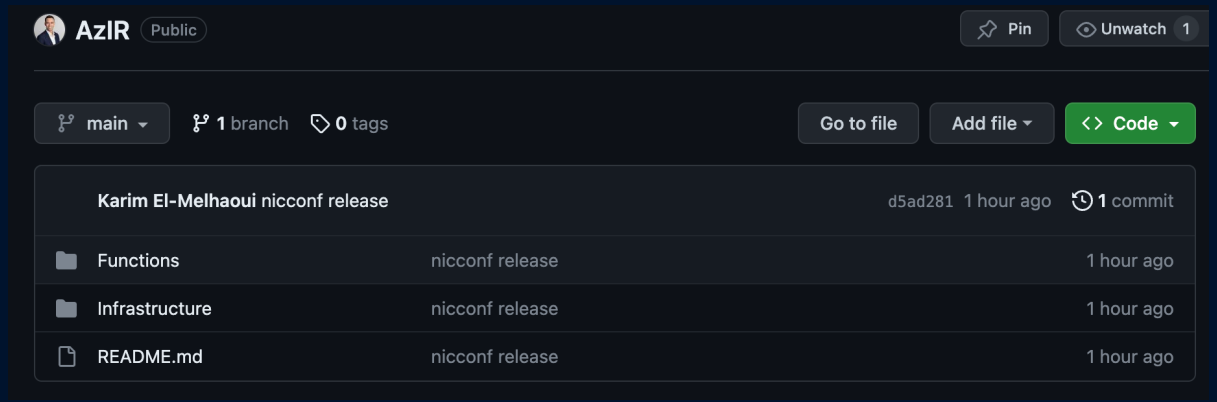
nic Cloud Connect

Karim EI-Melhaoui

Surviving in the Cloud Security Threat Landscape

What to expect in this session

- Real stories from cloud, security and operational transformation
- Hardening, Detection and IR scripts - Released today ☺



Background

Experience

- Norges Bank Investment Management - 2017 - 2022
- 03 Cyber, Principal and Cloud Security Researcher
- Cloud Security Alliance Norway, Board Member
- Podcaster, Microsoft Security MVP
- **o3c.no**
- **@karimscloud**

nic Cloud Connect

Research

AWS DevOps Blog

Building AWS CloudFormation Templates Using CloudFormer

by Evan Brown | on 18 DEC 2013 | Permalink | Comments | Share

In this week's post Chris Whitaker, AWS Senior Manager of Software Development, will discuss best practices for building CloudFormation templates with the CloudFormer tool.

AWS CloudFormation enables you to create and manage AWS infrastructure deployments in a predictable and repeatable way using templates. Once you have a template, you can use it to deploy any number of stacks in the same region (e.g., to deploy identical configurations for test, development, and production) as well as in several regions (e.g., to serve your customers in the US and in Europe). While you can create templates from scratch or use the built-in template editors provided by the AWS toolkits for Microsoft Visual Studio and Eclipse, you may already have a running application that you want to deploy repeatedly and reliably. The CloudFormer tool helps you to build a template from a running version of your application.

nic Cloud Connect

Research

Hello Karim,

Thank you for bringing your security concern to our attention. We have taken appropriate action. We greatly appreciate and encourage reports from the security community!

If you discover or become aware of another security concern specific to AWS products and services, please do not hesitate to contact us again at aws-security@amazon.com.

Thank you again for helping us protect our customers!

Best Regards

Zack G.
AWS Security
https://aws.amazon.com/security

nic Cloud Connect

Research

Hi Karim,

A timeline of the events and actions AWS took are detailed below.

1) AWS received notice of the issue on 9/27/20.
2) We then triaged the issue and decided to decommission CloudFormer on 9/30/20.
3) The decommission of CloudFormer and its guide on the AWS website were completed on 10/15/20.

Cloud Security Threat Landscape

Where are we now?

nic Cloud Connect

Azure AD B2C cryptographic flaw allowing account compromise

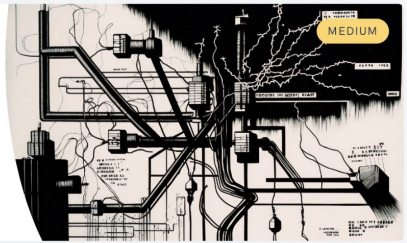
Azure Active Directory B2C service (AD B2C) mistakenly implemented RSA key authentication using the public part of the key pair instead of the private one. This cryptographic flaw could have allowe...

JOHN NOVAK, PRAETORIAN — WED, FEB 15TH, 2023

AWS Console rate limit bypass

AWS applies a rate limit to authentication requests made to the AWS Console in an effort to prevent brute-force and credential stuffing attacks. However, a weakness was discovered in the AWS Consol...

CHRISTOPHE TAFANI-DEREEPER,... — MON, FEB 6TH, 2023



EmojiDeploy

Multiple Azure Web services use a source control management (SCM) panel powered by Kudu and enabled by default. These services were all susceptible to a CSRF vulnerability due to an overly-permissi...

LIV MATAN, ERMETIC — THU, JAN 19TH, 2023

Microsoft Faces Mounting Scrutiny Over China-Linked Email Hack

Leading lawmaker accuses tech company of security negligence that enabled spying campaign

By Dustin Volz Follow and Robert McMillan Follow

July 27, 2023 9:00 am ET

Share Resize Listen (2 min)

Microsoft says hackers got to the emails by first gaining access to an obscure but critical part of its infrastructure called an MSA digital signing key. PHOTO: JACOB KEPLER FOR THE WALL STREET JOURNAL


NORGE NOREG NORGA
NORWAY
ID-KORT ID-DUOĐAŠTUS
IDENTITY CARD
Etternavn · Etternamn · Sohkanamma/ Surname
ØSTENBYEN
Fornavn · Førenamn · Ovdanamma/ Given names
ÅSAMUND SPECIMEN
Kjønn · Sohkabeallí/ Sex
M
Fødselsdato · Riegádanáigi/ Date of birth
23 APR /APR 56
Høyde · Hægd · Guhkkodat/ Height
179 CM
Dokumentnr. · Dokumeantanr./ Document No.
GC0001306
Kortet går ut · Mannmuš dohkkenbeaivi/ Date of expiry
15 APR /APR 25
Nasjonalitet · Riikkavuloš vuohta/ Nationality
Norsk/ Norwegian
Navnetrekk · Namnetrekk · Vuollái čálus/ Signature
CAN
313542


72 ALIVE
2:56
SINGLE
30
NORGE NOREG NORGA
NORWAY
ID-KORT ID-DUOĐAŠTUS
IDENTITY CARD
Etternavn · Etternamn · Sohkanamma/ Surname
ØSTENBYEN
Fornavn · Førenamn · Ovdanamma/ Given names
ÆSAMUND SPECIMEN
Kjønn · Sohkabeali/ Sex
M
Fødselsdato · Riegádanáigi/ Date of birth
23 APR /APR 56
Høyde · Høgd · Cuhkkodat/ Height
179 CM
Dokumentnr. · Dokumeantanr./ Document No.
GC0001306
Kortet går ut · Manjimuš dohkkenbeaivi/ Date of expiry
15 APR /APR 25
Nasjonalitet · Riikkavuloštuvohta/ Nationality
Norsk/ Norwegian
Navnetrekk · Namnetrekk · Vuollálčállus/ Signature
CAN
313542

