#NVSummit2021

Protecting Endpoints in a ZeroTrust world!

- Sami Laiho
- Senior Technical Fellow @ Adminize / Sulava
- Twitter @samilaiho
- MVP since 2011

NORDIC – VIRTUAL SUMMIT –

Sami Laiho

Senior Technical Fellow
adminize.com / Sulava

- IT Admin since 1996
- MVP in Windows OS since 2011
- **”100 Most Influencal people in IT in Finland” – TiVi’2019, 2020**
- Specializes in and trains:
  - Troubleshooting
  - Security, Social Engineering, Auditing
- Trophies:
  - **Ignite 2018 – Best Session and #2 (out of 1708) !**
  - Best speaker at Advanced Threat Summit 2020, Poland
  - Best Speaker at NIC, Oslo 2016, 2017, 2019 and 2020
  - Best Session at AppManagEvent 2017, 2018, Utrecht
  - TechEd Europe and North America 2014 - Best session, Best speaker
  - TechEd Australia 2013 - Best session, Best speaker

MEANWHILE IN FINLAND
VERY FINNISH PROBLEMS
THESE NEW SOCIAL DISTANCING RULES ARE CRAZY! WE HAVE TO STAND 2 METRES APART!
I KNOW! WHY DO THEY WANT US TO STAND CLOSER TOGETHER THAN NORMAL ?

Protecting Endpoints in a ZeroTrust world!

Twitter: @samilaiho

BYOD

New Zero-Trust Era

Why Zero Trust?

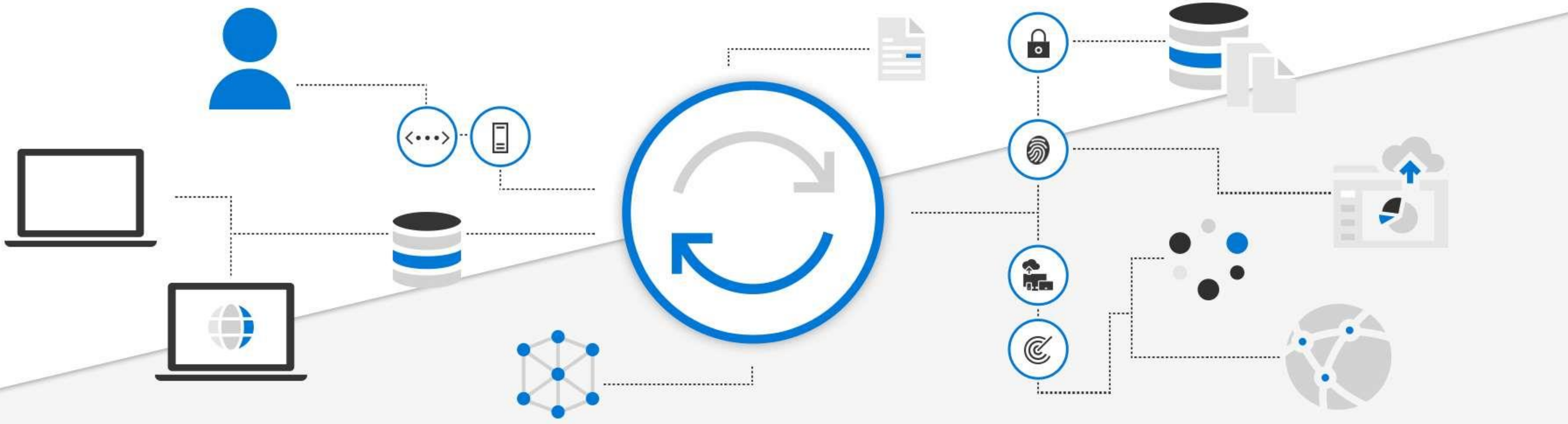
- Empower your users to work more securely anywhere and anytime, on any device
- Enable digital transformation with intelligent security for today’s complex environment
- Close security gaps and minimize risk of lateral movement

Zero Trust principles

- Verify explicitly
- Use least privileged access
- Assume breach

Zero Trust defined

- Instead of assuming everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an open network



“Never trust, always verify”

Zero Trust Components

- Identities
  - Verify and secure each identity with strong authentication across your entire digital estate.
- Devices
  - Gain visibility into devices accessing the network. Ensure compliance and health status before granting access.
- Applications
  - Discover shadow IT, ensure appropriate in-app permissions, gate access based on real-time analytics, and monitor and control user actions.

