WELCOME TO

Identifying Opportunities to Resolve Your Security Gaps

A PART OF THE CYBERSECURITY WEBINAR SERIES

We'll get started in just a few minutes

If you have any questions, or are having issues,
please email **membership@nstxl.org**.

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code:

18AUG

2020 Cybersecurity Webinar Series:

Identifying Opportunities to Resolve Your Security Gaps

August 18, 2020

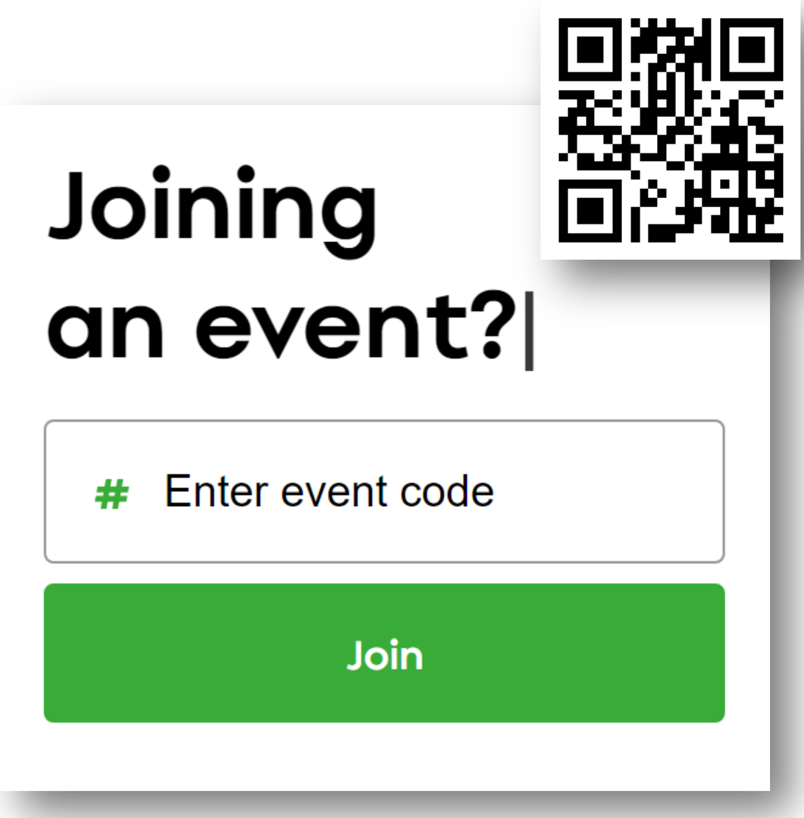
Brought to you by

ADVISICON & NSTXL

NATIONAL SECURITY TECHNOLOGY ACCELERATOR

Submit Questions

- Slido is how we will manage questions for this session; questions will be addressed at the end in the Q&A session
- To access Slido, please visit www.slido.com
- Enter the event code 18AUG in the event code box, hit “Join,” and input your questions



Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: 18AUG

ADVISICON

Our **MISSION** is to deliver technology, tools and training to maximize impact, productivity and purpose.

Project Management Institute.

Microsoft Partner

Microsoft

Gold Project and Portfolio Management
Gold Data Analytics
Gold Cloud Productivity
Gold Windows and Devices
Silver Collaboration and Content

