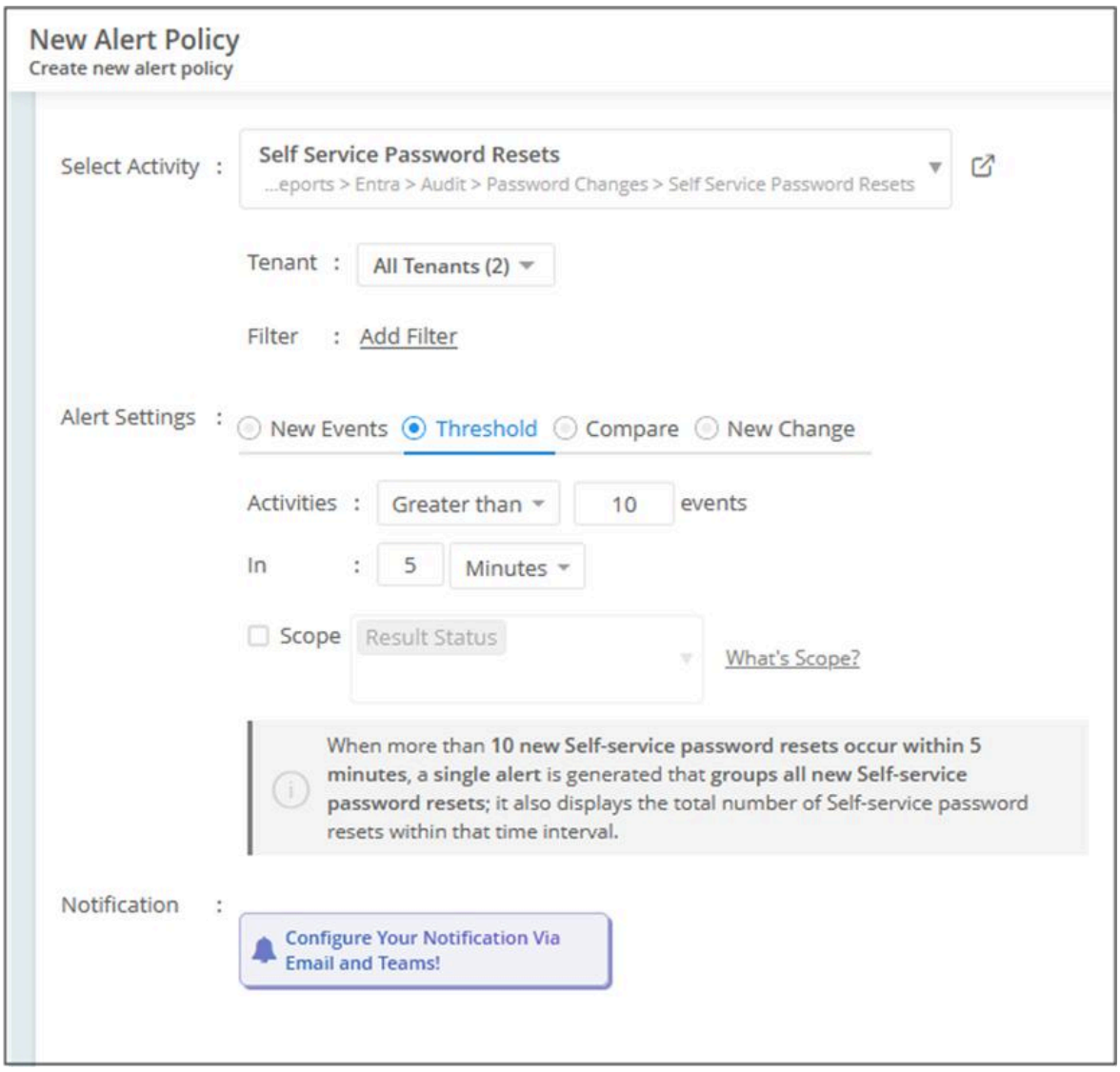
Suspicious SSPR Activity

Create an alert policy on the Self Service Password Resets report to detect SSPR volume spikes. These bursts typically indicate MFA fatigue attacks or attacker-driven bulk reset attempts.

Configure:

1. Create an alert policy with Self Service Password Resets as the source report.
2. Under **Alert Settings,** choose Threshold, set **Activities** to Greater than 10 events, and set in to 5 Minutes.
3. Assign notification recipients and save the policy.