nic Cloud Connect

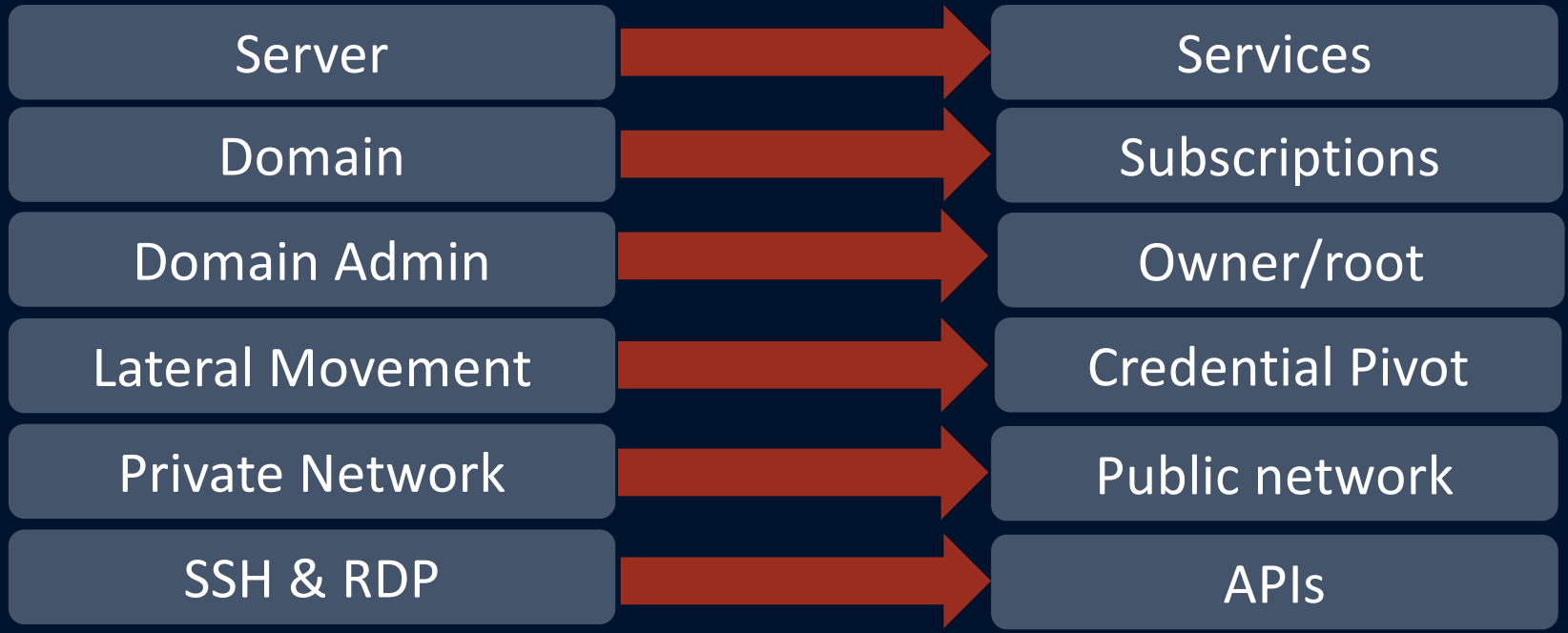
What characterizes the Cloud Threat Landscape?

- Opportunistic: Misconfigurations
- Risk Inheritance: CSP and Managed Service Providers
- Tailored Operations: Tools and Tradecraft

What makes cloud different?

nic Cloud Connect

Cloud is different



Credit: Sacha Faust

nic Cloud Connect

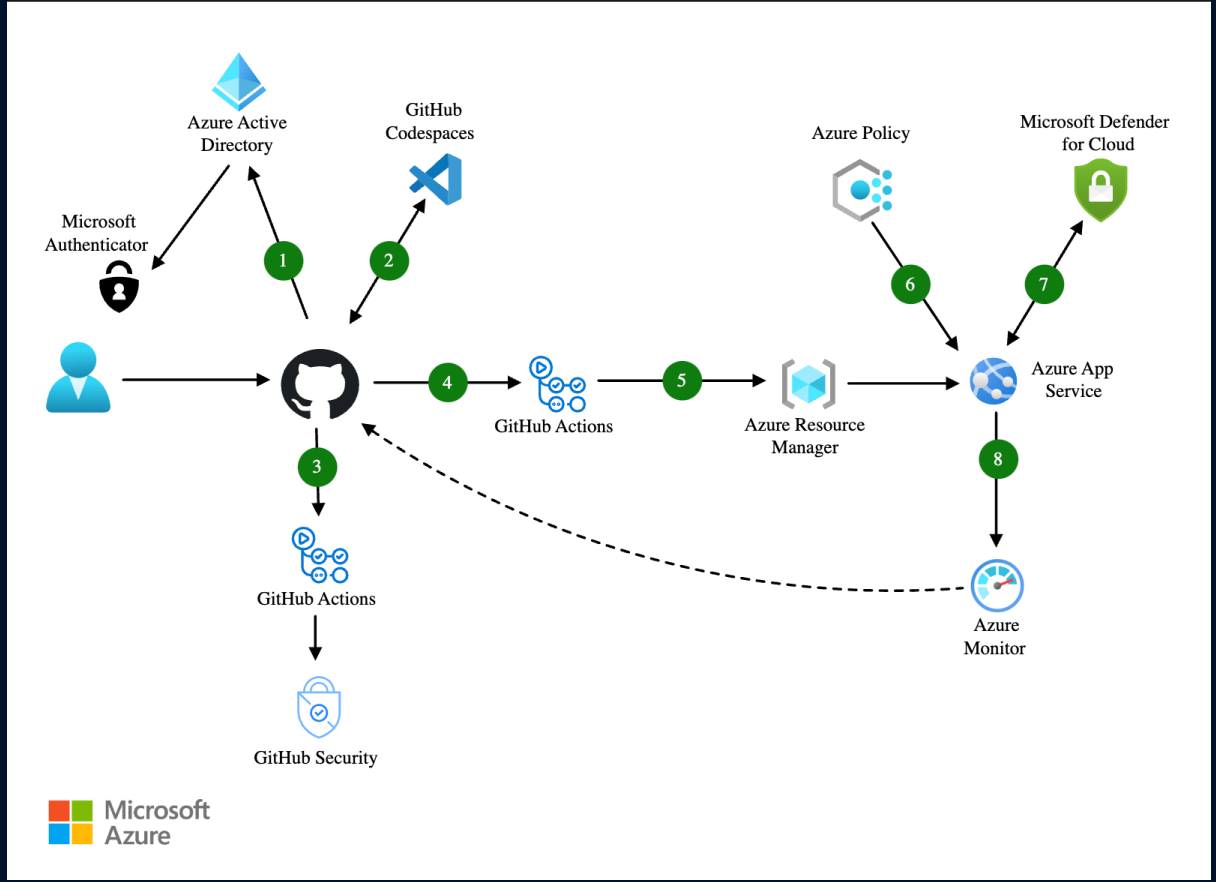
What we are seeing lately

- MFA-based phishing attacks
- Pivoting from Entra ID to Azure workloads
- Dumping data from Fabric Data Factory
- Resetting VM password management plane
- Serial Console for network persistence

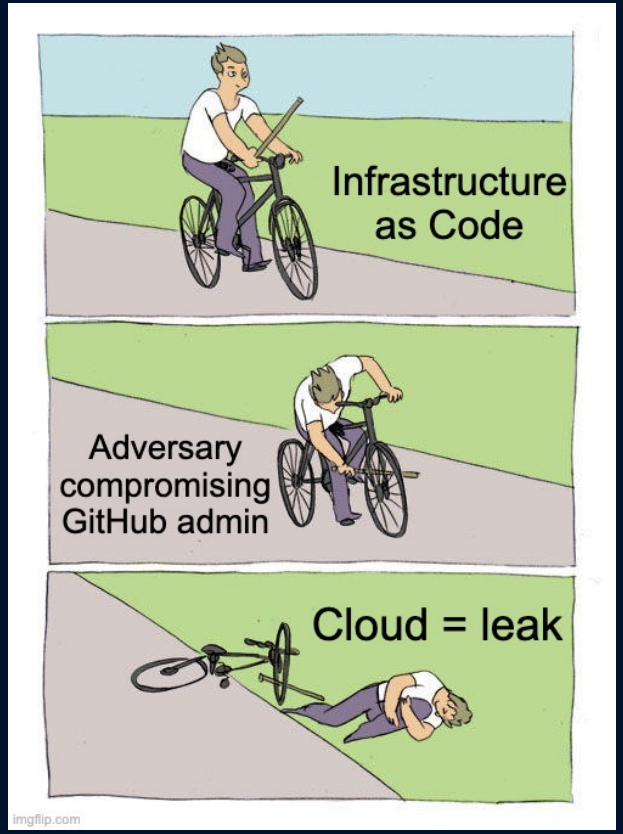
How to Survive in the Cloud

Part 0: Defensible Architecture

GitOps


Azure Active Directory
GitHub Codespaces
Azure Policy
Microsoft Defender for Cloud
Microsoft Authenticator
1
2
6
7
4
5
Azure App Service
GitHub Actions
Azure Resource Manager
3
8
GitHub Actions
Azure Monitor
GitHub Security
Microsoft Azure

GitOps


Infrastructure as Code
Adversary compromising GitHub admin
Cloud = leak
imgflip.com

GitOps

SCMKit

Description

Source **C**ode **M**anagement Attack Tool**kit** - SCMKit is a toolkit that can be used to attack SCM systems. SCMKit allows the user to specify the SCM system and attack module to use, along with specifying valid credentials (username/password or API key) to the respective SCM system. Currently, the SCM systems that SCMKit supports are GitHub Enterprise, GitLab Enterprise and Bitbucket Server. The attack modules supported include reconnaissance, privilege escalation and persistence. SCMKit was built in a modular approach, so that new modules and SCM systems can be added in the future by the information security community.

