NIC

Future Edition

Secure your cloud like a master.
Deep dive into Azure Security Center

Viktorija Almazova
Cloudworks

Azure Security Center

- ✓ Gain visibility and control into Azure infrastructure
- ✓ Monitor security also for on-premises machines
- ✓ Integrate 3rd party partner solutions
- ✓ Detect attacks on resources deployed in the environment

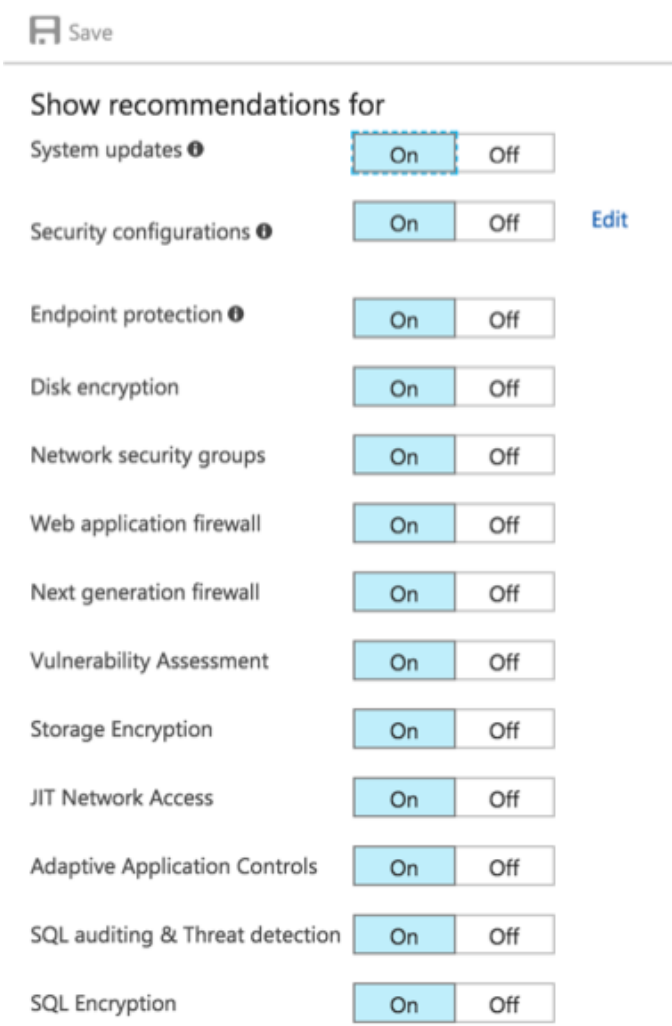
Azure Security Center is offered in two tiers: Free and Standard. The Standard tier is free for the first 60 days. Any usage beyond 60 days will be automatically charged as per the pricing scheme below.

FEATURES	FREE (AZURE RESOURCES ONLY)	STANDARD (HYBRID AND AZURE RESOURCES)
Security policy, assessment, and recommendations	✔	✔
Connected partner solutions	✔	✔
Security event collection and search	- -	✔
Just in time VM Access	- -	✔
Adaptive application controls	- -	✔
Advanced threat detection for networks, VMs/servers, and Azure services	- -	✔
Built-in and custom alerts	- -	✔
Threat intelligence	- -	✔
Included data	Not applicable	500 MB per day[1]
Price	Free	kr121.72 / node[2] / month

