

(ISC)² | SECURITY CONGRESS

EMPOWER

a Safer, More Secure Cyber World

Congress.isc2.org | [#ISC2Congress](https://twitter.com/ISC2Congress)

Emerging threats against cloud application identities and what you should do about it

Etan Basseri

Bailey Bercik

North Star

Prevent unauthorized access to a resource by an application or service

Agenda

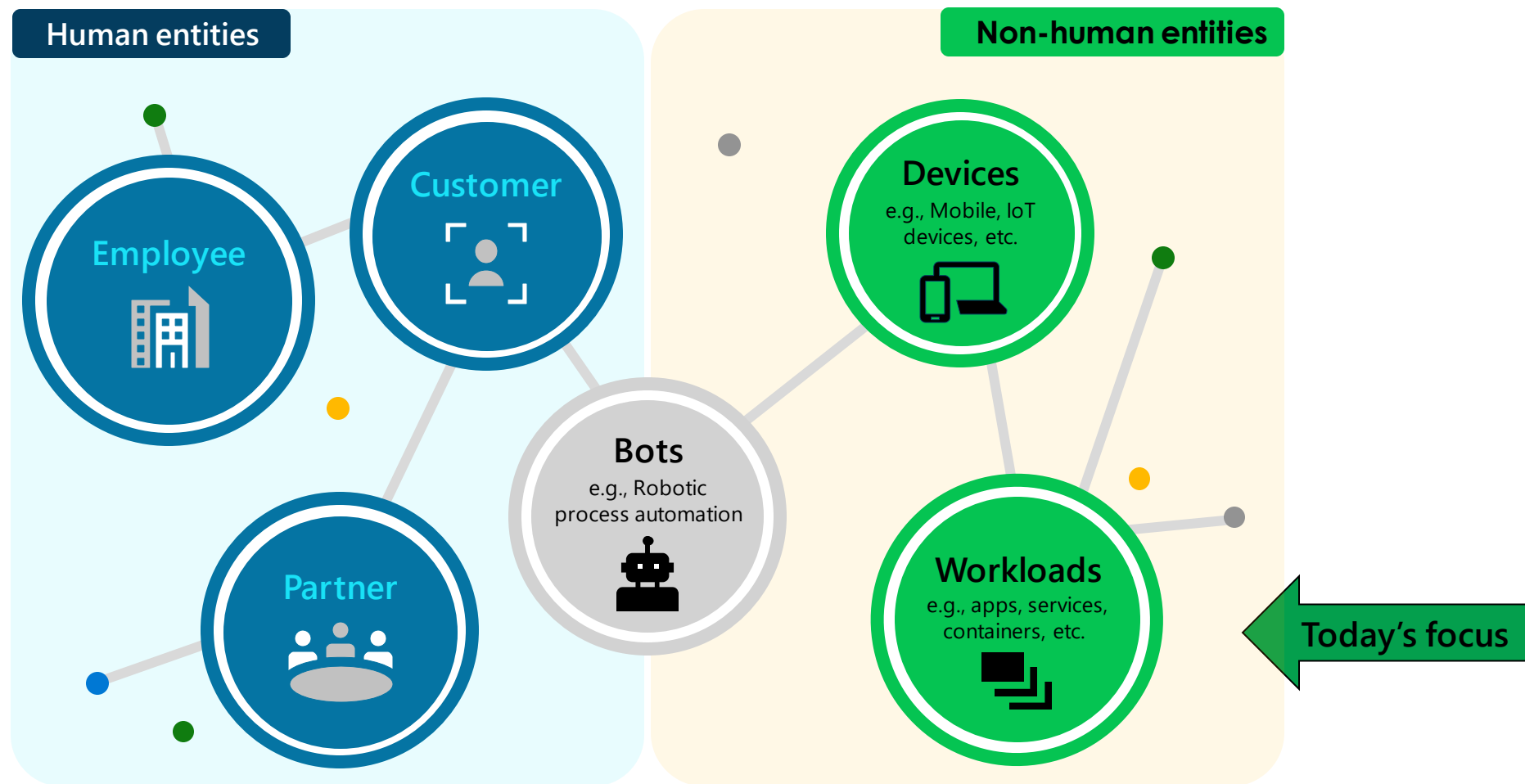
What is risk?

How to detect

How to contain, mitigate and remediate

How to protect

What are Workload Identities?



Examples of service-to-service scenarios

(confidential client flow)



Data Backup
Services



CRM Systems



Security Software



/ innovation

Home / Innovation / Security

Microsoft warns about this phishing attack that wants to read your emails

Attackers have targeted hundreds of organisations, says Microsoft security.



