Microsoft

Microsoft Ignite

Microsoft

End-to-end IoT Security

Eti Fakiri
Sr. Program Manager
Eti.Fakiri@Microsoft.com

Ofir Barzilay
Principal Engineering Manager
Ofir.Barzilay@Microsoft.com

Idan Perkal
Program Manager
Idan.Perkal@Microsoft.com

BRK2383

IoT Momentum

$130B

New monetization avenues due to IoT-related services

94%

Businesses projected to be using IoT by the end of 2021

80B

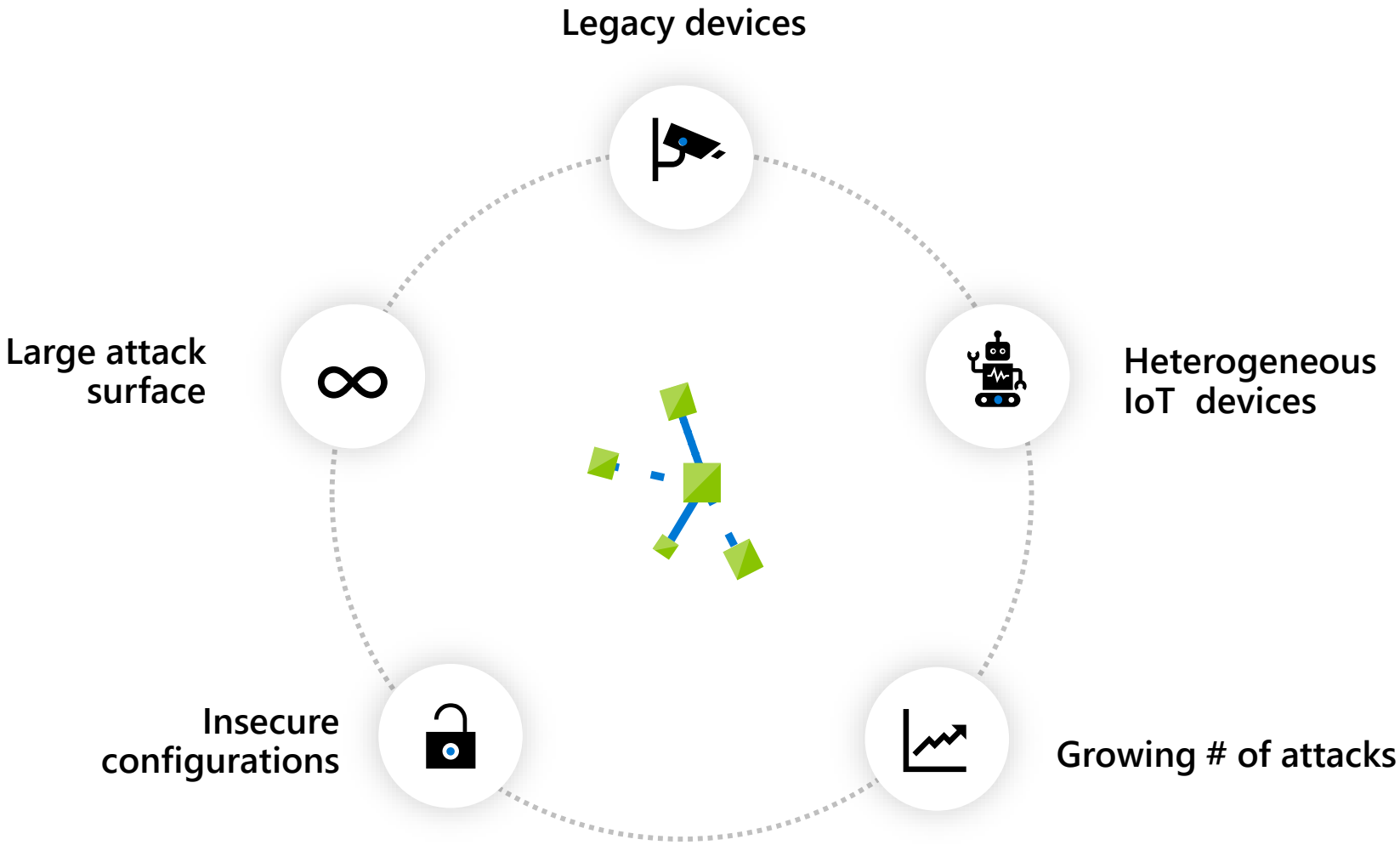
Connected “things” by 2025 generating 180ZB of data

80%

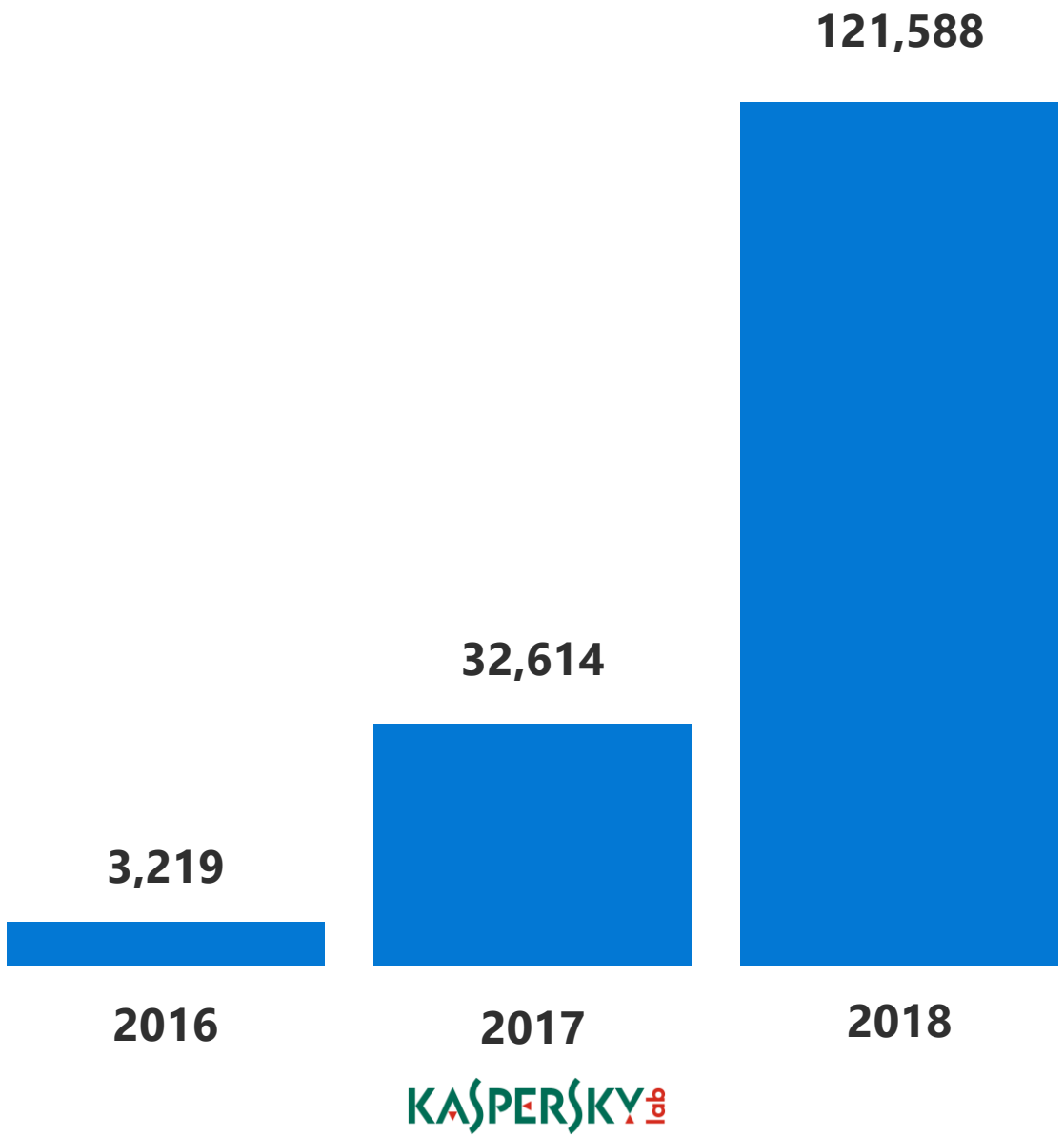
Companies that increased revenue as a result of IoT implementation

