RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: LAB4-T08

Cloud ctf: identifying and resolving attacks in azure

Johnathan Trull

Senior Director/Chief Strategist
Microsoft Cyber Solutions Group

Lesley Kipling

Lead investigator/Chief Security Advisor
Microsoft Cyber Solutions Group

Agenda

1. Welcome and introduction
2. Overview of Azure logging & monitoring
3. Review scenario, lab environment, and required tasks
4. Lab Time – Contoso Blue Team Activities
5. Wrap-up
   - Attacker Kill Chain Review
   - Post-Action Reporting and Lessons Learned Review

Welcome and Introduction

Jonathan Trull:
Mastermind

Henry
Parks

Ola
Peters

Red Team

Anthony
Petito

Chad
Munkelt

Lesley
Kipling

Blue Team

RSAConference2019

Overview of azure security logging & monitoring

What is Azure Log Analytics?

- Service that collects telemetry and other data from variety of sources, both on-premises and in the cloud
- Data stored in workspaces and organized into tables
- Provides a query language and analytics engine (Kusto) for analyzing the operations of Azure applications and resources
- Both Azure Security Center and Azure Insights stores its data in Log Analytics

Logs in Azure

Log Source	Description	Configuration Details
Azure Virtual Machines	Windows and Linux machines operating within Azure. Windows Events and Syslogs.	Use automatic provisioning of the Microsoft Monitoring Agent via Azure Security Center.
Subscriptions (Azure Activity Log) / Azure Resource Manager	Governs access to and use of Azure services and acts as a logical container for resources.	**Azure Activity Log** provides a history of subscription-level events in Azure.
Network Security Groups	Virtual firewall that can be applied to VMs, subnets, and Vnets.	Enable **NSG flow logging** for each NSG to ensure the source IP address that initiated the communication is captured
PaaS Services	Enable Azure Diagnostic logging. IIS Logging is enabled by default, and it is set to hourly generate files that contain all fields in W3C format http://download.microsoft.com/download/B/6/C/B6C0A98B-D34A-417C-826E-3EA28CDFC9DD/AzureSecurityandAuditLogManagement_11132014.pdf	RDP to the VM and run CollectGuestLogs.exe. CollectGuestLogs.exe ships with the Azure Guest Agent which is present on all PaaS VMs and most IaaS VMs and it will create a ZIP file of the logs from the VM.
Azure Security Center	Security Center collects data from your Azure VMs and non-Azure computers to monitor for security vulnerabilities and threats. Data is collected using the Microsoft Monitoring Agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. By default, Security Center will create a new workspace for you.	Ensure all subscriptions are onboarded and **enable standard tier**. When **automatic provisioning** is enabled, Security Center installs the **Microsoft Monitoring Agent** on all supported Azure VMs and any new ones that are created. Automatic provisioning is strongly recommended.
Azure Insights		

Log Analytics Query Language (Kusto)

Query	Description
Event	All Windows events
Event | where EventLevelName == “error”	All Windows events with severity of error
Event | summarize count() by Source	Count of Windows events by source
Event | where EventLevelName == “error” | summarize count() by Source	Count of Windows error events by source

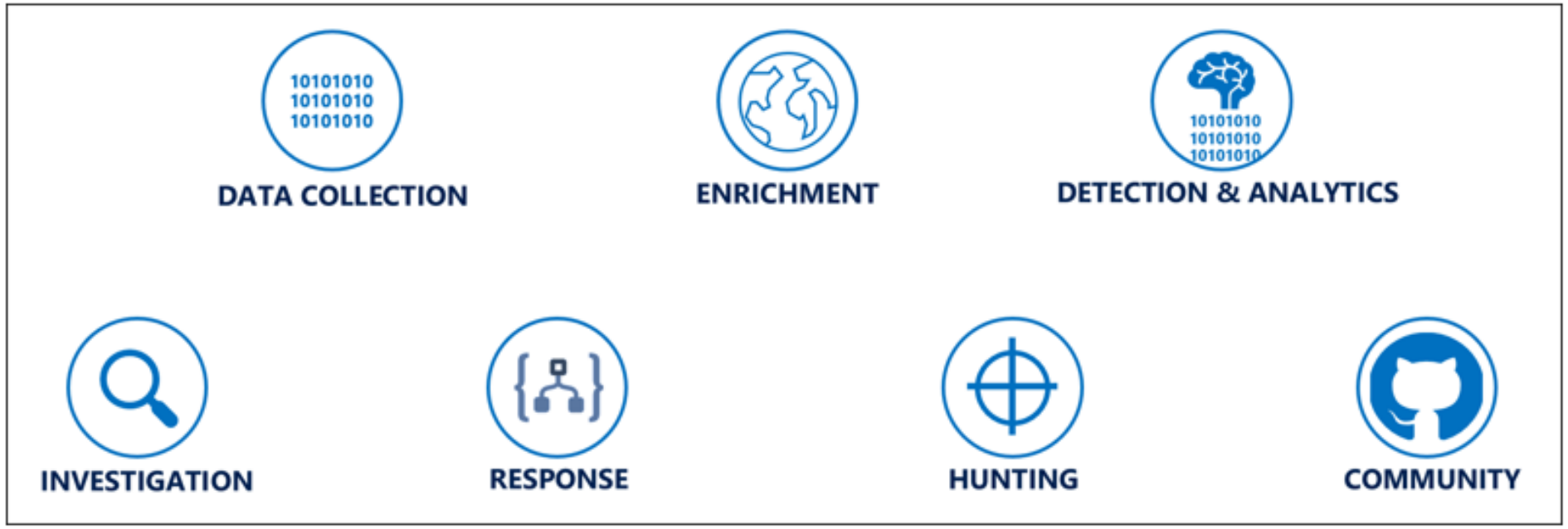
What is Azure Security Center?