Tune the threshold values to match your organization's baseline SSPR volume.



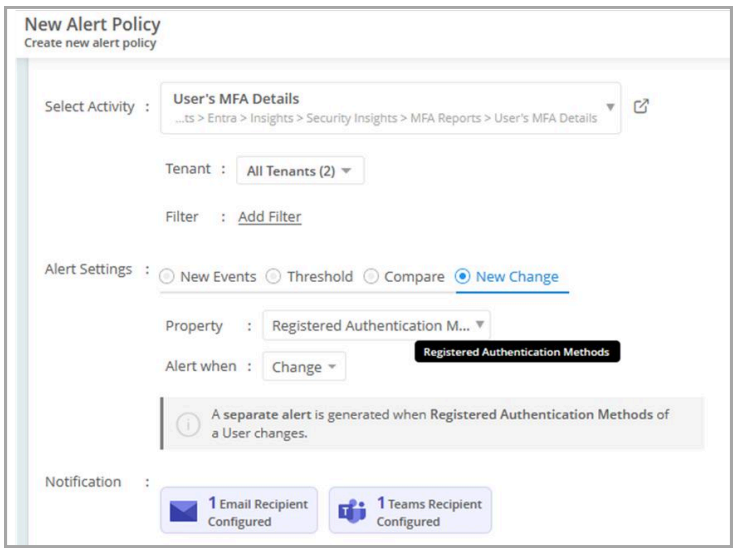
MFA Method Changes

Create an alert policy on the User's MFA Details report to fire when a user's registered MFA methods change. This single alert automatically covers MFA method additions and removals.

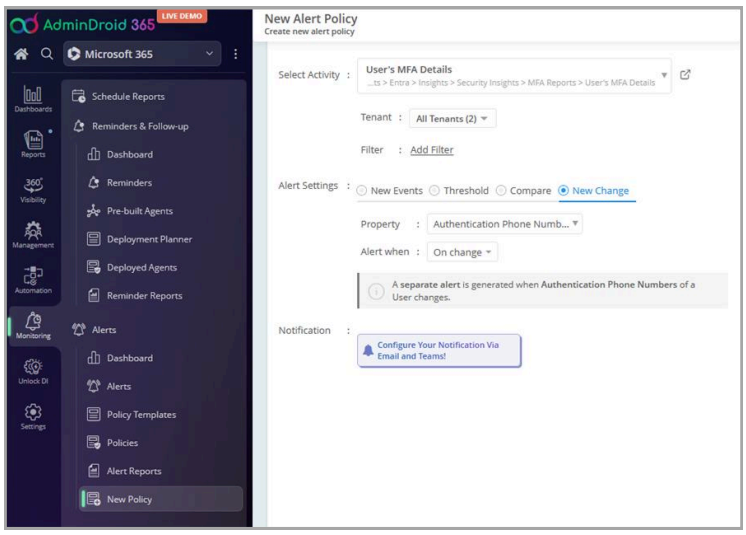
Configure:

1. Create an alert policy with User's MFA Details as the source report.
2. Under **Alert Settings**, choose New Change, set **Property** to Registered Authentication Methods, and set **Alert when** to Change.
3. Assign notification recipients and save the policy.

Tune the threshold values to match your organization's baseline SSPR volume.



To track Authentication Phone Number changes, create a separate alert policy on the same report with the **Authentication Phone Number** property selected.