Source: Gartner, 2018

IoT Security Challenges



Growing IoT Attacks



Source: Kaspersky Labs, The state of IoT Security 2018

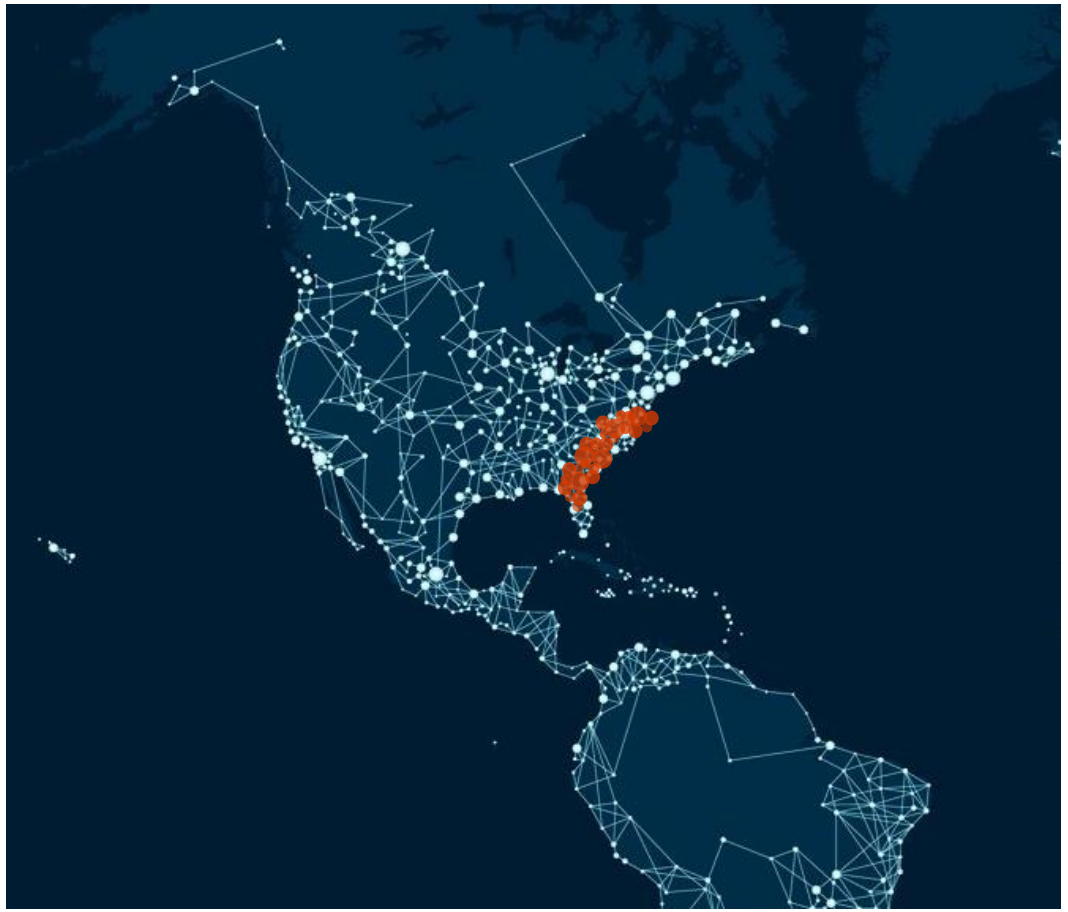
35%

of organizations reported that IoT devices were the primary source of data breaches in the past 12 months.

*Source: https://iiot-world.com/connected-industry/iot-vs-iiot-differences-you-must-know/

IoT attacks on the rise

DDOS



Hackers breach IoT devices to launch an attack that takes down the internet for a day

Data Breach

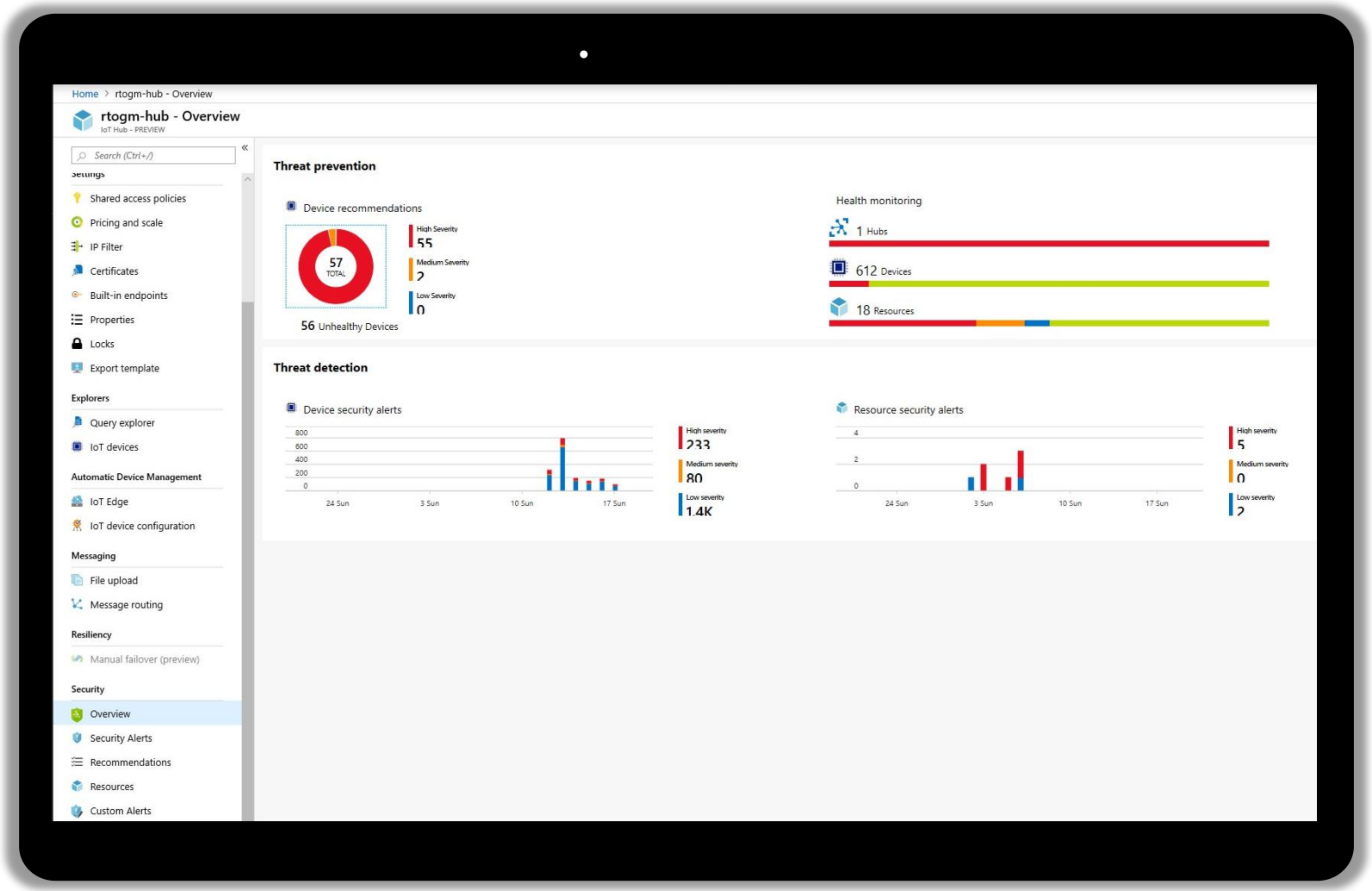
Attackers gain access to casino database through fish tank's connected filter device