Zero Trust Components

- Data
  - Move from perimeter-based data protection to data-driven protection. Use intelligence to classify and label data. Encrypt and restrict access based on organizational policies.
- Infrastructure
  - Use telemetry to detect attacks and anomalies, automatically block and flag risky behavior, and employ least privilege access principles.
- Network
  - Encrypt all internal communications, limit access by policy, and employ microsegmentation and real-time threat detection.

Forget INTERNAL networks!

Welcome VPNs and IPsec!

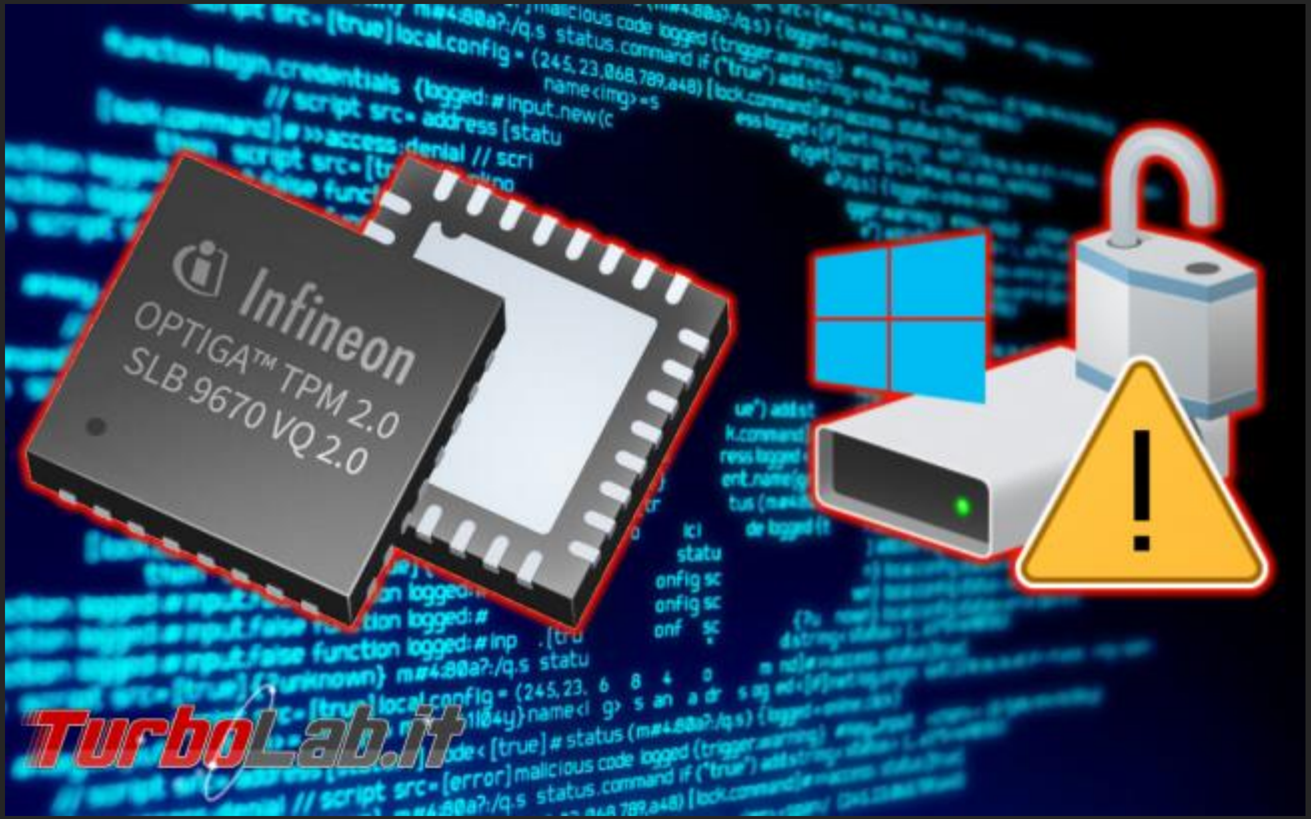
DEMO

IPsec

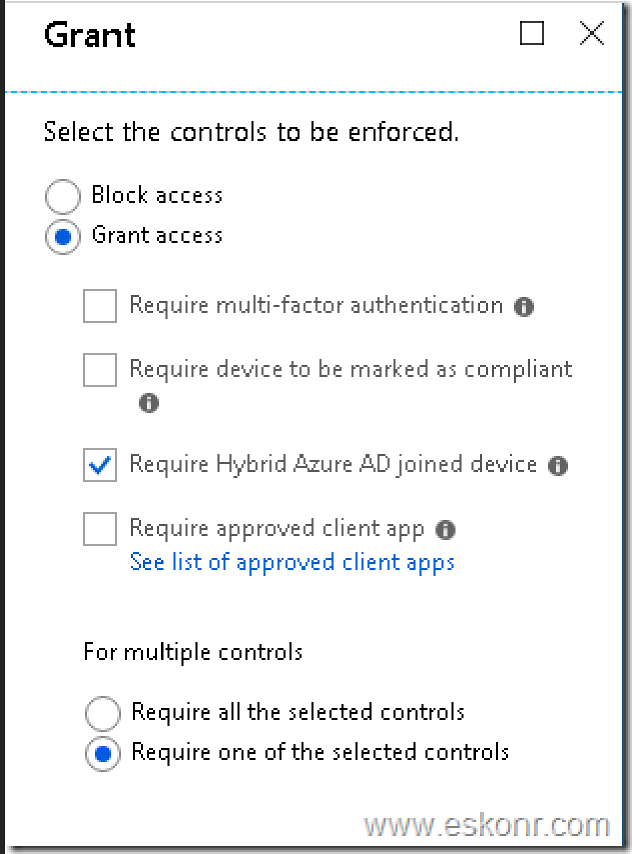
Known and Healthy Devices

MFA & Biometrics

- Really a game changer
- Great second factor!
  - There are still issues to think about



This Photo by Unknown Author is licensed under CC BY-SA-NC



Grant

Select the controls to be enforced.

○ Block access
● Grant access

□ Require multi-factor authentication
□ Require device to be marked as compliant
☑ Require Hybrid Azure AD joined device
□ Require approved client app
See list of approved client apps

For multiple controls

○ Require all the selected controls
● Require one of the selected controls

This Photo by Unknown Author is licensed under CC BY

This Photo by Unknown Author is licensed under CC BY-SA

DEMO

MFA

Trust

Admin Epoch

1985 - 2005

Users run as local admin
Users install their own software
Apps trusted by default

