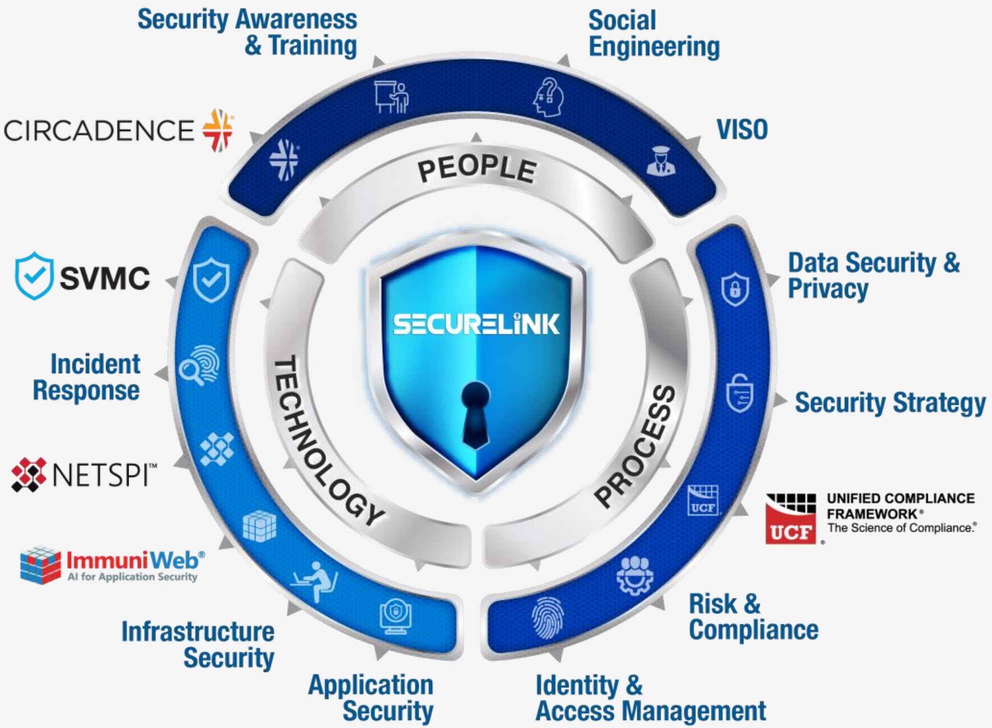
NETSPI®

13th December 2023

Cloud Pentesting Uncovered: Real Stories, Practical Solutions

NETSPI™ SECURELINK

Services:



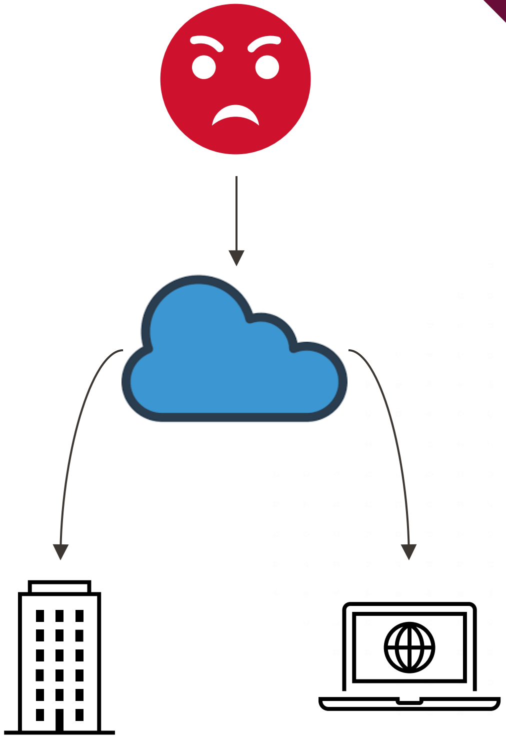
PRESENTER

SAM KIRKMAN

Director of EMEA Services

NETSPI®

Why Cloud Security Matters



NETSPI®

AGENDA

- Vulnerability trends from last year
- Common vulnerabilities and remediations
- Intro to cloud penetration testing methodology
- Recent real world examples
- Q&A

AZURE WAR STORY

Automation Accounts: What are they?