Written by **Liam Tung**, Contributing Writer on Jan. 25, 2022

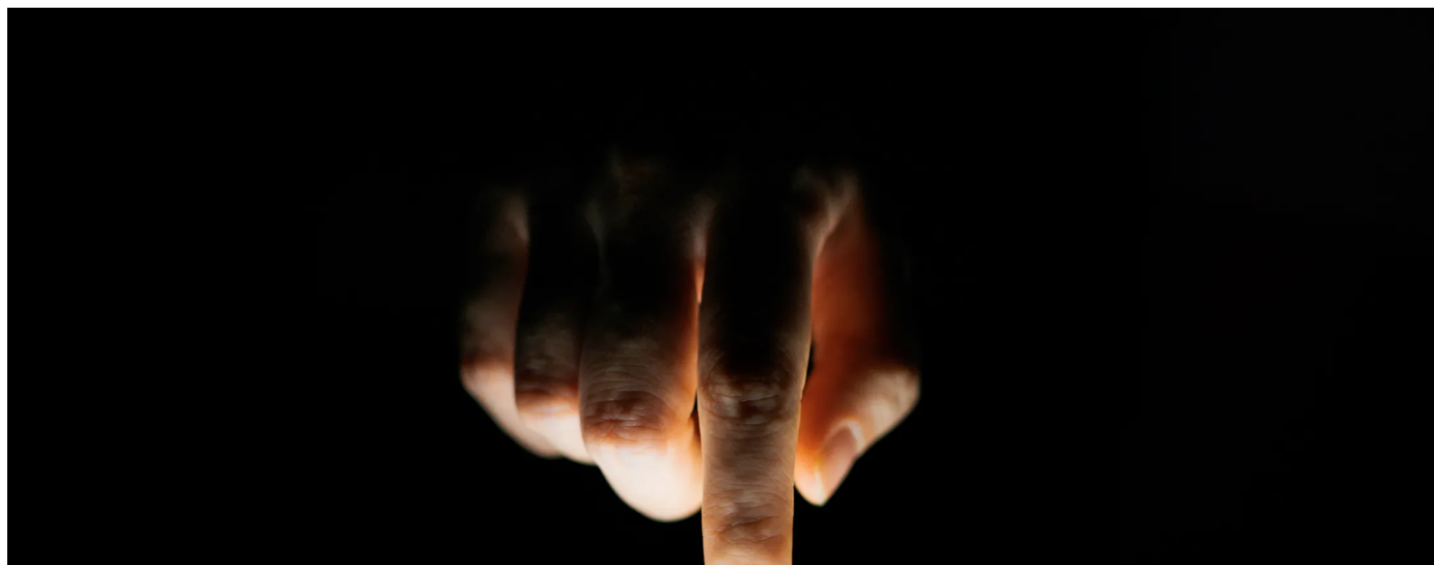


LILY HAY NEWMAN

SECURITY SEP 1, 2022 6:00 AM

Careless Errors in Hundreds of Apps Could Expose Troves of Data

Researchers found that mobile applications contain keys that could provide access to both user information and private files from unconnected apps.



BLOG

You Can't Audit Me: APT29 Continues Targeting Microsoft 365

DOUGLAS BIENSTOCK

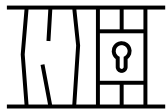
AUG 18, 2022 | 6 MINS READ

Application Threats

- **26 million** user creds stolen by malicious applications from 2018-2020
- **4.9:** Average number of incidents involving theft/misuse of a key or certificate an organization is likely to experience in a 24-month period
- **4k+** unique app identities leaked in Github in 2022

Parachute, 2022 Cyber Attack Statistics, Data and Trends
Ponemon Institute, State of Machine Identity Management 2021
Microsoft Identity & Network Access Division

Application identity threats



Compromised

Legitimate app that has
been hijacked



Malicious

Created by an attacker
for bad purposes



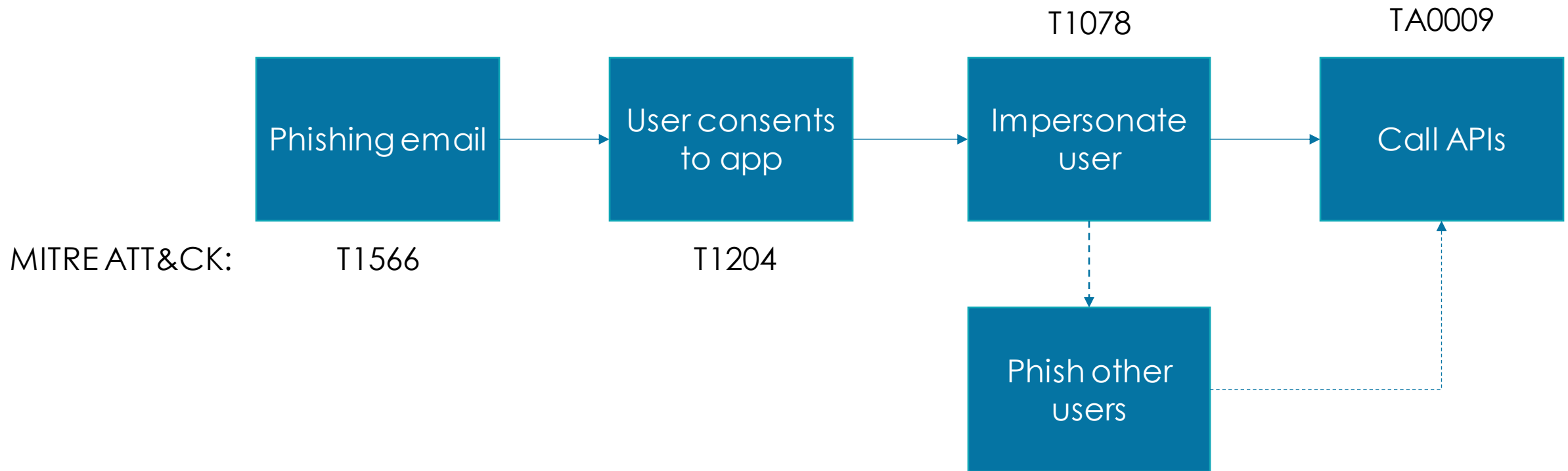
Misconfigured

Insecure configuration
in/outside your identity
provider that makes it
susceptible to
compromise