MVP Microsoft® Most Valuable Professional

ADVISICON

MICROSOFT 365 SECURITY

Identifying Opportunities to Resolve your Security Gaps

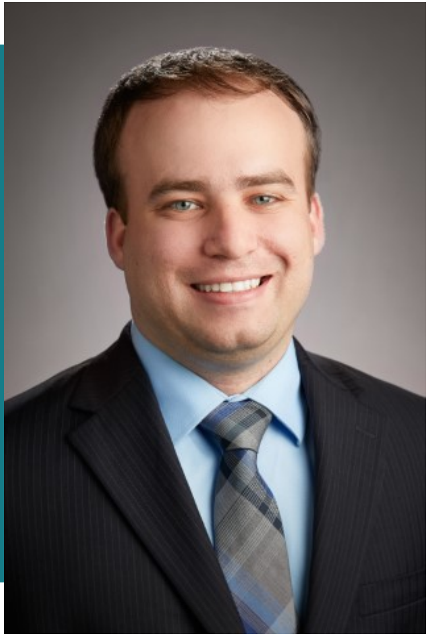
8/18/2020

Kevin Brouder
VP Technology Engineering & Services

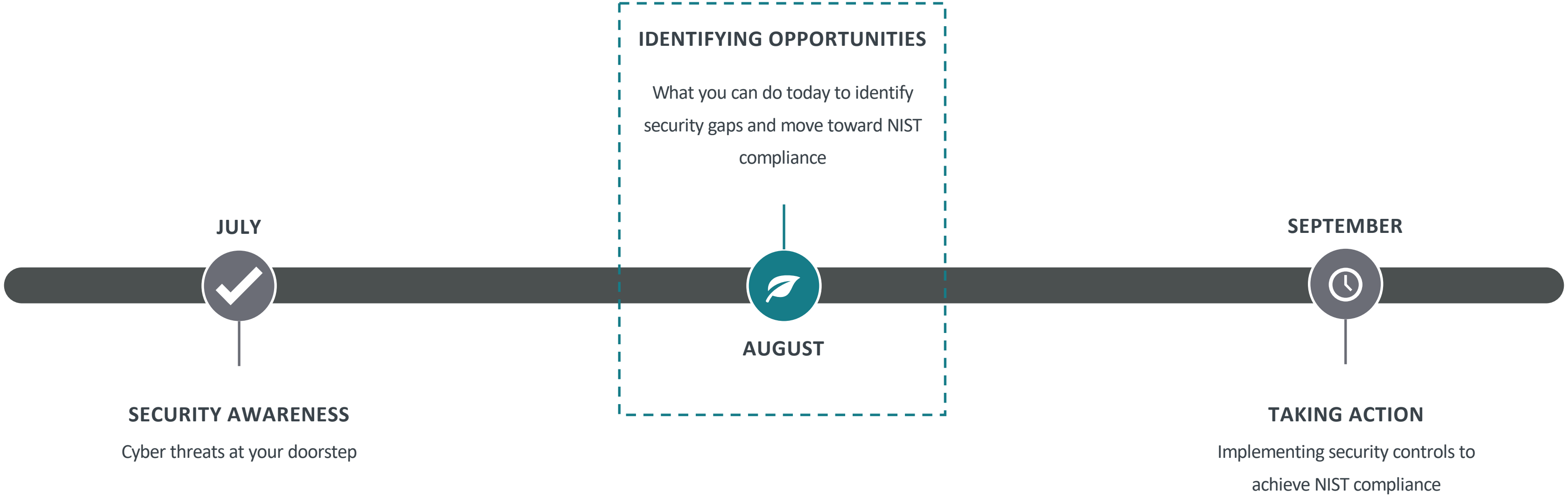
ABOUT THE PRESENTER KEVIN BROUDER *MCP*

VP Technology Engineering & Services

- BACKGROUND IN ENGINEERING & AEROSPACE
- EXPERIENCED PROJECT MANAGER & MICROSOFT PPM EXPERT
- IT INFRASTRUCTURE AND SECURITY EXPERTISE
- ACCOMPLISHED SOFTWARE DEVELOPER AND INTEGRATION SME
- POWER BI & SQL SERVER REPORTING SERVICES EXPERT
- VP TECHNOLOGY ENGINEERING & SERVICES ADVISICON



WEBINAR SERIES: SECURITY AND NIST COMPLIANCE



JULY

SECURITY AWARENESS

Cyber threats at your doorstep

AUGUST

IDENTIFYING OPPORTUNITIES

What you can do today to identify security gaps and move toward NIST compliance

SEPTEMBER

TAKING ACTION

Implementing security controls to achieve NIST compliance

TODAY'S AGENDA

- *Level Set*: Microsoft Compliance Center
- *Quick Wins:* Azure Active Directory
- *Achieve NIST 3.3:* Unified Audit Logging
- *Identifying Vulnerabilities:* Cloud App Security & Identity Protection
- *Beyond the Basics*: Comprehensive Enterprise Solution
- Demo!