PROCESS AUTOMATION IN AZURE

- Automate frequent management tasks:
  - Start/Stop VMs at regular intervals
  - Build and deploy resources
  - Periodic Maintenance

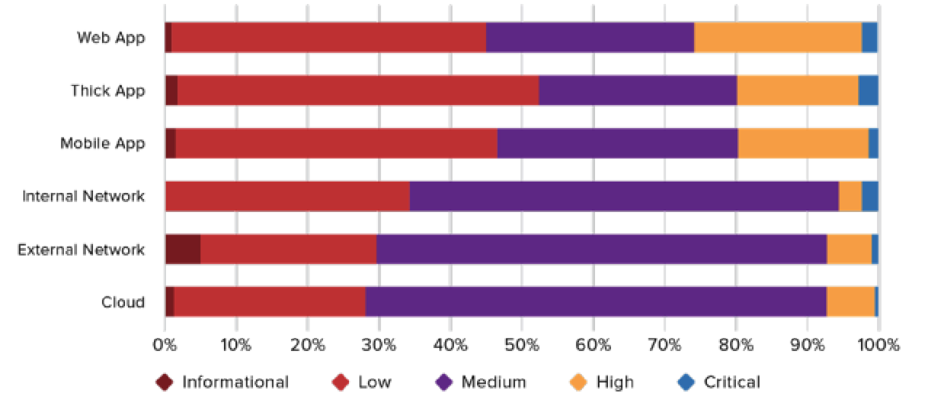
NETSPI®

VULNERABILITY TRENDS

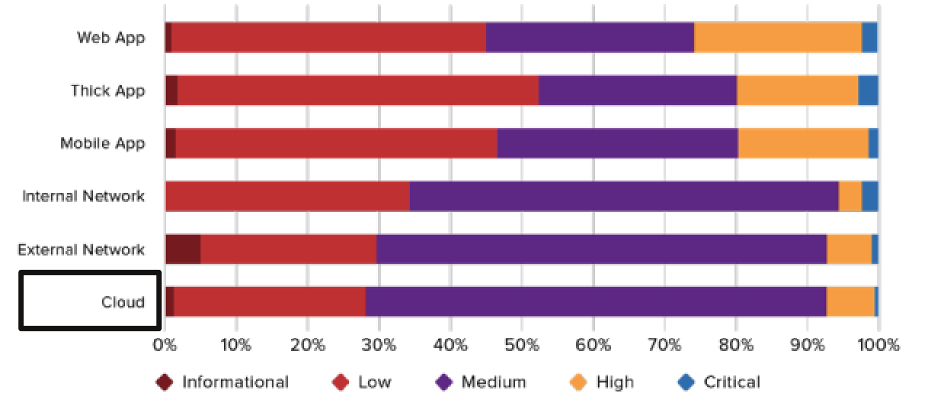
A look back on 2022
cloud pentest trends