$5B
Investment in IoT in 5 years

$1B
Annual investment
in cybersecurity

3500+
Global security experts

Unblock IoT innovation with End-to-End Security



SINGLE PANE OF GLASS | SECURITY POSTURE | VAST SECURITY INTELLIGENCE | BUILT FOR THE CLOUD

Azure Security Center for IoT

Flexible for your needs

USER INTERFACE

Azure Security Center

Enterprise IT Security and SecOps

Azure IoT Hub

OT and IoT solution DevOps

DETECTION ENGINES

Agent

Open source

Agentless

Based on IoT Hub telemetry

Anomaly detection

Edge Security Module

Securing the edge and connected devices

ADAPTIVE SECURITY

Recommendations

Security Hygiene

Alerts

Out-of-the-box coverage of IoT attacks

Microsoft Threat Intelligence

Custom Alerts

Customize to specific IoT scenarios

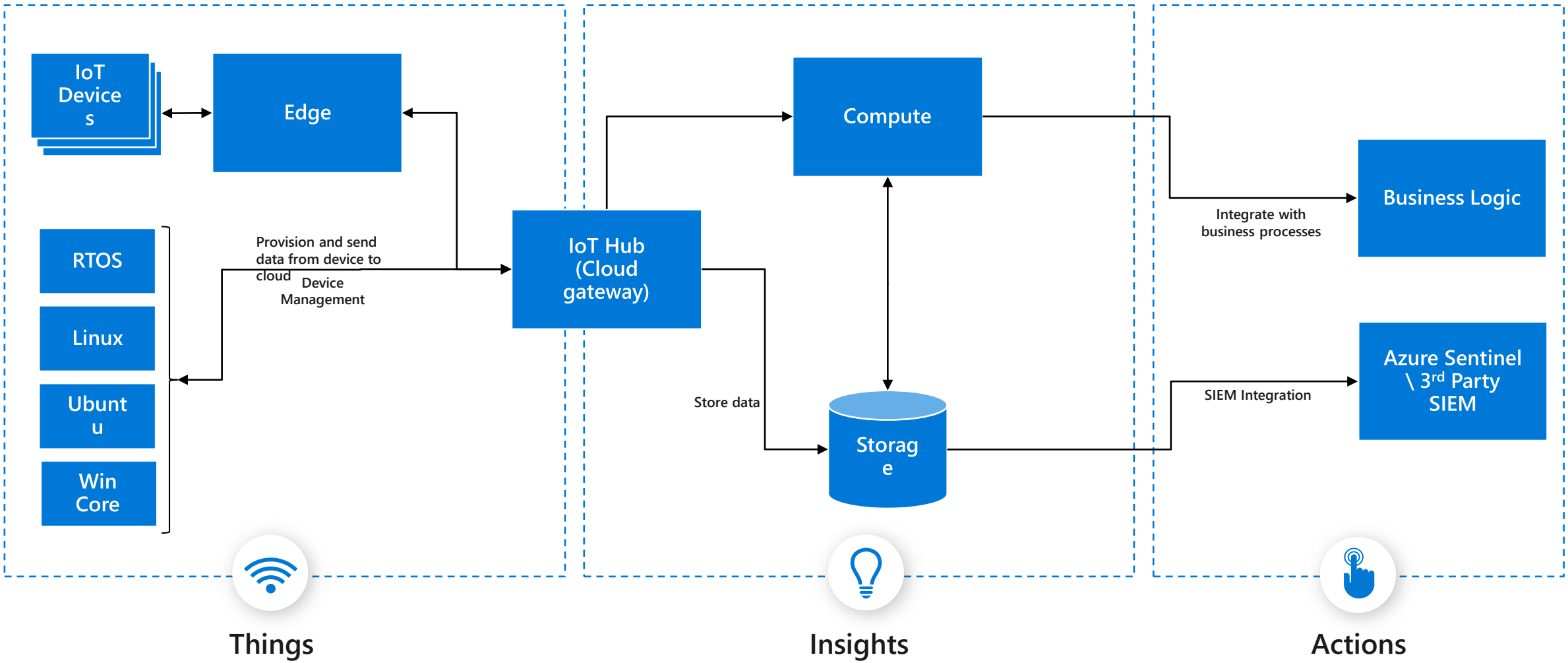
IoT reference architecture

Things

Insights

Actions

IoT reference architecture



Demo

Ofir Barzilay and Idan Perkal

Mirai Botnet attack

IoT devices are used to launch an attack that takes down the internet for a day

100k devices

Exploited a well-known weakness

No early detection, no remote update

2016

Early Sep 2016

KerbsOnSecurity forced down

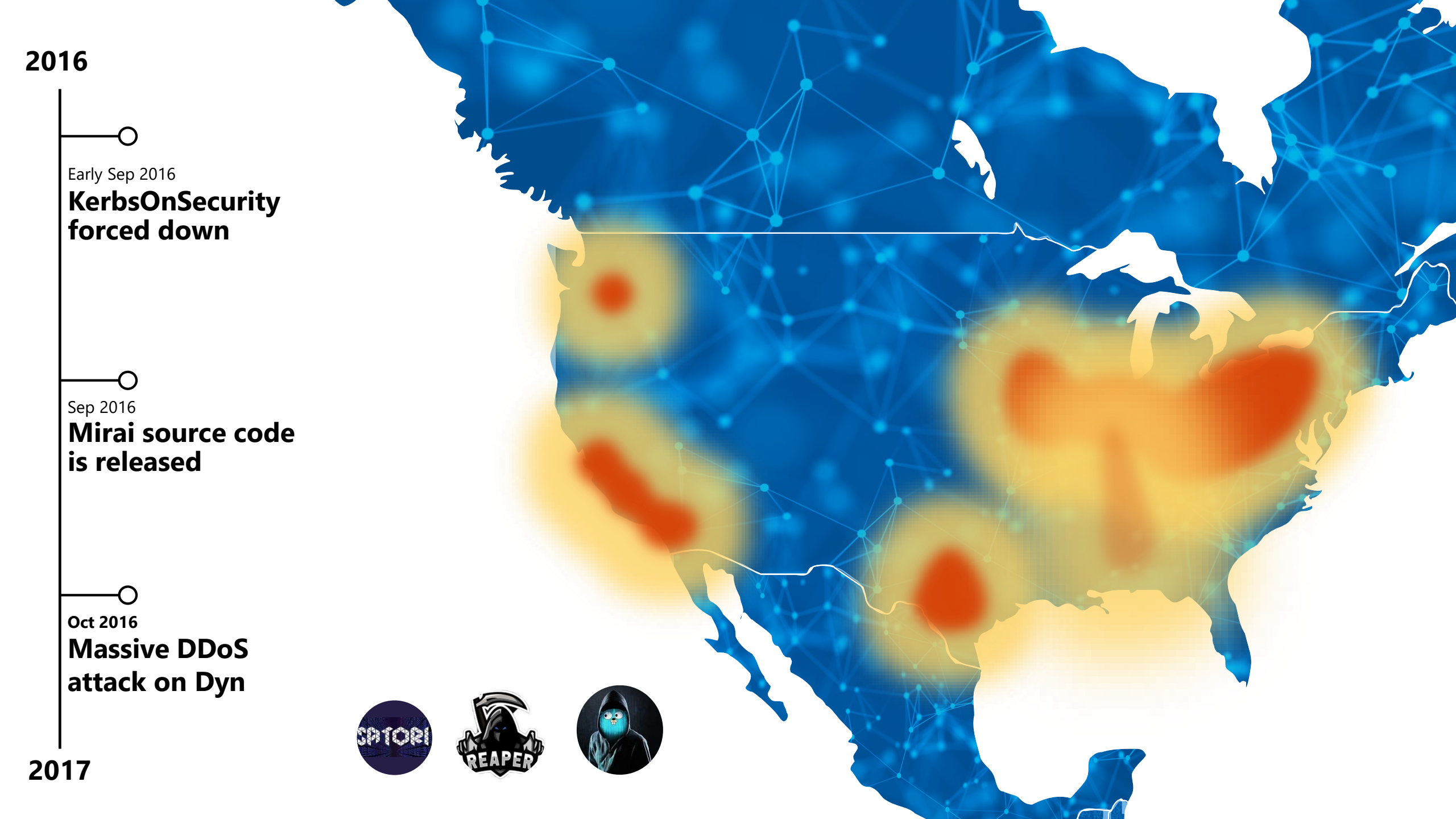
Sep 2016

Mirai source code is released

Oct 2016