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: 18AUG

MICROSOFT COMPLIANCE CENTER

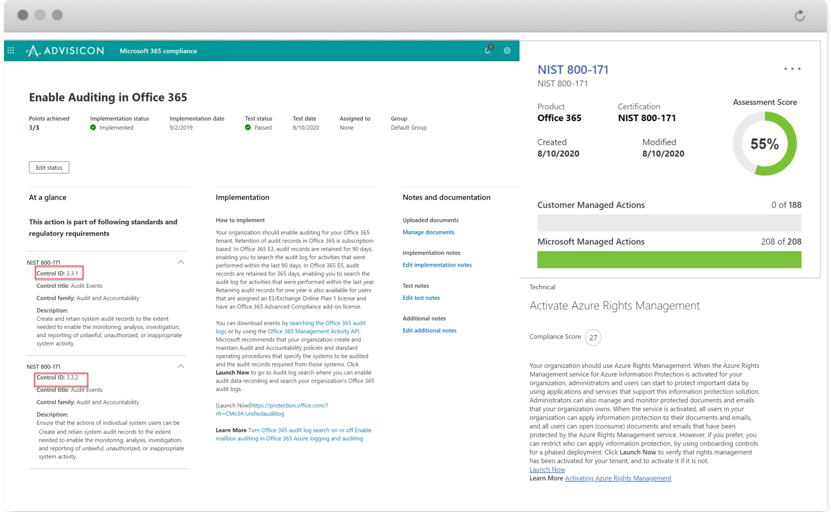
Utilize Microsoft 365 Compliance Center and Manager to track and assist with achieving NIST Compliance

EASY START FOR NIST COMPLIANCE

Microsoft 365 Compliance Center has a NIST 800-171 template built in to help you track and organize all the controls, identify improvement areas, and assign and track implementations.

Key Features:

- **Compliance Score:** Rates compliance levels against controls to identify areas for improvement.
- **Improvement Actions:** Recommendations for improving compliance that can be assigned, tracked, and recorded in the compliance center
- **Microsoft's Secure Environment:** Simply utilizing Microsoft's FEDRAMP approved environment wont make you NIST compliant, but this dashboard provides evidence of the elements achieved by just using Microsoft 365



Enable Auditing in Office 365

Points achieved	Implementation status	Implementation date	Test status	Test date	Assigned to	Group
3/3	✓ Implemented	9/2/2019	✓ Passed	8/10/2020	None	Default Group

Edit status

At a glance

This action is part of following standards and regulatory requirements

NIST 800-171

Control ID: 3.3.1

Control title: Audit Events

Control family: Audit and Accountability

Description:
Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.

NIST 800-171

Control ID: 3.3.2

Control title: Audit Events

Control family: Audit and Accountability

Description:
Ensure that the actions of individual system users can be
Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.

Implementation

How to implement

Your organization should enable auditing for your Office 365 tenant. Retention of audit records in Office 365 is subscription-based. In Office 365 E3, audit records are retained for 90 days, enabling you to search the audit log for activities that were performed within the last 90 days. In Office 365 E5, audit records are retained for 365 days, enabling you to search the audit log for activities that were performed within the last year. Retaining audit records for one year is also available for users that are assigned an E3/Exchange Online Plan 1 license and have an Office 365 Advanced Compliance add-on license.

You can download events by searching the Office 365 audit logs or by using the Office 365 Management Activity API. Microsoft recommends that your organization create and maintain Audit and Accountability policies and standard operating procedures that specify the systems to be audited and the audit records required from those systems. Click **Launch Now** to go to Audit log search where you can enable audit data recording and search your organization's Office 365 audit logs.

[Launch Now]https://protection.office.com/?rfr=CMv3#/unifiedauditlog

Learn More Turn Office 365 audit log search on or off Enable mailbox auditing in Office 365 Azure logging and auditing