- Azure service designed to unify security management, includes functions for unified security visibility & control, threat detection, and incident detection and response
- Integrated with Azure Log Analytics
- Designed for Compliance and Policy personas

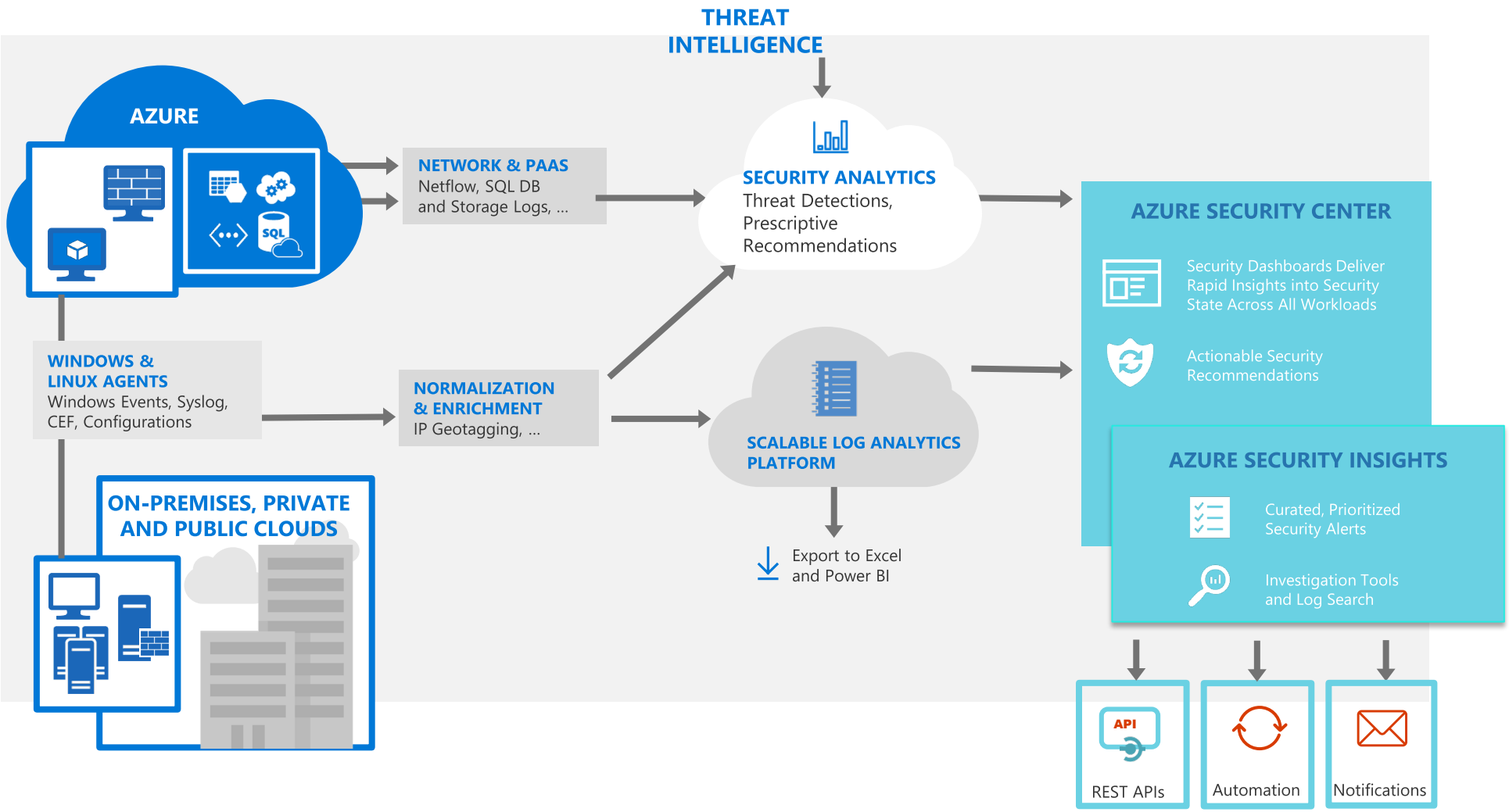
What is Azure Security Center?