VM Hardening

Hardening Cloud VMs

My career in cybersecurity started with OS hardening, so I am rather passionate about the topic. When it comes to the cloud, many organizations have embraced automation. Yet, most skip hardening of the operating system or only do a bare minimum hardening baseline. I've also seen the pre-hardened CIS images used, but to my frustration, it update less frequently than other images. I am writing this as a companion post to my talk at NICConf. So, what are the options for hardening images in the cloud?

4 min • Nov 08, 2023

nic Cloud Connect

VM Hardening

HardeningKitty

This is the stable version of *HardeningKitty* from the Windows Hardening Project by Michael Schneider. The stable version of *HardeningKitty* is signed with the code signing certificate of *scip AG*. **Since this is the stable version, we do not accept pull requests in this repo, please send them to the development repo.**

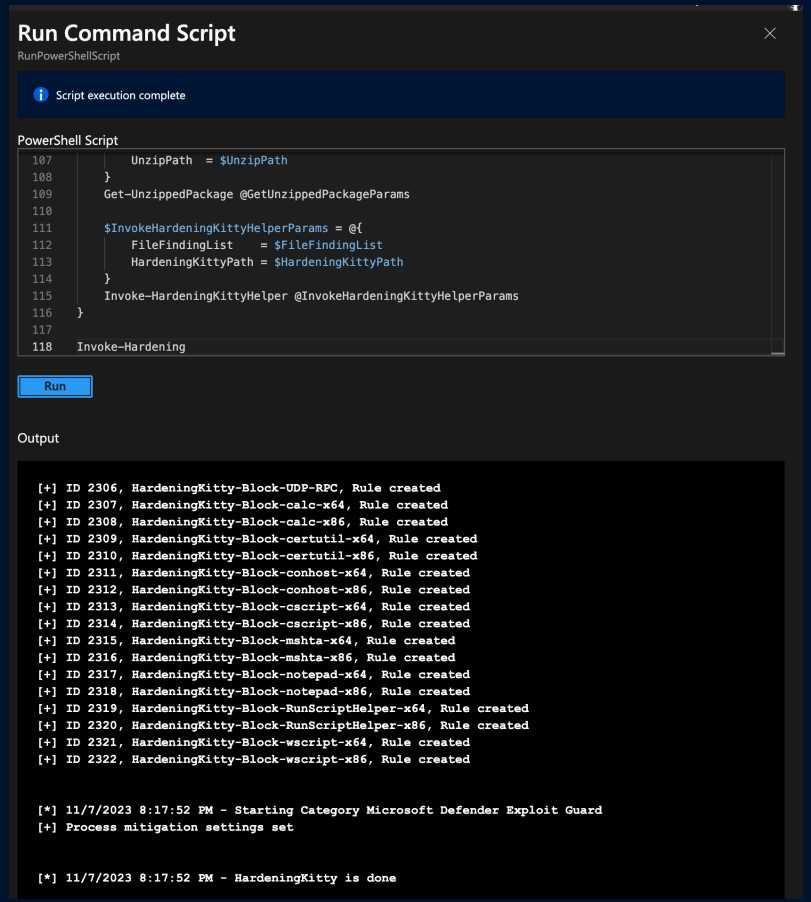
HardeningKitty supports hardening of a Windows system. The configuration of the system is retrieved and assessed using a finding list. In addition, the system can be hardened according to predefined values. *HardeningKitty* reads settings from the registry and uses other modules to read configurations outside the registry.

The script was developed for English systems. It is possible that in other languages the analysis is incorrect. Please create an issue if this occurs.

Invoke-Hardening.ps1

```
    2 references
function Invoke-Hardening {
    [CmdletBinding()]
    param (
        [Parameter(Mandatory = $false)]
        [string]
        $FileFindingList = (Join-Path -Path $env:TEMP -ChildPath "SecurityBaseline\HardeningKitty-v.0.9.0\lists\
        [string]
        $HardeningKittyPath = ( Join-Path $env:TEMP -ChildPath "SecurityBaseline\HardeningKitty-v.0.9.0" ),
        [Parameter(Mandatory = $false)]
        [string]
        $UnzipPath = ( Join-Path $env:TEMP -ChildPath "SecurityBaseline" ),
        [Parameter(Mandatory = $false)]
        [string]
        $PackageUrl = "https://github.com/scipag/HardeningKitty/archive/refs/tags/v.0.9.0.zip"
    )
```

VM Hardening

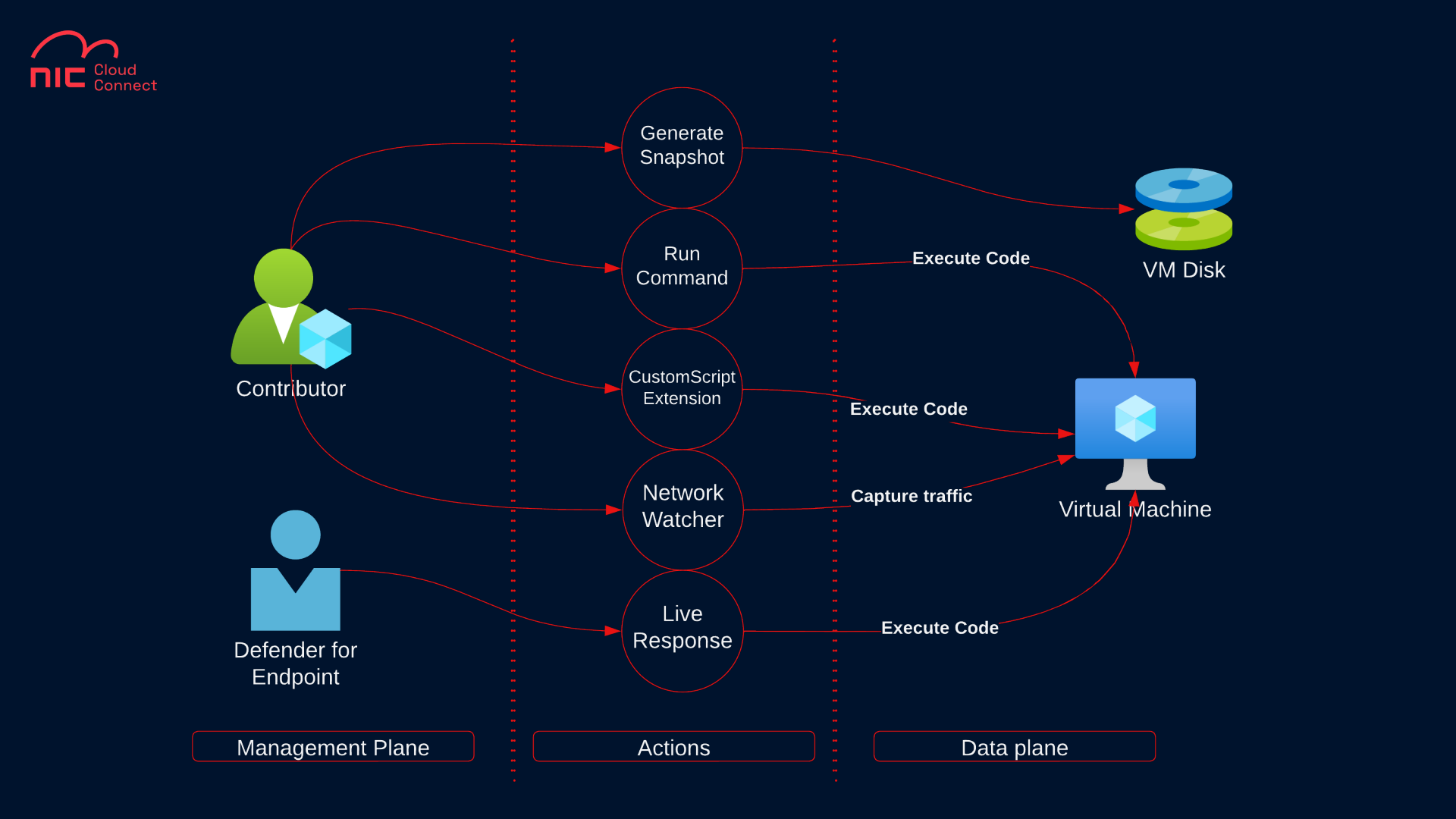


VM Hardening

```
resource configAppExtension 'Microsoft.Compute/virtualMachines/extensions@2022-11-01' = {

  name: '${vmName}/InvokeHardening'
  location: location
  properties: {
    publisher: 'Microsoft.Compute'
    type: 'CustomScriptExtension'
    typeHandlerVersion: '1.10'
    autoUpgradeMinorVersion: true
    settings: {
      managedIdentity: {}
      fileUris: [
        'https://gist.githubusercontent.com/karimelmel/9897d373502ccaed22ac3722aa13b878/raw/a68bc0d8dbad022980857106d0df8eaf64e561e6/Invoke-Hardening.ps1'
      ]
      commandToExecute: 'powershell.exe -ExecutionPolicy Bypass -File Invoke-Hardening.ps1'
    }
  }
}
```