Notes and documentation

Uploaded documents

Manage documents

Implementation notes

Edit implementation notes

Test notes

Edit test notes

Additional notes

Edit additional notes

NIST 800-171

NIST 800-171

Product	Certification
Office 365	NIST 800-171

Created	Modified
8/10/2020	8/10/2020

Assessment Score

55%

Customer Managed Actions 0 of 188

Microsoft Managed Actions 208 of 208

Technical

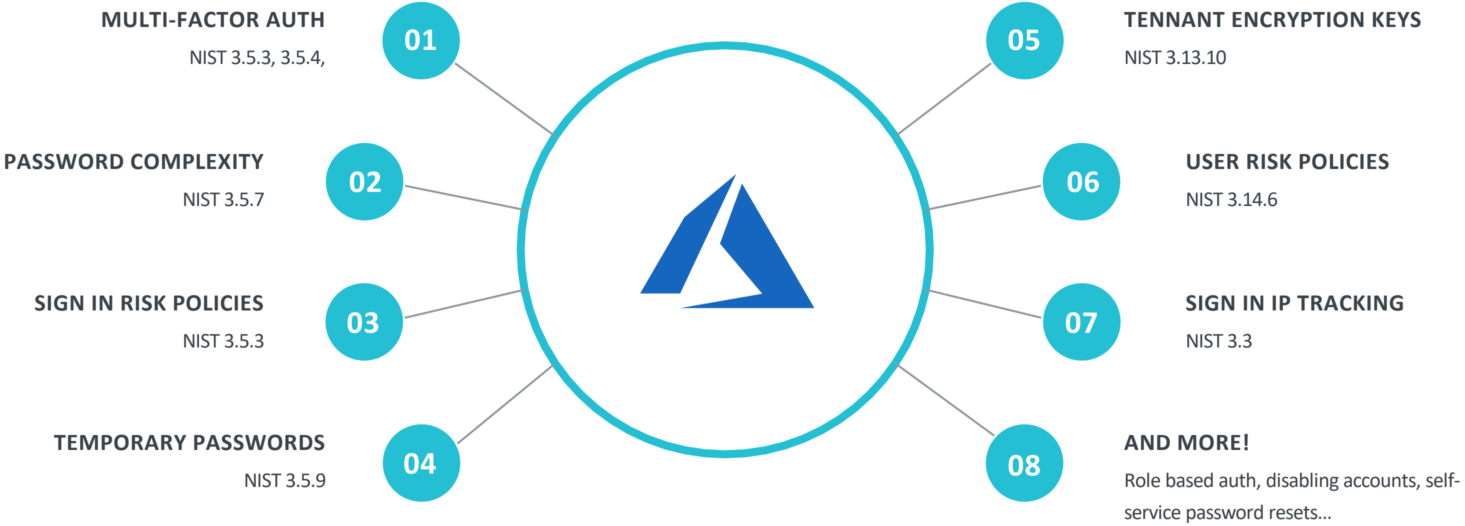
Activate Azure Rights Management

Compliance Score 27

Your organization should use Azure Rights Management. When the Azure Rights Management service for Azure Information Protection is activated for your organization, administrators and users can start to protect important data by using applications and services that support this information protection solution. Administrators can also manage and monitor protected documents and emails that your organization owns. When the service is activated, all users in your organization can apply information protection to their documents and emails, and all users can open (consume) documents and emails that have been protected by the Azure Rights Management service. However, if you prefer, you can restrict who can apply information protection, by using onboarding controls for a phased deployment. Click **Launch Now** to verify that rights management has been activated for your tenant, and to activate it if it is not.
Launch Now
Learn More Activating Azure Rights Management

AZURE ACTIVE DIRECTORY BENEFITS

Properly configuring and taking advantage of AAD features can boost NIST Compliance quickly



