

Microsoft Security Incident Communication and how to guide

Abbas Kudrati
APAC Chief Cybersecurity Advisor
Abbas.Kudrati@microsoft.com
<https://aka.ms/abbas>



Philosophy

Our goal is for Microsoft to earn customer trust.

We do this through being thorough with notifications, customer-obsessed, and constantly improving the experience.

During incidents, Microsoft endeavors to speak with one voice.

This means alignment between engineering, account teams, and support teams. This also means consistency between your experiences in Azure, Microsoft 365, and Dynamics 365.

Principles

Inform potentially affected customers and their associated field representatives through the right channels at the right time.

To protect the security and privacy of our customers and platform, notifications are as targeted as possible.

Safeguard sensitive information while providing guidance to impacted customers and internal stakeholders to protect their environment.

To ensure sensitive details regarding security or privacy incidents are not broadly communicated, information dissemination is controlled on a need-to-know basis.

Security Incidents Communication Principles

Accuracy - Communicate with valid and reliable content

Detail - Communicate with as much applicable and actionable content as possible

Scope - Communicate to the impacted and avoid overcommunication as best as possible

Speed - Communicate as fast as possible

Transparency - Communicate with customer/field need and trust in mind

Commitments

Microsoft outlines Data Breach Notification commitments in a document call, "Microsoft Products and Services Data Protection Addendum (DPA)" which can be viewed here:

<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>

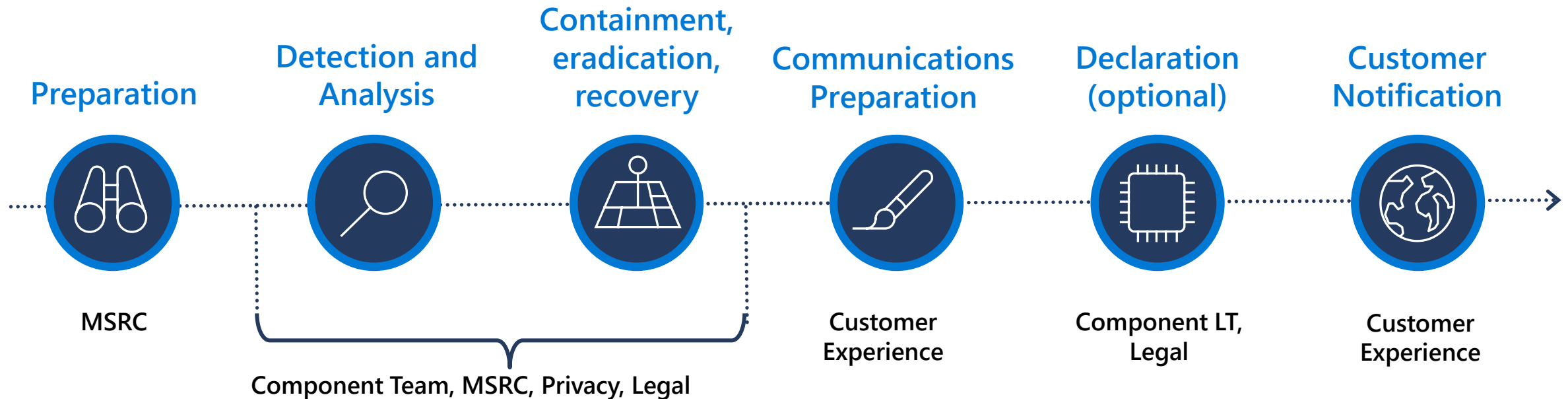
Security Incident Notification

If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, Professional Services Data, or Personal Data while processed by Microsoft (each a "Security Incident"), Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to Customer by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer maintains accurate contact information with Microsoft for each applicable Product and Professional Service. Customer is solely responsible for complying with its obligations under incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident.

Microsoft shall make reasonable efforts to assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

Security Incidents Timeline



A few things you need to know

- This timeline refers to a general timeline for security incidents. Depending on a number of key factors (e.g. Notification SLA/Obligation, impact scope, investigation timeline and complexity, etc.) of the security incidents, the process may vary case by case.
- The entire process is a collaboration among all internal stakeholders including MSRC, Component Teams, CSS, Customer Experience, Privacy and Legal, etc.. We only listed the key stakeholders in each process for better understandability.
- Generally, our "investigation" process refers to "Assessment, Diagnose, Stabilize/Recover" based on MSRC Workflow. Microsoft Security Response Center (MSRC) Incident Response team is the dedicated crisis response team around security/privacy issues.
- We will send out the customer notifications after declaration of the incident and when all necessary information has been captured. Due to our obligation to notify the customers, there is no guarantee that your Microsoft account managers will receive an earlier notification prior to customer communications.
- Security Incident management process found here: [Incident management overview - Microsoft Service Assurance | Microsoft Docs](#)

Security/Privacy Incident Reporting

Microsoft Security Response Center (MSRC)

Incident Response team is the dedicated crisis response team around security/privacy issues

MSRC Incident Response Phases include:

- **Detection:** Issues can be reported internally or externally from Microsoft. 24/7 team will respond accordingly
- **Assessment:** Provide preliminary analysis of risk, escalate internally, or determine if the issue needs to be further diagnosed. Alert Communications, CELA, or additional engineering teams as necessary*
- **Diagnose:** Appropriately classify the event, reassess severity of incident, and determine if the issues impacts other MSFT services. In parallel, execute customer communications if applicable.
- **Stabilize/Recover:** Identify mitigation and long term repair items to resolve customer and business impact.
- **Close:** Conduct Post Incident Review to identify any key failures in the current process.

**Parallel sub-process for customer and regulator reporting when necessary*

Affected customers are notified based on Microsoft's obligation and policies around GDPR breaches which can be found [here](#)



Detailed How to Guide

Azure Security Events Communication Framework

Scenarios	Description	Types of events:	Where will customer see notification	Where will notification contact pulled from	What are my alternatives if email notification isn't working
Security Incident	An incident when unlawful access to any Customer Data or Support Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, destroy, or alteration of Customer Data or Support Data has occurred.	<ul style="list-style-type: none"> •Vulnerability •Ransomware •Marketplace offering •Supplier compromise •Privacy Breach •Customer Reportable Security/Privacy Incident (CRSPI) 		<ul style="list-style-type: none"> •Global Tenant admin or Privacy contact: Azure AD built-in roles - Azure Active Directory Microsoft Docs; link •Email notification contact info pulled from: link •Service health alerts (custom configuration alerts): link 	<p>We would attempt to reach out to the account admin / tenant admin(s).</p> <p>Account team would be informed automatically if we send out portal notifications.</p>
Privacy incident	<p>A privacy incident is generally any event that falls into one of the following categories:</p> <ul style="list-style-type: none"> • An unapproved deviation from Microsoft's Privacy Standards by a product or service • A compromise or unauthorized disclosure/access to personal data (often referred to as a security event); or • A press/regulatory contact about failure to meet privacy commitments. Each team must create a guide that outlines types of incidents specific to their business groups, specifically focusing on the delineation between high-impact incidents (requiring intervention by the security teams) and low-impact incidents (handled solely by the privacy team). 	<ul style="list-style-type: none"> •Data Breach 			
Security takedown	<p>Violation of Online Service Terms (OST) & Online Services Data Protection Addendum (DPA): https://www.microsoft.com/en-us/licensing/product-licensing/products</p> <p>"We may suspend your use of the Online Services if: (1) it is reasonably needed to prevent unauthorized access to Customer Data; (2) you fail to respond to a claim of alleged infringement under Section 5 within a reasonable time; (3) you do not pay amounts due under this agreement; (4) you do not abide by the Acceptable Use Policy or you violate other terms of this agreement; or (5) for Limited Offerings, the Subscription becomes inactive from your failure to access the Online Services as described in the Offer Details. If one or more of these conditions occurs".... From Microsoft Online Subscription Agreement</p>	<ul style="list-style-type: none"> •Imminent Harm Personal Data Exposure Child Sexual Exploitation or Abuse Violent or Abhorrent Material Australia AVM law Terrorist or Violent Extremist Content Hate Speech Inciting Violence Defamation Access to copyrighted works Digital Millennium Copyright Act (DMCA) claim 	<p>1. Email notification – if incident requires direct action taken by global admin / account admin / owners</p> <p>2. Azure Portal notification via Service Health https://learn.microsoft.com/en-us/azure/service-health/stay-informed-security</p>	<ul style="list-style-type: none"> •Email notification contact info pulled from: link •Service health alerts (custom configuration alerts): link 	