- Integrated with Azure Log Analytics
- Collects and analyzes security events from multiple sources
  - Third party security solutions & appliances
  - Azure Active Directory
  - Any solution that supports Common Event Format (CEF)
- Designed for SOC personas

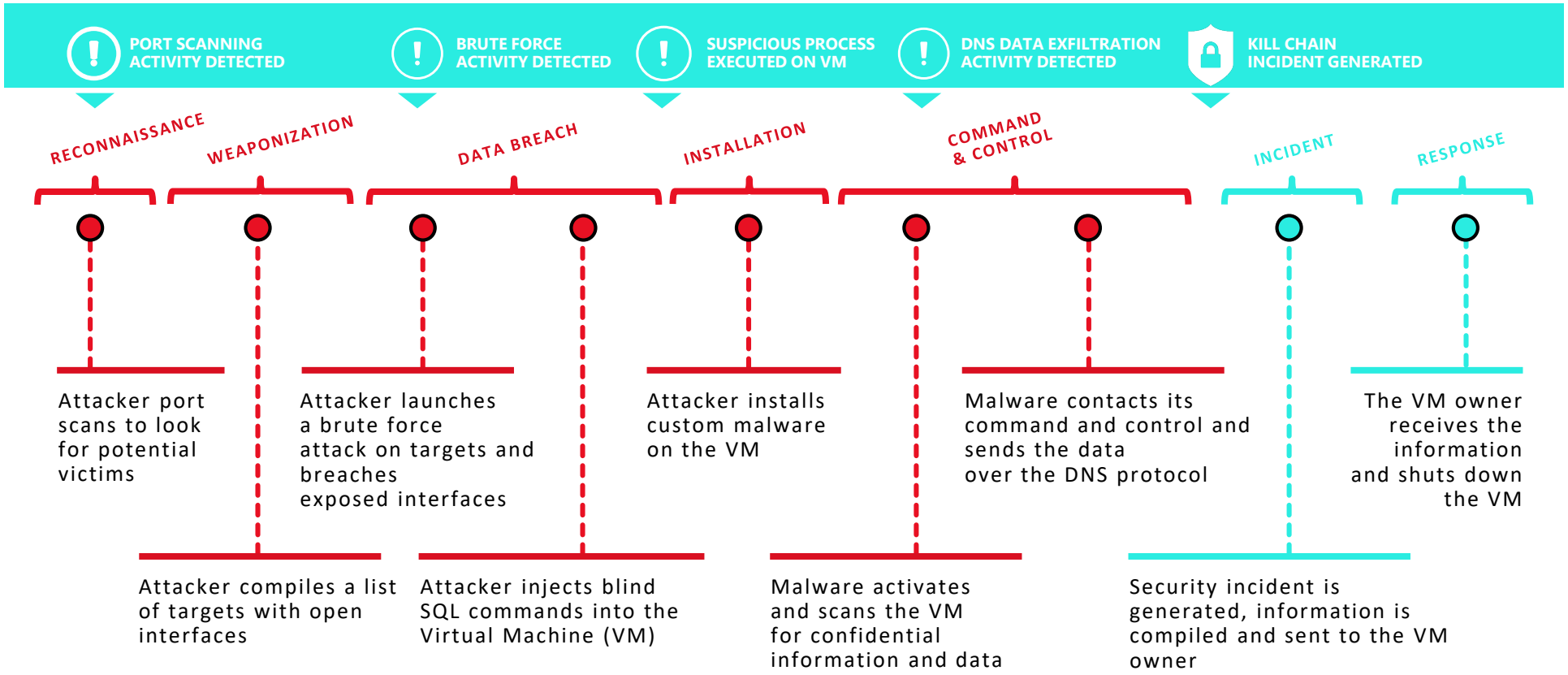
What is Azure Security Insights?