01 **MULTI-FACTOR AUTH**
NIST 3.5.3, 3.5.4,

02 **PASSWORD COMPLEXITY**
NIST 3.5.7

03 **SIGN IN RISK POLICIES**
NIST 3.5.3

04 **TEMPORARY PASSWORDS**
NIST 3.5.9

05 **TENNANT ENCRYPTION KEYS**
NIST 3.13.10

06 **USER RISK POLICIES**
NIST 3.14.6

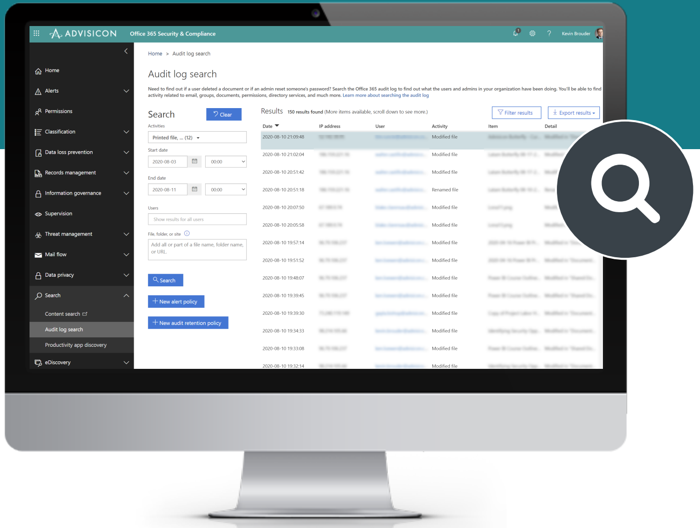
07 **SIGN IN IP TRACKING**
NIST 3.3

08 **AND MORE!**
Role based auth, disabling accounts, self-service password resets…

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: 18AUG

UNIFIED AUDIT LOG AND NIST 3.3

How to meet NIST 3.3 Audit and Accountability with Office 365 Unified Audit Log Search



Audit log search

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. Learn more about searching the audit log

Search

Activities: Printed file, ... (12)

Start date: 2020-08-03 00:00

End date: 2020-08-11 00:00

Users: Show results for all users

File, folder, or site: Add all or part of a file name, folder name, or URL.

Results 150 results found (More items available, scroll down to see more.)

Date	IP address	User	Activity	Item	Detail
2020-08-10 21:09:48	[redacted]	[redacted]	Modified file	[redacted]	[redacted]
2020-08-10 21:02:04	[redacted]	[redacted]	Modified file	[redacted]	[redacted]
2020-08-10 20:51:42	[redacted]	[redacted]	Modified file	[redacted]	[redacted]
2020-08-10 20:51:18	[redacted]	[redacted]	Renamed file	[redacted]	[redacted]
2020-08-10 20:07:50	[redacted]	[redacted]	Modified file	[redacted]	[redacted]
2020-08-10 20:05:58	[redacted]	[redacted]	Modified file	[redacted]	[redacted]
2020-08-10 19:57:14	[redacted]	[redacted]	Modified file	[redacted]	[redacted]
2020-08-10 19:51:52	[redacted]	[redacted]	Modified file	[redacted]	[redacted]
2020-08-10 19:48:07	[redacted]	[redacted]	Modified file	[redacted]	[redacted]
2020-08-10 19:39:45	[redacted]	[redacted]	Modified file	[redacted]	[redacted]
2020-08-10 19:39:30	[redacted]	[redacted]	Modified file	[redacted]	[redacted]
2020-08-10 19:34:33	[redacted]	[redacted]	Modified file	[redacted]	[redacted]
2020-08-10 19:33:08	[redacted]	[redacted]	Modified file	[redacted]	[redacted]
2020-08-10 19:32:14	[redacted]	[redacted]	Modified file	[redacted]	[redacted]

NIST 3.3: AUDIT AND ACCOUNTABILITY

NIST 3.3 is all about keeping monitoring and logging system activity, authorized and unauthorized. Office 365's Unified Audit Log helps achieve all NIST 3.3 controls

Unified Log: Brings Azure AD components into a unified interface for logs and records 3.3.1-2

Search and Report: Search logs and build reports to investigate and analyze unlawful, suspicious, or unusual activity 3.3.3-7

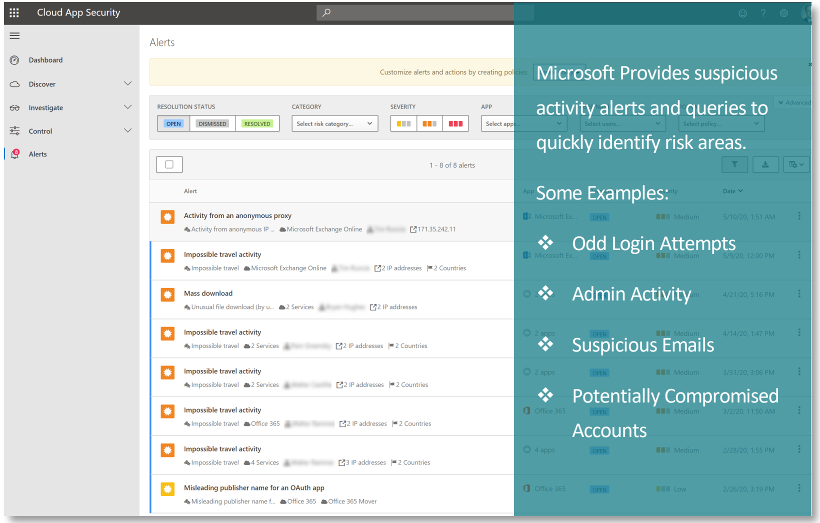
Alerts: Can be configured for policy changes or deletions to satisfy 3.3.8