Service Principal Credential Changes

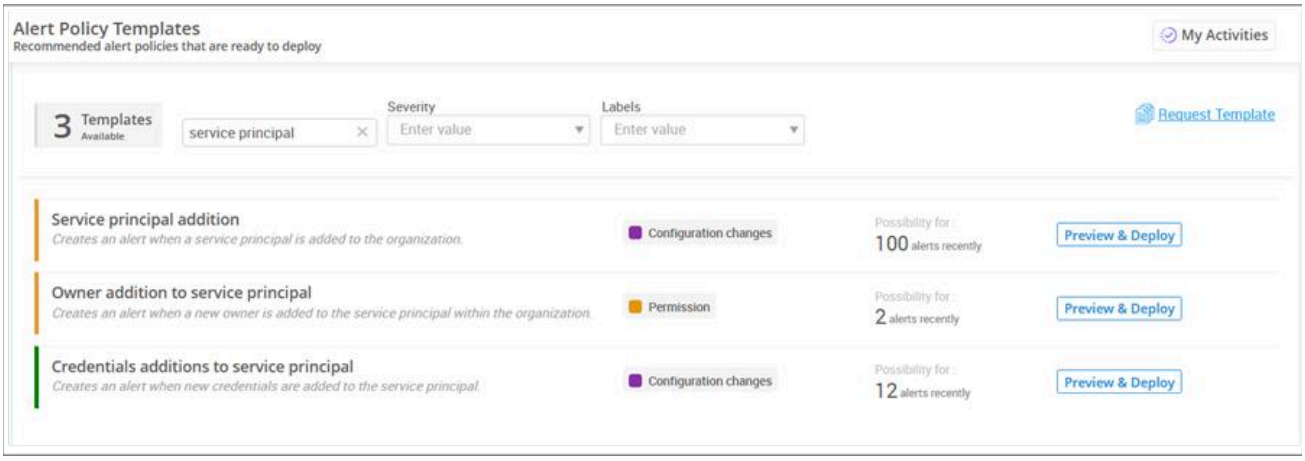
Deploy the pre-built alert policy template **Credentials additions to service principal** to detect when new client secrets or certificates are added to an existing service principal. This is the primary Storm-2949 persistence signal.

Configure:

1. Open the **Alert Policy Templates** catalog and search for Credentials additions to service principal.
2. Select the template and click **Preview & Deploy.**
3. Assign notification recipients and save the policy.

For broader service principal coverage, also deploy:

- **Service principal addition:** alerts when a new service principal is added to the organization
- **Owner addition to service principal:** alerts when a new owner is added to an existing service principal.