Azure Security Architecture

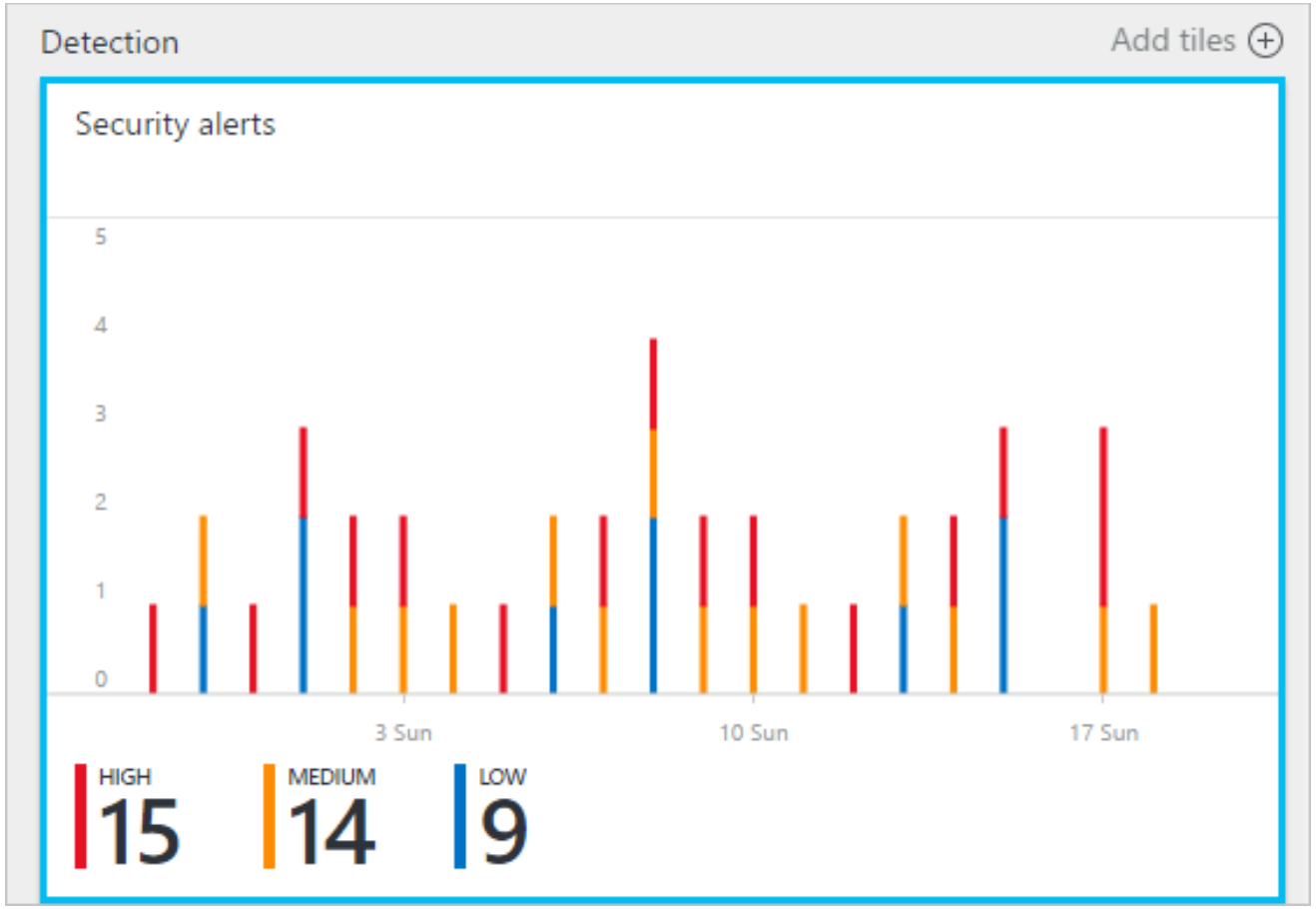


ASI detections across the kill chain



Detection Example

Azure Security Insights
Security Alerts tile



Detection Example

DESCRIPTION	COUNT	DETECTED BY	DATE	STATE	SEVERITY
Failed RDP Brute Force Attack	3	Microsoft	07/11/16	Active	Medium
Malicious SQL activity	1	Microsoft	07/17/16	Active	High
Modified system binary discovered in dump file 5bd7...	1	Microsoft	07/15/16	Active	High
Suspicious process executed	2	Microsoft	07/14/16	Active	High
Successful RDP brute force attack	1	Microsoft	07/12/16	Active	High
Network communication with a malicious machine de...	1	Microsoft	07/01/16	Active	Low
Malicious SQL activity	1	Microsoft	07/09/16	Active	High
Modified system binary discovered in dump file 5bd7...	1	Microsoft	07/08/16	Active	High
Suspicious process executed	2	Microsoft	07/07/16	Active	High
Successful RDP brute force attack	1	Microsoft	07/05/16	Active	High
Possible outgoing spam activity detected	1	Microsoft	07/01/16	Active	Low

Detection Example

VM Behavioral Analysis
Suspicious SVCHOST Execution

1. Collect VM process creation logs (4688 event id)
2. Analyze events with NewProcessName == “SVCHOST”
3. Verify executing user, command line params, parent process, integrity

Event 4688, Microsoft Windows security auditing.

General | Details

New Process ID:	0x388c
New Process Name:	C:\Program Files\WindowsApps\Microsoft.SkypeApp_3.2.1.0_x86__kzf8qxf3
Token Elevation Type:	%%1938
Mandatory Label:	Mandatory Label\Low Mandatory Level
Creator Process ID:	0x334
Creator Process Name:	C:\Windows\System32\svchost.exe
Process Command Line:	"C:\Program Files\WindowsApps\Microsoft.SkypeApp_3.2.1.0_x86__kzf8qxf

ServerName:App.AppXd9hrtyv8f50cbpnsp68wvxkhryqetej2.mca

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	5/14/2016 11:11:48 PM
Event ID:	4688	Task Category:	Process Creation
Level:	Information	Keywords:	Audit Success

Detection Example

Kusto Query for MiKatz

```
ProdProcessCreationEvents | where NewProcessName == "mimikatz.exe" or CommandLine contains "sekurlsa"
```