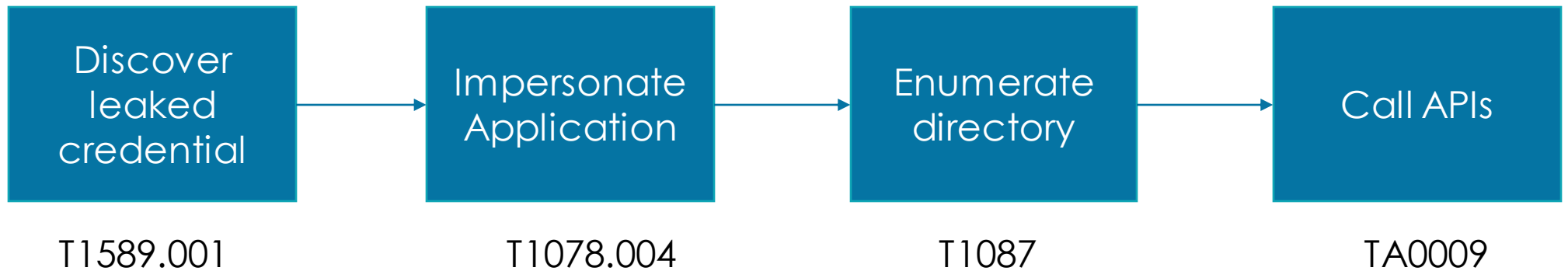
Attack graph – Compromised app



Attack graph – Malicious app



Attack graph – Misconfigured app



The “Street Light” Effect

What do we focus on?

What needs increased focus?

What new partnerships do we need?

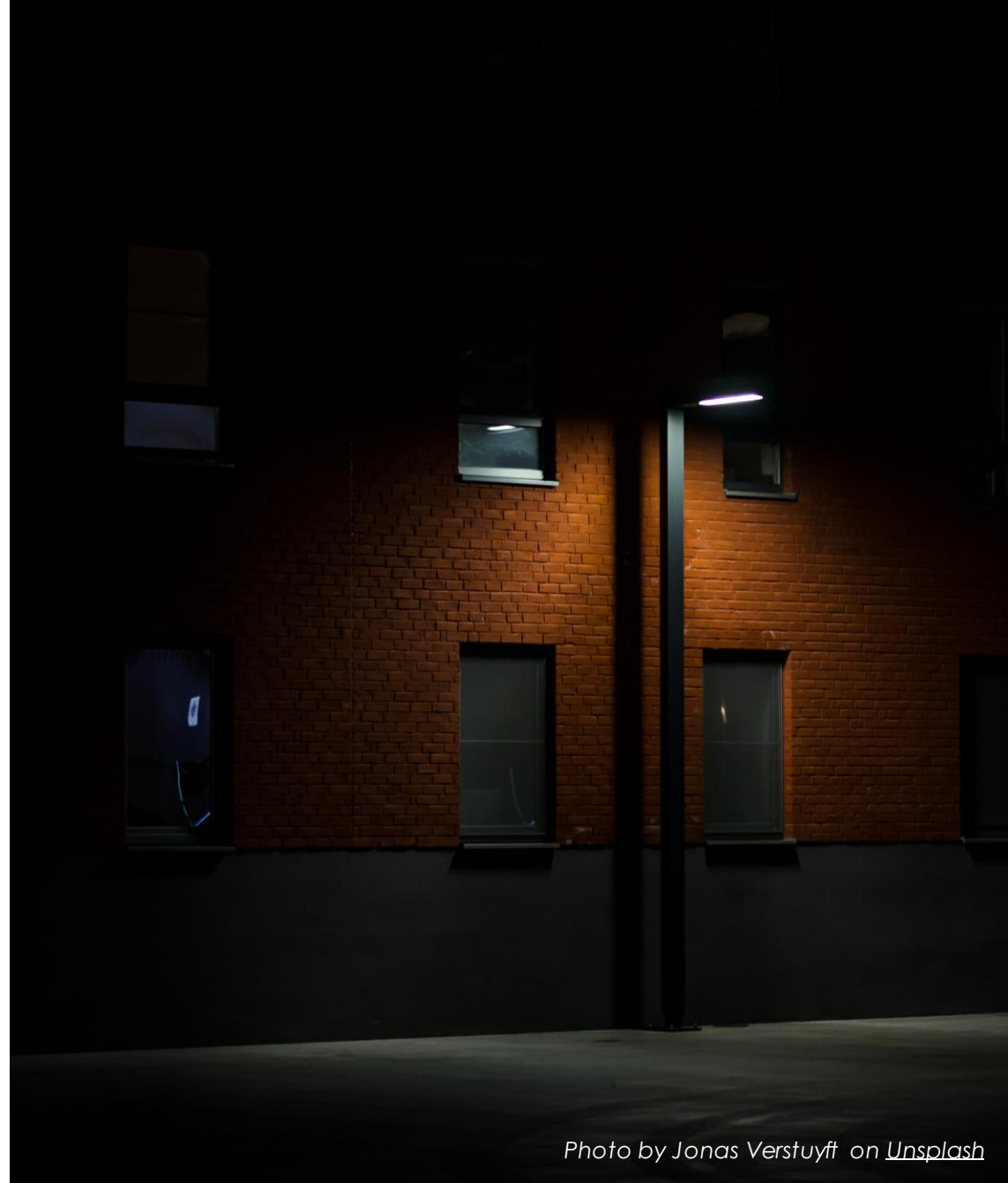


Photo by Jonas Verstuyft on [Unsplash](#)

Agenda

What is risk?

How to detect

How to contain, mitigate and remediate

How to protect

Sign-in logs



Location

IP address
ASN
Country



Frequency

Most have a
predictable
pattern



User agent

Anything
unexpected
or violates
security policy



Credential type

Anything
unexpected
or violates
security policy



Resource

Should this
identity be
accessing this
resource?