NETSPI®

SEVERITY BREAKDOWN

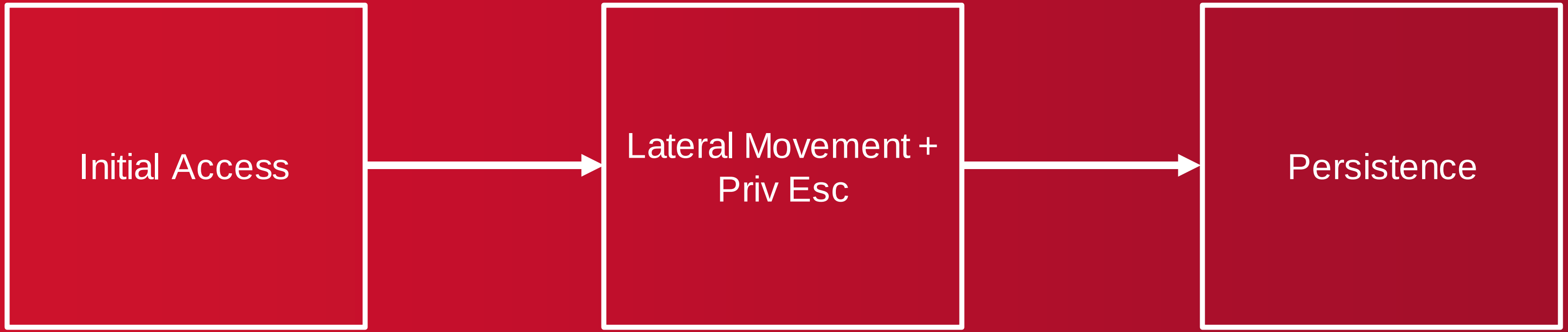


SEVERITY BREAKDOWN



NETSPI®

HIGH LEVEL STEPS



Initial Access

Lateral Movement + Priv Esc

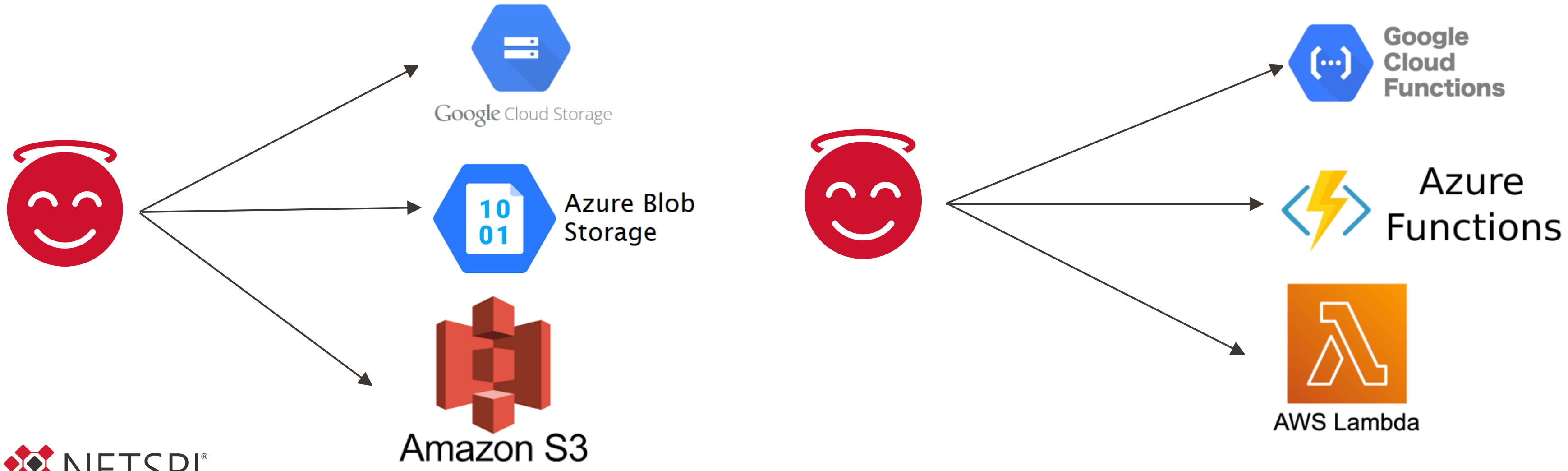
Persistence

MOST COMMON VULNERABILITIES

Current trends
on cloud pentests

NETSPI®