TimeCreated	NewProcessName	CommandLine
2016-02-23 04:19:22.3635227	C:\Users\SysmonAdmin\Desktop\x64\mimikatz.exe	mimikatz sekurlsa::pth
2016-02-23 04:21:21.7590425	C:\Users\SysmonAdmin\Desktop\x64\mimikatz.exe	mimikatz privilege::debug sekurlsa::logonpasswords
2016-02-23 04:21:29.9497724	C:\Users\SysmonAdmin\Desktop\x64\mimikatz.exe	mimikatz privilege::debug sekurlsa::pth
2016-02-23 04:22:03.9943399	C:\Users\SysmonAdmin\Desktop\x64\mimikatz.exe	mimikatz privilege::debug sekurlsa::pth exit
2016-02-23 04:23:01.2170367	C:\Users\SysmonAdmin\Desktop\x64\svchost.exe	svchost privilege::debug sekurlsa::pth exit
2016-02-23 04:23:22.5122936	C:\Users\SysmonAdmin\Desktop\x64\svchost.exe	svchost privilege::debug sekurlsa::pth exit
2016-02-23 04:23:30.6407026	C:\Users\SysmonAdmin\Desktop\x64\svchost.exe	svchost privilege::debug sekurlsa:logonpasswords exit
2016-02-23 04:23:39.5500934	C:\Users\SysmonAdmin\Desktop\x64\svchost.exe	svchost privilege::debug sekurlsa:logonpasswords
2016-02-23 04:23:56.0416915	C:\Users\SysmonAdmin\Desktop\x64\svchost.exe	svchost privilege::debug sekurlsa::logonpasswords

RSAConference2019

Review scenario, lab environment, and required tasks

Shadow IT Gone Wrong

CONTOSO LTD is a global trading company based in the United States but conducting business globally. The CTO has been under increasing pressure by the board to digitally transform their operations and services and close down capital intensive data center operations. As such, she directed her team to start using Azure about three months ago for testing purposes and to deploy some low-risk production workloads. CONTOSO's security team has not been part of the project, and has not been monitoring the workloads for threats.

You are the director of CONTOSO LTD's small information security team. On Friday just before 5 PM, the CTO calls you and says there might be a problem. "You know that Azure project we've been talking about. Well, we kicked it off about three months ago. And here's the thing, we're seeing some strange things and are worried we've been compromised. Sorry for not bringing you in sooner but I need you to look into it ASAP."

Lab time – contoso blue team activities – 60 Minutes

1. Get familiar with the lab environment
2. Identify sources of available logs, review configurations, and centralize logs as needed
3. Hunt through logs for evidence of attack
   - Suggest starting your investigation with the Security Alerts Tile located in Azure Security Insights
4. Document the details of the incident, including attack details and whether or not sensitive data was exposed
5. Identify control weaknesses that led to attack and recommend countermeasures

Rules of Engagement

- You have one hour to complete the lab
- Everything you need to know is in your lab handout
- If you have any questions or need help, please let us know
- Relax and have fun!

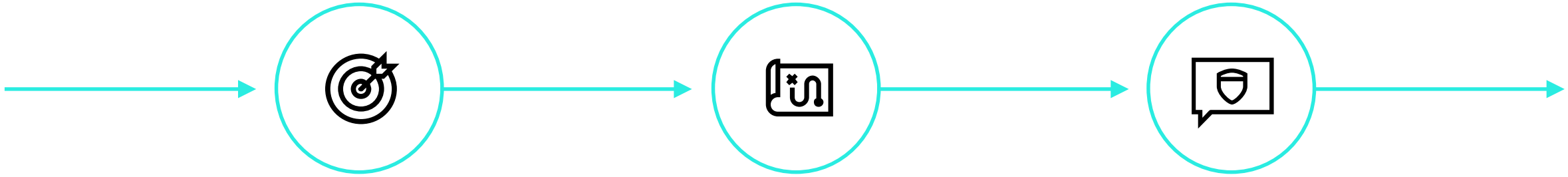
RSAConference2019

Wrap-up

Attacker Review

Initial Access	*Execution*	*Persistence*	*Lateral Movement*
RDP Brute Force	Command-Line Interface	New valid user accounts	SSH
SQL Injection Vulnerability	Regsvr32	Scheduled Task creation	Exfiltration
Legitimate Credentials/Access Keys			

Cloud attacks kill chain



Target and attack

Inbound brute-force RDP, SSH, SQL attacks and more

Application and DDoS attacks (WAF partners)

Intrusion detection (NG Firewall partners)