What we get

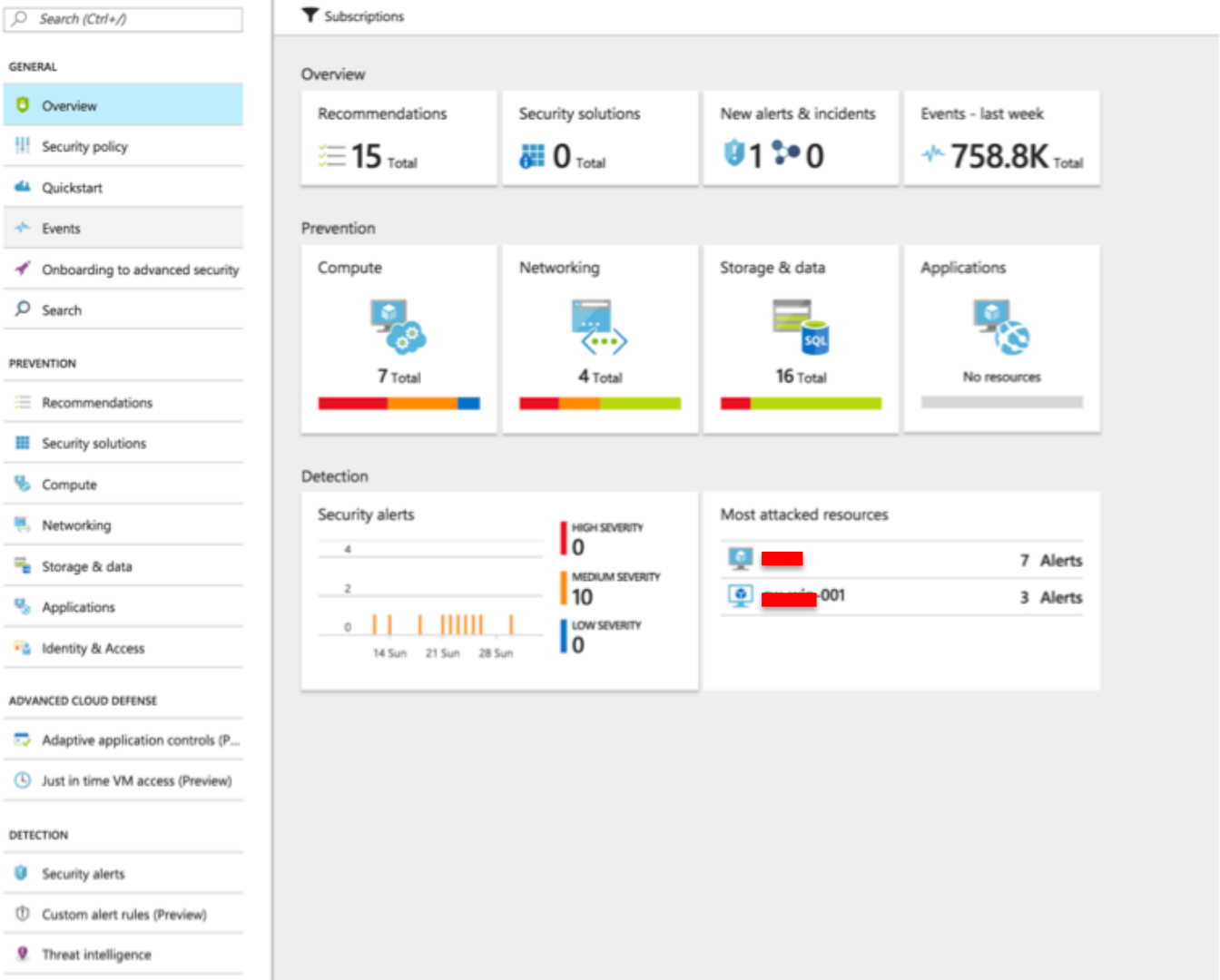
Security Center agent scans for various security related configurations and events for machines:

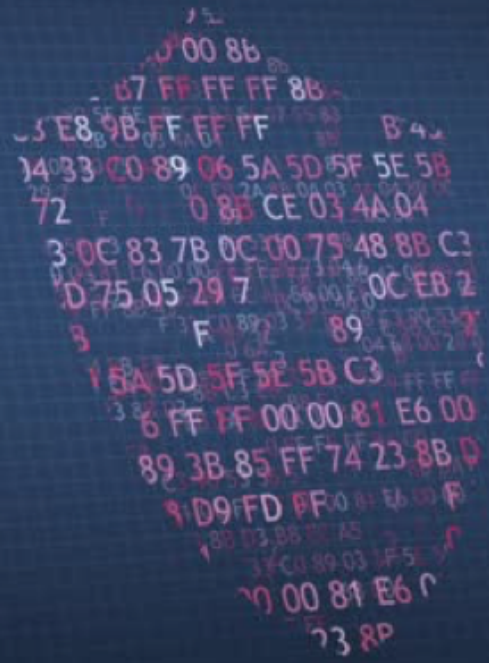
- ✓ Operating system type and version
- ✓ Operating system logs (Windows event logs)
- ✓ Running processes
- ✓ Machine name
- ✓ IP addresses
- ✓ Logged in user
- ✓ Tenant ID
- ✓ Crash dump files



How data is stored.. Workspace

- ✓ A workspace is an Azure resource that serves as a container for data
- ✓ Might be used multiple workspaces to manage different sets of data that is collected from all or portions of IT infrastructure
- ✓ Data collected from the Microsoft Monitoring Agent (on behalf of Azure Security Center) will be stored in either an existing Log Analytics workspace(s) associated with your Azure subscription or a new workspace(s), taking into account the Geo of the VM