Domain Controllers

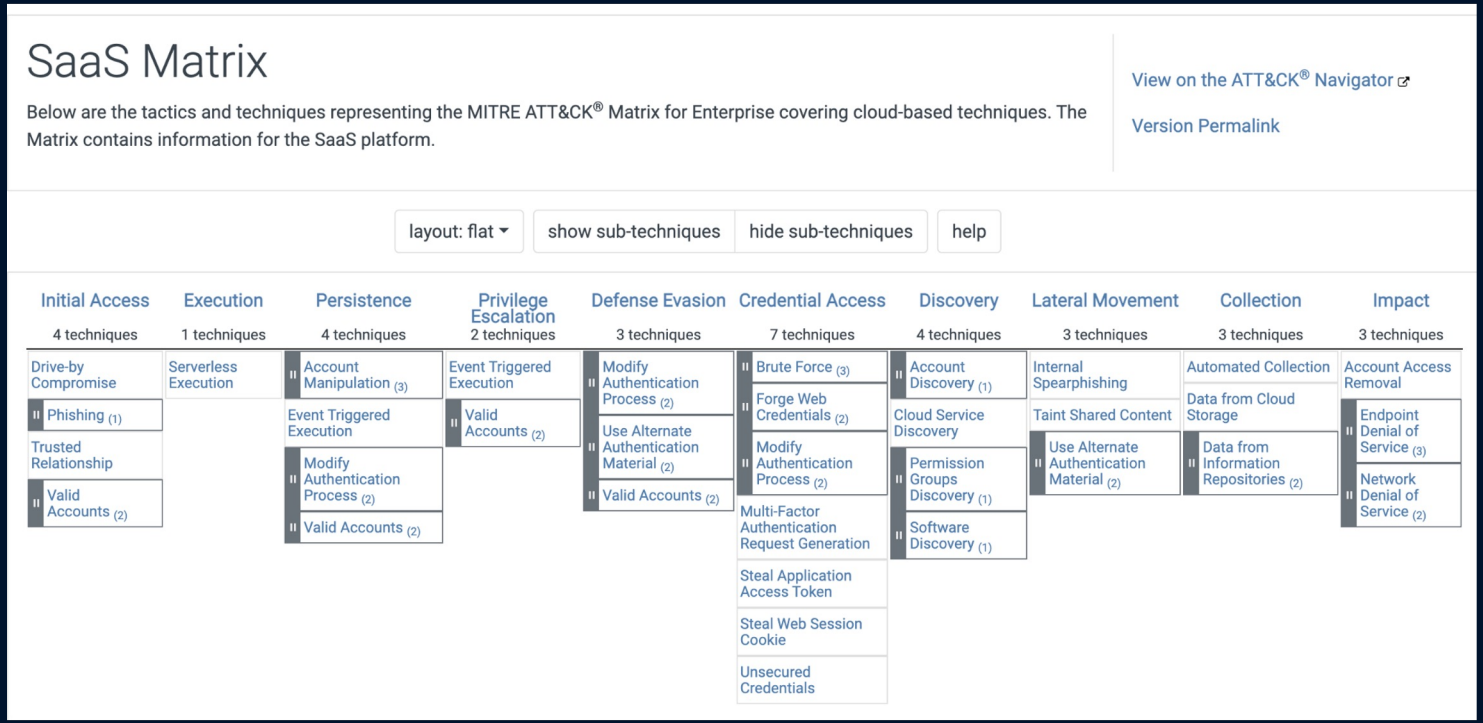

Cloud Connect
Generate Snapshot
Run Command
CustomScript Extension
Network Watcher
Live Response
Contributor
Defender for Endpoint
Execute Code
Execute Code
Capture traffic
Execute Code
VM Disk
Virtual Machine
Management Plane
Actions
Data plane

Defensible Architecture

How to Survive in the Cloud

Part 1: Threat Detection

MITRE Saas Matrix



SaaS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the SaaS platform.

View on the ATT&CK® Navigator

Version Permalink

layout: flat | show sub-techniques | hide sub-techniques | help

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
4 techniques	1 techniques	4 techniques	2 techniques	3 techniques	7 techniques	4 techniques	3 techniques	3 techniques	3 techniques
Drive-by Compromise	Serverless Execution	Account Manipulation (3)	Event Triggered Execution	Modify Authentication Process (2)	Brute Force (3)	Account Discovery (1)	Internal Spearphishing	Automated Collection	Account Access Removal
Phishing (1)		Event Triggered Execution	Valid Accounts (2)	Use Alternate Authentication Material (2)	Forge Web Credentials (2)	Cloud Service Discovery	Taint Shared Content	Data from Cloud Storage	Endpoint Denial of Service (3)
Trusted Relationship		Modify Authentication Process (2)		Valid Accounts (2)	Modify Authentication Process (2)	Permission Groups Discovery (1)	Use Alternate Authentication Material (2)	Data from Information Repositories (2)	Network Denial of Service (2)
Valid Accounts (2)		Valid Accounts (2)			Multi-Factor Authentication Request Generation	Software Discovery (1)			
					Steal Application Access Token				
					Steal Web Session Cookie				
					Unsecured Credentials				

Azure Threat Research Matrix

Azure Threat Research Matrix

Reconnaissance	Initial Access	Execution	Privilege Escalation	Persistence	Credential Access	Impact
Port Mapping	Valid Credentials	Virtual Machine Scripting	Privileged Identity Management Role	Account Manipulation	Steal Managed Identity JsonWebToken	SAS URI Generation
IP Discovery	Password Spraying	Unmanaged Scripting	Elevated Access Toggle	Account Creation	Steal Service Principal Certificate	File Share Mounting
Public Accessible Resource	Malicious Application Consent	Managed Device Scripting	Local Resource Hijack	HTTP Trigger	Service Principal Secret Reveal	Replication
Gather User Information			Principal Impersonation	Watcher Tasks	Azure KeyVault Dumping	Soft-Delete Recovery
Gather Application Information			Azure AD Application	Scheduled Jobs	Resource Secret Reveal	Azure Backup Delete
Gather Role Information				Network Security Group Modification		
Gather Resource Data				External Entity Access		
Gather Victim Data				Azure Policy		

nic Cloud Connect

Cloud Threat Detection

Defender for Cloud

Security Command Center

GuardDuty

API Activity Logs

Network Security Logs

Access Logs

Sign-in and Audit Logs

nic Cloud Connect

Cloud Threat Detection

aws

Google Cloud

Microsoft Azure

Cloud Threat Detection

Defender for Cloud

Security Command Center

GuardDuty

Cloud Threat Detection

API Activity Logs

Network Security Logs

Access Logs

Sign-in and Audit Logs

Cloud Threat Detection

```
1  MicrosoftGraphActivityLogs
2  | project TimeGenerated, Location, RequestMethod, ResponseStatusCode, IPAddress, AppId
```