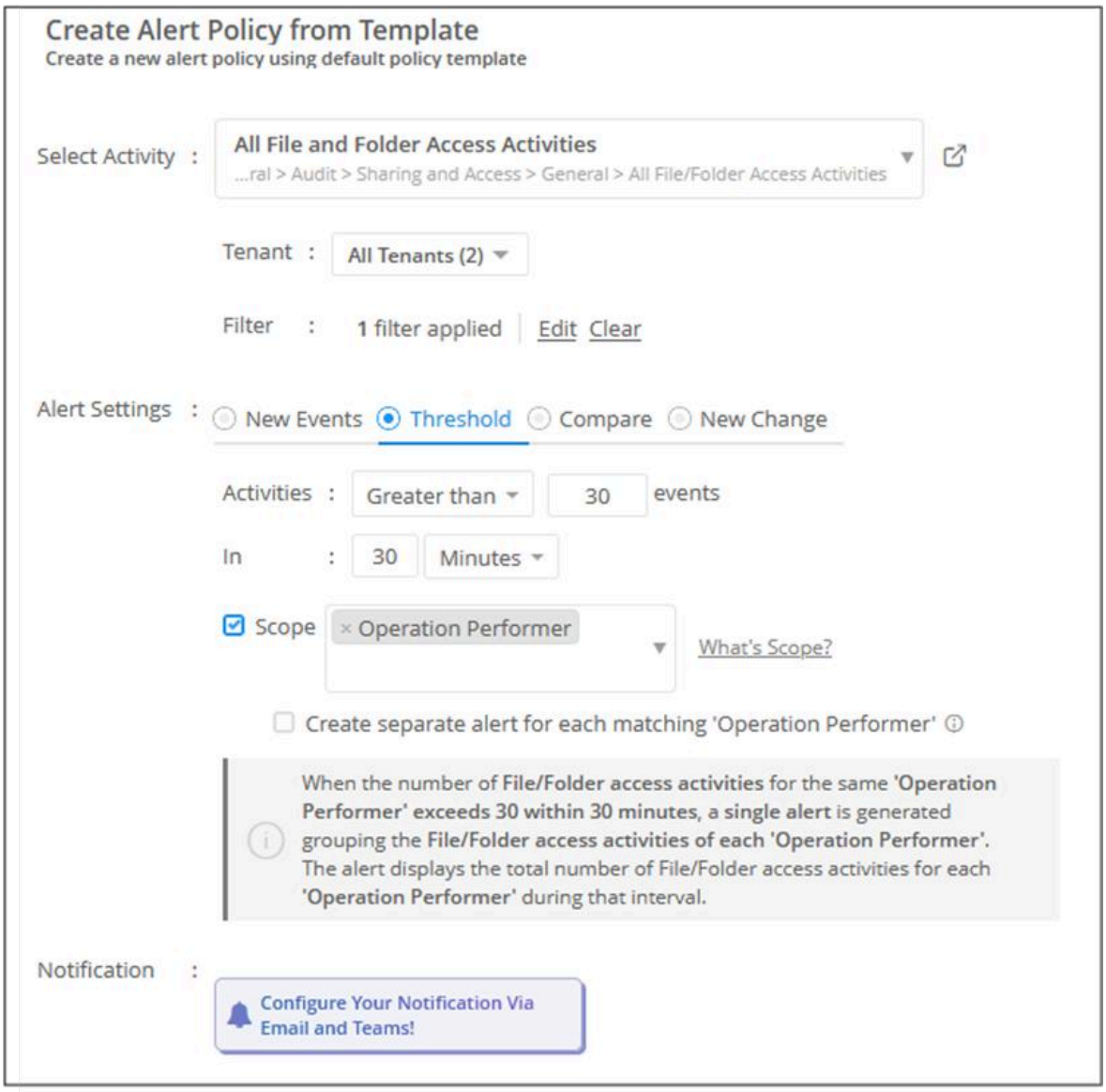


Bulk SharePoint and OneDrive Downloads

Deploy the pre-built alert policy template **Unusual volume of file downloading activities** to detect when a single user downloads an unusually high number of files from SharePoint or OneDrive. This is Storm-2949's primary data exfiltration channel

Configure:

1. Open the **Alert Policy Templates** catalog and search for Unusual volume of file downloading activities.
2. Select the template and click **Preview & Deploy.** The template comes pre-configured with the filter **Operation** equal to Downloaded file.
3. Tune the default threshold (Greater than 30 events in 30 Minutes) to match your organization's baseline.
4. Assign notification recipients and save the policy.