Admin Roles: Set to ensure secure access to log information, along with retention polices and additional capabilities for admin approval workflows. 3.3.8-9

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: 18AUG

ACTIVITY MONITORING CLOUD APP SECURITY

Utilize Built in Queries to Identify Security Risks



Alerts

Customize alerts and actions by creating policies:

RESOLUTION STATUS: OPEN | DISMISSED | RESOLVED
CATEGORY: Select risk category...
SEVERITY
APP: Select apps...

1 - 8 of 8 alerts

Alert

- Activity from an anonymous proxy — Activity from anonymous IP ... · Microsoft Exchange Online · [redacted] · 171.35.242.11
- Impossible travel activity — Impossible travel · Microsoft Exchange Online · [redacted] · 2 IP addresses · 2 Countries
- Mass download — Unusual file download (by u... · 2 Services · [redacted] · 2 IP addresses
- Impossible travel activity — Impossible travel · 2 Services · [redacted] · 2 IP addresses · 2 Countries
- Impossible travel activity — Impossible travel · 2 Services · [redacted] · 2 IP addresses · 2 Countries
- Impossible travel activity — Impossible travel · Office 365 · [redacted] · 2 IP addresses · 2 Countries
- Impossible travel activity — Impossible travel · 4 Services · [redacted] · 3 IP addresses · 2 Countries
- Misleading publisher name for an OAuth app — Misleading publisher name f... · Office 365 · Office 365 Mover

Microsoft Provides suspicious activity alerts and queries to quickly identify risk areas.

Some Examples:

- Odd Login Attempts
- Admin Activity
- Suspicious Emails
- Potentially Compromised Accounts

MICROSOFT CLOUD APP SECURITY

A simplified place to start for identifying current Security Vulnerabilities and Remediation.

Pre-Configured: Many pre-configured queries to identify suspicious activity and attack vectors.

User Investigation Priority: Automatically identifies users with risk factors to investigate, what items to investigate, and resolution.

Policies to take action: Send Alerts, create Risk Actions, or apply Governance Actions based on automated analysis. Such as automatically suspending compromised accounts.

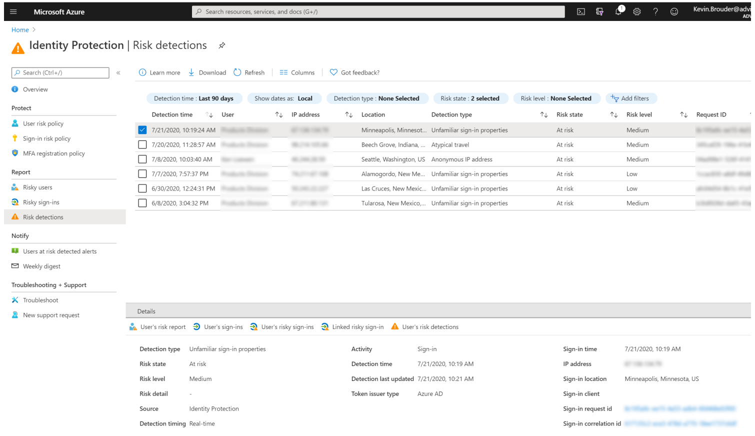
OAuth Authorizations: Review apps your users have authorized, permission levels, and related activities. Approve and Ban apps.