Stay informed about security incidents in the Microsoft Cloud



With the growing presence and sophistication of online threats like cloud viruses, ransomware, etc., it's important to stay informed about Microsoft security incidents and take the right action to protect your environment. We suggest you do the following to stay informed on security incidents.



1. Check Privacy Contact and Tenant Admin - Tenant

Ensure that there is a **contactable email address** entered for your organization's privacy contact and tenant admin on your tenant.

→ This email address will be used for security incidents that would have impact at the tenant level (i.e. AAD, M365, etc.)

- **Privacy Contact:** [click here to learn more](#)
- **Global Admin:** [click here to learn more](#)



2. Check Contact on Admin or Owner role - Subscription

Ensure that there is a **contactable email address** as the subscription administrator or subscription owner: [click here to learn more](#).

→ This email address will be used for security incidents that would have impact at the subscription level



3. Create Azure Service Health Alerts - Subscription

Create **Azure Service Health** alerts for security events so that your organization can be alerted for any security event that Microsoft identifies. This is the same channel you would configure to be alerted of outages, or maintenance information on the platform: [click here to learn more](#).

There is a main difference for when you are alerted for security issues through Azure Security Center and through Azure Service Health - Security Advisories. Please read more about this [here](#).

The Incident Handling & Notification Procedures:

- **Overview** - <https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-notification>
- **Azure Service Health** – [Stay informed](#)
- **Azure, Dynamics 365, and Windows:** <https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-azure-dynamics-windows>
- **Microsoft 365/Office 365:** <https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365>
- **Microsoft Support and Professional Services:** <https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-microsoft-support-professional-services>

The notification mechanisms : M365 / O365 Message Center

In order to view **Incident Breach Notifications** from in the **Message Center**, your AAD account will need to have the **"Message Center Privacy Reader"** role or your account will need to be a **Global Administrator** - <https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide>

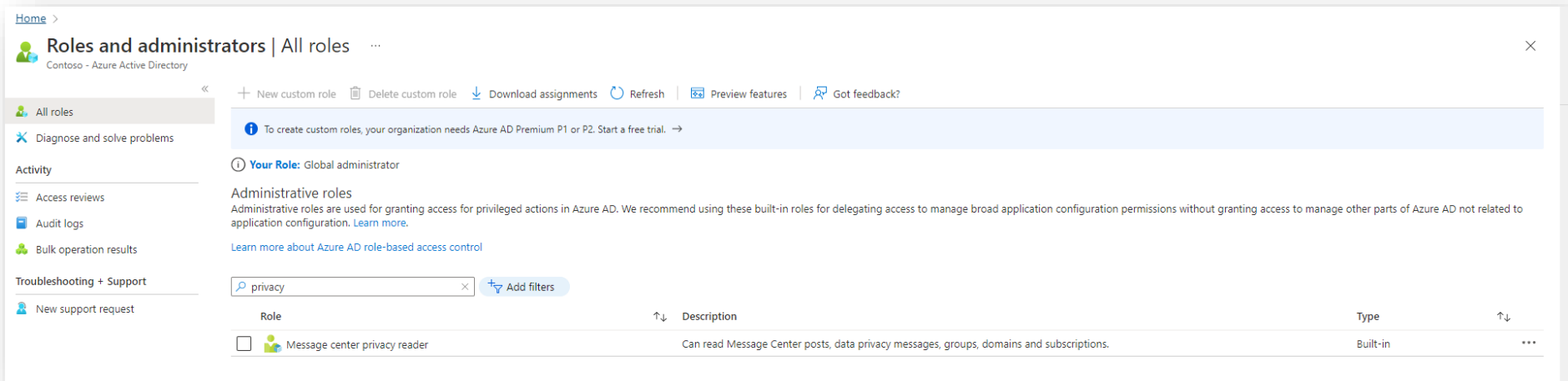
Message center privacy reader

Assign the Message center privacy reader role to users who need to read privacy and security messages and updates in the Microsoft 365 Message center. Message center privacy readers may get email notifications related to data privacy, depending on their preferences, and they can unsubscribe using Message center preferences. **Only global administrators and Message center privacy readers can read data privacy messages.** This role has no permission to view, create, or manage service requests.

Message center privacy readers can also:

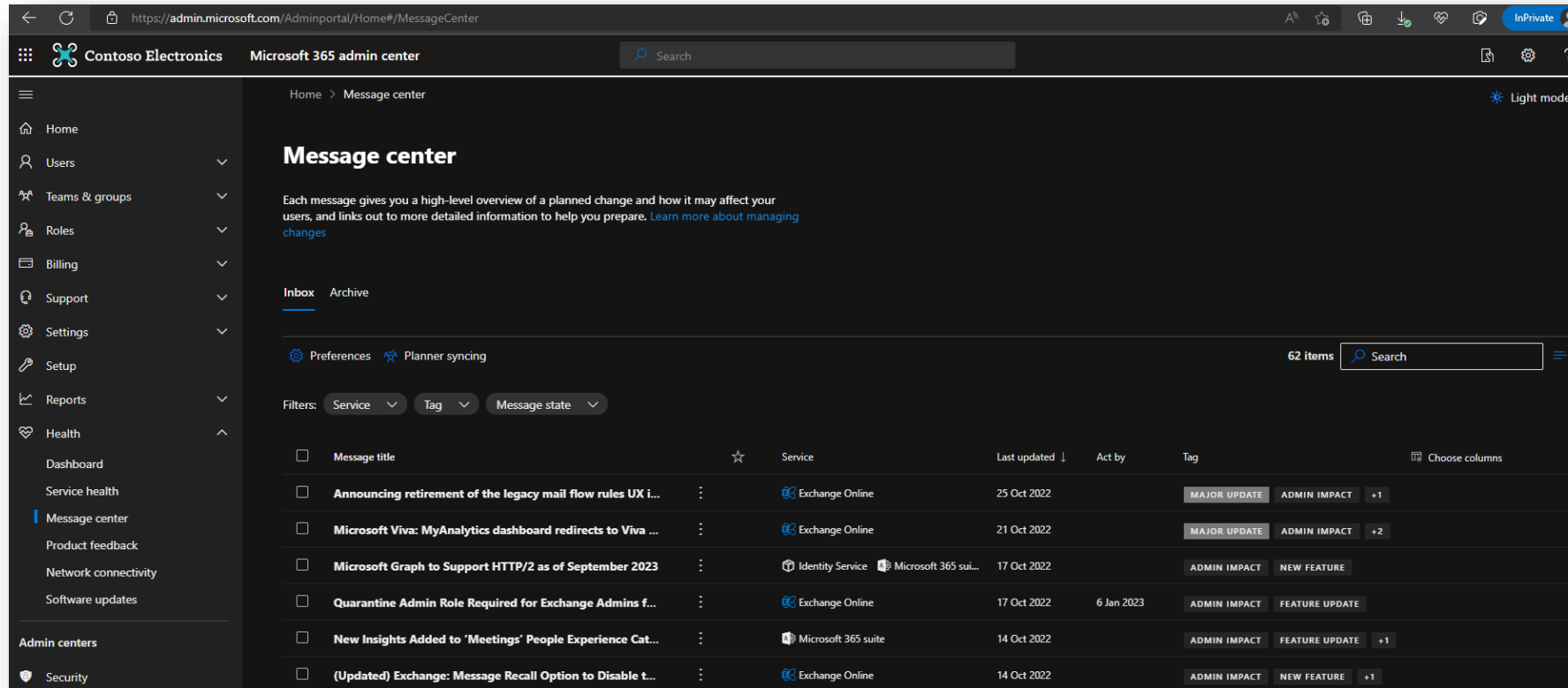
- Monitor all notifications in the Message Center, including data privacy messages
- View groups, domains, and subscriptions