Publicly Available Resources Hosting Sensitive Data



Google Cloud Storage

Azure Blob Storage

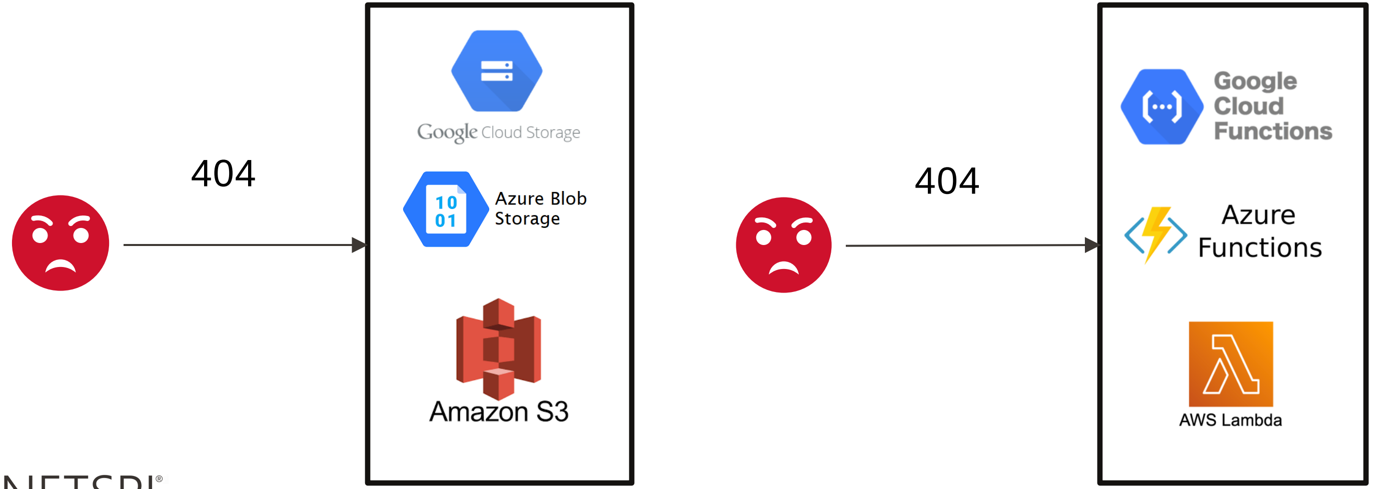
Amazon S3

Google Cloud Functions

Azure Functions

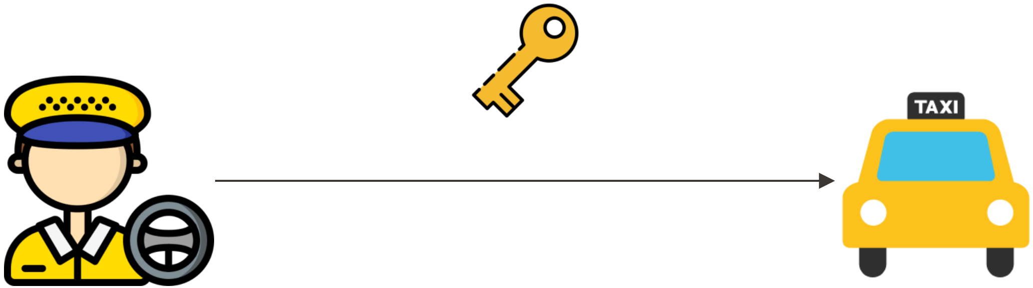
AWS Lambda

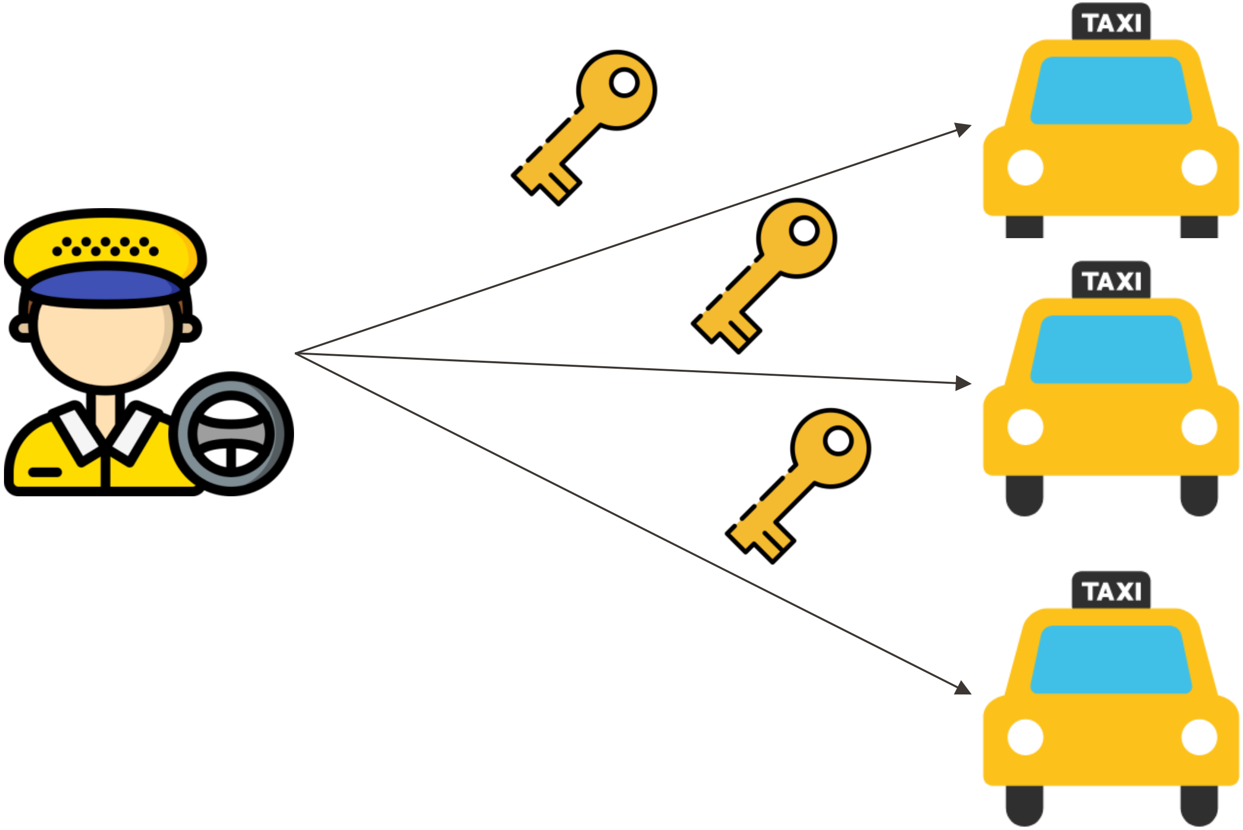
Publicly Available Resources Hosting Sensitive Data