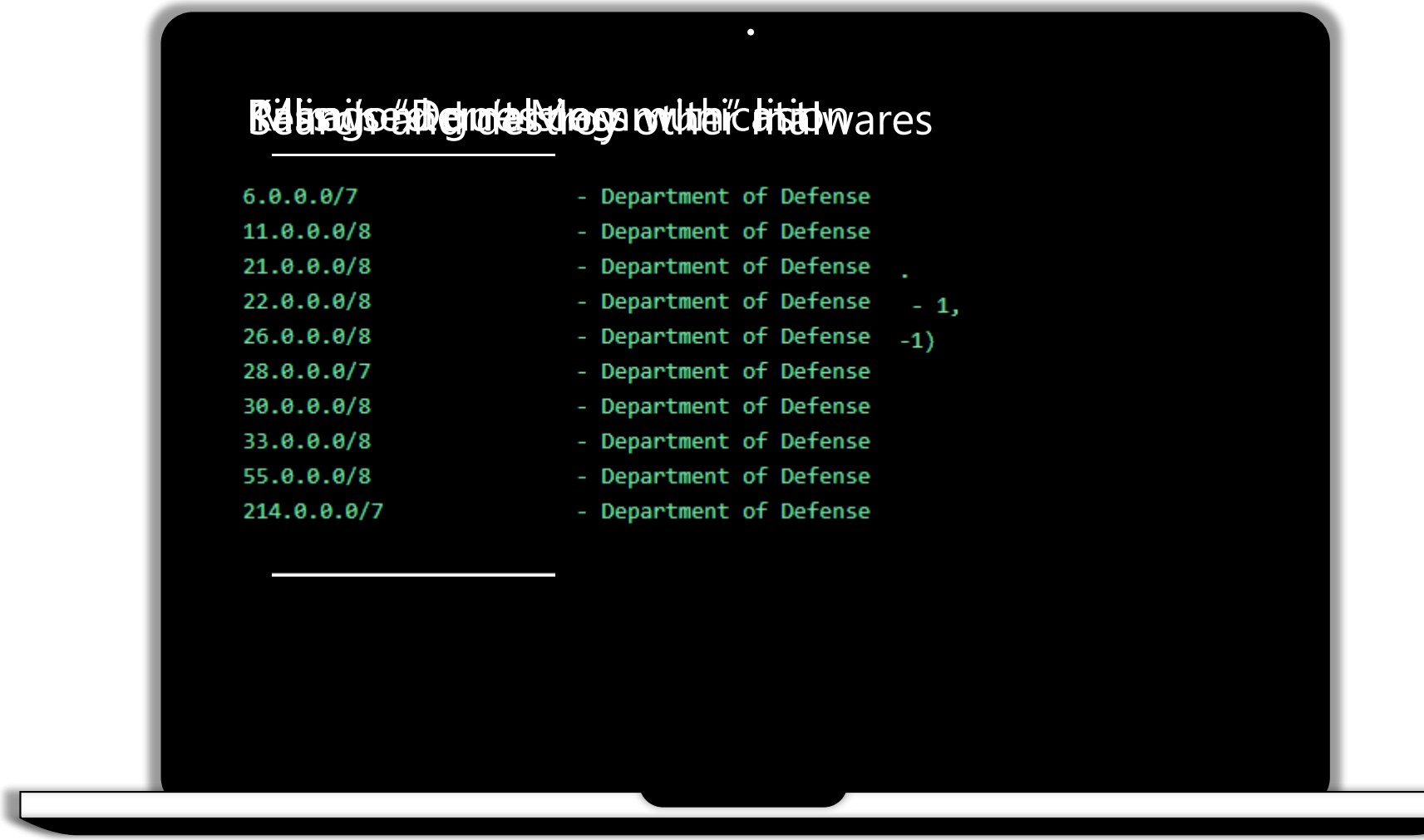
Massive DDoS attack on Dyn

2017



Mirai malware payload

Highlights



*Source: Imperva, Breaking Down Mirai

Demo

Ofir Barzilay and Idan Perkal

Recommendations baseline

75.40%

Telnet

11.59%

SSH

13.01%

Samba

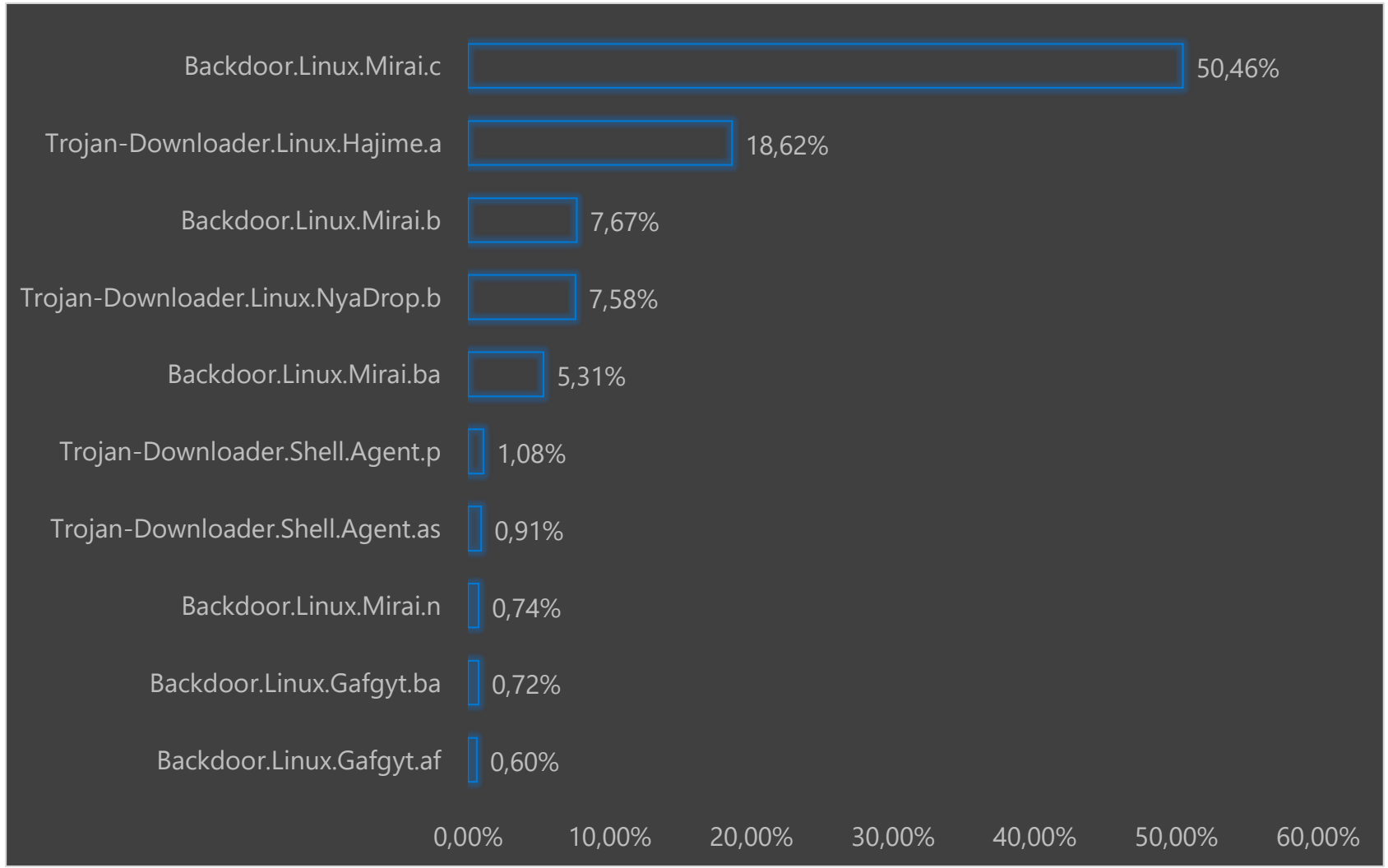
Recommendations baseline

75.40%
Telnet

11.59%
SSH

13.01%
Samba

Top 10 Threat Verdicts



Source: Securelist 2018 - IoT a Malware Story

What our customers say about ASC for IoT

volpara solutions™

"**Microsoft Azure IoT Security solution provides us management and threat protection for the full stack**, including IoT devices, IoT hubs as well as the computing and data resources utilized by out solutions. Effectively saving us from 'rolling our own' and aligning our IoT security neatly with our other Azure based solutions and line of business application usage."

—Gareth Beaumont, CISO & CIO

RapidDeploy
CLOUD AIDED DISPATCH™

"RapidDeploy has partnered with Microsoft on the Azure IoT Security because of our belief that **IoT platforms bring significant value when secured properly**.

By partnering with Microsoft, together we are able to ensure the device security and enable life and safety operations that protect people and communities around the world."