Admin Roles in Microsoft 365: Message Center Privacy Reader



Azure active Directory - Roles and Administrators Blade - Message center privacy reader

Microsoft M365 Message Center setup



<https://admin.microsoft.com/AdminPortal/Home#/messagecenter>

NOTE: If you don't want to have to login to the Message Center Portal to know if a Microsoft Data breach has affected your Office Suite of services, you can optionally setup Mail notifications for the "Data Privacy" tagged events:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/step-by-step-guides/stay-informed-with-message-center?view=o365-worldwide>

Microsoft Azure Active Directory setup

For Azure Active Directory related Data Breaches, there is a Tenant-Level configuration needed to specify the **"Global Privacy Contact"**

This person is also who Microsoft contacts if there's a data breach specifically related to Azure Active Directory services. If there's no person listed here, Microsoft contacts your global administrators.

Azure Active Directory Global Privacy Contact

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-properties-area>

Microsoft Azure

Home > Contoso

Contoso | Properties

Azure Active Directory

Save Discard Got feedback?

Tenant properties

Name *
Contoso_Abbas

Country or region
United States

Location
United States datacenters

Notification language
English

Tenant ID
5e6007a2-56ce-4543-aa6c-ad612f7aa53d

Technical contact
Abbas_Tech@contoso.com

Global privacy contact
Abbas_Privacy@contoso.com

Privacy statement URL
<https://www.contoso.com/privacy>

Access management for Azure resources

Allan Deyoung (admin@M365x859503.onmicrosoft.com) can manage access to all Azure subscriptions and management groups in this tenant. [Learn more](#)

Yes No

[Manage security defaults](#)

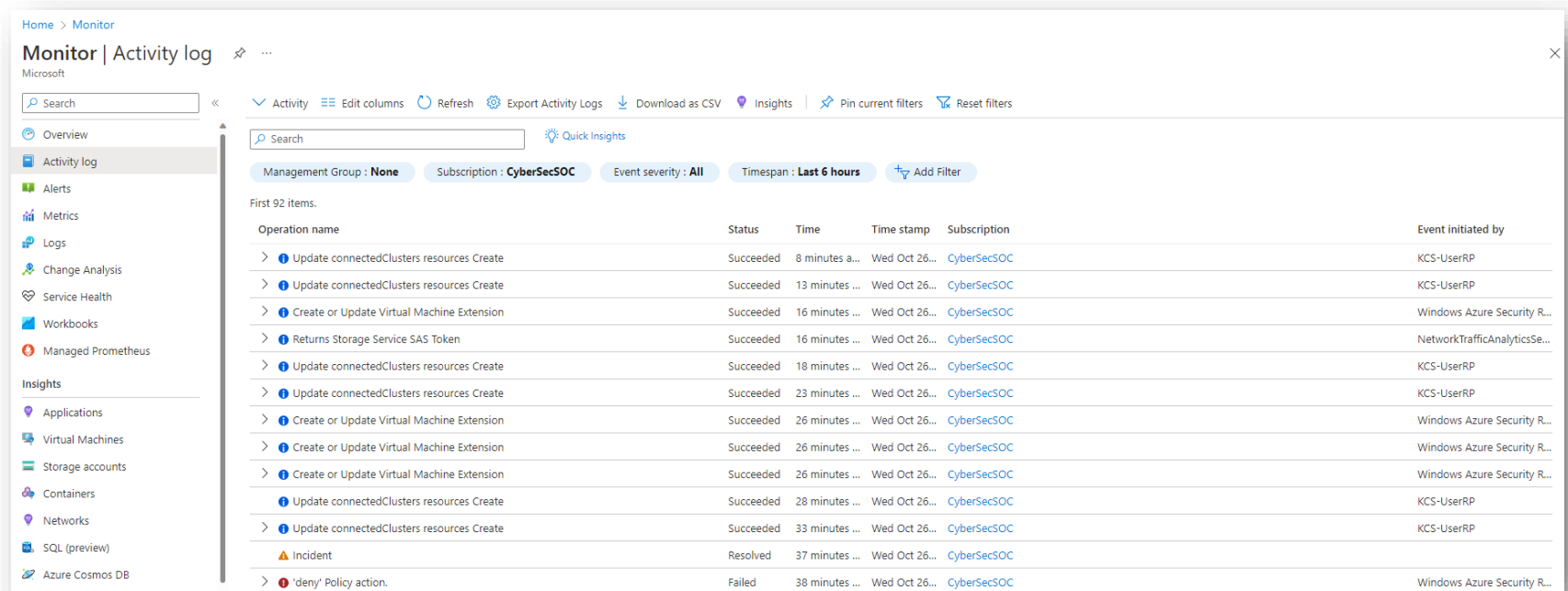
Azure Portal - Azure Active Directory Tenant Properties

Microsoft Azure Service Health Notifications Setup

As you'll see, Azure is the most nuanced and potentially complicated as it pertains to awareness of a Microsoft Data Breach as there can be incidents which only affect singular Azure Subscriptions as opposed to a Tenant-wide impact.

In these **Subscription-level, events**, in addition to a **'Toast' Pop-Up** that will appear when the admin authenticates into the **Azure Portal** (<https://portal.azure.com>), the email address associated with **Azure Subscription Admin/Sub RBAC Owner** will receive an email notification.

For your Security Team, Security Operations Center to be centrally aware of these notifications, it is necessary to configure a security notification **Policy Definition** in the **Azure Service Health** portal. Refer to this link to learn more on Azure Service Health <https://learn.microsoft.com/en-us/azure/service-health/alerts-activity-log-service-notifications-porta>



The screenshot displays the Azure Monitor 'Activity log' interface. The left sidebar contains navigation options: Overview, Activity log (selected), Alerts, Metrics, Logs, Change Analysis, Service Health, Workbooks, and Managed Prometheus. Below these are 'Insights' for Applications, Virtual Machines, Storage accounts, Containers, Networks, SQL (preview), and Azure Cosmos DB. The main panel shows filters for Management Group (None), Subscription (CyberSecSOC), Event severity (All), and Timespan (Last 6 hours). A table lists the first 92 items, showing various operations like 'Update connectedClusters resources Create' and 'Create or Update Virtual Machine Extension' with their status, time, and the user who initiated them.