Search (Ctrl+/)
GENERAL
Overview
Security policy
Quickstart
Events
Onboarding to advanced security
Search
PREVENTION
Recommendations
Security solutions
Compute
Networking
Storage & data
Applications
Identity & Access
ADVANCED CLOUD DEFENSE
Adaptive application controls (P...
Just in time VM access (Preview)
DETECTION
Security alerts
Custom alert rules (Preview)
Threat intelligence
Subscriptions
Overview
Recommendations
15 Total
Security solutions
0 Total
New alerts & incidents
1
0
Events - last week
758.8K Total
Prevention
Compute
7 Total
Networking
4 Total
Storage & data
16 Total
Applications
No resources
Detection
Security alerts
4
2
0
14 Sun
21 Sun
28 Sun
HIGH SEVERITY
0
MEDIUM SEVERITY
10
LOW SEVERITY
0
Most attacked resources
7 Alerts
3 Alerts

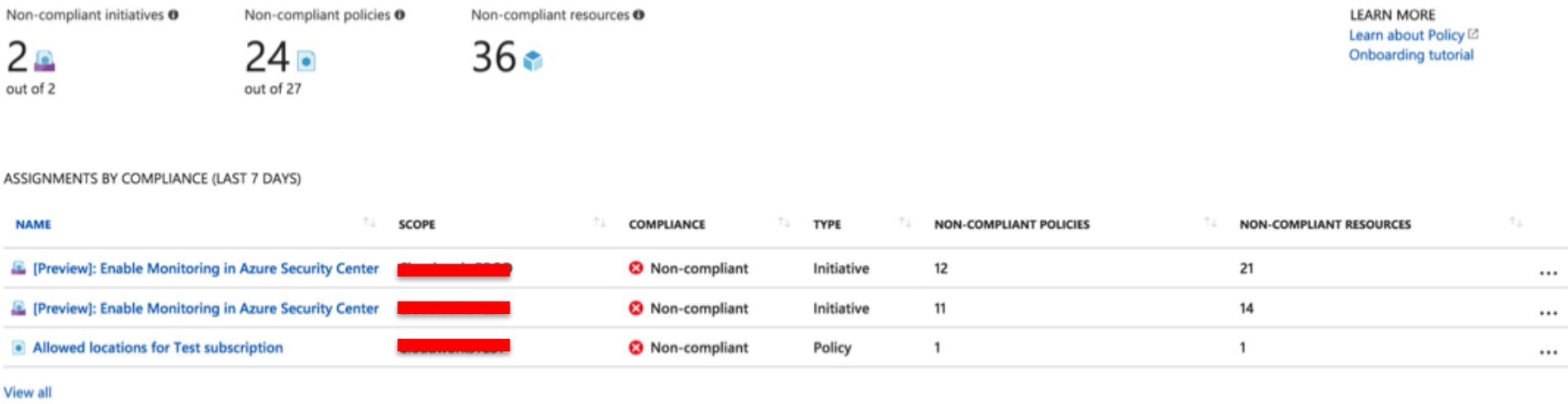


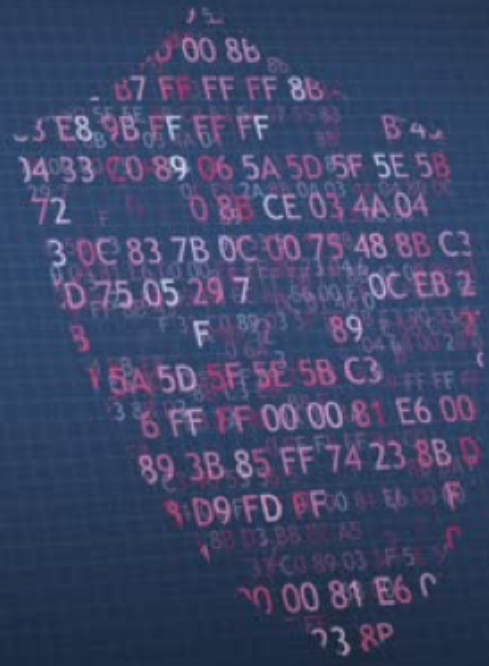
Demo

Azure Security Center Dashboard

Azure Policy

- ✓ Currently Private Preview
- ✓ Allows to create, assign and, manage policy definitions
- ✓ Policy definitions enforce different rules and actions over resources
- ✓ Integrates with Security Center