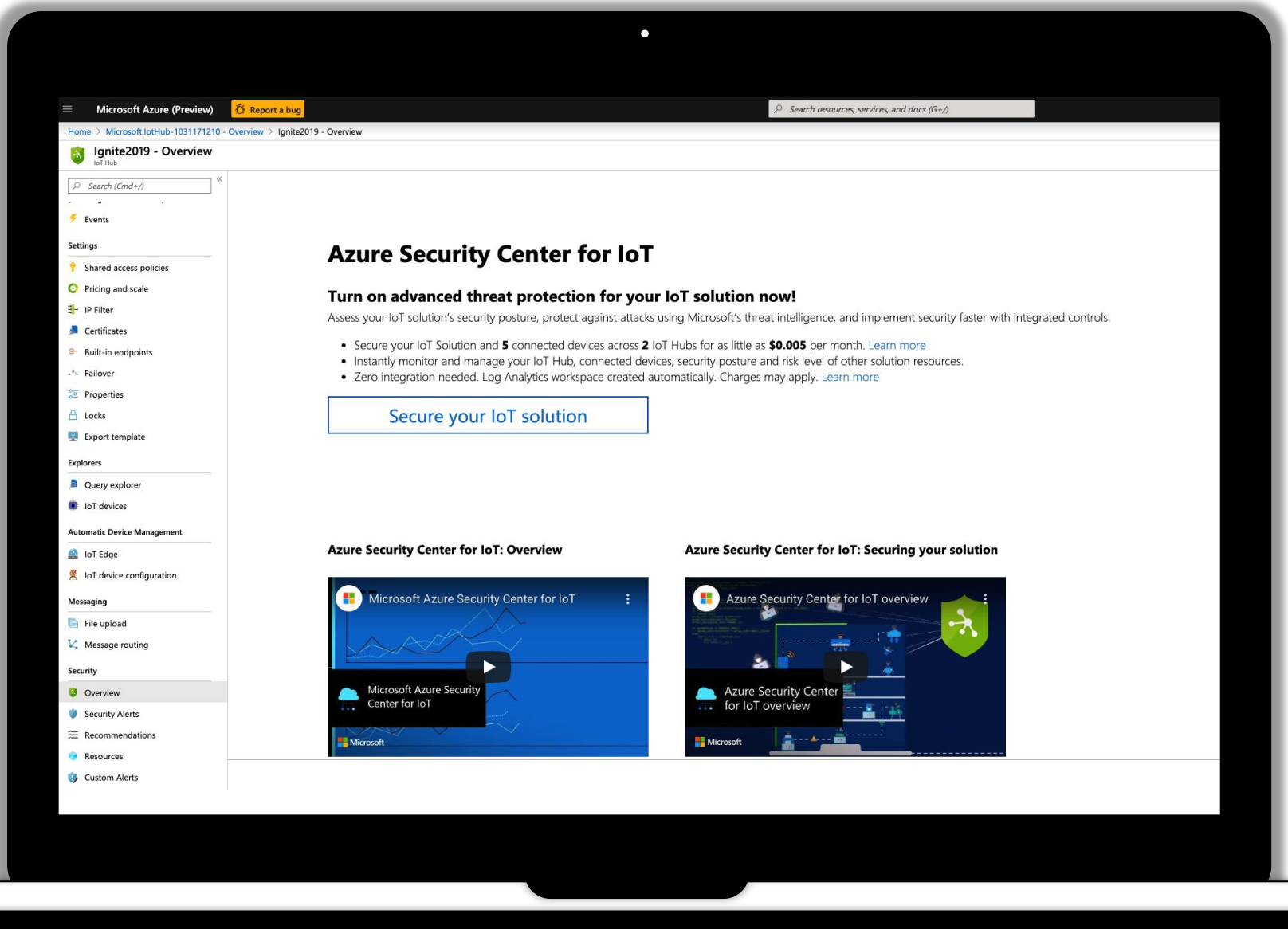
—Alex Kreilein, CISO

Support for national clouds

NEW Since GA

Azure Sentinel Integration is on the way

STAY SAFE


Microsoft Azure (Preview)
Report a bug
Search resources, services, and docs (G+/)
Home > Microsoft.IotHub-1031171210 - Overview > Ignite2019 - Overview
Ignite2019 - Overview
IoT Hub
Search (Cmd+/)
Events
Settings
Shared access policies
Pricing and scale
IP Filter
Certificates
Built-in endpoints
Failover
Properties
Locks
Export template
Explorers
Query explorer
IoT devices
Automatic Device Management
IoT Edge
IoT device configuration
Messaging
File upload
Message routing
Security
Overview
Security Alerts
Recommendations
Resources
Custom Alerts
Azure Security Center for IoT
Turn on advanced threat protection for your IoT solution now!
Assess your IoT solution's security posture, protect against attacks using Microsoft's threat intelligence, and implement security faster with integrated controls.
Secure your IoT Solution and 5 connected devices across 2 IoT Hubs for as little as $0.005 per month. Learn more
Instantly monitor and manage your IoT Hub, connected devices, security posture and risk level of other solution resources.
Zero integration needed. Log Analytics workspace created automatically. Charges may apply. Learn more
Secure your IoT solution
Azure Security Center for IoT: Overview
Microsoft Azure Security Center for IoT
Azure Security Center for IoT: Securing your solution
Azure Security Center for IoT overview

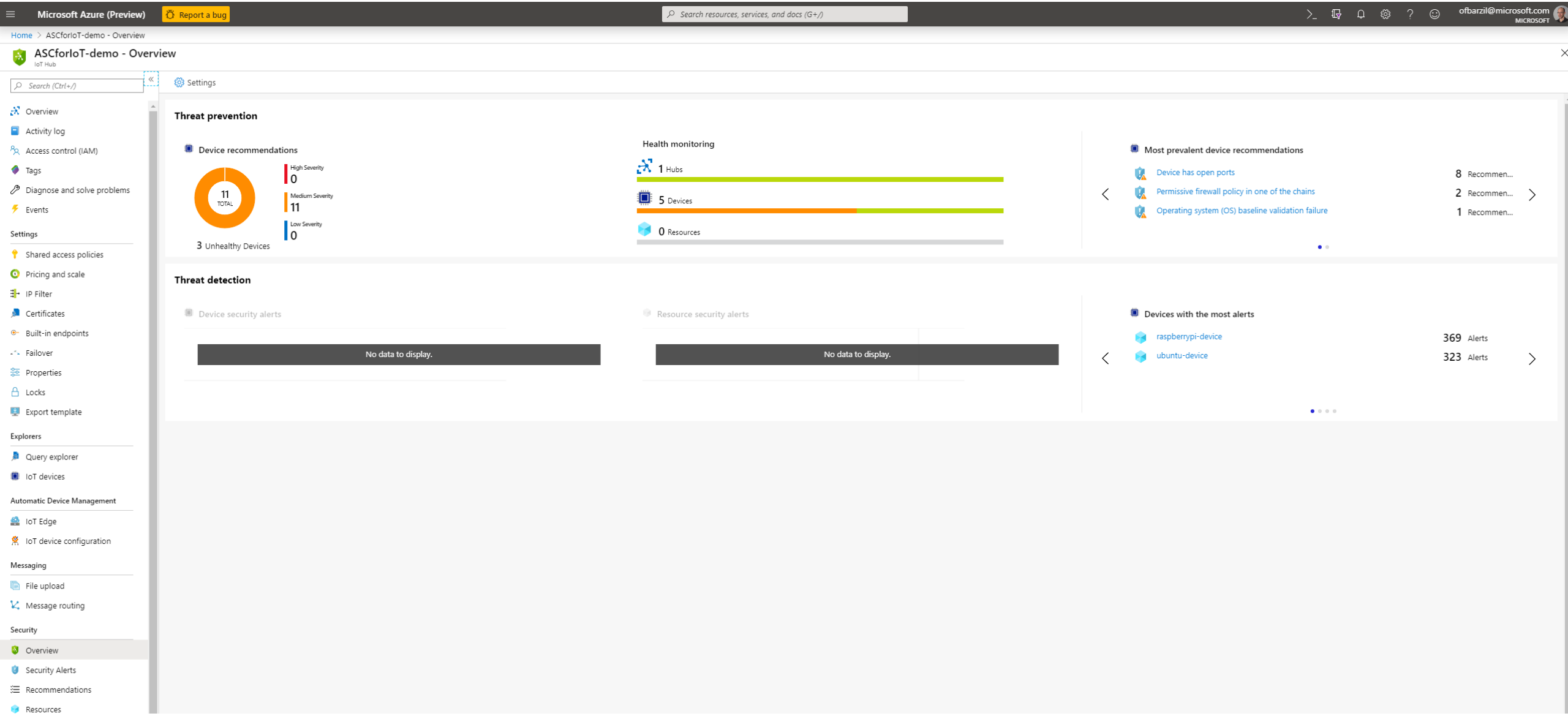
Microsoft

Thank you

Eti Fakiri
Sr. Program Manager
Eti.Fakiri@Microsoft.com

Demo

Ofir Barzilay and Idan Perkal


Microsoft Azure (Preview)
Report a bug
Search resources, services, and docs (G+/)
ofbarzil@microsoft.com
MICROSOFT
Home
ASCforIoT-demo - Overview
ASCforIoT-demo - Overview
IoT Hub
Search (Ctrl+/)
Settings
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events
Settings
Shared access policies
Pricing and scale
IP Filter
Certificates
Built-in endpoints
Failover
Properties
Locks
Export template
Explorers
Query explorer
IoT devices
Automatic Device Management
IoT Edge
IoT device configuration
Messaging
File upload
Message routing
Security
Overview
Security Alerts
Recommendations
Resources
Threat prevention
Device recommendations
11
TOTAL
3 Unhealthy Devices
High Severity
0
Medium Severity
11
Low Severity
0
Health monitoring
1 Hubs
5 Devices
0 Resources
Most prevalent device recommendations
Device has open ports
8 Recommen...
Permissive firewall policy in one of the chains
2 Recommen...
Operating system (OS) baseline validation failure
1 Recommen...
Threat detection
Device security alerts
No data to display.
Resource security alerts
No data to display.
Devices with the most alerts
raspberrypi-device
369 Alerts
ubuntu-device
323 Alerts

ASCforIoT-demo - Recommendations

IoT Hub

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events

Settings
Shared access policies
Pricing and scale
IP Filter
Certificates
Built-in endpoints
Failover
Properties
Locks
Export template

Explorers
Query explorer
IoT devices

Automatic Device Management
IoT Edge
IoT device configuration

Messaging
File upload
Message routing

Security
Overview
Security Alerts
Recommendations

Recommendation	Total	Severity
Device has open ports	8 of 5 IoT devices	
Permissive firewall policy in one of the chains	2 of 5 IoT devices	
Operating system (OS) baseline validation failure	1 of 5 IoT devices	

ASCforIoT-demo - Security Alerts

IoT Hub

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events

Settings
Shared access policies
Pricing and scale
IP Filter
Certificates
Built-in endpoints
Failover
Properties
Locks
Export template