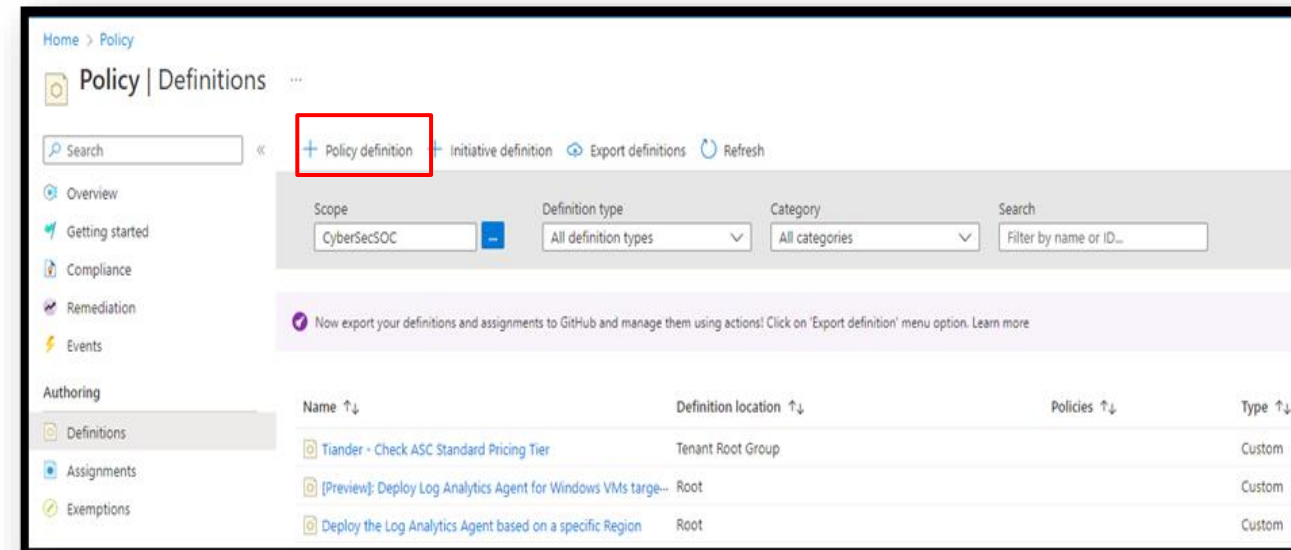
Operation name	Status	Time	Time stamp	Subscription	Event initiated by
> Update connectedClusters resources Create	Succeeded	8 minutes a...	Wed Oct 26...	CyberSecSOC	KCS-UserRP
> Update connectedClusters resources Create	Succeeded	13 minutes ...	Wed Oct 26...	CyberSecSOC	KCS-UserRP
> Create or Update Virtual Machine Extension	Succeeded	16 minutes ...	Wed Oct 26...	CyberSecSOC	Windows Azure Security R...
> Returns Storage Service SAS Token	Succeeded	16 minutes ...	Wed Oct 26...	CyberSecSOC	NetworkTrafficAnalyticsSe...
> Update connectedClusters resources Create	Succeeded	18 minutes ...	Wed Oct 26...	CyberSecSOC	KCS-UserRP
> Update connectedClusters resources Create	Succeeded	23 minutes ...	Wed Oct 26...	CyberSecSOC	KCS-UserRP
> Create or Update Virtual Machine Extension	Succeeded	26 minutes ...	Wed Oct 26...	CyberSecSOC	Windows Azure Security R...
> Create or Update Virtual Machine Extension	Succeeded	26 minutes ...	Wed Oct 26...	CyberSecSOC	Windows Azure Security R...
> Create or Update Virtual Machine Extension	Succeeded	26 minutes ...	Wed Oct 26...	CyberSecSOC	Windows Azure Security R...
> Update connectedClusters resources Create	Succeeded	28 minutes ...	Wed Oct 26...	CyberSecSOC	KCS-UserRP
> Update connectedClusters resources Create	Succeeded	33 minutes ...	Wed Oct 26...	CyberSecSOC	KCS-UserRP
> Incident	Resolved	37 minutes ...	Wed Oct 26...	CyberSecSOC	
> 'deny' Policy action.	Failed	38 minutes ...	Wed Oct 26...	CyberSecSOC	Windows Azure Security R...

Creating a Security Notification Policy Definition in Azure Service Health

1. Navigate to Policy, in the Azure portal (<https://portal.azure.com>). Click "+ Policy Definition"
2. Set the Definition location (*where the policy definition is saved*) to "Tenant Root Group", *specify a name, create a new category* "Service Health" and paste the contents of the linked Policy JSON configuration (https://github.com/akudrati/Sec_Threat_Intelligence/blob/main/26102002Abbas.json) into the "Policy Rule" box. Then click "Save".
3. At the Policy Definitions screen, type "service health" into the Search box, then click your newly created policy.
4. Click "Assign"
5. For Testing (Recommended), set "Scope" to an individual test subscription and click "Next" (do not click "Review + create" yet)
6. Uncheck "Only show parameters that need input or review", enter appropriate values for all parameters and click "Next"
7. Click "Create a remediation task", change the "System assigned

identity location" to "West US 2", and now click "Review + create"

8. Review details and then click "Create"
9. If all goes well, you should have three notifications, like these:
10. You may navigate to Policy -> Remediation -> Remediation tasks to track the progress
11. When the task is finished, the Remediation Status will change to "Complete"
12. Once this has completed, you can navigate to Service Health -> Health alerts to *review the configuration*.



Testing your alerts

Once you have tested this successfully, re-run steps to create a new assignment, but this time expand the “Scope” in step 5 to now target a management group that has multiple new/test subscriptions under it. If your management group or additional test subscriptions don’t exist, create a couple of new subscriptions, create a new management group at a level of your choice, and move the new subscriptions under this management group. (Management group docs: <https://docs.microsoft.com/en-us/azure/governance/management-groups/overview>)

To test applying this settings at both the management group level and to multiple subscriptions under the management group:

Click “**Prod**” (or the equivalent management group in your environment. Subscriptions expanded just for display), then click “**Select**”. Proceed with **step 6** onwards as per previous slide.

The screenshot displays the Azure portal interface for configuring a policy assignment. The main heading is "Email SoC on Security Advisory in Service Health". The "Scope" section is expanded, showing a tree view of management groups. The "Prod (prod)" management group is selected and highlighted with a red box. Below it, the "Subscription" section is also expanded, showing a list of subscriptions. One subscription is highlighted with a red box. The "Basics" section shows the policy definition and assignment name.

Microsoft Azure

Home > Policy > Email SoC on Security Advisory in Service Health >

Email SoC on Security Advisory in Service Health

Assign policy

Basics Parameters Remediation Non-compliance messages Review + create

Scope

Scope [Learn more about setting the scope *](#)

Tenant Root Group

Exclusions

Optionally select resources to exclude from the policy assignment.