Install and exploit

In-memory malware and exploit attempts

Suspicious process execution

Lateral movement

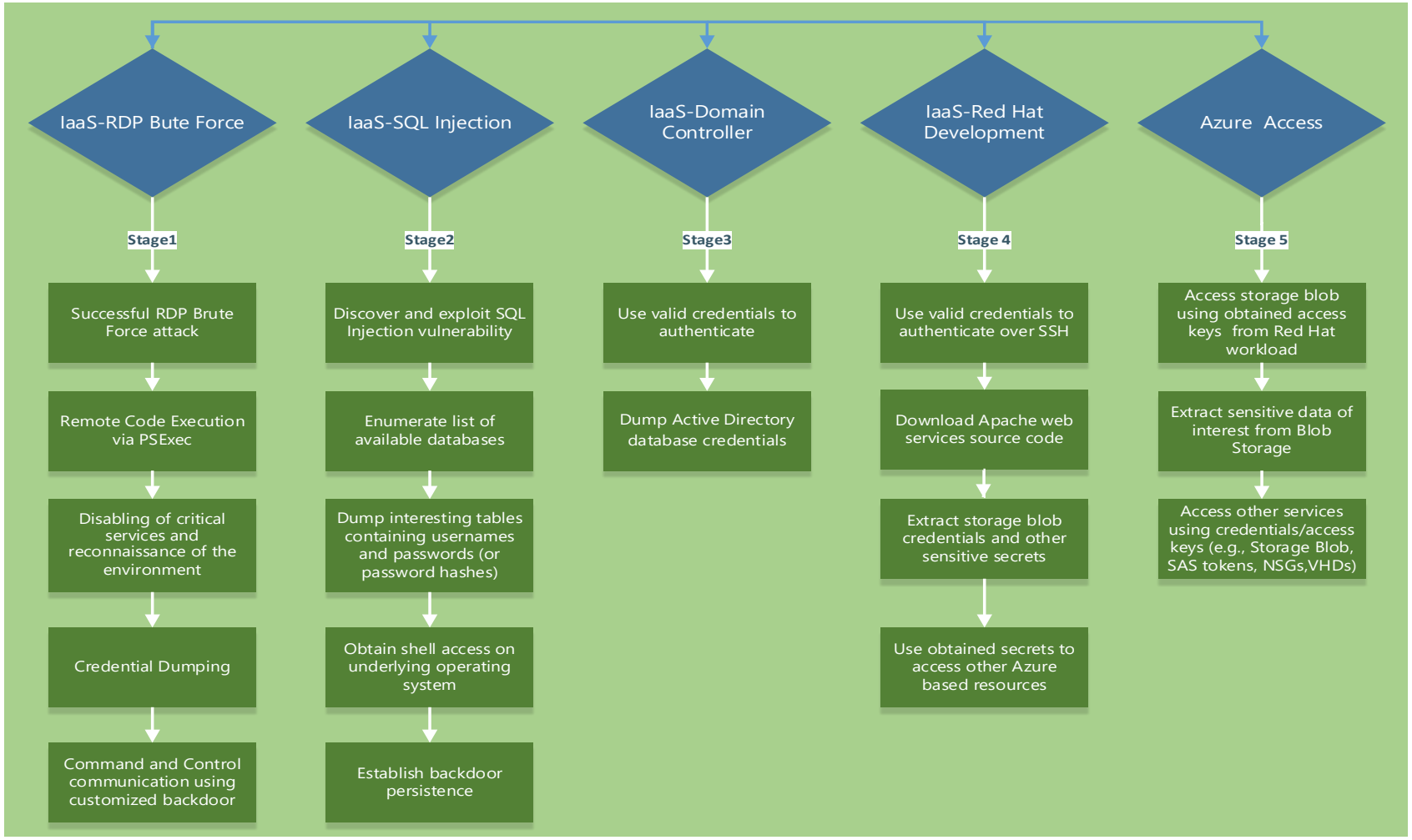
Internal reconnaissance

Post breach

Communication to a known malicious IP (data exfiltration or command and control)

Using compromised resources to mount additional attacks (outbound port scanning, brute-force RDP/SSH attacks, DDoS, and spam)

Red Team Activities Overview



RSAConference2019

Protection mechanisms

Control Weaknesses & mitigations

- **Control Weakness 1 – Administrative endpoints exposed to the internet**
  - Remediation action: Disable direct RDP and SSH access to Azure Virtual Machines from the internet. More secure mechanisms include:
    - Network Security Groups (NSG)
    - Point-to-Site VPN
    - Site-to-Site VPN
    - ExpressRoute
- **Control Weakness 2 - SQL Server Web Application Firewall Not Enabled**
  - Remediation action: Enable and monitor alerts from a Web Application Firewall (WAF) to protect against web vulnerabilities and attacks.
- **Control Weakness 3 - Storing of sensitive access keys**
  - Remediation action: Use Azure Key Vault to safeguard cryptographic keys and secrets used by cloud application and services.
- **Control Weakness 4 - Monitoring of Azure Security Center alerts**
  - Remediation action: Review Azure Security Center alerts to ensure that both existing vulnerabilities and threats are being remediated.

Advanced Cloud Defence

ADVANCED CLOUD DEFENSE

- Adaptive application controls
- Just in time VM access
- File Integrity Monitoring (Pre...

Block Malware

Block Brute Force

What is application control?

Application control helps you deal with malicious and/or unauthorized software, by allowing only specific applications to run on your VMs

How does it work?