Non-Admin Epoch

2005 - 2025

Users run as standard user
Admins install software
Apps trusted by default

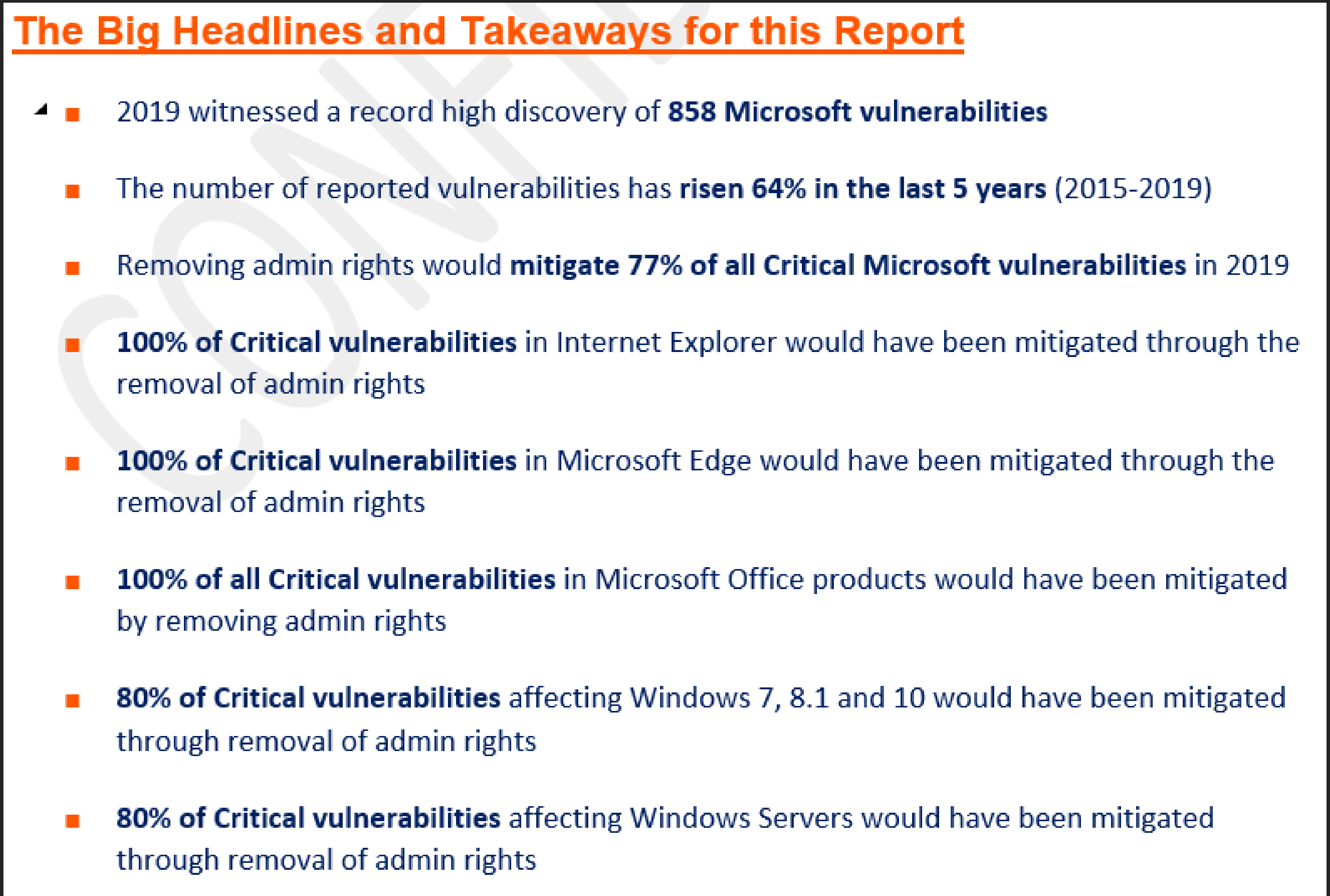
App Control Epoch

2025 - ?

Users run as standard user
Admins install software
Apps trusted when trust is earned

Principle of Least Privilege

- In Windows there is no Security if you logon as an admin
- The security subsystem was not built to withstand the use of admin rights
- With "No-Admin" approach
  - We get better performance
  - We get less tickets
  - We get less reinstallation
  - We get more productive users!
  - We get less malware
  - We get to be lazier as admins!



The Big Headlines and Takeaways for this Report

- 2019 witnessed a record high discovery of **858 Microsoft vulnerabilities**
- The number of reported vulnerabilities has **risen 64% in the last 5 years** (2015-2019)
- Removing admin rights would **mitigate 77% of all Critical Microsoft vulnerabilities** in 2019
- **100% of Critical vulnerabilities** in Internet Explorer would have been mitigated through the removal of admin rights
- **100% of Critical vulnerabilities** in Microsoft Edge would have been mitigated through the removal of admin rights
- **100% of all Critical vulnerabilities** in Microsoft Office products would have been mitigated by removing admin rights
- **80% of Critical vulnerabilities** affecting Windows 7, 8.1 and 10 would have been mitigated through removal of admin rights
- **80% of Critical vulnerabilities** affecting Windows Servers would have been mitigated through removal of admin rights