Basics

Policy definition

Email SoC on Security Advisory in Service Health

Assignment name *

Email SoC on Security Advisory in Service Health

Scope

Management Group

▼ Tenant Root Group

▼ IT (it)

DMZ (dmz)

Prod (prod)

Subscription

Please choose a Subscription

Testing your alerts (Cont'd)

The end goal of this testing is to apply it to a **progressively higher management group level**, to have it **apply to all subscriptions**, until you're able to assign it to the **"Tenant Root Group"**, which will apply the policy to **ALL** existing as well as any newly created subscriptions.

(**Note:** the option to create a remediation task might not be available at this stage, but you will need to create it separately by browsing back to the assignment after it is created and has evaluated all subscriptions, and then clicking **"create remediation"**)

The screenshot displays the Microsoft Azure portal interface for configuring a policy assignment. The breadcrumb trail at the top indicates the path: Home > Policy > Email SoC on Security Advisory in Service Health >. The main heading is "Email SoC on Security Advisory in Service Health" with a three-dot menu icon to its right. Below the heading is the "Assign policy" link. The page features several tabs: "Basics" (selected), "Parameters", "Remediation", "Non-compliance messages", and "Review + create". Under the "Basics" tab, the "Scope" section shows a dropdown menu with "Prod" selected, which is highlighted by a red rectangular box. A link "Learn more about setting the scope *" is visible next to the dropdown. Below the scope, there is an "Exclusions" section with a text input field and a plus icon. The "Basics" section also includes a "Policy definition" dropdown set to "Email SoC on Security Advisory in Service Health". The "Assignment name *" field contains the text "Email SoC on Security Advisory in Service Health". The "Description" field is a large empty text area. The "Policy enforcement" section has two radio buttons, "Enabled" (selected) and "Disabled". The "Assigned by" field shows a user profile picture. At the bottom of the page, there are four buttons: "Review + create" (blue), "Cancel", "Previous", and "Next".

Testing your alerts (Cont'd)

Microsoft Azure

Search resources, services, and docs (G+)

Home > Service Health

Service Health | Health alerts

Search (Ctrl+)

Add service health alert

ACTIVE EVENTS

Service issues

Planned maintenance

Health advisories

Security advisories

HISTORY

Health history

RESOURCE HEALTH

Resource health

ALERTS

Health alerts

Details

History

Alert name

serviceHealthAlert

Alert criteria

Health event type

Security advisory

Subscription

Region(s)

all

Service(s)

All

Alert via

Action group name

serviceHealthActionGroup

Short name

SoCEmailAG

Actions

ACTION TYPE

ACTION DETAILS

NAME

Email

emailReceiver

Microsoft Azure

Search resources, services, and docs (G+)

Home > Policy

Policy | Remediation

Search (Ctrl+)

Refresh

Scope

3 selected

Overview

Getting started

Compliance

Remediation

Events

Authoring

Assignments

Definitions

Exemptions

Policies to remediate

Remediation tasks

Search

Filter by name or ID...

Remediation State

All

Start Time

Remediation Sta...

Policy Definition

Scope

Locations

Remediated Resources

Last Upd...

10/20/2021, 9:45 PM

Complete

Email SoC on Security Advisory in Service Health

All

1 out of 1

10/20/2021

Microsoft Azure

Search resources, services, and docs (G+)

Home > Policy

Policy | Remediation

Search (Ctrl+)

Refresh

Scope

3 selected

Overview

Getting started

Compliance

Remediation

Events

Authoring

Assignments

Definitions

Exemptions

Policies to remediate

Remediation tasks

Search

Filter by name or ID...

Remediation State

All

Start Time

Remediation Sta...

Policy Definition

Scope

Locations

Remediated Resources

Last Upd...

10/20/2021, 9:45 PM

Evaluating

Email SoC on Security Advisory in Service Health

All

Pending

10/20/2021

Testing your alerts (Cont'd)

✓

Remediation task creation succeeded

✕

Creating remediation task '1ef3adf4-0af2-4ce2-affc-3ce228c08b6b' was successful.

✓

Role Assignments creation succeeded

✕

All role assignments were created successfully.

✓

Creating policy assignment succeeded

✕

Creating policy assignment 'Email SoC on Security Advisory in Service Health' in 'rspitzpersonal' was successful. Please note that the assignment takes around 30 minutes to take effect.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Policy > Email SoC on Security Advisory in Service Health >

Email SoC on Security Advisory in Service Health

Assign policy

BasicsParametersRemediationNon-compliance messagesReview + create

Basics

Scope

Exclusions

Policy definition

Assignment name

Description

Policy enforcement

Assigned by

Parameters

resourceGroupName

emailAddress

Remediation

Create managed identity

System assigned identity location

Create a remediation task

Non-compliance messages

--

--

Email SoC on Security Advisory in Service Health

Email SoC on Security Advisory in Service Health

--

Enabled

ServiceHealth-Policy-EmailSoC-RG

Yes

westus2

Yes

No non-compliance messages associated with this assignment.

Create

Cancel

Previous

Next

Testing your alerts (Cont'd)

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Policy > Email SoC on Security Advisory in Service Health >

Email SoC on Security Advisory in Service Health ...

Assign policy

BasicsParametersRemediationNon-compliance messagesReview + create

By default, this assignment will only take effect on newly created resources. Existing resources can be updated via a remediation task after the policy is assigned. For deployIfNotExists policies, the remediation task will deploy the specified template. For modify policies, the remediation task will edit tags on the existing resources.

☒ Create a remediation task ⓘ

Policy to remediate

Email SoC on Security Advisory in Service Health ▾

Managed Identity

Policies with the deployIfNotExists and modify effect types need the ability to deploy resources and edit tags on existing resources respectively. To do this, choose between an existing user assigned managed identity or creating a system assigned managed identity. [Learn more about Managed Identity.](#)

☒ Create a Managed Identity ⓘ

Type of Managed Identity ⓘ

☒ System assigned managed identity ☐ User assigned managed identity

System assigned identity location

West US 2 ▾

Permissions

This identity will also be given the following permissions:

Contributor ⓘ

ⓘ

Role assignments (permissions) are created based on the role definitions specified in the policies.

Review + create

Cancel

Previous

Next

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Policy > Email SoC on Security Advisory in Service Health >

Email SoC on Security Advisory in Service Health ...

Assign policy

BasicsParametersRemediationNon-compliance messagesReview + create

Scope

Scope [Learn more about setting the scope *](#)

██████████ ✓ ...

Exclusions

Optionally select resources to exclude from the policy assignment.

██████████ ...

Basics

Policy definition

Email SoC on Security Advisory in Service Health

Assignment name * ⓘ

Email SoC on Security Advisory in Service Health

Description

Policy enforcement ⓘ

Enabled

Disabled

Assigned by

██████████

Review + create

Cancel

Previous

Next

Testing your alerts (Cont'd)

Microsoft Azure

Search resources, services, and docs (G+)

[Home](#) > [Policy](#) >

Email SoC on Security Advisory in Service Health

Policy definition

Assign

Edit definition

Duplicate definition

Delete definition

Export definition

Essentials

Name

: Email SoC on Security Advisory in Service Health

Description

: --

Available Effects

: DeployIfNotExists, AuditIfNotExists, Disabled

Category

: Service Health

Definition

Assignments (0)

Parameters

1

{

2

"properties": {

3

"displayName": "Email SoC on Security Advisory in Service Health",

4

"policyType": "Custom",

Microsoft Azure

Search resources, services, and docs (G+)

[Home](#) > [Policy](#)

Policy | Definitions

...