Security Center analyzes data of applications to find VMs for which there is a constant set of running applications. Security Center creates whitelisting rules for each group and presents the rules in the form of a recommendation. Once the recommendation is resolved, Security Center configures it by leveraging Applocker capabilities.

Some subscriptions have limited protection. Upgrade to Standard to enhance their security →

What is just in time VM access?

Just in time VM access enables you to lock down your VMs in the network level by blocking inbound traffic to specific ports. It enables you to control the access and reduce the attack surface to your VMs, by allowing access only upon a specific need.

How does it work?

Upon a user request, based on Azure RBAC, Security Center will decide whether to grant access. If a request is approved, Security Center automatically configures the NSGs to allow inbound traffic to these ports, for the requested amount of time, after which it restores the NSGs to their previous states.

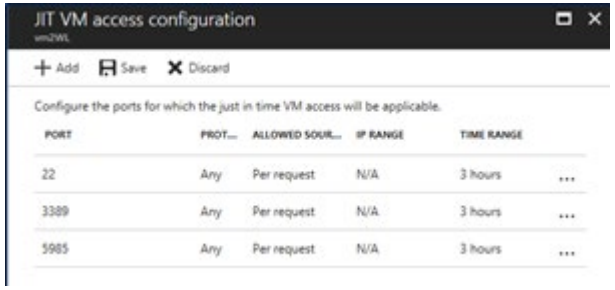
File Integrity Monitoring (Preview)

Choose a workspace to view its File Integrity Monitoring dashboard

Security Center's File Integrity Monitoring validates the integrity of Windows files, Windows registry, and Linux files. You select the files that you want monitored by enabling FIM. Security Center monitors files with FIM enabled for activity such as:

- File and Registry creation and removal
- File modifications (changes in file size, access control lists, and hash of the content)
- Registry modifications (changes in size, access conrol lists, type, and the content)

Brute Force Attack mitigations



When just-in-time access is enabled, network security group rules are created that limit inbound traffic to management ports

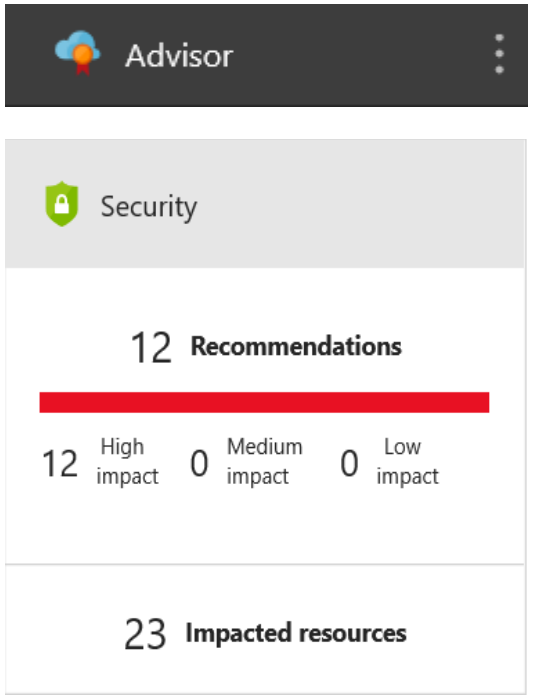
REMEDIATION STEPS

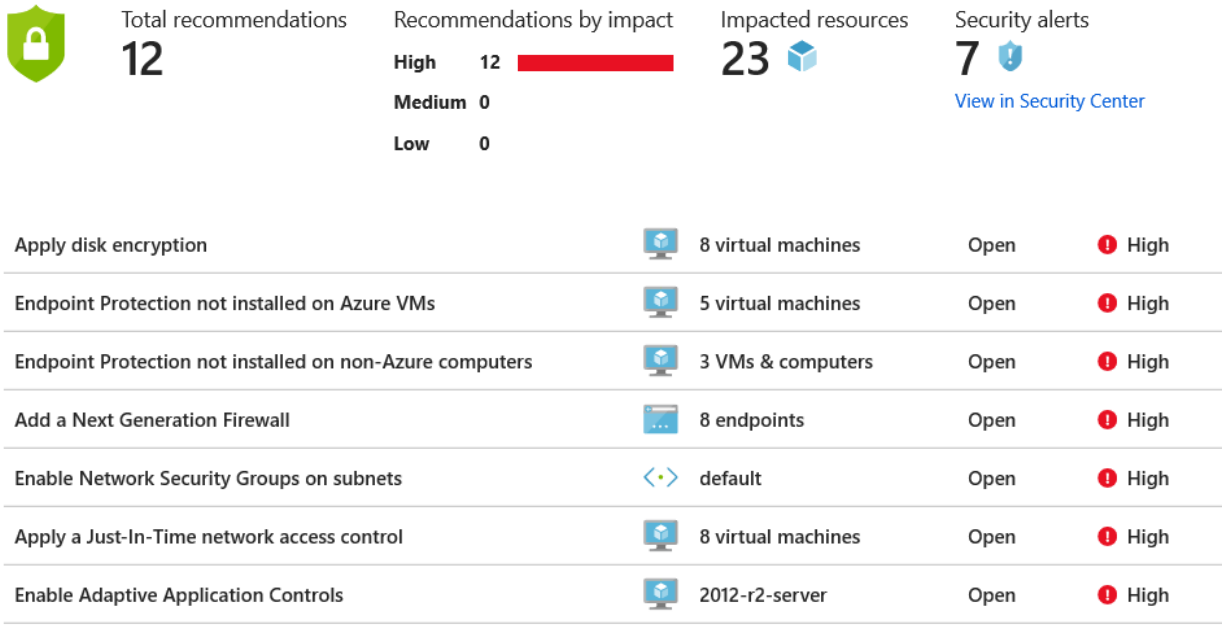
1. If available, add the source IP to NSG block list for 24 hours (see https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/)
2. Enforce the use of strong passwords and do not re-use them across multiple VMs and services (see http://windows.microsoft.com/en-us/Windows7/Tips-for-creating-strong-passwords-and-passphrases)
3. Create an allow list for RDP access in NSG (see https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/)