Demo

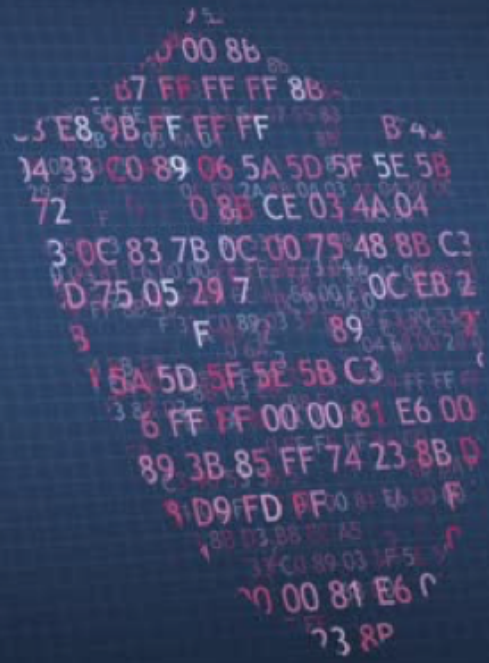
Security Policies in Azure Security Center

Applying recommendations: Just in time

- ✓ The just in time feature is in preview and available on the Standard tier
- ✓ When just in time is enabled, Security Center locks down inbound traffic to Azure VMs by creating an NSG rule.
- ✓ You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the just in time solution.

Demo

Just in time

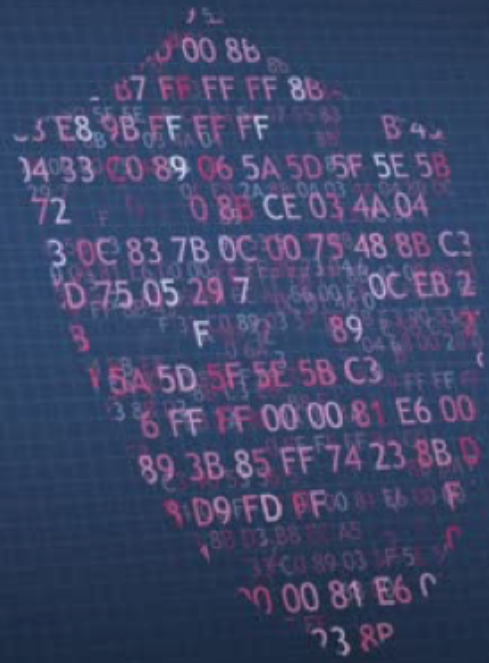


Applying recommendations: Adaptive Application Controls

- ✓ The just in time feature is in preview and available on the Standard tier
- ✓ Controls which applications can run on your VMs located in Azure
- ✓ SC uses machine learning to analyze the processes running in the VM
- ✓ SC relies on a minimum of two weeks of data in order to create a baseline
- ✓ By default a new application control policy is always configured in *Audit* mode

Demo

Adaptive application controls



Detections capabilities

Threat intelligence

Looks for known malicious actors

Examples
- Network traffic to malicious IP address
- Malicious process executed

Behavioral analytics

Looks for known patterns and malicious behaviors

Examples
- Process executed in a suspicious manner

Anomaly detection

Uses statistical profiling to build historical baselines

Alert on deviations that conform to a potential attack vector

Example
- Remote desktop connections to a specific VM typically occur 5 times a day, today there were 100 connection attempts

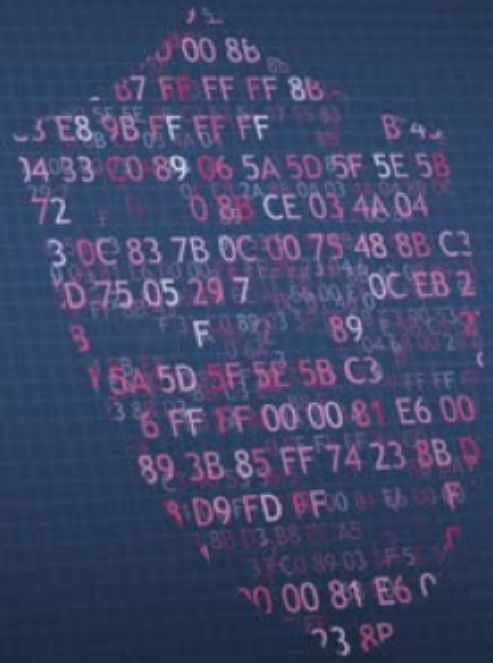
Fusion

Combine events and alerts from across the kill chain to map the attack timeline

Examples
- SQL injections (WAF + Azure SQL Logs)
- Malicious process (Crash dump… and later… suspicious process execution)
- Breach detection (Brute force attempt… and later… suspicious VM activity)