DEMO

Principle of Least Privilege

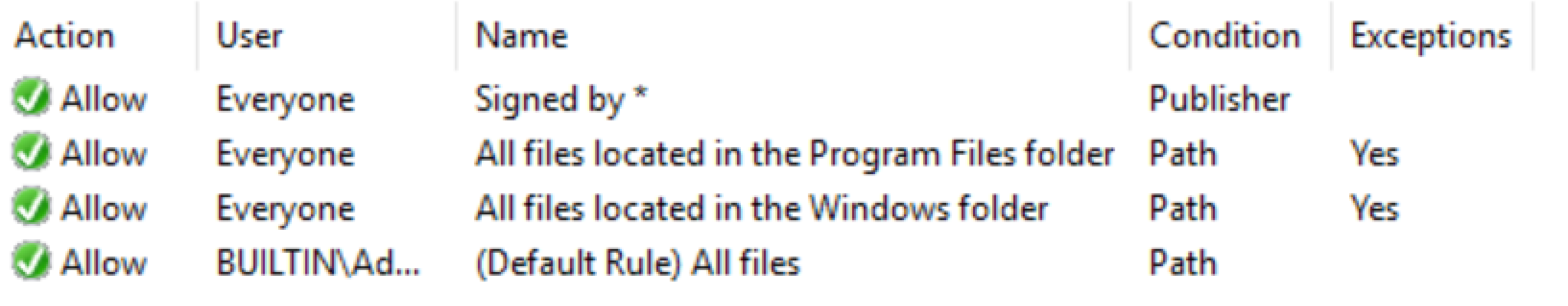
Allow-Listing

1 Million New Malware Variants per day

A03

Simplest AppLocker

- THIS KILLS 950000+ PIECES OF MALWARE PER DAY!! With no Anti-Malware ☺



Action	User	Name	Condition	Exceptions
✓ Allow	Everyone	Signed by *	Publisher	
✓ Allow	Everyone	All files located in the Program Files folder	Path	Yes
✓ Allow	Everyone	All files located in the Windows folder	Path	Yes
✓ Allow	BUILTIN\Ad...	(Default Rule) All files	Path	