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: 18AUG

AZURE AD IDENTITY PROTECTION

Investigate Risk areas and configure policies

- Detects risky users, sign-ins, and more
- Provides Identity Security Score and recommended actions to improve security
- Ranks users Risk Level, provides areas of investigation, allows remediation
- Setup Policies to automatically remediate risk, for example:
  - Force password change when high risk activity occurs
  - Require multi-factor authentication for high sign in risks



Identity Protection | Risk detections

Detection time : **Last 90 days** · Show dates as: **Local** · Detection type : **None Selected** · Risk state : **2 selected** · Risk level : **None Selected**

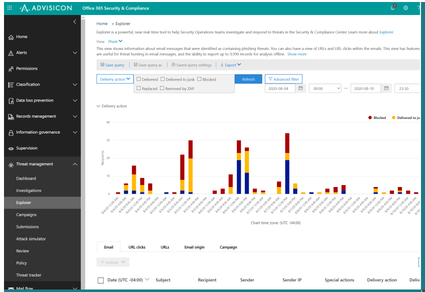
	Detection time	User	IP address	Location	Detection type	Risk state	Risk level	Request ID
☑	7/21/2020, 10:19:24 AM	[redacted]	[redacted]	Minneapolis, Minnesot...	Unfamiliar sign-in properties	At risk	Medium	[redacted]
□	7/20/2020, 11:28:57 AM	[redacted]	[redacted]	Beech Grove, Indiana, ...	Atypical travel	At risk	Medium	[redacted]
□	7/8/2020, 10:03:40 AM	[redacted]	[redacted]	Seattle, Washington, US	Anonymous IP address	At risk	Medium	[redacted]
□	7/7/2020, 7:57:37 PM	[redacted]	[redacted]	Alamogordo, New Me...	Unfamiliar sign-in properties	At risk	Low	[redacted]
□	6/30/2020, 12:24:31 PM	[redacted]	[redacted]	Las Cruces, New Mexic...	Unfamiliar sign-in properties	At risk	Low	[redacted]
□	6/8/2020, 3:04:32 PM	[redacted]	[redacted]	Tularosa, New Mexico,...	Unfamiliar sign-in properties	At risk	Medium	[redacted]

Details

Detection type	Unfamiliar sign-in properties	**Activity**	Sign-in	**Sign-in time**	7/21/2020, 10:19 AM
Risk state	At risk	**Detection time**	7/21/2020, 10:19 AM	**IP address**	[redacted]
Risk level	Medium	**Detection last updated**	7/21/2020, 10:21 AM	**Sign-in location**	Minneapolis, Minnesota, US
Risk detail	-	**Token issuer type**	Azure AD	**Sign-in client**	
Source	Identity Protection			**Sign-in request id**	[redacted]
Detection timing	Real-time			**Sign-in correlation id**	[redacted]

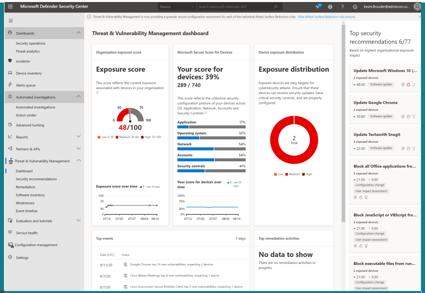
BEYOND THE BASICS WITH MICROSOFT

Even more solutions from Microsoft for a comprehensive security suite for your enterprise



MICROSOFT ENDPOINT MANAGER

Unified Solution to Endpoint Security and Device Management. Efficiently manage security for all devices in your environment, even mobile and BYOD scenarios.

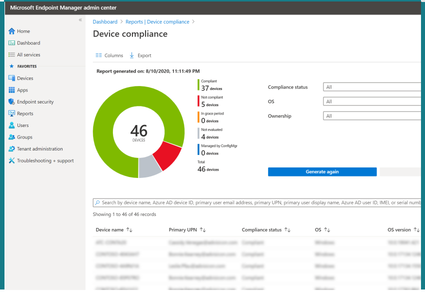

Microsoft Defender Security Center
Threat & Vulnerability Management dashboard
Exposure score
48/100
Your score for devices: 39%
289 / 740
Exposure distribution
Top security recommendations 6/77
Top events
No data to show

AZURE SENTINEL

The first cloud native SIEM to provide AI powered security analytics for your entire enterprise. Not only cloud data, but also analyze data from on-premise devices and servers.

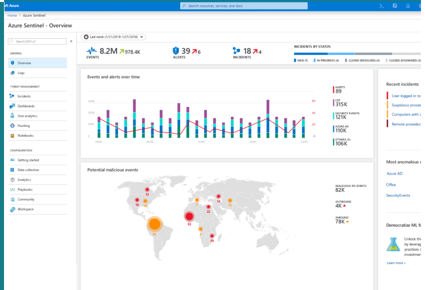
OFFICE 365: THREAT EXPLORER

Review Email and Malware threats to find opportunities to prevent phishing and other attacks.