Demo

Security Incident

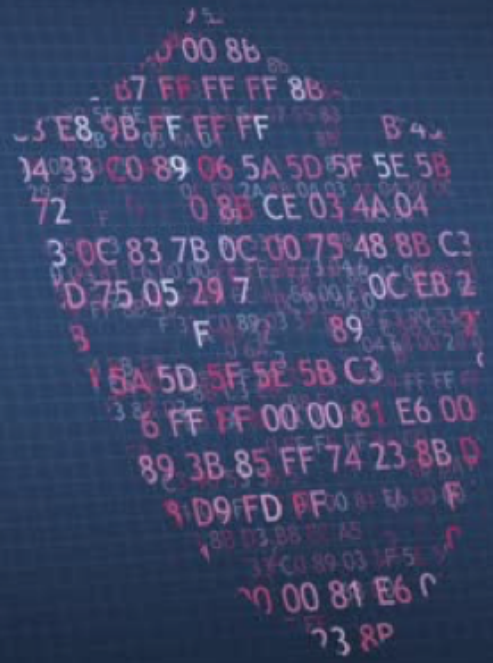


Creating Custom Alerts

- ✓ In a preview
- ✓ Custom alert rules in Security Center allows to define new security alerts based on data that is already collected from environment
- ✓ You can create queries, and the result of these queries can be used as criteria for the custom rule, and once this criteria is matched, the rule is executed
- ✓ You can use computers security events, partner's security solution logs or data ingested using APIs to create your custom queries

Demo

Custom security Incident



Threat Intelligence in Security Center

- ✓ By using the threat intelligence option available in Security Center, IT administrators can identify security threats against the environment

- ✓ Scenario: computers can become nodes in a botnet when attackers illicitly install malware that secretly connects the computer to the command and control. Threat intelligence can also identify potential threats coming from underground communication channels, such as the dark web