Search (Ctrl+/)

+ Policy definition

+ Initiative definition

Export definitions

Refresh

Overview

Getting started

Compliance

Remediation

Events

Authoring

Assignments

Definitions

Exemptions

Scope

3 selected

...

Definition type

All definition types

Type

All types

Category

All categories

Search

service health

Now export your definitions and assignments to GitHub and manage them using actions! Click on 'Export definition' menu option. Learn more

Name ↑↓

Definition location ↑↓

Policies ↑↓

Type ↑↓

Definition type ↑↓

Category ↑↓

Email SoC on Security Advisory in Service Health

Tenant Root Group

Custom

Policy

Service Health

Testing your alerts (Cont'd)

Microsoft Azure

Search resources, services, and docs (G+J)

Home > Policy >

Policy definition

New Policy definition

BASICS

Definition location *

Tenant Root Group

Name *

Email SoC on Security Advisory in Service Health

Description

Category

Create new Use existing

Service Health

POLICY RULE

Import sample policy definition from GitHub

Learn more about policy definition structure

```
249 "defaultValue": "ServiceHealthActionGroup"
250 },
251 "actionGroupShortName": {
252   "type": "String",
253   "metadata": {
254     "displayName": "actionGroupShortName",
255     "description": "Short name for the Action group."
256   },
257   "defaultValue": "SoCEmailAG"
258 },
259 "emailAddress": {
260   "type": "String",
261   "metadata": {
262     "displayName": "emailAddress",
263     "description": "Email address."
264   },
265 },
266 "activityLogAlertName": {
267   "type": "String",
268   "metadata": {
269     "displayName": "activityLogAlertName",
270     "description": "Name for the Activity log alert."
271   },
272   "defaultValue": "serviceHealthAlert"
273 },
274 "effect": {
275   "type": "String",
276   "metadata": {
277     "displayName": "Effect",
278     "description": "Enable or disable the execution of the policy"
279   },
280   "allowedValues": [
281     "DeployIfNotExists",
282     "AuditIfNotExists",
283     "Disabled"
284   ],
285   "defaultValue": "DeployIfNotExists"
286 },
287 }
288 }
```

Role definitions

Contributor

Save Cancel

Microsoft Azure

Search resources, services, and docs (G+J)

Home > Policy

Policy | Definitions

Search (Ctrl+J)

Policy definition Initiative definition Export definitions

Overview Getting started Compliance Remediation Events

Scope 3 selected Definition type All definition types

Now export your definitions and assignments to GitHub and manage them



What exactly is a “service incident”?

Service incident is the term that Microsoft uses to refer to an event (or series of events) that typically causes multiple customers to have a degraded experience with one or more of our services.

These incidents are effectively platform issues that cause **unplanned downtime** – including unavailability, performance degradation, and problems interfering with service management.

When an Azure incident is declared, **we send updates** to all impacted subscriptions to provide visibility and relevant guidance.

Why should I use Service Health instead of status.azure.com?

Many customers check **status.azure.com** at the first signs of potential issues, to see if there are known issues on the Azure platform at the time. This page shows widespread issues, but doesn't show smaller incidents that impact fewer customers.

Azure Service Health (within the Azure portal) knows which subscriptions you manage, so it shows a much more accurate view of any known issues impacting your resources. It also lets you configure health alerts, to find out about any issues through your preferred communication channel(s) – email, SMS, webhook, etc.

When do I need to open a Microsoft support case?

During an **active incident**, many customers and partners contact support (or their account teams) asking for information – but all of the details about an active incident, including the latest updates, are available in Service Health and through its health alerts.

Customers can and should contact Microsoft support to troubleshoot **issues that don't match** the impact described in Service Health, but don't need to contact support just for updates. This way, support engineers are available to assist customers with failover activities, or to help with any unrelated but urgent issues.

Before an incident



1. Understand **resilience** and ensure that all of your critical services are architected for high availability.



2. Get familiar with **Azure Service Health** in the Azure portal – your 'go to' place in case of issues.



3. Configure **Service Health alerts** to notify you about any issues – by email, SMS, webhook, etc.



4. Consider **Resource Health alerts** or **Scheduled Events** to inform you of resource-specific issues.

During an incident



1. Review **Azure Service Health** within the Azure portal for the latest updates from our engineers.



2. If there are issues accessing Service Health or the portal itself, check the public **Azure Status page**.



3. If there are ever issues with the Status page, check for any updates via **@AzureSupport** on Twitter.



4. If your impact/issues don't match the incident (or if these persist after mitigation) **contact support**.

What exactly is a “service incident”?

Service incident is the term that Microsoft uses to refer to an event (or series of events) that typically causes multiple customers to have a degraded experience with one or more of our services.

These incidents are effectively platform issues that cause **unplanned downtime** – including unavailability, performance degradation, and problems interfering with service management.

When a Microsoft 365 incident is declared, **we send updates** to all impacted tenants to provide visibility and relevant guidance.

Why should I use Service Health instead of status.office.com?

The **status.office.com** page is only used when an active service issue is preventing customers from accessing the Microsoft 365 admin center or its Service Health functionality, so this public page should just be considered a backup notification page.

Service Health (within the Microsoft 365 admin center) knows which tenants you manage, so it shows a much more accurate view of any known issues impacting your services.

When do I need to open a Microsoft support case?

During an **active incident**, many customers and partners contact support (or their account teams) asking for information – but all of the details about an active incident, including the latest updates, are available in Service Health and through its health alerts.

Customers can and should contact Microsoft support to troubleshoot **issues that don't match** the impact described in Service Health, but don't need to contact support just for updates. This way, support engineers are available to assist customers with any unrelated but urgent issues.

Before an incident



1. Get familiar with **Service health** within the M365 admin center – your ‘go to’ place in case of issues.



2. Install the Microsoft 365 **Admin mobile app** to be updated about service issues while on the go.



3. Consider the **service communications API V2** for problem management integration/automation.

During an incident



1. Review **Service Health** in the M365 admin center for the latest updates from our engineers.



2. If your issue is not already posted there, use the **'report an issue'** feature to notify Microsoft



3. If Service health is unavailable, refer to the **M365 status page** or **@MSFT365Status** on Twitter.



4. If your impact/issues don't match the incident (or if these persist after mitigation) **contact support**.

What exactly is a “service incident”?

Service incident is the term that Microsoft uses to refer to an event (or series of events) that typically causes multiple customers to have a degraded experience with one or more of our services.

These incidents are effectively platform issues that cause **unplanned downtime** – including unavailability, performance degradation, and problems interfering with service management.

When a Dynamics 365 incident is declared, **we send updates** to all impacted tenants to provide visibility and relevant guidance.

Why should I use Service Health instead of status.office.com?

The **status.office.com** page is only used when an active service issue is preventing customers from accessing the Microsoft 365 admin center or its Service Health functionality, so this public page should just be considered a backup notification page.

Service Health (within the Microsoft 365 admin center) knows which tenants you manage, so it shows a much more accurate view of any known issues impacting your services.

When do I need to open a Microsoft support case?

During an **active incident**, many customers and partners contact support (or their account teams) asking for information – but all of the details about an active incident, including the latest updates, are available in Service Health and through its health alerts.