Results | Chart

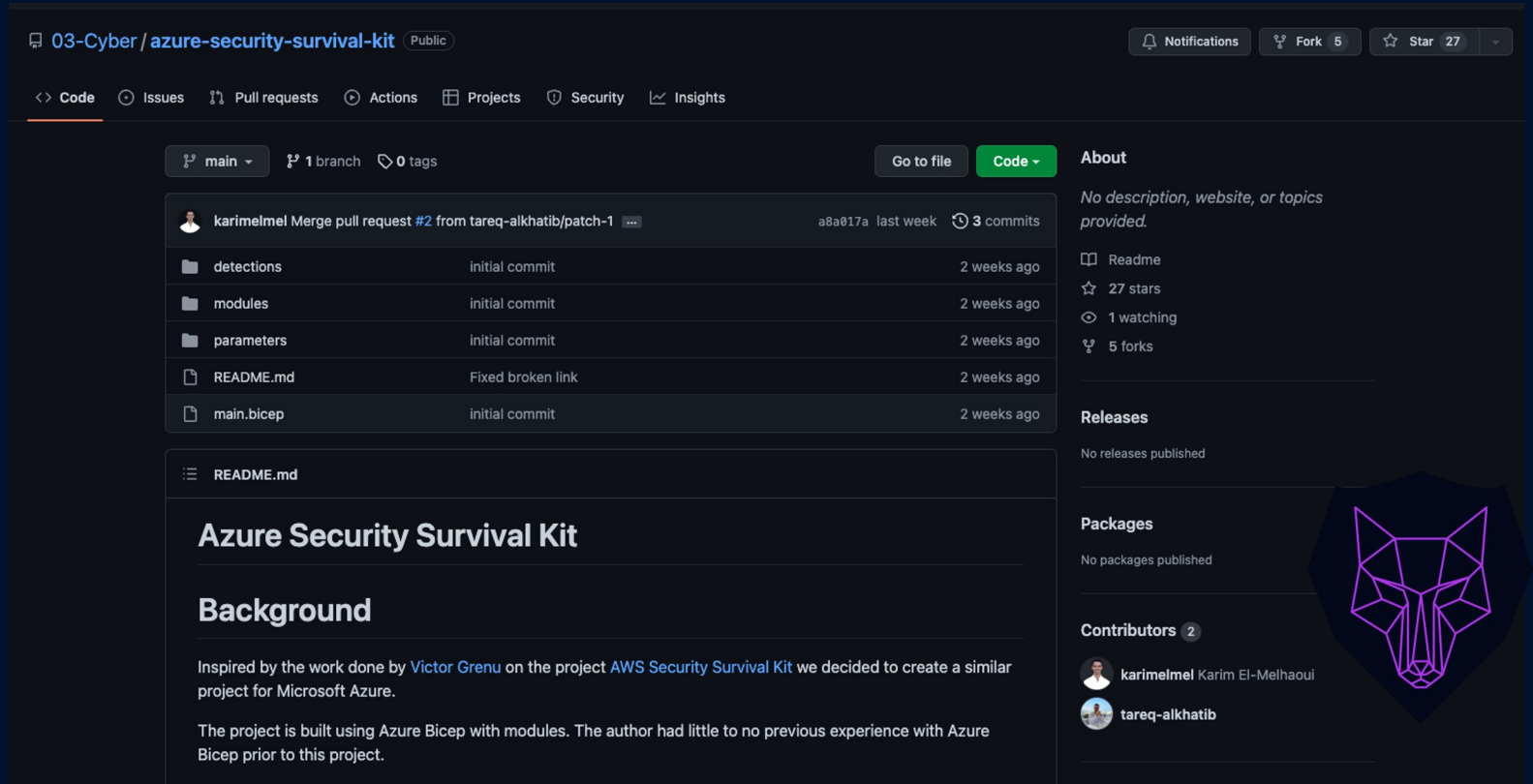
TimeGenerated [UTC]	Location	RequestMe...	ResponseStatusCode	IPAddress	AppId
07/11/2023, 16:12:32.081	West Europe	GET	200	20.31.8.247	fc780465-2017-40d4-a0c5-30702...
07/11/2023, 16:05:36.626	West Europe	GET	200	20.31.12.196	8ee8fdad-f234-4243-8f3b-15c294..
07/11/2023, 15:35:35.049	West Europe	GET	200	20.31.12.196	8ee8fdad-f234-4243-8f3b-15c294..
07/11/2023, 15:20:30.158	West Europe	GET	200	20.31.12.196	8ee8fdad-f234-4243-8f3b-15c294..
07/11/2023, 15:14:40.590	Sweden Central	GET	401	51.120.42.63	c44b4083-3bb0-49c1-b47d-974e...
07/11/2023, 15:14:40.258	Sweden Central	GET	401	51.120.42.63	c44b4083-3bb0-49c1-b47d-974e...
07/11/2023, 15:13:32.766	Sweden Central	POST	200	85.19.207.6	74658136-14ec-4630-ad9b-26e16..
07/11/2023, 15:13:32.766	Sweden Central	GET	200	85.19.207.6	74658136-14ec-4630-ad9b-26e16..
07/11/2023, 15:13:32.735	Sweden Central	GET	200	85.19.207.6	74658136-14ec-4630-ad9b-26e16..
07/11/2023, 15:13:32.730	Sweden Central	GET	200	85.19.207.6	74658136-14ec-4630-ad9b-26e16..
07/11/2023, 15:13:32.728	Sweden Central	GET	200	85.19.207.6	74658136-14ec-4630-ad9b-26e16..

Cloud Threat Detection

Challenges

- No logging on GET requests in Azure (except Graph)
- Reader allows enumeration
- Adversaries has plenty of attack paths as Reader

Azure Security Survival Kit

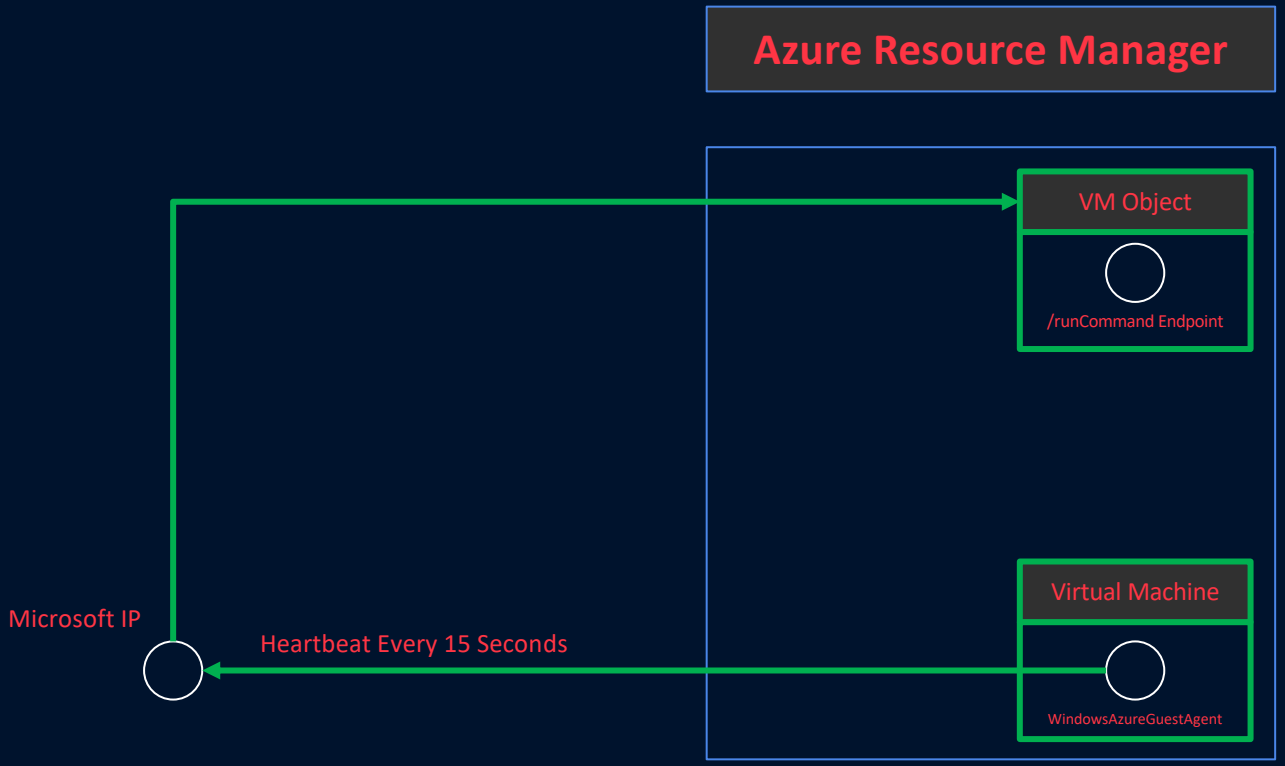


Azure Security Survival Kit

Detections

- ConditionalAccessModified
- VMDiskSnapshotGenerated
- VMPasswordResetInvoked

Azure Security Survival Kit: Run Command



Credit: Andy Robbins @ SpecterOps

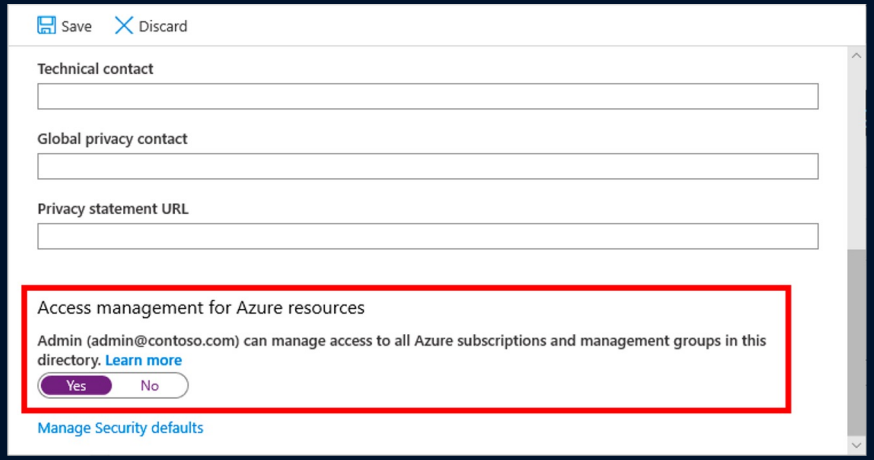
Azure Security Survival Kit: Run Command