Audit logs

Permissions

High privilege grant

End user granting applications consent

End user consent blocked on risk level

In Azure – service principal assigned to an Azure AD or Azure RBAC role; changes to Azure Key Vault

Time/process

Changes made outside of normal business processes and schedules

Credential type

Unauthorized changes or types

Configuration

Universal resource identifier (URI) changed or non-standard

Changes to application owners

Logout URLs modified

Secret scanning

Your own tool

Use on-prem / cloud

Customizable

Some OSS options

Vendor tools

Most are cloud-based

Scalable

More current (secret format)

More recall (scans entire service not just your repos)

More precision (some will tell you if the secret is still valid)

demo

Home

Azure Active Directory

Overview

Users

Groups

Devices

Applications

Protect & secure

Conditional Access

Identity Protection

Authentication methods

Password reset

Custom attributes

Risky activities

Identity Governance

External Identities

Show more

Permissions Management

Learn & support

Identity Protection | Risky workload identities (preview)

Search

Learn more Download Select all Confirm service principal(s) compromised Dismiss service principal risk

Auto refresh : Off Show dates as : Local Risk state : 2 selected Add filters

<input type="checkbox"/> Service principal	Service principal ID	App ID	Risk state
<input type="checkbox"/> Microsoft Teams AuditService	092f8424-5b96-46c5-95cb-9bcb...	978877ea-b2d6-458b-80c7-05df...	At risk
<input type="checkbox"/> Contoso	24fc6665-00c3-44a4-9f47-30577...	0b50e6f1-b5b5-44a5-be3c-ceae...	At risk
<input type="checkbox"/> Contoso Front Desk	db734a9a-e775-4847-9a40-557...	e1337603-ebe0-4739-82ce-f3c8...	At risk
<input type="checkbox"/> Contoso Expense	285c6a30-8993-45da-ae96-cd2c...	0feb38ac-a572-491d-a9db-b071...	At risk
<input type="checkbox"/> Contoso Sales Tracker	1baef386-7491-4ee6-9376-72c5...	971b68fa-7541-4192-be59-c0ff3...	At risk
<input type="checkbox"/> ContosoDevOps	079d96b3-3d68-49fd-8b25-9da...	7b37ac67-48c3-4913-87b0-3b6c...	At risk
<input type="checkbox"/> Contoso Chat Bot	12d68440-f39c-4ce7-bf86-5cd9...	1e429928-7ff6-432e-a2a4-c46f4...	At risk
<input type="checkbox"/> AutomateContoso	8b8b93e3-fd4c-4dd2-9869-592...	f91ebafb-19a8-41db-b38e-8f13...	At risk

Overview

Diagnose and solve problems

Protect

User risk policy

Sign-in risk policy

Multifactor authentication registration policy

Report

Risky users

Risky workload identities (preview)

Risky sign-ins

Risk detections

Notify

Users at risk detected alerts

Weekly digest

Troubleshooting + Support

Virtual assistant (Preview)

Troubleshoot

New support request

Risky Workload Identity Details

Service principal's sign-ins Service principal's audit logs

Basic Info Risk history

Service principal

Roles

Service principal enabled

Service principal's risk detections

Confirm service principal compromised

Dismiss service principal risk

Disable Service Principal

Service principal ID

24fc6665-00c3-44a4-9f47-305776da2a54

Risk state

At risk

Risk level

High

Risk detail

-

Risk last updated

9/10/2022, 9:13:15 AM

Service principal type

Application

App ID

0b50e6f1-b5b5-44a5-be3c-ceae51f6a041

Home

Azure Active Directory

Overview

Users

Groups

Devices

Applications

Protect & secure

Conditional Access

Identity Protection

Authentication methods

Password reset

Custom attributes

Risky activities

Identity Governance

External Identities

Show more

Permissions Management

Learn & support

Identity Protection | Risk detections

Search

Learn moreDownloadRefreshColumnsGot feedback?

Overview

Diagnose and solve problems

Protect

User risk policy

Sign-in risk policy

Multifactor authentication registration policy

Report

Risky users

Risky workload identities (preview)

Risky sign-ins

Risk detections

Notify

Users at risk detected alerts

Weekly digest

Troubleshooting + Support

Virtual assistant (Preview)

Troubleshoot

New support request

Auto refresh : Every 5 minutes

Detection time : Last 90 days

Show dates as : Local

Detection type

Add filters

User detections

Workload identity detections

Detection time	Service principal name	Detection type
9/9/2022, 4:05:00 PM	Contoso	Leaked credentials
9/6/2022, 10:04:21 AM	ContosoDevOps	Azure AD threat intelligence
9/6/2022, 10:04:21 AM	Contoso Sales Tracker	Suspicious sign-ins
9/6/2022, 10:04:21 AM	Contoso Front Desk	Suspicious sign-ins
9/27/2022, 8:52:52 PM	Microsoft Teams AuditService	Azure AD threat intelligence
9/22/2022, 11:32:31 AM	Microsoft Teams AuditService	Azure AD threat intelligence
9/10/2022, 9:12:57 AM	Contoso	Leaked credentials
9/6/2022, 10:04:21 AM	Contoso Expense	Azure AD threat intelligence

Risk Detection Details

Service principal's risk reportService principal's sign-ins

Detection typeSuspicious sign-ins

Learn how to investigate

Risk stateAt risk

Risk levelHigh

Risk detail-

SourceIdentity Protection

Detection timingOffline

ActivityService Principal

Detection time9/6/2022, 10:04 AM

Detection last updated9/6/2022, 10:04 AM

Application ID971b68fa-7541-4192-be59-c0ff3b5e1851

Key ID

Service principal nameContoso Sales Tracker

Service principal ID1baef386-7491-4ee6-9376-72c5a66e7805

Additional InfoThis account's sign-ins are suspicious for the following reasons: unfamiliar sign-in frequency of IP subnet, unfamiliar sign-in frequency of resource, unfamiliar sign-in frequency of user agent, unfamiliar sign-in frequency of ASN.