Customers can and should contact Microsoft support to troubleshoot **issues that don’t match** the impact described in Service Health, but don’t need to contact support just for updates. This way, support engineers are available to assist customers with failover activities, or to help with any unrelated but urgent issues.

Before an incident



1. Get familiar with **Service health** within the M365 admin center – your ‘go to’ place in case of issues.



2. Install the Microsoft 365 **Admin mobile app** to be updated about service issues while on the go.



3. Consider using the **service communications API** for problem management integration/automation.

During an incident



1. Review **Service Health** in the M365 admin center for the latest updates from our engineers.



2. If there are issues accessing Service Health or the admin center itself, check the **M365 status page**.



3. If your impact/issues don’t match the incident (or if these persist after mitigation) **contact support**.

How to Engage Microsoft's IR Team - DART

Possible Incident

- Escalate all security incidents via CSS by opening a Sev A support case with the Security queue (on-prem) or O365 Security & Compliance queue (O365) and sending a note to EngageIR - (EngageIR@Microsoft.com) along with the CSS case #.

Confirmed Incident

- Cybersecurity Incident Response (CIR) escalations of confirmed on-premise compromises, or Office 365/AAD compromises, will be directed to dartalert@microsoft.com.
- Please review <https://aka.ms/dartalert> first.
- Include the CSS case number, customer name, and a brief description of the issue.

Reference and Learning material

- **General Guide** Incident response process and planning
- **Overview for Microsoft security products and resources for new-to-role and experienced analysts:** <https://review.learn.microsoft.com/en-us/security/compass/incident-response-overview>
- **Planning checklist for your SOC:** <https://review.learn.microsoft.com/en-us/security/compass/incident-response-planning?branch=main>
- **Playbooks for detailed guidance on responding to common attack methods:** <https://review.learn.microsoft.com/en-us/security/compass/incident-response-playbooks?branch=main>
- **Microsoft 365 Defender incident response :** <https://review.learn.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?branch=main&view=o365-worldwide>
- **Microsoft Sentinel incident response:** <https://review.learn.microsoft.com/en-us/azure/sentinel/investigate-cases?branch=main>



Know & Reach Abbas:

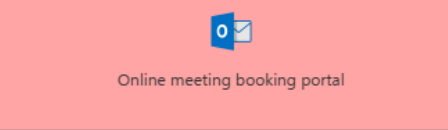
- My LinkedIn
- Abbas Kudrati (@askudrati) / Twitter
- My YouTube Channel (new)
- Abbas Kudrati: books, biography, latest up...
- Abbas Kudrati, Author at Microsoft Securit...
- My conference's slides collection
- My monthly newsletter archive.
- GitHub Repo Collection

My Short Bio / Profile

List of cool collections of interesting portals a...

- Cybersecurity-copilot.com
- Security Adoption Resources
- The History of Microsoft Azure
- Chief Information Security Officer (CISO) ...
- Mark Simos's List
- Microsoft 365 Licensing
- Collection of Microsoft Portals Link
- CISO MindMap 2023: What do InfoSec Pro...
- CISO Bookmarks
- John Savill's Technical Training

Online meeting booking portal for Abbas Ku...



Microsoft Products Blogs

- Microsoft Security Blog
- Microsoft Security for all
- Azure Security Blogs
- Security, Compliance, and Identity Blog
- Microsoft Entra (Azure AD) Blog
- Microsoft 365 Blog
- Microsoft Defender Threat Intelligence Blog
- Zero Trust Security
- Zero Trust Guidance Center
- Microsoft Cloud Adoption Framework for ...
- Tech Community Blogs
- https://aka.ms/MustLearnAISecurity

www.microsoft.com/en-us/security/blog (Liv...

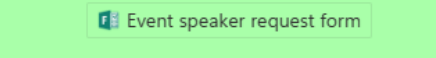
Best EDR Of The Market (BEOTM) – Endpoint Detection and Response Testing Tool

5 months ago – BestEDROfTheMarket is a naive user-mode EDR (Endpoint Detection and Response) tool designed to...

AgentSmith HIDS – Host Based Intrusion Detection

9 months ago – AgentSmith HIDS is a powerful

Event speaker request form for Abbas Kudrati



Microsoft Threat Intel Collection

- Global Threat Activity
- Defender for Threat Intelligence
- Microsoft Threat Intelligence Blog
- Microsoft Security Intelligence (@MsftSecI...
- Threat Briefs
- Threat Actor Insights and Profiles
- Security Insider Reports (Cyber signals, Nat...
- Microsoft Digital Defense Report and Secu...
- Human-operated ransomware
- Lessons learned from the Microsoft SOC
- Sneak Peak of how Microsoft Runs its Cyb...

Msrc-blog.microsoft.com/feed/report/list (Li...

Updating our Vulnerability Severity Classification for AI Systems

10 months ago – The Microsoft Security Response Center (MSRC) is always looking for ways to provide clarity and transparency around how w...

Congratulations to the MSRC 2023 Most Valuable Security Researchers!

10 months ago – The Microsoft Researcher Recognition Program offers public thanks and recognition to security researchers who help...

Microsoft Bug Bounty Program Year in Review...

Incident and Crisis Management relate... Shared

- New Microsoft Incident Response team gu...
- Report a Microsoft issue or vulnerability
- Microsoft Bounty Programs
- Microsoft Security Response Center
- Prepare your security posture for your first...
- Responding to your first incident
- Incident response playbooks
- Incident response with Microsoft 365 Defe...
- Incident response overview
- Incident Response Reference Guide
- Incident response Insights
- Microsoft On The Issues
- What is the Security Update Validation Pro...
- Microsoft Active Protections Program
- How the Microsoft Incident Response tea...
- NIST Guide for Cybersecurity Event Recovery
- Security Operations Self-Assessment Tool| ...
- What's New: SOC Process Framework is N...
- SOC-CMM Maturity Model tool
- The Evolution of Security Operations and S...
- Best Practices and Lessons Learned from t...

Microsoft Product Ninja Trainings

- Security 101 Training
- Become a Microsoft Sentinel Ninja: The co...
- Become a Microsoft Defender for Cloud Ni...
- Microsoft-Defender-for-Cloud/Labs at mai...
- Microsoft Defender External Attack Surface...
- Become a Microsoft Defender for Endpoint...
- Become a Microsoft 365 Defender Ninja
- Become a Microsoft Defender for Office 36...
- Microsoft Defender for Cloud Apps Ninja T...
- Microsoft Defender for Identity Ninja Traini...
- Microsoft Defender for IoT Ninja Training
- Microsoft Purview Compliance Manager (...)
- Azure Network Security Ninja Training
- Chief Information Security Officer (CISO) ...
- Microsoft Learn: Build skills that open door...
- Join Microsoft Security Community

Microsoft Security Update Guide (Live feed)

- Chromium: CVE-2024-5274 Type Confusion in ...
- Chromium: CVE-2024-5160 Heap buffer overfl...
- Chromium: CVE-2024-5158 Type Confusion in ...
- Chromium: CVE-2024-5157 Use after free in Sc...
- Chromium: CVE-2024-5159 Heap buffer overfl...