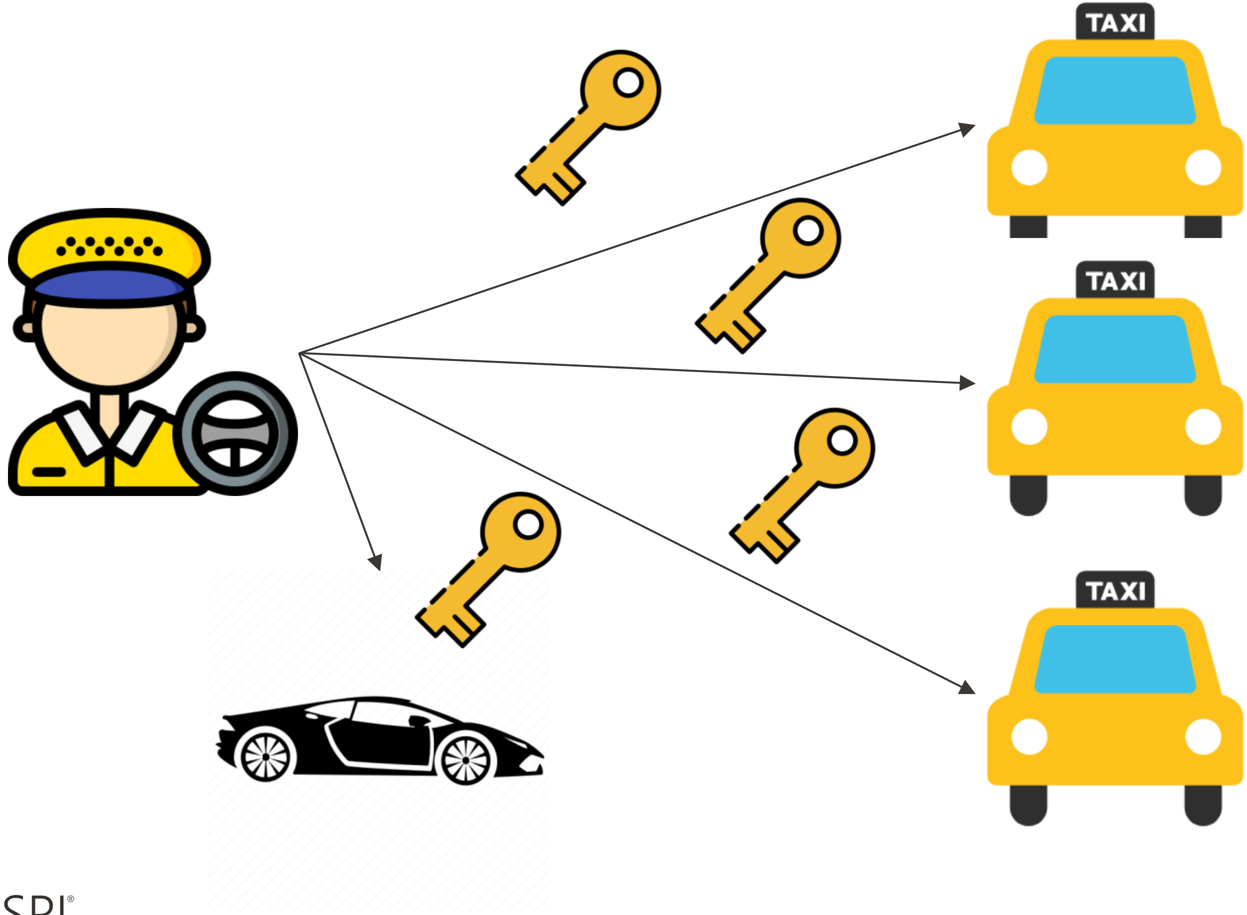


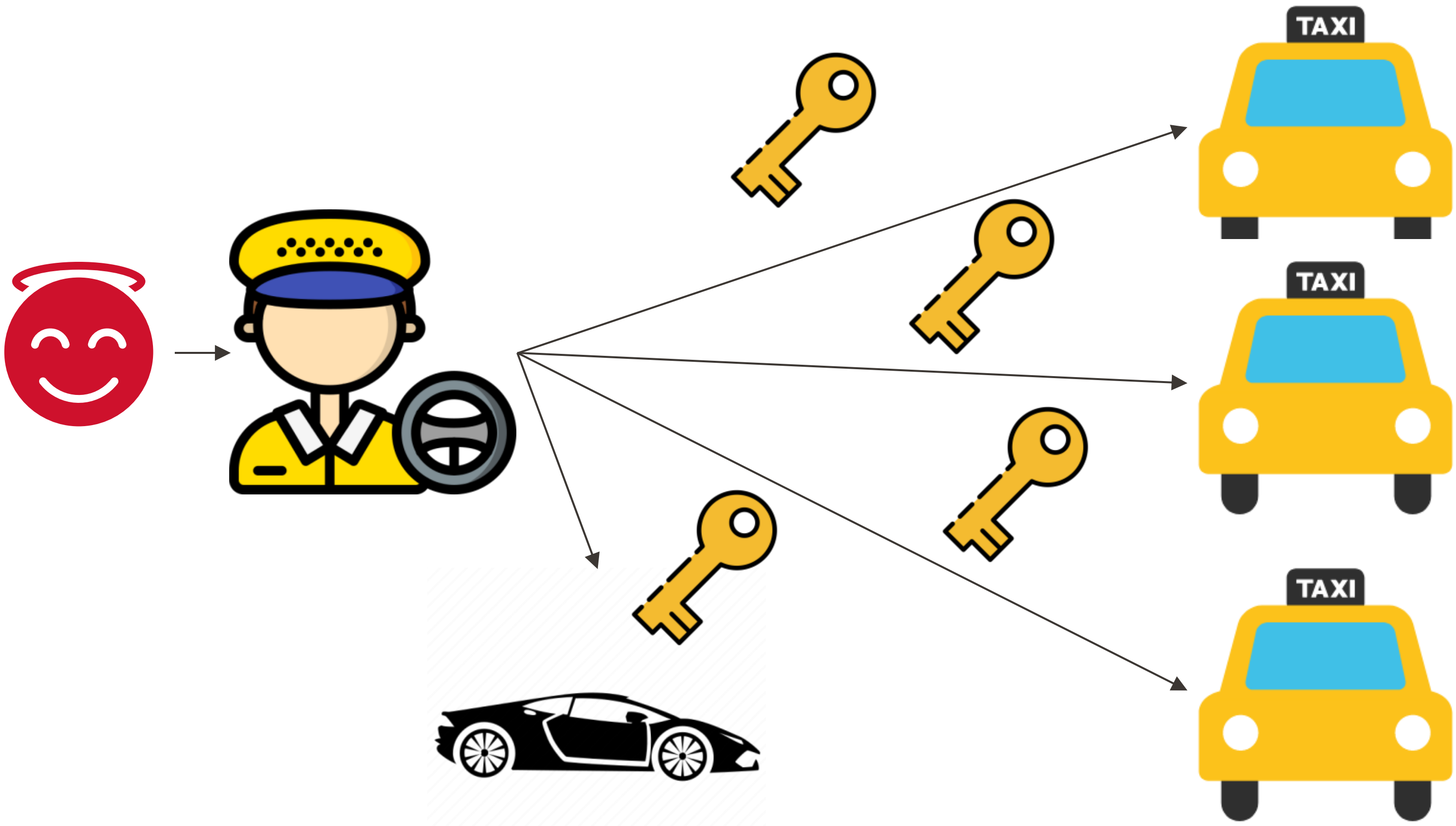
Misconfigured or Permissive

IAM Permissions



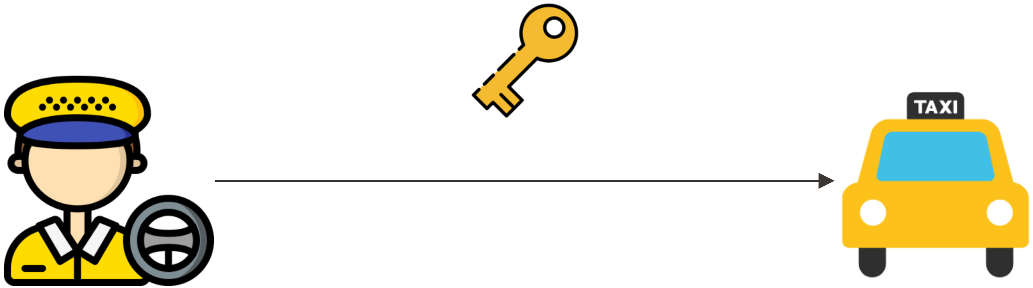

TAXI
TAXI
TAXI


TAXI
TAXI
TAXI


TAXI
TAXI
TAXI

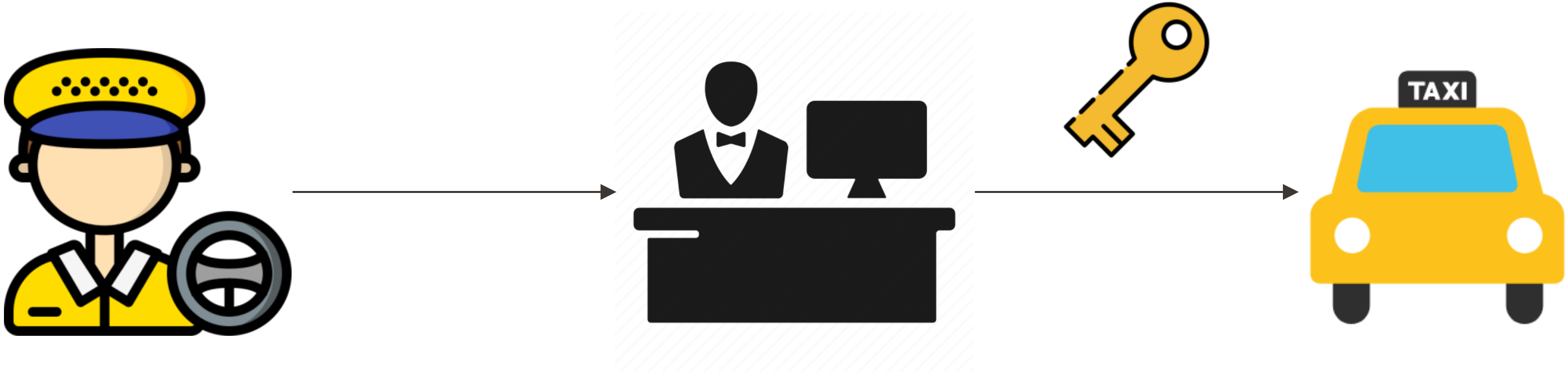
Misconfigured or Permissive

IAM Permissions - Scope



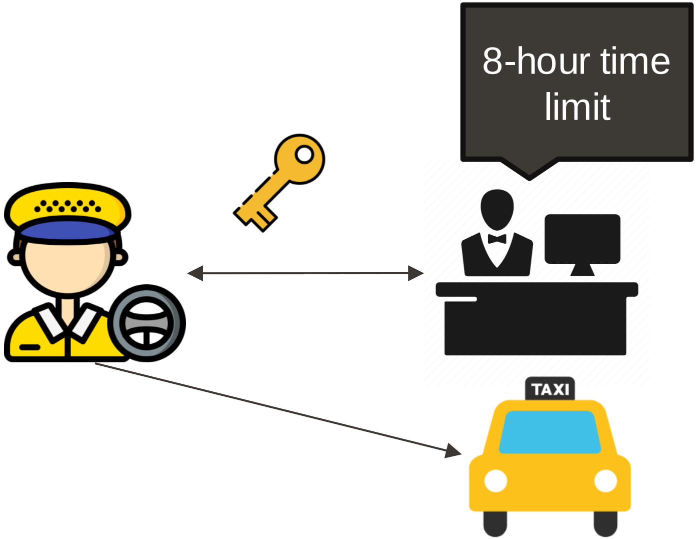