(ISC)² | SECURITYCONGRESS

Congress.isc2.org | #ISC2Congress

Home

Azure Active Directory

Overview

Users

Groups

Devices

Applications

Protect & secure

Conditional Access

Identity Protection

Authentication methods

Password reset

Custom attributes

Risky activities

Identity Governance

External Identities

Show more

Permissions Management

Learn & support

Identity Protection | Risk detections

Search

Learn moreDownloadRefreshColumnsGot feedback?

Auto refresh : Every 5 minutesDetection time : Last 90 daysShow dates as : LocalDetection type

Add filters

Protect

User risk policy

Sign-in risk policy

Multifactor authentication registration policy

Report

Risky users

Risky workload identities (preview)

Risky sign-ins

Risk detections

Notify

Users at risk detected alerts

Weekly digest

Troubleshooting + Support

Virtual assistant (Preview)

Troubleshoot

New support request

User detectionsWorkload identity detections

Detection time	Service principal name	Detection type
9/9/2022, 4:05:00 PM	Contoso	Leaked credentials
9/6/2022, 10:04:21 AM	ContosoDevOps	Azure AD threat intelligence
9/6/2022, 10:04:21 AM	Contoso Sales Tracker	Suspicious sign-ins
9/6/2022, 10:04:21 AM	Contoso Front Desk	Suspicious sign-ins
9/27/2022, 8:52:52 PM	Microsoft Teams AuditService	Azure AD threat intelligence
9/22/2022, 11:32:31 AM	Microsoft Teams AuditService	Azure AD threat intelligence
9/10/2022, 9:12:57 AM	Contoso	Leaked credentials
9/6/2022, 10:04:21 AM	Contoso Expense	Azure AD threat intelligence


Risk Detection Details

Service principal's risk reportService principal's sign-ins

Detection type	Leaked credentials
	Learn how to investigate
Risk state	At risk
Risk level	High
Risk detail	-
Source	Identity Protection
Detection timing	Offline
Activity	Service Principal
Detection time	9/10/2022, 9:12 AM
Detection last updated	9/10/2022, 9:12 AM
Application ID	0b50e6f1-b5b5-44a5-be3c-ceae51f6a041
Key ID	2d3fb79b-71c4-4f78-a073-98269babe198
Service principal name	Contoso
Service principal ID	24fc6665-00c3-44a4-9f47-305776da2a54
Additional info	Click here for more details

4b3c2d580a SecidentityTechAADIPDemo / contosoapp.txt

Go to file ...

 **cuixi1222** Create contosoapp.txt

Latest commit 4b3c2d5 28 days ago [History](#)

1 contributor

3 lines (3 sloc) | 167 Bytes

Raw Blame

```
1 "AadClientId": "0b50e6f1-b5b5-44a5-be3c-ceae51f6a041",
2 "AadSecret": "UZY8Q~t_piRGbz_sey3dw-zziRLWUHoAsCPNmaRj",
3 "AadTenantId": "536279f6-15cc-45f2-be2d-61e352b51eef",
```


Agenda

What is risk?