Explorers
Query explorer
IoT devices

Automatic Device Management
IoT Edge
IoT device configuration

Messaging
File upload
Message routing

Security
Overview
Security Alerts
Recommendations

Description	Count	Detected By	Environment	Date	State	Severity
NEW Successful remote login	8	Microsoft	Devices	10/29/19	Active	High
NEW Reverse shells	2	Microsoft	Devices	10/29/19	Active	High
NEW Suspicious IP address communication	4	Microsoft	Devices	10/29/19	Active	High
NEW Crypto coin miner image	2	Microsoft	Devices	10/29/19	Active	High
NEW Bruteforce attempt	8	Microsoft	Devices	10/29/19	Active	Medium
NEW Removal of system logs files detected	6	Microsoft	Devices	10/29/19	Active	Medium
NEW Detected file download from a known malicious source	2	Microsoft	Devices	10/29/19	Active	Medium
NEW Local host reconnaissance detected	2	Microsoft	Devices	10/29/19	Active	Medium
NEW Detected suspicious use of the useradd command	2	Microsoft	Devices	10/29/19	Active	Medium
NEW Attempted Spray Attack	1	Microsoft	Devices	10/29/19	Active	Medium

ASCforIoT-demo - Security Alerts

IoT Hub

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events

Settings
Shared access policies
Pricing and scale
IP Filter
Certificates
Built-in endpoints
Failover
Properties
Locks
Export template

Explorers
Query explorer
IoT devices

Automatic Device Management
IoT Edge
IoT device configuration

Messaging
File upload
Message routing

Security
Overview
Security Alerts
Recommendations

Description	Count	Detected By	Environment	Date
NEW Successful remote login	8	Microsoft	Devices	10/29/19
NEW Reverse shells	2	Microsoft	Devices	10/29/19
NEW Suspicious IP address communication	4	Microsoft	Devices	10/29/19
NEW Crypto coin miner image	2	Microsoft	Devices	10/29/19
NEW Bruteforce attempt	8	Microsoft	Devices	10/29/19
NEW Removal of system logs files detected	6	Microsoft	Devices	10/29/19
NEW Detected file download from a known malicious source	2	Microsoft	Devices	10/29/19
NEW Local host reconnaissance detected	2	Microsoft	Devices	10/29/19
NEW Detected suspicious use of the useradd command	2	Microsoft	Devices	10/29/19
NEW Attempted Spray Attack	1	Microsoft	Devices	10/29/19

Successful remote login

General information

Description	Successful remote login to the device detected
Detection time	2019-10-29
Resource type	IoT device
Severity	High
State	Active
Subscription	075423e9-7d33-4166-8bdf-3920b04e3735
Detected by	Microsoft
Action Taken	Detected
Environment	Devices

Remediation steps

Make sure the logged in user is an authorized party.

Last 10 Affected Devices

Name	Alerts Count	Last Occurrence
ubuntu-device	8	07:12

Show all devices related to the alert

ASCforIoT-demo - Security Alerts

IoT Hub

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events

Settings
Shared access policies
Pricing and scale
IP Filter
Certificates
Built-in endpoints
Failover
Properties
Locks
Export template

Explorers
Query explorer
IoT devices

Automatic Device Management
IoT Edge
IoT device configuration

Messaging
File upload
Message routing

Security
Overview
Security Alerts
Recommendations

Description	Count	Detected By	Environment	Date
NEW Successful remote login	8	Microsoft	Devices	10/29/19
NEW Reverse shells	2	Microsoft	Devices	10/29/19
NEW Suspicious IP address communication	4	Microsoft	Devices	10/29/19
NEW Crypto coin miner image	2	Microsoft	Devices	10/29/19
NEW Bruteforce attempt	8	Microsoft	Devices	10/29/19
NEW Removal of system logs files detected	6	Microsoft	Devices	10/29/19
NEW Detected file download from a known malicious source	2	Microsoft	Devices	10/29/19
NEW Local host reconnaissance detected	2	Microsoft	Devices	10/29/19
NEW Detected suspicious use of the useradd command	2	Microsoft	Devices	10/29/19
NEW Attempted Spray Attack	1	Microsoft	Devices	10/29/19

Reverse shells

General information

Description	Analysis of host data on %{Compromised Host} detected a potential reverse shell. Reverse shells are often used to get a compromised machine to call back into a machine controlled by a malicious actor.
Detection time	2019-10-29
Resource type	IoT device
Severity	High
State	Active
Subscription	075423e9-7d33-4166-8bdf-3920b04e3735
Detected by	Microsoft
Action Taken	Detected
Environment	Devices

Remediation steps

Review with the user that ran the command if this was legitimate activity that you expect to see on the device. If not, escalate the alert to the information security team.

Last 10 Affected Devices

Name	Alerts Count	Last Occurrence
ubuntu-device	2	07:36

Show all devices related to the alert

ASCforIoT-demo - Security Alerts

IoT Hub

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events

Settings
Shared access policies
Pricing and scale
IP Filter
Certificates
Built-in endpoints
Failover
Properties
Locks
Export template

Explorers
Query explorer
IoT devices

Automatic Device Management
IoT Edge
IoT device configuration

Messaging
File upload
Message routing

Security
Overview
Security Alerts
Recommendations

Description	Count	Detected By	Environment	Date
NEW Successful remote login	8	Microsoft	Devices	10/29/19
NEW Reverse shells	2	Microsoft	Devices	10/29/19
NEW Suspicious IP address communication	4	Microsoft	Devices	10/29/19
NEW Crypto coin miner image	2	Microsoft	Devices	10/29/19
NEW Bruteforce attempt	8	Microsoft	Devices	10/29/19
NEW Removal of system logs files detected	6	Microsoft	Devices	10/29/19
NEW Detected file download from a known malicious source	2	Microsoft	Devices	10/29/19
NEW Local host reconnaissance detected	2	Microsoft	Devices	10/29/19
NEW Detected suspicious use of the useradd command	2	Microsoft	Devices	10/29/19
NEW Attempted Spray Attack	1	Microsoft	Devices	10/29/19

Suspicious IP address communication

General information

Description	Communication with a suspicious IP address detected.
Detection time	2019-10-29
Resource type	IoT device
Severity	High
State	Active
Subscription	075423e9-7d33-4166-8bdf-3920b04e3735
Detected by	Microsoft
Action Taken	Detected
Environment	Devices

Remediation steps

Verify if the connection is legitimate. Consider blocking communication with the suspicious IP.

Last 10 Affected Devices

Name	Alerts Count	Last Occurrence
ubuntu-device	4	07:13

Show all devices related to the alert

ASCforIoT-demo - Security Alerts

IoT Hub

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events

Settings
Shared access policies
Pricing and scale
IP Filter
Certificates
Built-in endpoints
Failover
Properties
Locks
Export template

Explorers
Query explorer
IoT devices

Automatic Device Management
IoT Edge
IoT device configuration

Messaging
File upload
Message routing

Security
Overview
Security Alerts
Recommendations

Description	Count	Detected By	Environment	Date
NEW Successful remote login	8	Microsoft	Devices	10/29/19
NEW Reverse shells	2	Microsoft	Devices	10/29/19
NEW Suspicious IP address communication	4	Microsoft	Devices	10/29/19
NEW Crypto coin miner image	2	Microsoft	Devices	10/29/19
NEW Bruteforce attempt	8	Microsoft	Devices	10/29/19
NEW Removal of system logs files detected	6	Microsoft	Devices	10/29/19
NEW Detected file download from a known malicious source	2	Microsoft	Devices	10/29/19
NEW Local host reconnaissance detected	2	Microsoft	Devices	10/29/19
NEW Detected suspicious use of the useradd command	2	Microsoft	Devices	10/29/19
NEW Attempted Spray Attack	1	Microsoft	Devices	10/29/19

Crypto coin miner image

General information

Description	Execution of a process normally associated with digital currency mining detected.
Detection time	2019-10-29
Resource type	IoT device
Severity	High
State	Active
Subscription	075423e9-7d33-4166-8bdf-3920b04e3735
Detected by	Microsoft
Action Taken	Detected
Environment	Devices

Remediation steps

Verify with the user that ran the command this was legitimate activity on the device. If not, escalate the alert to the information security team.

Last 10 Affected Devices

Name	Alerts Count	Last Occurrence
ubuntu-device	2	07:37

Show all devices related to the alert

ASCforIoT-demo - Security Alerts

IoT Hub

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events

Settings
Shared access policies
Pricing and scale
IP Filter
Certificates
Built-in endpoints
Failover
Properties
Locks
Export template

Explorers
Query explorer
IoT devices

Automatic Device Management
IoT Edge
IoT device configuration

Messaging
File upload
Message routing

Security
Overview
Security Alerts
Recommendations

Description	Count	Detected By	Environment	Date
NEW Successful remote login	8	Microsoft	Devices	10/29/19
NEW Reverse shells	2	Microsoft	Devices	10/29/19
NEW Suspicious IP address communication	4	Microsoft	Devices	10/29/19
NEW Crypto coin miner image	2	Microsoft	Devices	10/29/19
NEW Bruteforce attempt	8	Microsoft	Devices	10/29/19
NEW Removal of system logs files detected	6	Microsoft	Devices	10/29/19
NEW Detected file download from a known malicious source	2	Microsoft	Devices	10/29/19
NEW Local host reconnaissance detected	2	Microsoft	Devices	10/29/19
NEW Detected suspicious use of the useradd command	2	Microsoft	Devices	10/29/19
NEW Attempted Spray Attack	1	Microsoft	Devices	10/29/19

Bruteforce attempt

General information

Description	Multiple login attempts identified. Potential Bruteforce attack attempted on the device.
Detection time	2019-10-29
Resource type	IoT device
Severity	Medium
State	Active
Subscription	075423e9-7d33-4166-8bdf-3920b04e3735
Detected by	Microsoft
Action Taken	Detected
Environment	Devices

Remediation steps

Review SSH bruteforce alert and the activity on the devices. If the activity was malicious: 1.Roll out password reset for compromised accounts. 2.Investigate and remediate(if found) devices for malware.