Misconfigured or Permissive

IAM Permissions - JIT



Misconfigured or Permissive

IAM Permissions - JIT



Cleartext Credentials Storage

Google Cloud Storage

Google Cloud Functions

Google Kubernetes Engine

Azure Blob Storage

Azure Functions

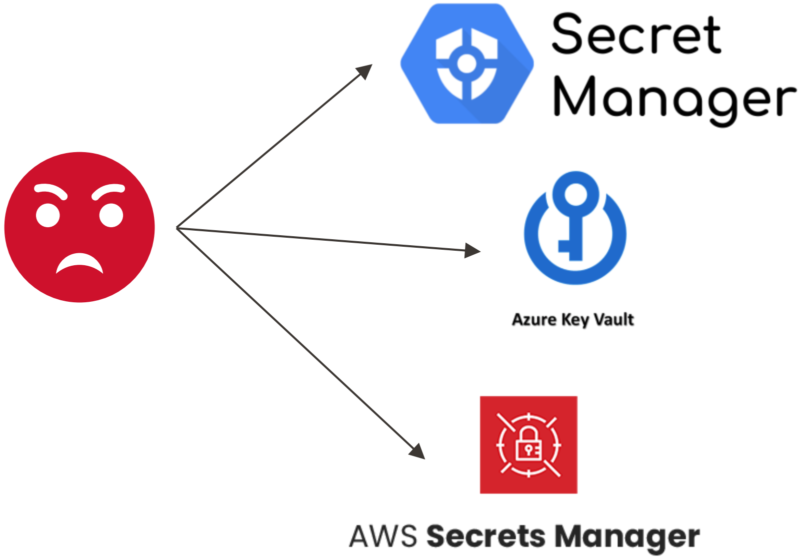
Azure Automation

Amazon S3

AWS Lambda

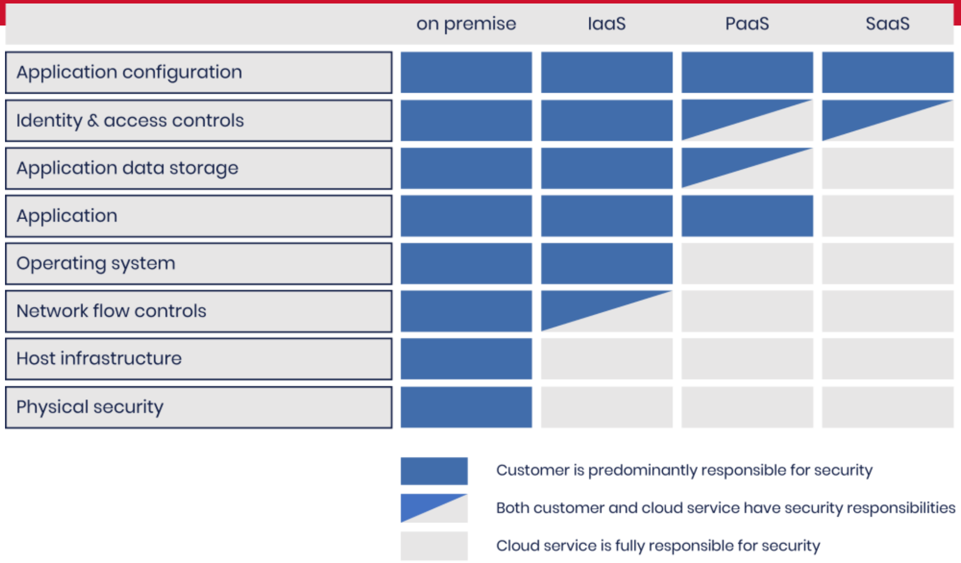
AWS ECS

Cleartext Credentials Storage



Vulnerable Software and OS Versions

(MISSING CRITICAL PATCHES)



	on premise	IaaS	PaaS	SaaS
Application configuration	■	■	■	■
Identity & access controls	■	■	◪	◪
Application data storage	■	■	◪	□
Application	■	■	■	□
Operating system	■	■	□	□
Network flow controls	■	◪	□	□
Host infrastructure	■	□	□	□
Physical security	■	□	□	□