How to detect

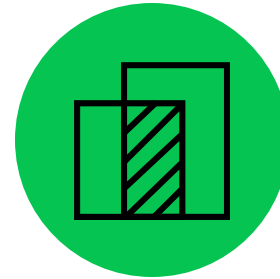
How to contain, mitigate and remediate

How to protect

Incident Response Basics



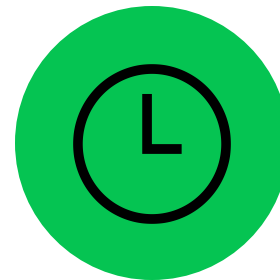
Stay calm and do no harm



Involve your legal team



Be careful when sharing information publicly



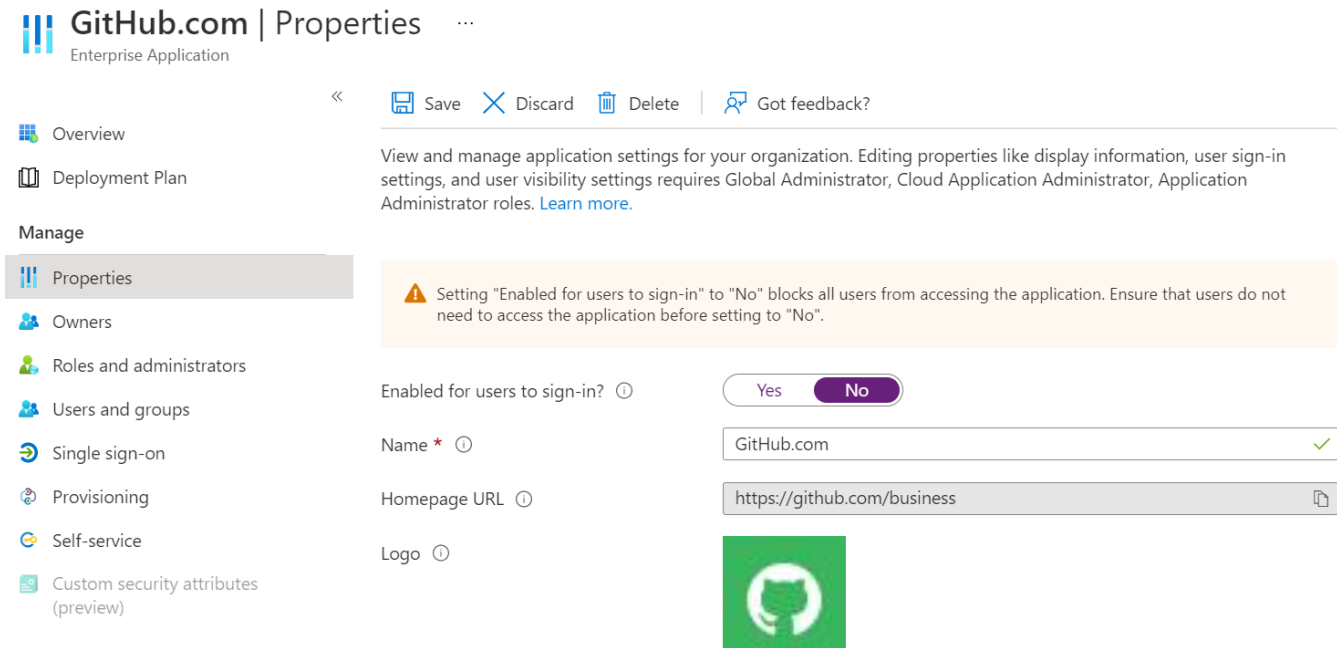
Get help when needed

Containment

Disable compromised application


- If admin creds are compromised, coordinate with eviction


Weigh impact of deletion or key rolling





The screenshot shows the 'Properties' page for the 'GitHub.com' Enterprise Application. The left sidebar lists navigation options: Overview, Deployment Plan, Manage (Properties, Owners, Roles and administrators, Users and groups), Single sign-on, Provisioning, Self-service, and Custom security attributes (preview). The main content area has a top bar with 'Save', 'Discard', 'Delete', and 'Got feedback?' buttons. Below this is a descriptive text about application settings. A prominent yellow warning box states: 'Setting "Enabled for users to sign-in" to "No" blocks all users from accessing the application. Ensure that users do not need to access the application before setting to "No".' The settings include: 'Enabled for users to sign-in?' with a 'No' button selected; 'Name' set to 'GitHub.com'; 'Homepage URL' set to 'https://github.com/business'; and a 'Logo' field containing the GitHub logo.


demo


 Home


 Azure Active Directory


 Overview

 Users

 Groups

 Devices

 Applications

 Protect & secure

Conditional Access


Identity Protection


Authentication methods

Password reset


Custom attributes


Risky activities

 Identity Governance

 External Identities

Show more

 Permissions Management

 Learn & support

Conditional Access | Policies

Azure Active Directory

«

+

New policy

+

New policy from template (Preview)

What If

Refresh

Got feedback?

Overview (Preview)

Policies

Insights and reporting

Diagnose and solve problems

Manage

Named locations

Custom controls (Preview)

Terms of use

VPN connectivity

Authentication context (Preview)

Classic policies

Monitoring

Sign-in logs

Audit logs

Troubleshooting + Support

Virtual assistant (Preview)

New support request

Search policies

Add filters

55 out of 55 policies found

Policy Name ↑↓	State ↑↓	Creation Date ↑↓	Modified Date ↑↓
CA01 - MFA - All Apps - All Users - Do Not Change - Policy is monitored	On		10/3/2022, 3:16:54 AM ...
CA02 - Restrict - Security Apps - NOAM Offices	On		4/21/2022, 6:37:25 AM ...
CA03- Require Compliant Device - Register Security Information	On		9/2/2022, 2:42:55 PM ...
CA04 - Block Sensitive Apps from High sign-in risk users	On		7/27/2022, 3:33:04 PM ...
CA06 - All User - Block Legacy Auth	On		9/12/2022, 5:11:43 PM ...
CAX - TOU - All Woodgrove (and Guest) Users	On		4/10/2022, 2:01:13 PM ...
CA08 - MCAS Session Control - All Users	On		8/16/2022, 3:48:54 PM ...
CA09 - All Apps - Allow only Trusted Locations	On		1/14/2022, 11:05:59 AM ...
CA10 - Require MFA for VPN Access	On		9/18/2020, 11:58:52 AM ...
CA11 - TOU - Partner Orgs	On	12/16/2020, 1:09:44 PM	3/4/2021, 6:32:42 PM ...
RO - Require Compliant device for all users all apps	Report-only	2/4/2021, 6:48:28 PM	3/13/2021, 5:32:29 PM ...
RO - Require MFA for medium risk user activating roles	Report-only	2/5/2021, 12:46:40 PM	3/23/2021, 5:47:29 PM ...
CA12 - All Admins TOU - Reminder	On	4/7/2021, 8:26:32 AM	8/18/2022, 1:59:08 PM ...
CA13 - Woodgrove Compliant device - Auth Context	On	8/3/2021, 11:47:20 AM	8/19/2022, 9:38:55 AM ...
CAX - Secure Admin Workstations - Project TNT Required	On	2/1/2022, 10:14:21 AM	2/2/2022, 11:34:20 AM ...
CA12 - Silverfort MFA - On-prem	On	2/3/2022, 2:13:02 PM	6/15/2022, 5:31:31 PM ...
CA15 - TOU Security Reminder	On	2/17/2022, 8:52:10 PM	2/24/2022, 12:59:38 PM ...
RO - Workload ID Block on risk, report-only	Report-only	3/1/2022, 11:18:06 PM	8/24/2022, 1:26:12 PM ...
CA16 - Require Partners Compliant Devices	On	3/10/2022, 4:41:44 PM	...
CA17 - Require Compliant Device - Social Media Apps	On	4/6/2022, 3:47:22 PM	8/24/2022, 1:26:46 PM ...
CA18 - Cloud PC - Require Compliant	On	4/22/2022, 2:59:59 PM	8/24/2022, 1:30:29 PM ...
RO - Block - MFA Registrion non-compliant devices	Report-only	5/4/2022, 2:29:52 PM	8/24/2022, 1:30:43 PM ...