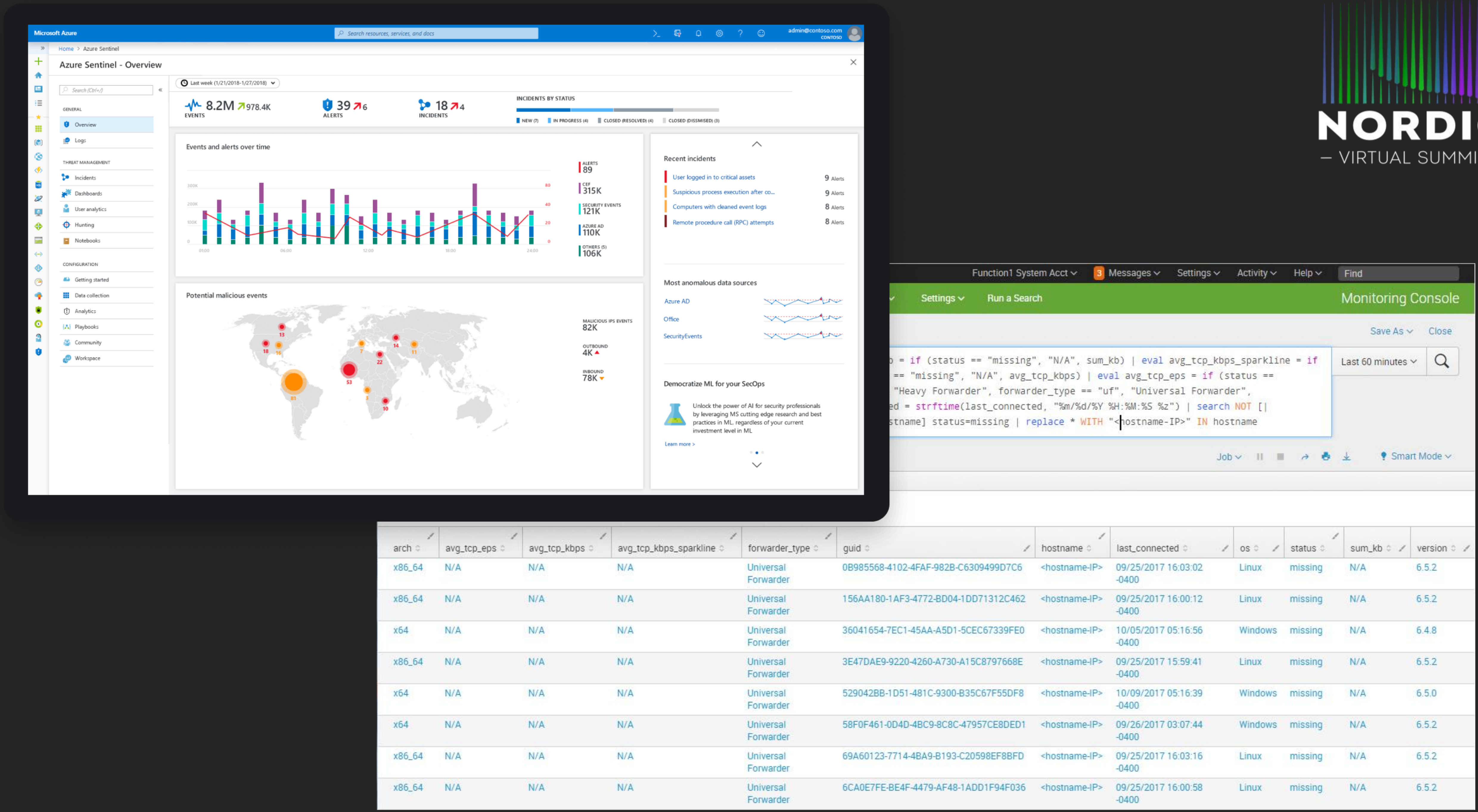
DEMO

Apps Required to Have Earned Trust – Aka Allow-Listing

Monitoring

SIEM & SOC

NORDIC
— VIRTUAL SUMMIT —



Microsoft Azure

Home > Azure Sentinel

Azure Sentinel - Overview

Last week (1/21/2018-1/27/2018)

8.2M 978.4K EVENTS

39 6 ALERTS

18 4 INCIDENTS

INCIDENTS BY STATUS

NEW (7) IN PROGRESS (4) CLOSED (RESOLVED) (4) CLOSED (DISSMISED) (3)

Recent incidents

User logged in to critical assets	9 Alerts
Suspicious process execution after co...	9 Alerts
Computers with cleaned event logs	8 Alerts
Remote procedure call (RPC) attempts	8 Alerts

Most anomalous data sources

Azure AD

Office

SecurityEvents

Democratize ML for your SecOps

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML

Learn more >

```
p = if (status == "missing", "N/A", sum_kb) | eval avg_tcp_kbps_sparkline = if
== "missing", "N/A", avg_tcp_kbps) | eval avg_tcp_eps = if (status ==
"Heavy Forwarder", forwarder_type == "uf", "Universal Forwarder",
ed = strftime(last_connected, "%m/%d/%Y %H:%M:%S %z") | search NOT [|
tname] status=missing | replace * WITH "<hostname-IP>" IN hostname
```

arch	avg_tcp_eps	avg_tcp_kbps	avg_tcp_kbps_sparkline	forwarder_type	guid	hostname	last_connected	os	status	sum_kb	version
x86_64	N/A	N/A	N/A	Universal Forwarder	0B985568-4102-4FAF-982B-C6309499D7C6	<hostname-IP>	09/25/2017 16:03:02 -0400	Linux	missing	N/A	6.5.2