MICROSOFT DEFENDER ATP

Cloud powered agentless complete Endpoint Security Solution: preventive protection, automated investigation, post-breach detection and response.



ADVISICON INC

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: 18AUG

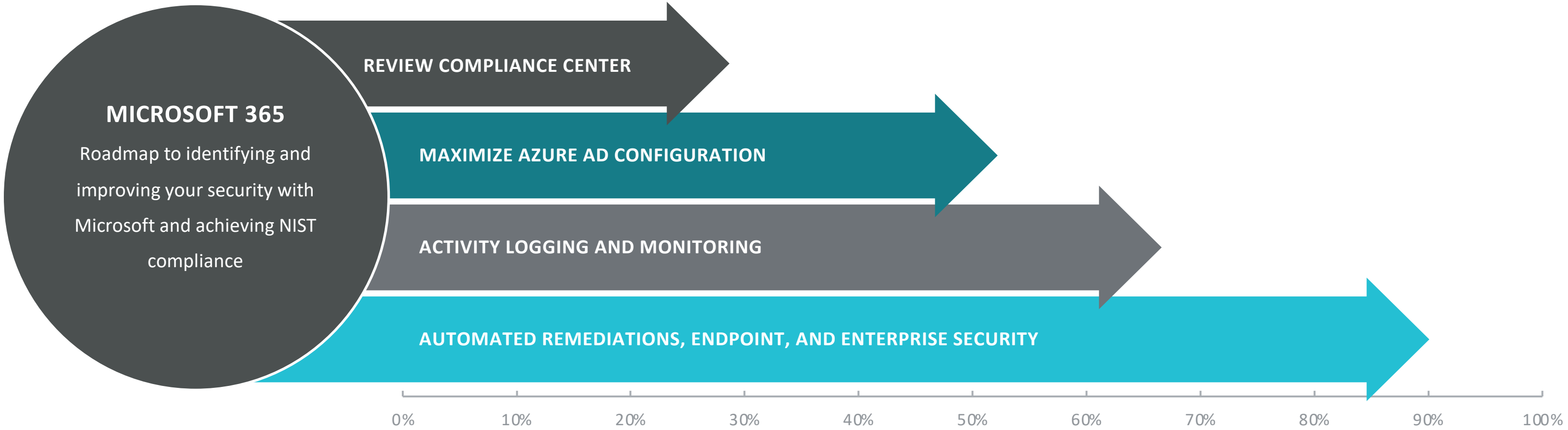
MICROSOFT SECURITY DEMOS

“Demos are more fun.”

-Anonymous

SUMMARY MICROSOFT SECURITY

Identifying Opportunities to Resolve your Security Gaps



MICROSOFT 365

Roadmap to identifying and improving your security with Microsoft and achieving NIST compliance

REVIEW COMPLIANCE CENTER

MAXIMIZE AZURE AD CONFIGURATION

ACTIVITY LOGGING AND MONITORING

AUTOMATED REMEDIATIONS, ENDPOINT, AND ENTERPRISE SECURITY

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code: 18AUG

AUDIENCE QUESTIONS?

Interested in submitting a question?
Go to **www.slido.com** and enter the following event code:

18AUG

ADVISICON

THANKS FOR WATCHING!

Contact us:

5411 NE 107th Ave, Vancouver, WA

☎ 866.362.3847

Contact@Advisicon.com

Follow us on:

facebook.com/Advisicon

@Advisicon

youtube.com/Advisicon

ADVISICON

“Helping You Build A Project Management Culture.”

Contact us:

5411 NE 107th Ave, Vancouver, WA

866.362.3847

Contact@Advisicon.com

Follow us on:

facebook.com/Advisicon

@Advisicon

youtube.com/Advisicon

2020 Cybersecurity Webinar Series:

Taking Action to Mitigate Security Issues and Achieve NIST Compliance

September 15, 2020

Brought to you by

ADVISICON & NSTXL

NATIONAL SECURITY TECHNOLOGY ACCELERATOR

Thank you!

If you have any questions,
please email **membership@nstxl.org**.