Home

Azure Active Directory

Overview

Users

Groups

Devices

Applications

Protect & secure

Conditional Access

Identity Protection

Authentication methods

Password reset

Custom attributes

Risky activities

Identity Governance

External Identities

Show more

Permissions Management

Learn & support

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

Name *

Block workload identities on High Risk

Assignments

Users or workload identities

All owned service principals

Cloud apps or actions

All cloud apps

Conditions

1 condition selected

Access controls

Grant

Block access

Session

0 controls selected

Enable policy

Report-only

On

Off

Create

Service principal risk (Preview)

1 included

Locations (Preview)

Not configured

Some conditions are not available due to 'Workload identities (preview)' selection in policy assignment

Service principal ri...

Configure

Yes

No

Configure service principal risk levels needed for policy to be enforced

☒ High

☐ Medium

☐ Low

Done

Home

Azure Active Directory

Overview

Users

Groups

Devices

Applications

Protect & secure

Identity Governance

External Identities

Show more

Permissions Management

Verified ID

Learn & support

Conditional Access | Insights and reporting

Azure Active Directory

Overview (Preview)

Policies

Insights and reporting

Diagnose and solve problems

Manage

Named locations

Custom controls (Preview)

Terms of use

VPN connectivity

Authentication context (Preview)

Classic policies

Monitoring

Sign-in logs

Audit logs

Troubleshooting + Support

Virtual assistant (Preview)

New support request

Auto refresh: Off

Impact summary

Click on the tiles below to filter the report by the selected Conditional Access result.

Total
14
service principals

Success
10
service principals

Failure
1
service principals

Not applied
4
service principals

Total: Number of service principals in the Last 24 hours

Success: Number of service principals where the selected polic(ies) granted access and the required controls were satisfied

Failure: Number of service principals where the selected polic(ies) denied access and the required controls were not satisfied

Not applied: Number of service principals that are bypassing the selected polic(ies) because the sign-in did not match at least one of the assignments or conditions.

Breakdown per condition and sign-in status

Location - Total

Resources - Total

ResourceDisplayName	Count
Azure Key Vault	5
Microsoft Graph	5
Windows Azure Service Management API	3
Microsoft Intune API	2
Windows Azure Active Directory	2

Recovery

Remediate service principals

Remediate affected service principal resources

Disable or delete malicious apps

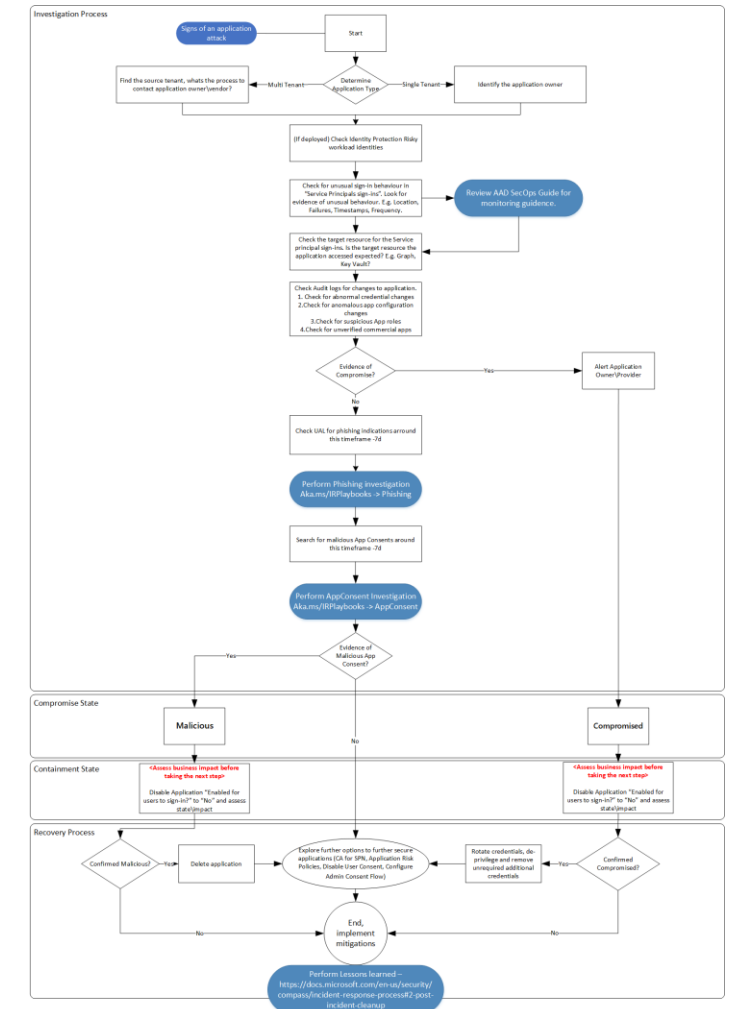
Implement Identity Protection for workload identities

aka.ms/IRPlaybooks

Detailed walkthrough at above link

Investigation process

- Whether an app is malicious or compromised
- Containment and assessing business impact
- Recovery process



Agenda

What is risk?

How to detect

How to contain, mitigate and remediate

How to protect

Treat workload identities like user accounts

Good security principles:

- Use strong credentials
- Least privilege
- Lifecycle management
- Monitor anomalies



Strong Credentials

Users

Use modern password guidance

- Discourage weak, easy to guess passwords
- Avoid arbitrary password rules that encourage patterns
- Monitor for leaked credentials

Leverage FIDO2 keys or other passwordless methods

Workload identities

Use X509 certs or managed identities instead of client secrets

Monitor applications to identify those with long credential expiration times

Replace long-lived credentials with credentials that have a short life span

Ensure that credentials don't get committed in code repositories and are stored securely

Least Privilege

Users

Assign admin roles only necessary permissions

Limit admin roles whenever possible

Use just-in-time (JIT) elevation and just-enough-administration (JEA)