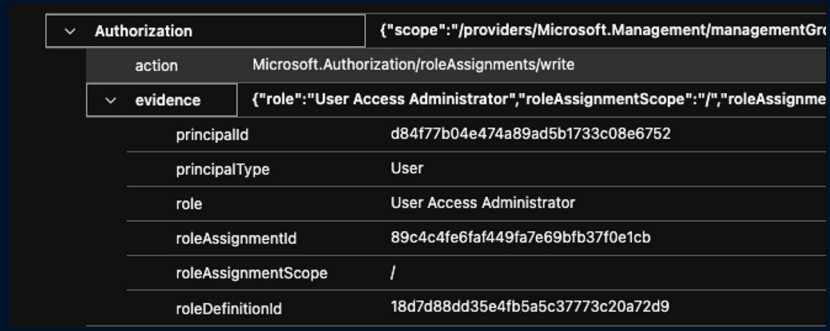
```
Function Invoke-AzureRmVMBulkCMD
{
<#
    .SYNOPSIS
        Runs a Powershell script against all (or select) VMs in a subscription/resource group/etc.
    .DESCRIPTION
        This function will run a PowerShell script on all (or a list of) VMs in a subscription/resource group/etc. This can be handy for creating reverse she
    .PARAMETER Subscription
        Subscription to use.
    .PARAMETER ResourceGroup
        Restrict the script to a specific Resource Group.
    .EXAMPLE
        PS C:\MicroBurst> Invoke-AzureRmVMBulkCMD -Verbose -Script .\Mimikatz.ps1
        Executing C:\MicroBurst\Mimikatz.ps1 against all (1) VMs in the Testing-Resources Subscription
        Are you Sure You Want To Proceed: (Y/n):
        VERBOSE: Running .\Mimikatz.ps1 on the Remote-West - (10.2.0.5 : 40.112.160.13) virtual machine (1 of 1)
        VERBOSE: Script Status: Succeeded
        Script Output:
          .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Feb 16 2015 22:15:28)
         .## ^ ##.
         ## / \ ##  /* * *
         ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
         '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
          '#####'                                     with 15 modules * * */


        mimikatz(powershell) # sekurlsa::logonpasswords
        [Truncated]
        mimikatz(powershell) # exit
        Bye!

        VERBOSE: Script Execution Completed on Remote-West - (10.2.0.5 : 40.112.160.13)
        VERBOSE: Script Execution Completed in 37 seconds
```

Azure Security Survival Kit: Elevated Access Toggle





Azure Security Survival Kit: Elevated Access Toggle

Detecting usage of Elevated Access Toggle in Azure environments

Sep 4, 2022

As I've started looking into Microsoft Azure, one of the risks I've identified is that a Global Administrator can elevate access to manage all Azure subscriptions and management groups, this technique is also covered in the Azure Threat Research Matrix as AZT402. My first instinct would be to eliminate this risk completely, which unfortunately is not possible. Global Admins should be rare and well protected, but is still a risk of interest.

Given the risk cannot be completely mitigated, my next instinct is to look for a detective approach. My assumption that the Management Group logs would be part of the Azure Activity logs by default was quickly proven wrong.

I came across two blog posts from @samilamppu that covers two ways of extracting the logs to detect the specific scenario:

- https://samilamppu.com/2022/04/08/detect-elevate-access-activity-in-azure-with-microsoft-sentinel-native-capabilities/
- https://samilamppu.com/2021/02/09/monitor-elevate-access-activity-in-azure-with-azure-sentinel/

The problem here is that the data relies on another source, Microsoft Defender for Cloud Apps which all Azure customers may not have due to license constraints.

I did some digging into the API and came across the API for Management Group Diagnostic Settings. Great!

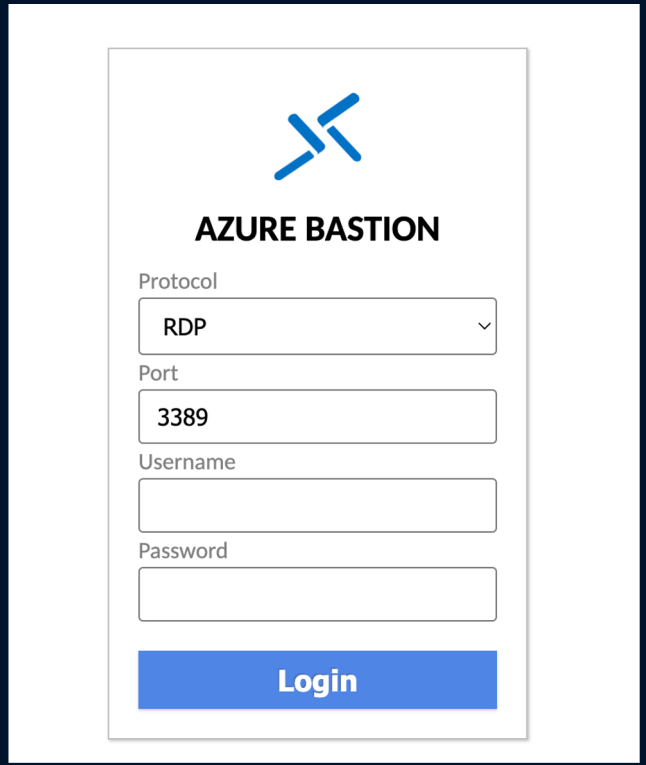
To enable it on the Tenant Root Level (top-level management group), all I would have to do is run the following one-liner followed by payload:

```
az rest --method put --uri "https://management.azure.com/providers/microsoft.mana
```

```
{
    "properties": {
        "workspaceId": "/subscriptions/{SubcriptionID}/resourceGroups/{ResourceGr
        "logs": [
        {
```

Azure Security Survival Kit: Elevated Access Toggle

https://bst-c6bf3220-015d-4d6e-8c19-32ac484e341f.bastion.azure.com/api/shareable-url/074fa24e-8614-47ea-94f7-f9f901003598



Azure Security Survival Kit: Elevated Access Toggle

Yet Another Azure VM Persistence Using Bastion Shareable Links

Nov 26, 2022

Earlier this week Microsoft announced the public preview of Shareable Links in Azure Bastion.

Out-of-the-box persistence for a Virtual Machine that is reachable through an Azure Bastion, allowing for yet another persistence mechanism in Azure?

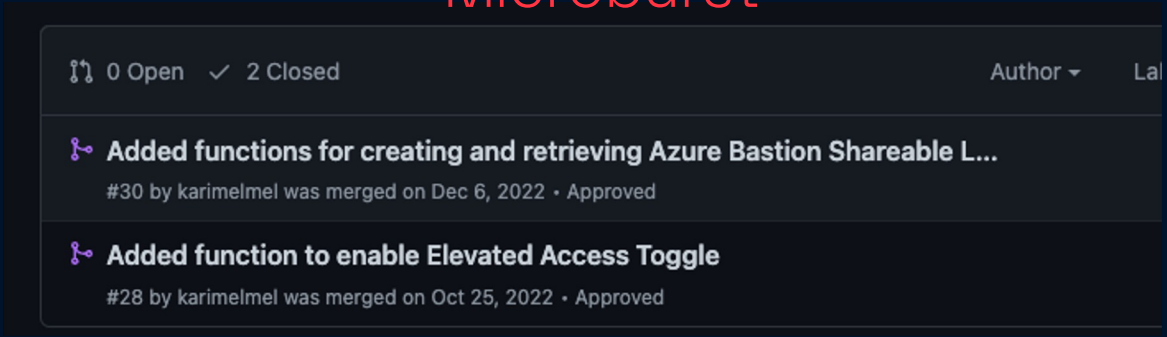
I deployed an Azure Bastion to validate, enabled the feature, and generated a Shareable Link for a VM. The link has no additional authentication and is publicly accessible.

This may enable an adversary to abuse the feature to gain access to Remote Desktop or SSH, without requiring network access OR authentication.