- Do not allow persistent network access to management ports
- Control and audit network access requests
- Monitor inbound network traffic to detect active threats
- Block traffic from malicious sources
- Monitor VMs events for signs of successful logins resulting from brute force attacks

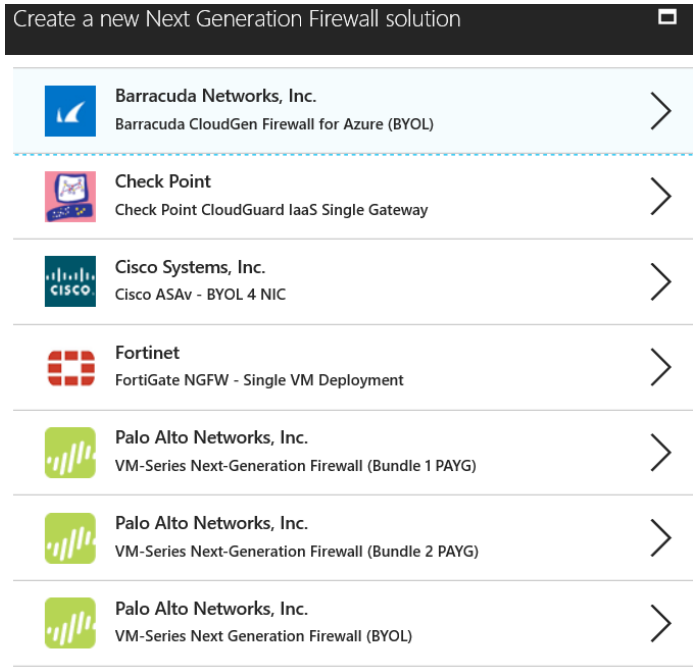
https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time

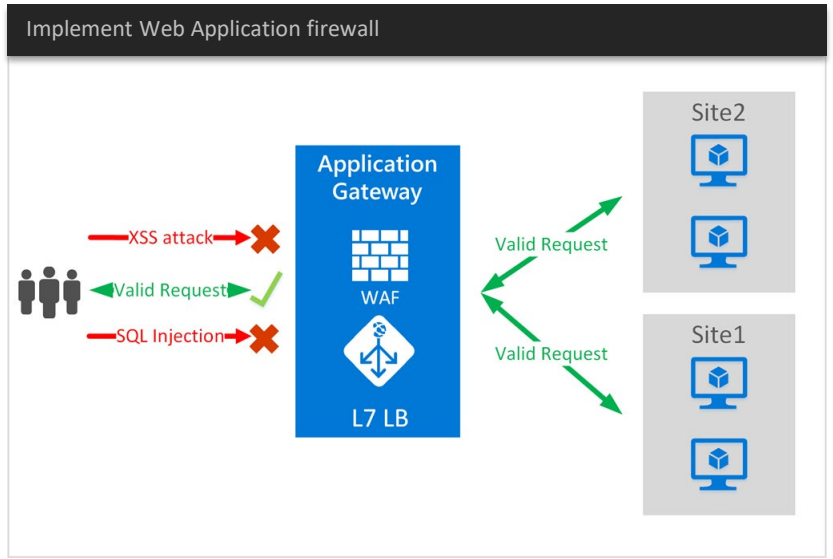
Advisor recommendations





Implement Firewalls





RSAConference2019

Apply

Apply what you have learnt

- Today:
  - Try Advanced threat detection capabilities in the standard tier, free for 60 days.
- Next week you should:
  - Review Azure Best Practice Security Guidelines:
    - https://docs.microsoft.com/en-us/azure/security/security-best-practices-and-patterns
- In the first three months following this presentation you should:
  - Prioritize implementation of **CIS controls 1 – 6, 9, 12, 13, 14, 16, 18**
    - https://learn.cisecurity.org/20-controls-download

Lessons Learned

- Group Discussion – What did we learn?

RSAConference2019