Workload identities

Investigate application permissions and ensure they're truly needed

Identify existing applications with highly privileged permissions

Consider limiting end user consent

Analyze when end user consent is blocked

Lifecycle Management

Users

Clean up stale accounts

Recertify access for the accounts

Workload identities

Clean up stale apps and credentials

Recertify access for the accounts

Monitor apps with high permissions

Lower application permissions

Example: If your app only needs to read mail, lower permission from *Mail.ReadWrite.All* to *Mail.Read.All*

Monitor Anomalies

Users

Unfamiliar locations

New devices

Actions taken outside of typical working hours

Accessing unusual files

Workload identities

Universal resource identifier (URI) changed or non-standard

Changes to application owners

Logout URLs modified

Unauthorized changes to credentials

demo

Home

Azure Active Directory

Overview

Users

Groups

Devices

Applications

Protect & secure

Identity Governance

Entitlement management

Access reviews

Privileged Identity Management

Lifecycle workflows

External Identities

Show more

Permissions Management

Verified ID

Learn & support

Woodgrove | Access reviews

Privileged Identity Management | Azure AD roles

New

Filter

Group

Settings

Quick start

Overview

Tasks

My roles

Pending requests

Approve requests

Review access

Manage

Roles

Assignments

Alerts

Access reviews

Discovery and insights (Preview)

Settings

Activity

Resource audit

My audit

Access reviews for Azure AD directory roles

Search by name or owner

Role	Owner	Start Date	End Date	Status
WI				
Global Administrator	Stefan van der Wiele stvand@woodgrove.ms	9/27/2022	12/26/2022	Active
TestAccessReviewincluding member				
Virtual Visits Administrator	Nandan Tripathi natripat@woodgrove.ms	6/23/2022	9/21/2022	Result applied
FordTestSecurityReader				
Security Reader	Nandan Tripathi natripat@woodgrove.ms	6/15/2022	7/15/2022	Complete
Security Admin Ford Test				
Security Administrator	Nandan Tripathi natripat@woodgrove.ms	6/15/2022	7/15/2022	Result applied
Forrester Access Review				
Privileged Role Administrator	Ricky Pullan ripull@woodgrove.ms	9/28/2020	12/29/2020	Complete
Reviews created by PIM discovery tool				
Cloud Application Administrator	Yusuke Kodama ykodama@woodgrove.ms	6/29/2020	7/29/2020	Result applied
Global Admin V2				
Global Administrator	Joey Cruz joeyc@contosoorg.net	1/19/2020	2/18/2020	Complete
Global Admins				
Global Administrator	Joey Cruz joeyc@contosoorg.net	1/16/2020	1/17/2020	Complete
Application Developers				
Application Developer	Peggy Merchan PeggyM@ContosoOrg.net	5/1/2019	5/31/2019	Complete

- Home
- Azure Active Directory
 - Overview
 - Users
 - Groups
 - Devices
 - Applications
 - Protect & secure
 - Identity Governance
 - Entitlement management
 - Access reviews
 - Privileged Identity Management
 - Lifecycle workflows
 - External Identities
 - Show more
- Permissions Management
- Verified ID
- Learn & support

Create an access review ...

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name * Workload Identity with Global Admin review ✓

Description ⓘ reviewing which WI have global admin role ✓

Start date * 10/07/2022

Frequency Quarterly

Duration (in days) ⓘ
----- 2.

End ⓘ
Never End by Occurrences

Number of times 0

End date 01/05/2023

Users

Scope
☐ All users and groups
☒ Service Principals ⓘ

Role *
Global Administrator

Assignment type Active assignments only

Reviewers
Reviewers Selected user(s) or group(s)

Start

Select reviewers

Audit

AT Audit Team
Selected

AU auditTestGroup

PA parentAuditGroup

TE Test_AuditLogs

Selected reviewers

AT Audit Team Remove

Select

Home

Azure Active Directory

Overview

Users

Groups

Devices

Applications

Protect & secure

Identity Governance

Entitlement management

Access reviews

Privileged Identity Management

Lifecycle workflows

External Identities

Show more

Permissions Management

Verified ID

Learn & support

Create an access review

End

Never

End by

Occurrences

Number of times

0

End date

01/05/2023

Users

Scope

All users and groups

Service Principals

Role *

Global Administrator

Assignment type

Active assignments only

Reviewers

Reviewers

Selected user(s) or group(s)

Select reviewers *

Audit Team

Upon completion settings

Auto apply results to resource

Enable

Disable

If reviewers don't respond

Take recommendations

At end of review, send notification to

Compliance Management

Advanced settings

Start

Review WI in Global Admin roles ...



Filter

Essentials ^

Owner Etan Basseri[etbasser@woodgrove.ms] Require reason on approval true End date 1/5/2023 Remaining 3	Role Global Administrator Start date 10/7/2022 Description
--	--

Approve or deny role memberships using the buttons below

Search

Name	Reason	Reviewed by	Audit Details	Recommended action	
Not reviewed					
<input type="checkbox"/>	Portal View 961844d2-febf-4aae-ab91-87fc2fa1dbd0		View		
<input checked="" type="checkbox"/>	Sec-Removal-Guest 6d70064d-7677-492d-b69c-18b736fccd11		View		
<input type="checkbox"/>	ZT-Removal-90-Days 4d1d55b0-a72d-4695-82db-8911eed9729d		View		

*Reason ⓘ

No longer needed as this service is being retired.

Approve

Deny

Reset

Go-Do's

1. Identify your app owners
2. Security operations guidance
aka.ms/AzureADSecOps
3. Incident response guidance
aka.ms/IRPlaybooks

Questions or comments?

aka.ms/SecurityCongress2022Deck

 Etan Basseri

 @ebasseri

 Bailey Bercik

 @BaileyBercik

aka.ms/SecurityCongress2022Deck

 **Etan Basseri**

 **@ebasseri**

 **Bailey Bercik**

 **@BaileyBercik**

Demo