Example link: Public link for Bastion - https://bst-c6bf3220-015d-4d6e-8c19-32ac484e341f.bastion.azure.com/api/shareable-url/074fa24e-8614-47ea-94f7-f9f901003598

Azure Security Survival Kit - Contributions

Microburst

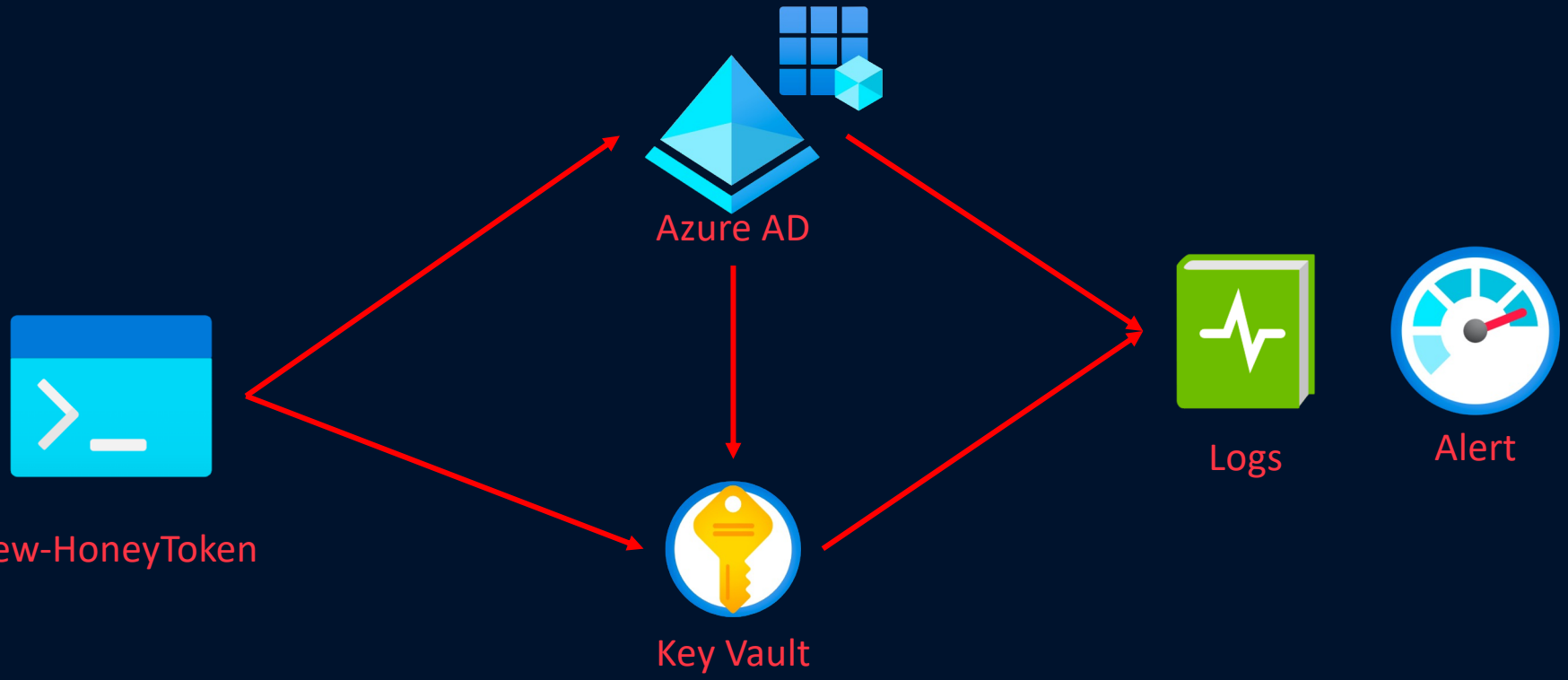


Azure Threat Research Matrix

nic Cloud Connect

Demo: AZSSK

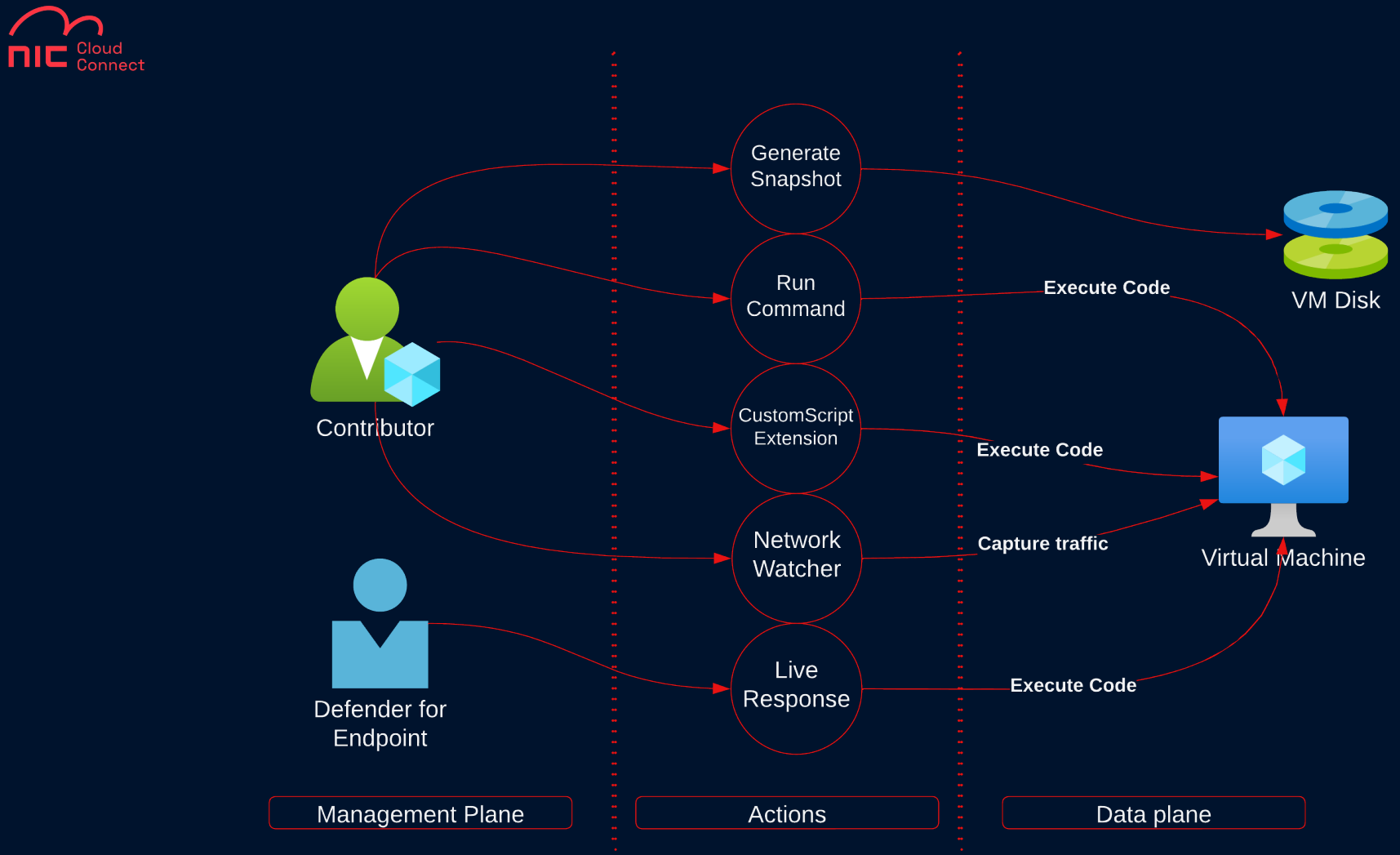
Bonus: Honeytoken



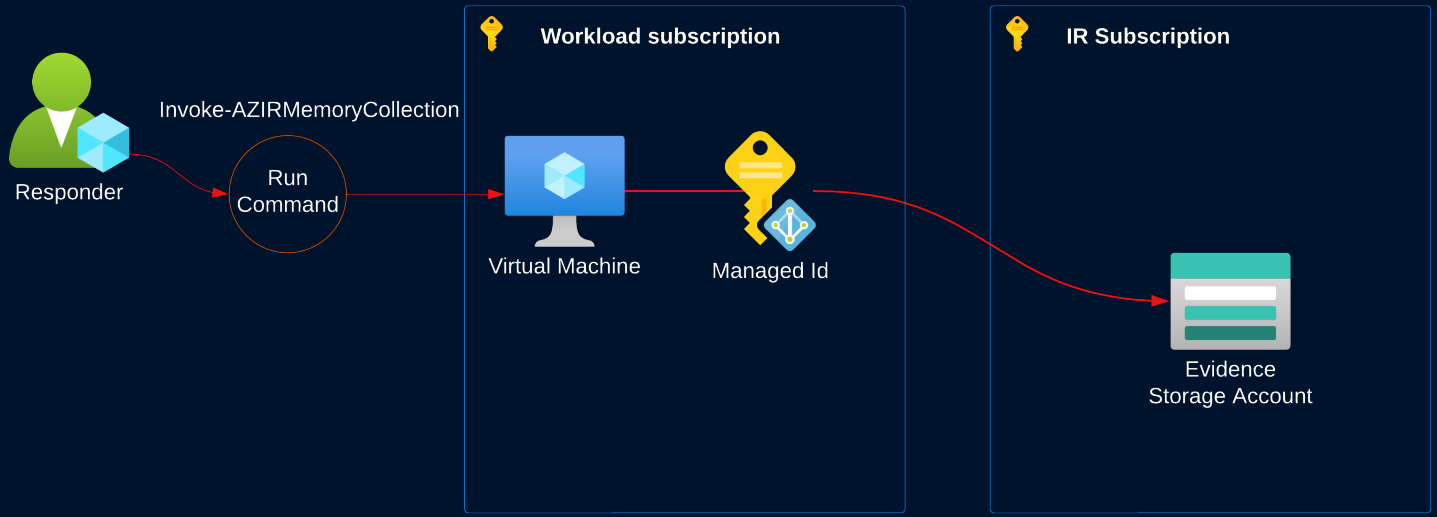
New-HoneyToken.ps1

How to Survive in the Cloud

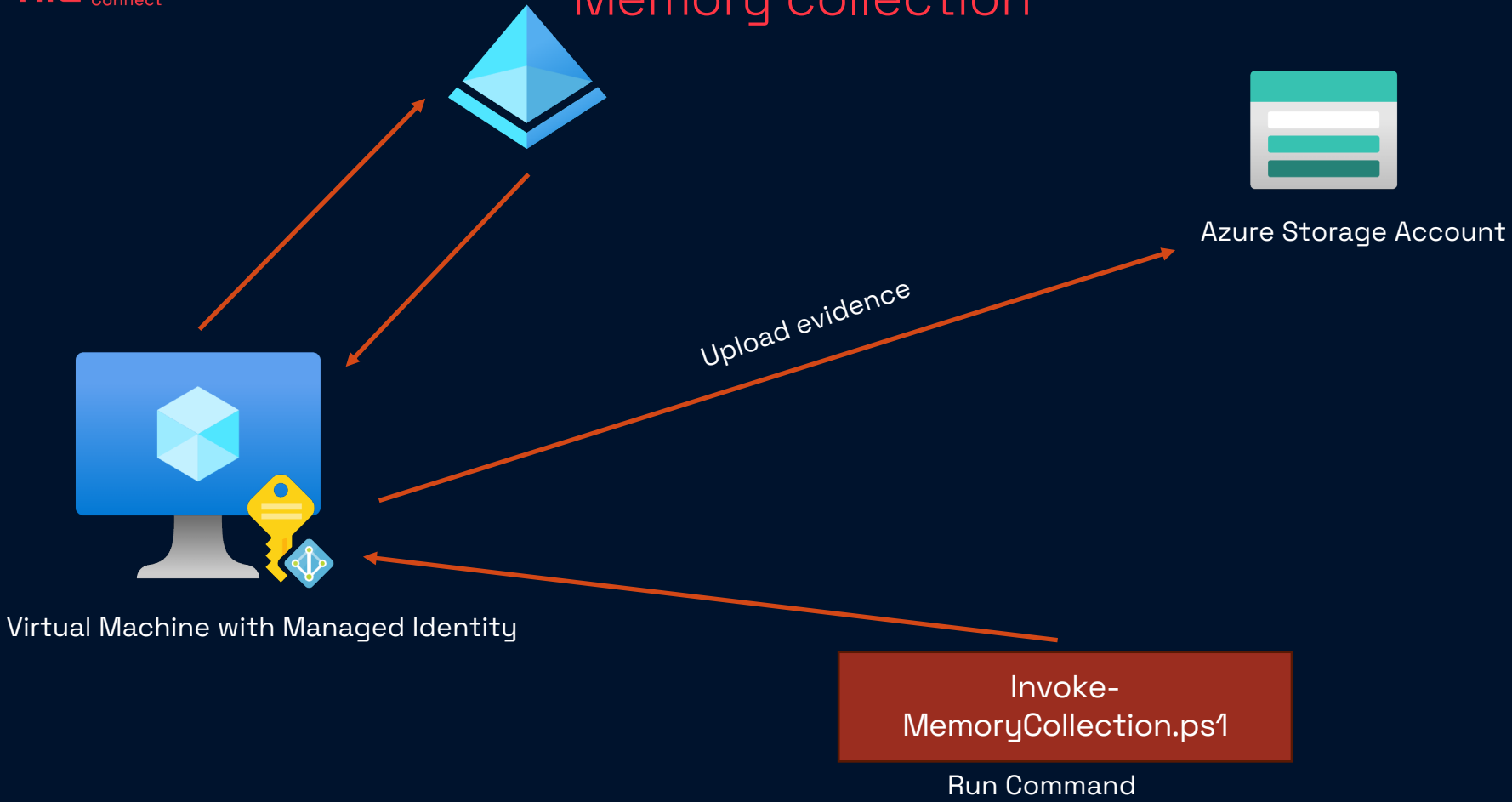
Part 2: Incident Response


Cloud Connect
Generate Snapshot
Run Command
CustomScript Extension
Network Watcher
Live Response
Contributor
Defender for Endpoint
VM Disk
Execute Code
Execute Code
Capture traffic
Execute Code
Virtual Machine
Management Plane
Actions
Data plane

IR Collection Architecture



Memory collection



Memory collection

```powershell
$GetUnzippedPackagesParams = @{
    PackageUrls = $PackageUrls
    UnzipPath   = $UnzipPath