Threat intelligence

contoso77

Refresh | Analytics | Filter

Time: Last 24 hours

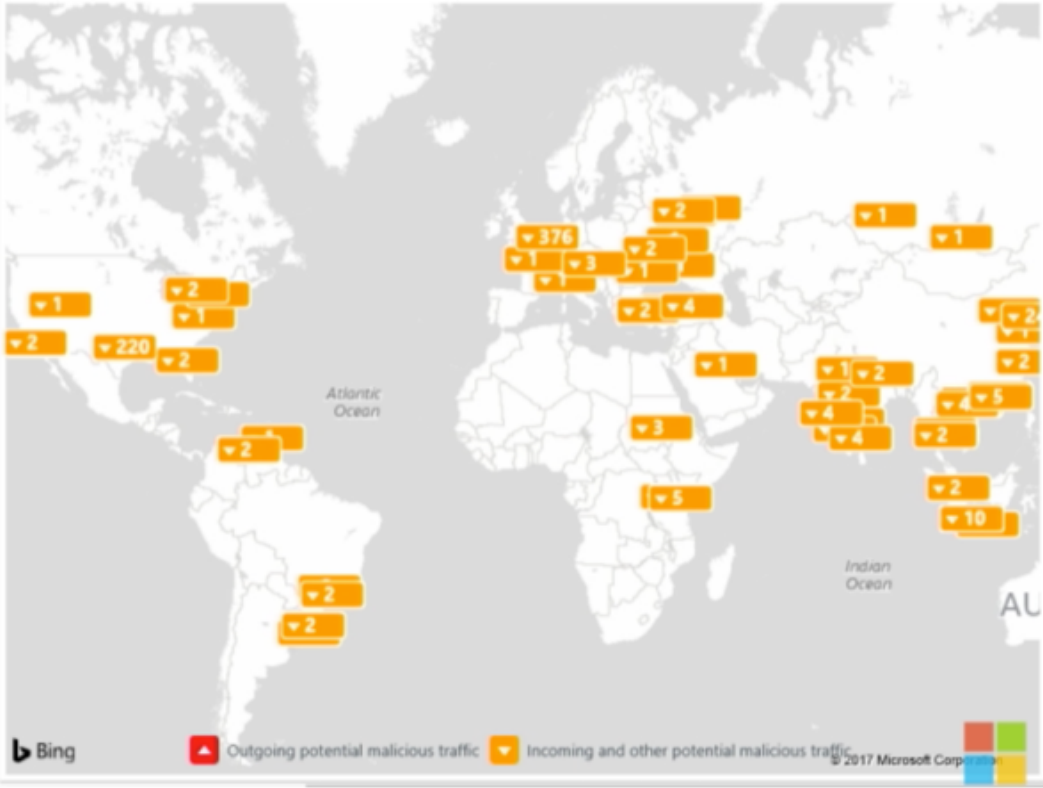
THREAT BREAKDOWN

Threat types

BOTNET
781

ORIGIN COUNTRY	COUNT
Netherlands	376
United States	231
People's Republic of China	40
Indonesia	27
Vietnam	19
India	16
Brazil	9
Russia	9
Turkey	8
Kenya	6

THREAT LOCATION



THREAT DETAILS

Select an item on the map to v

Microsoft

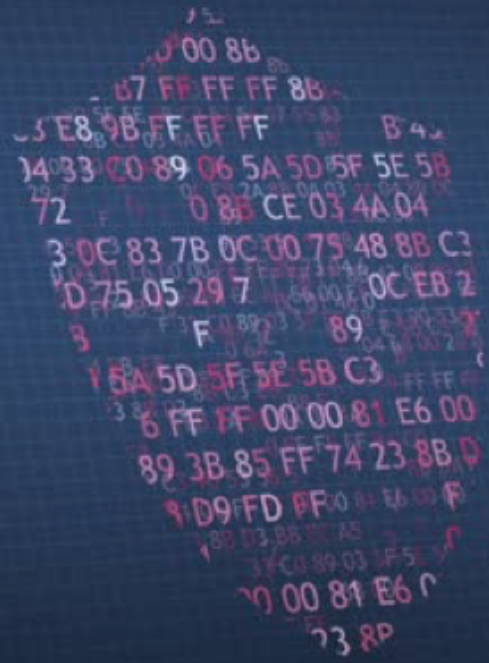
Security Playbooks

- ✓ Security playbook is a collection of procedures that can be executed from Security Center once a certain playbook is triggered from selected alert

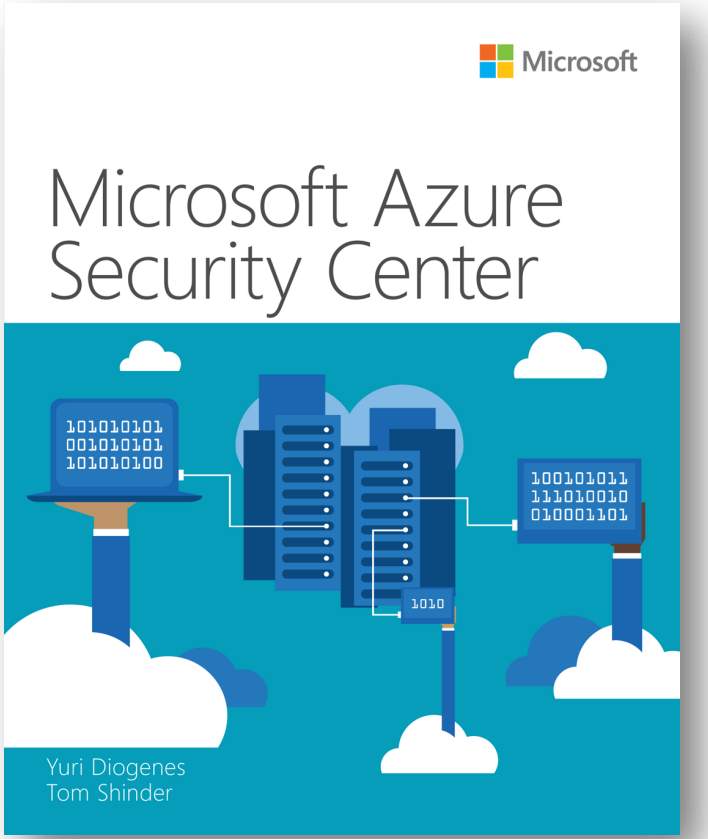
- ✓ Security playbook can help to automate and orchestrate your response to a specific security alert detected by Security Center. Security Playbooks in Security Center are based on Azure Logic Apps

Demo

Security Playbooks



Thanks!


Microsoft
Microsoft Azure Security Center
1010101010
0010101010
1010101000
1001010111
1110100100
0100001101
1010
Yuri Diogenes
Tom Shinder

Resources

Slides and demos from the conference will be available at github.com/nordicinfrastructureconference/2018 (bit.ly/2y7JhA3)