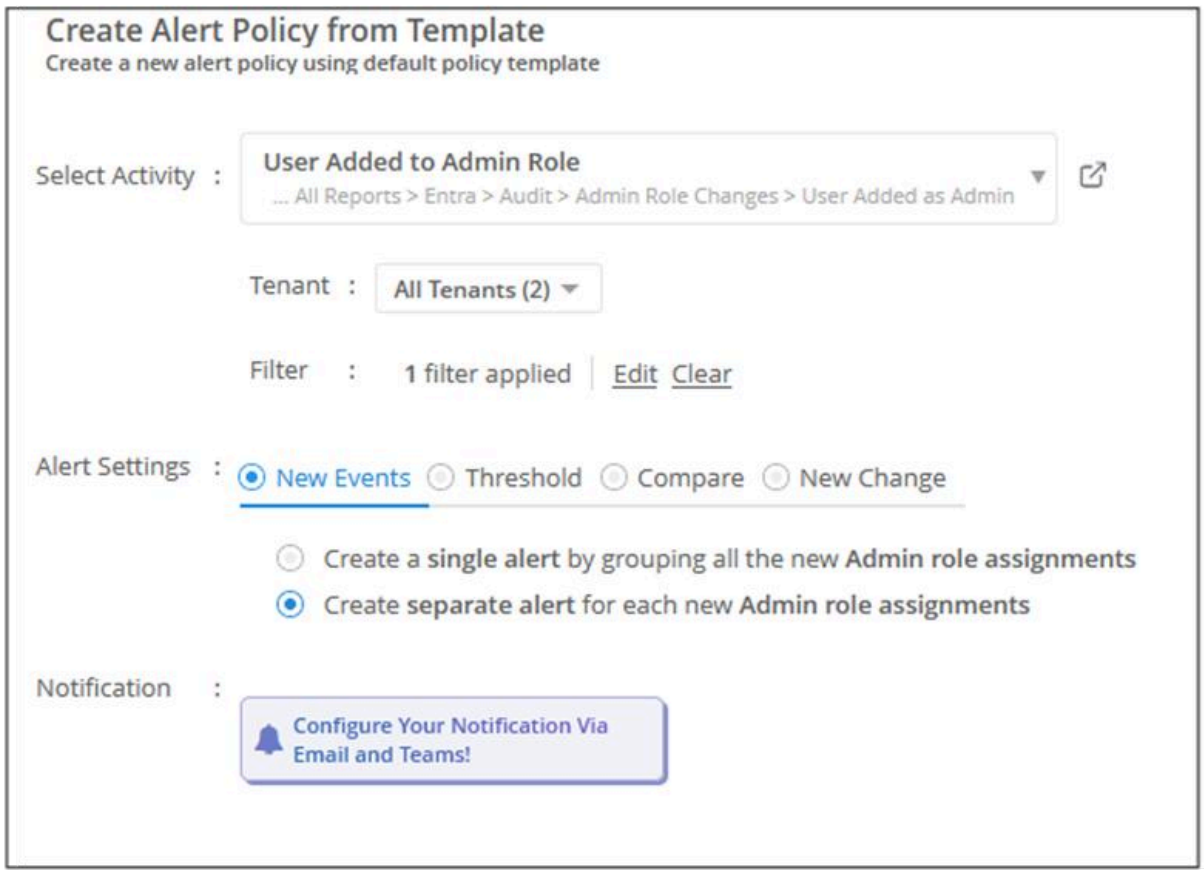


Privileged Role Escalations

Deploy the pre-built alert policy template **Elevation of administrative privilege** to detect when an account is promoted to a privileged role. This is the earliest signal that a Storm-2949 attacker has expanded beyond a single compromised account.

Configure:

1. Open the **Alert Policy Templates** catalog and search for Elevation of administrative privilege.
2. Select the template and click **Preview & Deploy.**
3. (Optional) Apply a filter on the **Added role** field to scope alerts to specific roles (such as Global Administrator only).
4. Assign notification recipients and save the policy.



HARDENING RECOMMENDATIONS

Strengthen Identity Security

- Enforce phishing-resistant MFA (FIDO2 keys, Windows Hello, certificate-based authentication) for all administrators
- Ensure MFA is enabled for all users, not just administrators
- Implement CA policy to prevent attacker registering MFA for user account
- Configure **Conditional Access authentication strength** policies for privileged operations
- Enable Microsoft Entra ID Protection risk-based policies for sign-in and user risk
- Monitor Microsoft Graph API activity for unusual enumeration of users, groups, and directory objects, and restrict Graph API access for non-admin users to prevent reconnaissance enumeration.
- Continuously monitor risky sign-ins using the Risky sign-in patterns report
- **Restrict or disable SSPR** for highly privileged accounts; require admin-initiated resets instead

Reduce Exposure to Data Exfiltration and Cloud Resource Abuse

- Disable **legacy authentication** protocols across the organization
- Restrict **VM extension deployment** to approved publishers; audit **VMAccess** and **Azure Run Command** usage and alert on executions outside change windows
- Limit **Contributor and Owner** role permanence by enforcing PIM with approval workflows
- Review service principal permissions quarterly; remove unused secrets and certificates
- Enforce **managed identity** usage in Azure App Service and restrict access to publishing credentials
- Enable **purge protection** and **soft delete** on all Azure Key Vaults; retain Key Vault logs for at least one year
- Adopt **Azure RBAC** for Key Vaults instead of legacy access policies
- Use **private endpoints** for Key Vaults, Storage Accounts, and SQL; disable public network access where possible
- Restrict **SQL firewall rules** to known address ranges; prefer Entra authentication over SQL authentication
- Disable **anonymous access** on storage containers; review SAS token issuance regularly
- Enable **immutable storage** and configure **blob backups** to protect against malicious deletion
- Enable **Azure VM Backup** to recover from VM extension abuse or backdoor scenarios
- For SharePoint/OneDrive: monitor bulk downloads, restrict unmanaged-device access, review external sharing settings, and apply sensitivity labels to documents.

WHERE TO START

If you suspect Storm-2949 activity or want baseline coverage today, follow these threee steps in order:

1. **Validate sign-ins first.** Open the AdminDroid All user login report and search for the published Storm-2949 IOC IPs: 176.123.4.44, 91.208.197.87, 185.241.208.243.
2. **Enable the six alerts** listed in the Real-time Alerts to Enable section above. They cover the highest-signal indicators of Storm-2949 activity.
3. **Apply the two hardening pillars.** Start with identity, since Storm-2949 always begins with identity compromise. Then address the data and resource exposure gaps.

Storm-2949 succeeds when suspicious identity activity goes unnoticed while attackers expand further into the environment. The earlier those signals are detected, the smaller the overall attack impact becomes.

Need help implementing these recommendations? Contact AdminDroid support at support@admindroid.com for guidance on configuring hardening steps in your environment.