x86_64	N/A	N/A	N/A	Universal Forwarder	156AA180-1AF3-4772-BD04-1DD71312C462	<hostname-IP>	09/25/2017 16:00:12 -0400	Linux	missing	N/A	6.5.2
x64	N/A	N/A	N/A	Universal Forwarder	36041654-7EC1-45AA-A5D1-5CEC67339FE0	<hostname-IP>	10/05/2017 05:16:56 -0400	Windows	missing	N/A	6.4.8
x86_64	N/A	N/A	N/A	Universal Forwarder	3E47DAE9-9220-4260-A730-A15C8797668E	<hostname-IP>	09/25/2017 15:59:41 -0400	Linux	missing	N/A	6.5.2
x64	N/A	N/A	N/A	Universal Forwarder	529042BB-1D51-481C-9300-B35C67F55DF8	<hostname-IP>	10/09/2017 05:16:39 -0400	Windows	missing	N/A	6.5.0
x64	N/A	N/A	N/A	Universal Forwarder	58F0F461-0D4D-4BC9-8C8C-47957CE8DED1	<hostname-IP>	09/26/2017 03:07:44 -0400	Windows	missing	N/A	6.5.2
x86_64	N/A	N/A	N/A	Universal Forwarder	69A60123-7714-4BA9-B193-C20598EF8BFD	<hostname-IP>	09/25/2017 16:03:16 -0400	Linux	missing	N/A	6.5.2
x86_64	N/A	N/A	N/A	Universal Forwarder	6CA0E7FE-BE4F-4479-AF48-1ADD1F94F036	<hostname-IP>	09/25/2017 16:00:58 -0400	Linux	missing	N/A	6.5.2

GLOBAL NETWORK
at&t

Thank you!

NORDIC
– VIRTUAL SUMMIT –

MSEndPointMgr.com
#MSEndPointMgr

System Center User Group
Finland
#SCUGFI

System Center User Group
Denmark

#SCUGDK

System Center User Group
Sweden
#SCUGSE

Modern Management User Group
Norway
#MMUGNO

“In Security don’t let perfect be the enemy of good”

@samilaiho

If you are not on Twitter – Get on Twitter!