Last 10 Affected Devices

Name	Alerts Count	Last Occurrence
ubuntu-device	8	10:15

Show all devices related to the alert

ASCforIoT-demo - Security Alerts

IoT Hub

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events

Settings
Shared access policies
Pricing and scale
IP Filter
Certificates
Built-in endpoints
Failover
Properties
Locks
Export template

Explorers
Query explorer
IoT devices

Automatic Device Management
IoT Edge
IoT device configuration

Messaging
File upload
Message routing

Security
Overview
Security Alerts
Recommendations

Description	Count	Detected By	Environment	Date
NEW Successful remote login	8	Microsoft	Devices	10/29/19
NEW Reverse shells	2	Microsoft	Devices	10/29/19
NEW Suspicious IP address communication	4	Microsoft	Devices	10/29/19
NEW Crypto coin miner image	2	Microsoft	Devices	10/29/19
NEW Bruteforce attempt	8	Microsoft	Devices	10/29/19
NEW Removal of system logs files detected	6	Microsoft	Devices	10/29/19
NEW Detected file download from a known malicious source	2	Microsoft	Devices	10/29/19
NEW Local host reconnaissance detected	2	Microsoft	Devices	10/29/19
NEW Detected suspicious use of the useradd command	2	Microsoft	Devices	10/29/19
NEW Attempted Spray Attack	1	Microsoft	Devices	10/29/19

Removal of system logs files detected

General information

Description	Suspicious removal of log files on the host detected.
Detection time	2019-10-29
Resource type	IoT device
Severity	Medium
State	Active
Subscription	075423e9-7d33-4166-8bdf-3920b04e3735
Detected by	Microsoft
Action Taken	Detected
Environment	Devices

Remediation steps

Review with the user that ran the command if this was legitimate activity that you expect to see on the device. If not, escalate the alert to the information security team.

Last 10 Affected Devices

Name	Alerts Count	Last Occurrence
ubuntu-device	6	07:35

Show all devices related to the alert

ASCforIoT-demo - Security Alerts

IoT Hub

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events

Settings
Shared access policies
Pricing and scale
IP Filter
Certificates
Built-in endpoints
Failover
Properties
Locks
Export template

Explorers
Query explorer
IoT devices

Automatic Device Management
IoT Edge
IoT device configuration

Messaging
File upload
Message routing

Security
Overview
Security Alerts
Recommendations

Description	Count	Detected By	Environment	Date
NEW Successful remote login	8	Microsoft	Devices	10/29/19
NEW Reverse shells	2	Microsoft	Devices	10/29/19
NEW Suspicious IP address communication	4	Microsoft	Devices	10/29/19
NEW Crypto coin miner image	2	Microsoft	Devices	10/29/19
NEW Bruteforce attempt	8	Microsoft	Devices	10/29/19
NEW Removal of system logs files detected	6	Microsoft	Devices	10/29/19
NEW Detected file download from a known malicious source	2	Microsoft	Devices	10/29/19
NEW Local host reconnaissance detected	2	Microsoft	Devices	10/29/19
NEW Detected suspicious use of the useradd command	2	Microsoft	Devices	10/29/19
NEW Attempted Spray Attack	1	Microsoft	Devices	10/29/19

Detected file download from a known malicious source

General information

Description	Download of a file from a known malware source detected.
Detection time	2019-10-29
Resource type	IoT device
Severity	Medium
State	Active
Subscription	075423e9-7d33-4166-8bdf-3920b04e3735
Detected by	Microsoft
Action Taken	Detected
Environment	Devices

Remediation steps

Review with the user that ran the command if this was legitimate activity that you expect to see on the device. If not, escalate the alert to the information security team.

Last 10 Affected Devices

Name	Alerts Count	Last Occurrence
ubuntu-device	2	07:41

Show all devices related to the alert

ASCforIoT-demo - Security Alerts

IoT Hub

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events

Settings
Shared access policies
Pricing and scale
IP Filter
Certificates
Built-in endpoints
Failover
Properties
Locks
Export template

Explorers
Query explorer
IoT devices

Automatic Device Management
IoT Edge
IoT device configuration

Messaging
File upload
Message routing

Security
Overview
Security Alerts
Recommendations

Description	Count	Detected By	Environment	Date
NEW Successful remote login	8	Microsoft	Devices	10/29/19
NEW Reverse shells	2	Microsoft	Devices	10/29/19
NEW Suspicious IP address communication	4	Microsoft	Devices	10/29/19
NEW Crypto coin miner image	2	Microsoft	Devices	10/29/19
NEW Bruteforce attempt	8	Microsoft	Devices	10/29/19
NEW Removal of system logs files detected	6	Microsoft	Devices	10/29/19
NEW Detected file download from a known malicious source	2	Microsoft	Devices	10/29/19
NEW Local host reconnaissance detected	2	Microsoft	Devices	10/29/19
NEW Detected suspicious use of the useradd command	2	Microsoft	Devices	10/29/19
NEW Attempted Spray Attack	1	Microsoft	Devices	10/29/19

Local host reconnaissance detected

General information

Description	Execution of a command normally associated with common Linux bot reconnaissance detected.
Detection time	2019-10-29
Resource type	IoT device
Severity	Medium
State	Active
Subscription	075423e9-7d33-4166-8bdf-3920b04e3735
Detected by	Microsoft
Action Taken	Detected
Environment	Devices

Remediation steps

Review the suspicious command line to confirm that it was executed by a legitimate user. If not, escalate the alert to your information security team.

Last 10 Affected Devices

Name	Alerts Count	Last Occurrence
ubuntu-device	2	07:41

Show all devices related to the alert

ASCforIoT-demo - Security Alerts

IoT Hub

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events

Settings
Shared access policies
Pricing and scale
IP Filter
Certificates
Built-in endpoints
Failover
Properties
Locks
Export template

Explorers
Query explorer
IoT devices

Automatic Device Management
IoT Edge
IoT device configuration

Messaging
File upload
Message routing

Security
Overview
Security Alerts
Recommendations

Description	Count	Detected By	Environment	Date
NEW Successful remote login	8	Microsoft	Devices	10/29/19
NEW Reverse shells	2	Microsoft	Devices	10/29/19
NEW Suspicious IP address communication	4	Microsoft	Devices	10/29/19
NEW Crypto coin miner image	2	Microsoft	Devices	10/29/19
NEW Bruteforce attempt	8	Microsoft	Devices	10/29/19
NEW Removal of system logs files detected	6	Microsoft	Devices	10/29/19
NEW Detected file download from a known malicious source	2	Microsoft	Devices	10/29/19
NEW Local host reconnaissance detected	2	Microsoft	Devices	10/29/19
NEW Detected suspicious use of the useradd command	2	Microsoft	Devices	10/29/19
NEW Attempted Spray Attack	1	Microsoft	Devices	10/29/19

Detected suspicious use of the useradd command

General information

Description	Suspicious use of the useradd command detected on the device.
Detection time	2019-10-29
Resource type	IoT device
Severity	Medium
State	Active
Subscription	075423e9-7d33-4166-8bdf-3920b04e3735
Detected by	Microsoft
Action Taken	Detected
Environment	Devices

Remediation steps

Review with the user that ran the command if this was legitimate activity that you expect to see on the device. If not, escalate the alert to the information security team.

Last 10 Affected Devices

Name	Alerts Count	Last Occurrence
ubuntu-device	2	07:33

Show all devices related to the alert

ASCforIoT-demo - Security Alerts

IoT Hub

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events

Settings
Shared access policies
Pricing and scale
IP Filter
Certificates
Built-in endpoints
Failover
Properties
Locks
Export template

Explorers
Query explorer
IoT devices

Automatic Device Management
IoT Edge
IoT device configuration

Messaging
File upload
Message routing

Security
Overview
Security Alerts
Recommendations

Description	Count	Detected By	Environment	Date
NEW Successful remote login	8	Microsoft	Devices	10/29/19
NEW Reverse shells	2	Microsoft	Devices	10/29/19
NEW Suspicious IP address communication	4	Microsoft	Devices	10/29/19
NEW Crypto coin miner image	2	Microsoft	Devices	10/29/19
NEW Bruteforce attempt	8	Microsoft	Devices	10/29/19
NEW Removal of system logs files detected	6	Microsoft	Devices	10/29/19
NEW Detected file download from a known malicious source	2	Microsoft	Devices	10/29/19
NEW Local host reconnaissance detected	2	Microsoft	Devices	10/29/19
NEW Detected suspicious use of the useradd command	2	Microsoft	Devices	10/29/19
NEW Attempted Spray Attack	1	Microsoft	Devices	10/29/19

Attempted Spray Attack

General information

Description	Multiple login attempts were identified. Potential Spray Attack attack on the device.
Detection time	2019-10-29
Resource type	IoT device
Severity	Medium
State	Active
Subscription	075423e9-7d33-4166-8bdf-3920b04e3735
Detected by	Microsoft
Action Taken	Detected
Environment	Devices

Remediation steps

Review Spray Attack alert and the activity on the devices. If the activity was malicious: 1.Roll out password reset for compromised accounts. 2.Investigate and remediate(if found) devices for malware.