Appendix: Secure Foundation

A secure foundation at global scale

Each **physical datacenter**
protected with world-class,
multi-layered protection



Over **100**
datacenters
across the
planet

Global cloud infrastructure
with custom hardware and
network protection



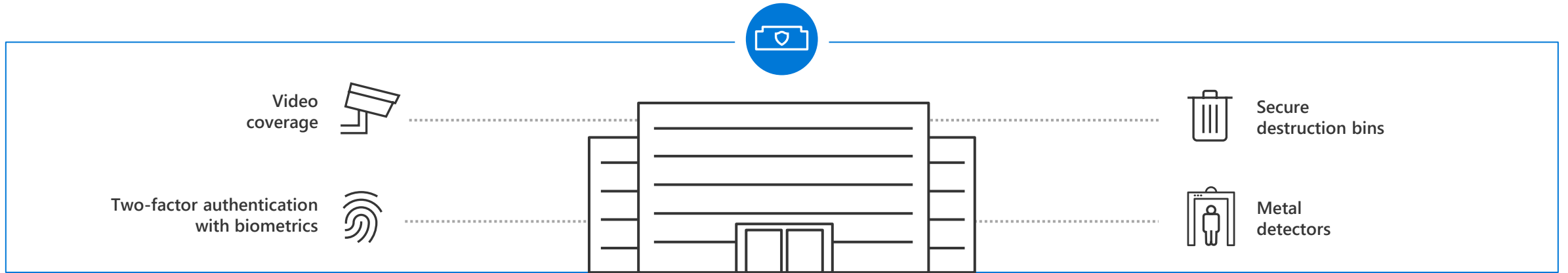
Secured with cutting-
edge **operational security**

- Restricted access
- 24x7 monitoring
- Global security experts



Secure Foundation

Physical datacenter security



Global datacenters designed and operated by Microsoft

Protected by industry leading security systems

Extensive layers of protection

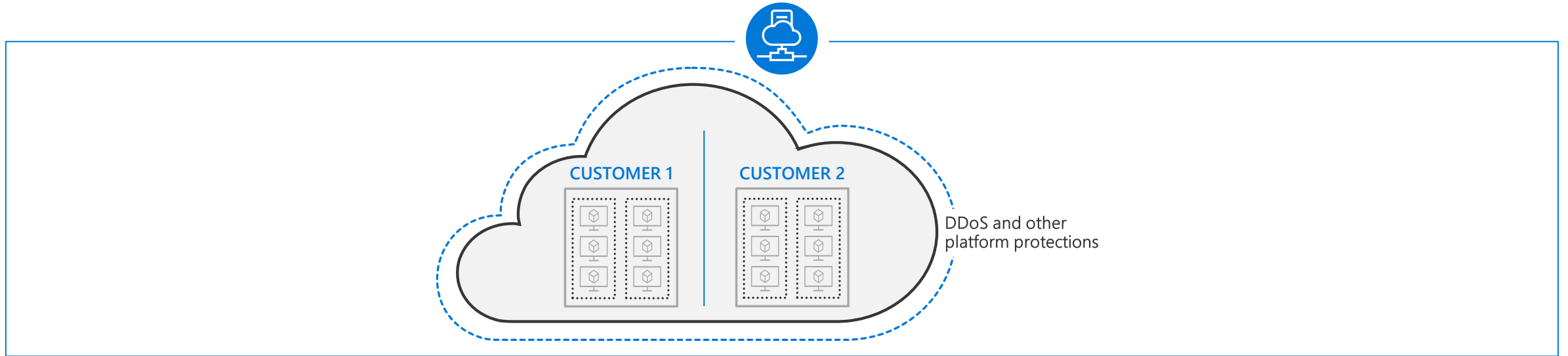
Helps reduce unauthorized physical access

Industry leading compliance

Most comprehensive portfolio of internationally recognized standards and certifications

Secure Foundation

Global Cloud Infrastructure



Customer data safeguards

Data, network segregation. Platform level protections like DDoS

Secure hardware

Custom-built hardware with integrated security and attestation

Continuous testing

War game exercises by Microsoft teams, continuous monitoring

Secure Foundation

Operational Security



Restricted access for Microsoft admins

On-demand only access to the platform

Grants least privilege required to complete task

Incident response

Multi-step incident response process

Focus on containment & recovery

8500+ security professionals

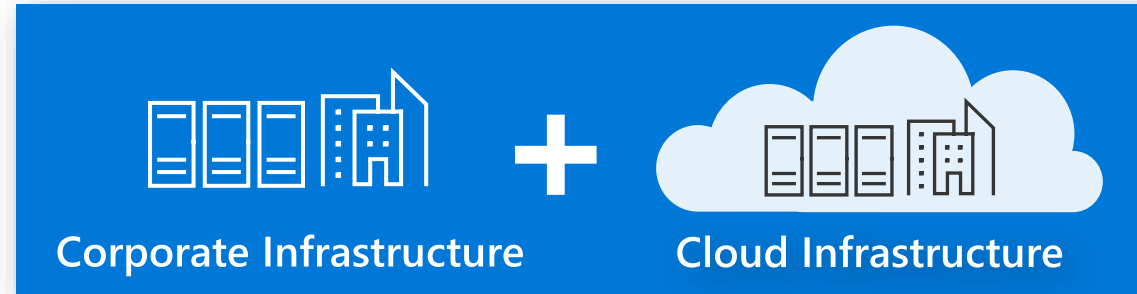
Working to harden, patch and protect the platform

24x7 monitoring for threats

Microsoft protecting Microsoft

Hardening (Physical, OS
App/Data, etc.)
Whitelisting
Auto-Patching
and more...

**Traditional
Defenses**



Continual Scanning
Penetration Testing
Red Team Ops
Bug Bounties

Attackers View 



People

Background Checks
Security Training
Conferences



Least Privilege

Least Privilege Access
Just-in-time Access
and more...



Authentication

Multi-factor Auth
Anomaly Detection



Privileged Access Workstations

Secure Access Workstations
isolation from web/email risks



**Rigorous Security
For Privileged Access**

Automated Assessments
Secure DevOps toolkit
and more...

**Security
Development
Lifecycle** 

CDOC



**Monitoring &
Vigilance**



Working together: coordinated response



Using intelligence gained, Microsoft security teams work together to secure our platform

Cyber Defense Operations Center (CDOC)

Microsoft's finest combating threats in real time

Digital Security and Risk Engineering (DSRE)

Keeping all Microsoft data secure

Detection and Response Team (DART)

Helping customers with incident response

Microsoft Digital Crimes Unit (DCU)

Tracking cybercrime in real time



Microsoft Threat Intelligence Center (MSTIC)

Infusing threat intelligence into products and services

Microsoft Security Response Center (MSRC)

Defending customers when things go pear-shaped

Microsoft Security Intelligence (MSI)

Educating about the current state of threats

Cyber Resiliency

Aligned - Align and Integrate cybersecurity with business strategy, processes, and initiatives



Mindset

Adopt a mindset that **assumes compromise** and focus on:

- Raising attacker costs/friction
- Rapid response/recovery



Cloud

Use cloud technologies to

- Tap into community resources and knowledge
- Accelerate innovation (security and productivity)



Hygiene

Pay down “technical debt” of legacy systems & decisions

1. Commit to burning down list
2. Start with top risks



Defender Success = Attacker Pain/Failure

A. Hard to get in (high cost/friction)

B. Quickly discovered and kicked out

Thank you!

Abbas Kudrati
APAC Chief Cybersecurity Advisor
Abbas.Kudrati@microsoft.com
<https://aka.ms/abbas>