}
Get-UnzippedPackages @GetUnzippedPackagesParams

Get-AzIrInstanceMetadata

$StartMemoryAcquisitionParams = @{
    DumpItExecuteable = $DumpItExecuteable
    MemoryFile        = $MemoryFile
}
Start-MemoryAcquisition @StartMemoryAcquisitionParams

$WriteMemoryDumpToStorAcc = @{
    StorageAccountName   = $StorageAccountName
    StorAccContainerName = $StorAccContainerName
    MemoryFile           = $MemoryFile
}
Write-MemoryDumpToStorAcc @WriteMemoryDumpToStorAcc
```

Demo: Memory Collection

Cloud Incident Response

Work In Progress

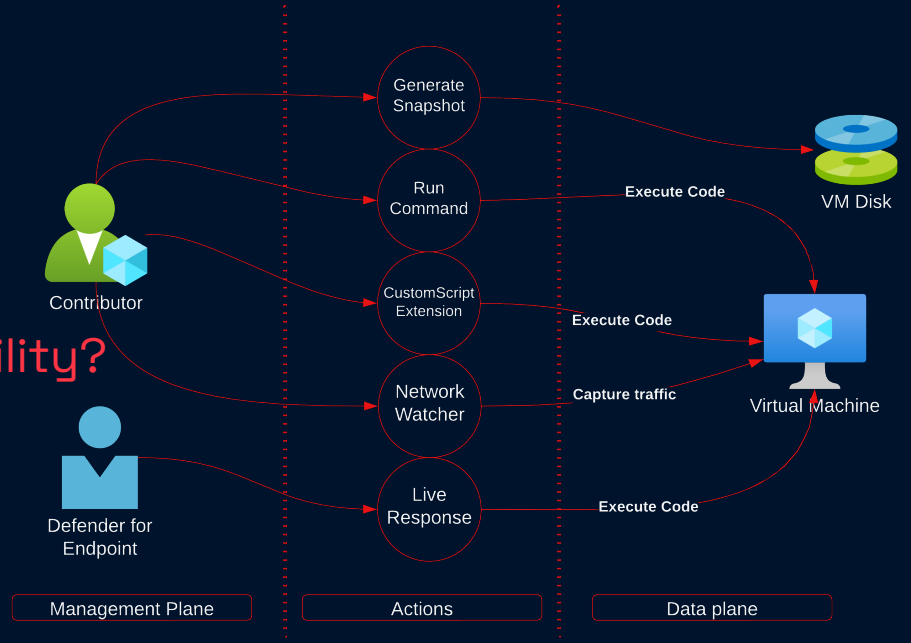
- Hibernation for memory gathering
- Isolating hosts using NSG (doesn't break active connections)
- Collect Instance Metadata as an artifact

Cloud Incident Response

Is it an Attack Surface

or an ..

Operational/Incident Response capability?



nic Cloud Connect

That’s all.

RATE THE SESSION

github.com/karimelmel/AzIR

nic Cloud Connect

PLEASE RATE THE SESSION