Last 10 Affected Devices

Name	Alerts Count	Last Occurrence
ubuntu-device	1	07:15

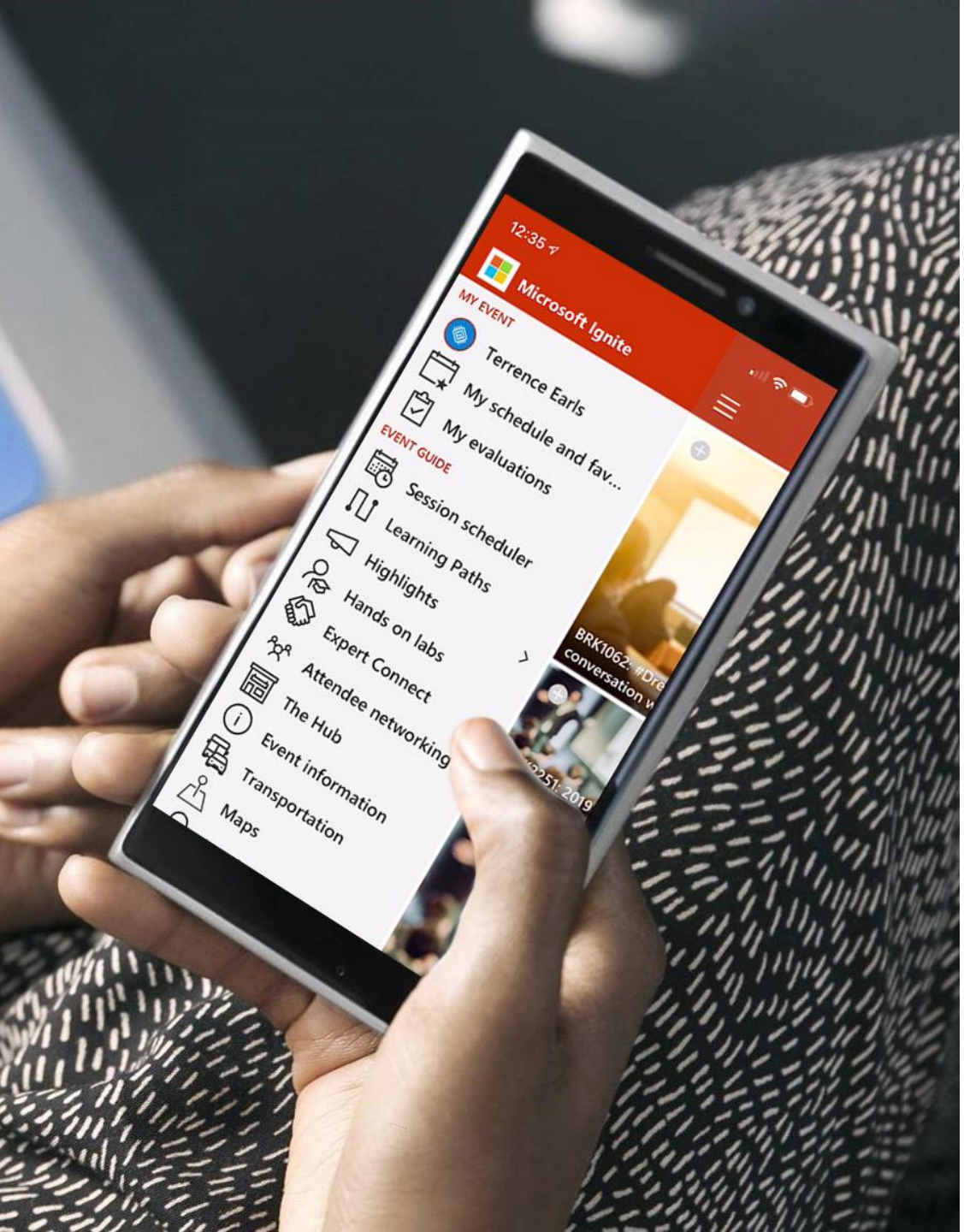
Show all devices related to the alert

```
##############################################################
        Brute Force Password Guessing
##############################################################
Mon Oct 28 17:02:02 UTC 2019  Using real Mirai credentials to try to connect...
Mon Oct 28 17:02:02 UTC 2019  Trying to connect to target with username root and password root...
Permission denied, please try again.
Mon Oct 28 17:02:06 UTC 2019  Trying to connect to target with username root and password user...
Permission denied, please try again.
Mon Oct 28 17:02:10 UTC 2019  Trying to connect to target with username root and password anko...
Permission denied, please try again.
Mon Oct 28 17:02:13 UTC 2019  Trying to connect to target with username root and password 0...
Permission denied, please try again.
Mon Oct 28 17:02:17 UTC 2019  Trying to connect to target with username root and password vizxv...
Permission denied, please try again.
Mon Oct 28 17:02:23 UTC 2019  Trying to connect to target with username root and password root...
Permission denied, please try again.
.....[after more similar trials].....
Mon Oct 28 17:03:10 UTC 2019  Trying to connect to target with username ubuntu and password password...
Permission denied, please try again.
Mon Oct 28 17:03:14 UTC 2019  Trying to connect to target with username ubuntu and password ******...
Mon Oct 28 17:03:17 UTC 2019  Successfully connected to the device
total 16
-rw-r--r-- 1 root root   98 Oct 28 08:32 README
drwxr-xr-x 2 root root 4096 Oct 28 08:32 helloworld
-rwxr-xr-x 1 root root  121 Oct 28 08:32 helloworld.py
-rw-r--r-- 1 root root 1029 Oct 28 08:32 setup.py
Connection to target closed.
```

##
Covering traces in System Log Files
##
Mon Oct 28 17:03:22 UTC 2019 Removing system logs...
Mon Oct 28 17:03:25 UTC 2019 Removed system logs
##
Extracting Second Payload and Infecting Device
##
Mon Oct 28 17:03:25 UTC 2019 Downloading second payload from actor loader...
Mon Oct 28 17:03:25 UTC 2019 Extracting second payload and making it executable...
Mon Oct 28 17:03:33 UTC 2019 Installing and running malicious payload...

##
Getting device information
##
Mon Oct 28 17:03:35 UTC 2019 Conducting analysis of host data...
Linux ubuntu-vm 5.0.0-1022-azure #23~18.04.1-Ubuntu SMP Mon Sep 30 19:47:06 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
Mon Oct 28 17:03:35 UTC 2019 Got host data
##
Create User and Escalate Privilege
##
Mon Oct 28 17:03:35 UTC 2019 Adding user named privilegeduser10317 with privilege root to the system...
Mon Oct 28 17:03:36 UTC 2019 Successfully added user named privilegeduser10317 with privilege root to the system

##
Communicating with CnC for getting attack commands
##
Mon Oct 28 17:03:36 UTC 2019 Opening reverse shell...
Mon Oct 28 17:03:36 UTC 2019 Reverse shell established
Mon Oct 28 17:03:36 UTC 2019 Communicating with CnC server...
Mon Oct 28 17:03:36 UTC 2019 Listening to CnC for future attack commands...
##
Covering Tracks - Deleting Logs and Executables
##
Mon Oct 28 17:03:36 UTC 2019 Deleting history files...
Mon Oct 28 17:03:36 UTC 2019 Deleted history files
##
Installing (Fake) Crypto Currency miner
##
Mon Oct 28 17:03:36 UTC 2019 Setting up crypto miner...
Mon Oct 28 17:03:36 UTC 2019 Cloning into 'cpuminer'...
Mon Oct 28 17:03:36 UTC 2019 Mining crypto with device resources



Please evaluate this session

Your feedback is important to us!

Please evaluate this session through MyEvaluations on the mobile app or website.

Download the app:
https://aka.ms/ignite.mobileapp

Go to the website:
https://myignite.techcommunity.microsoft.com/evaluations

Find this session in Microsoft Tech Community

Visit aka.ms/MicrosoftIgnite2019/BRK2383

- ✓ Download slides and resources
- ✓ Access session recordings in 48 hours
- ✓ Ask questions & continue the conversation