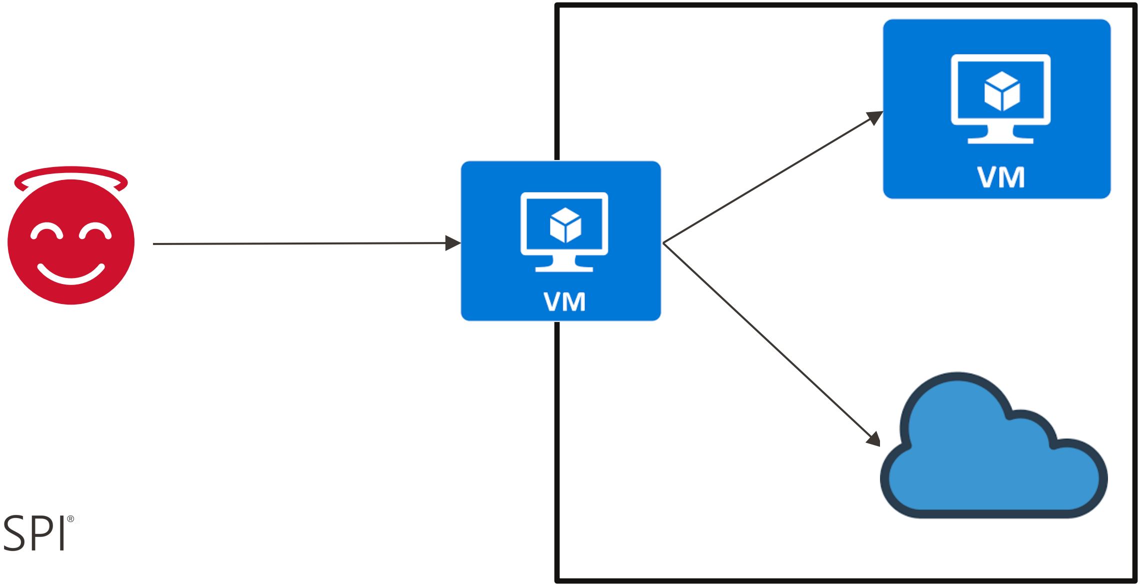
■ Customer is predominantly responsible for security

◪ Both customer and cloud service have security responsibilities

□ Cloud service is fully responsible for security

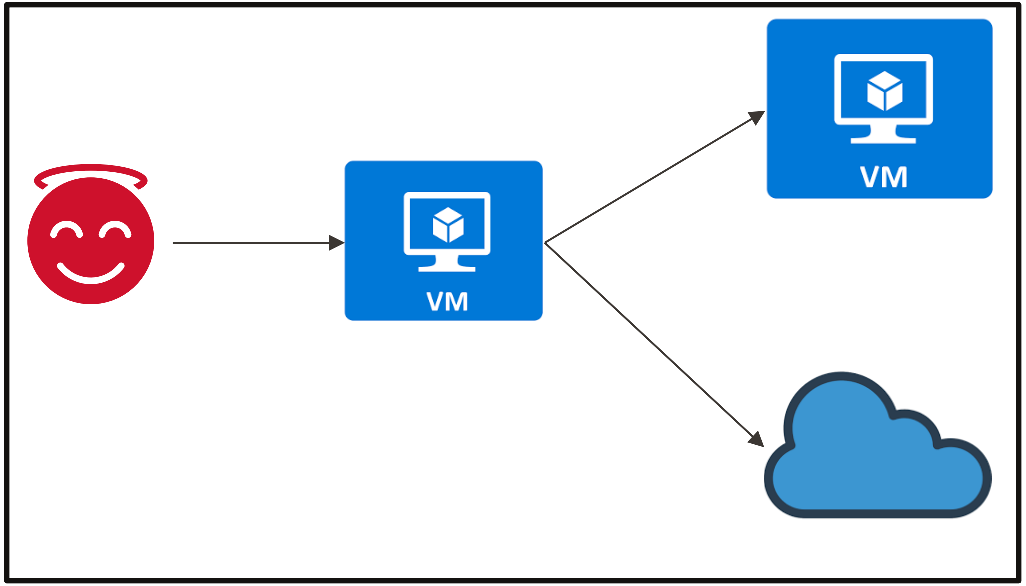
Vulnerable Software and OS Versions

External



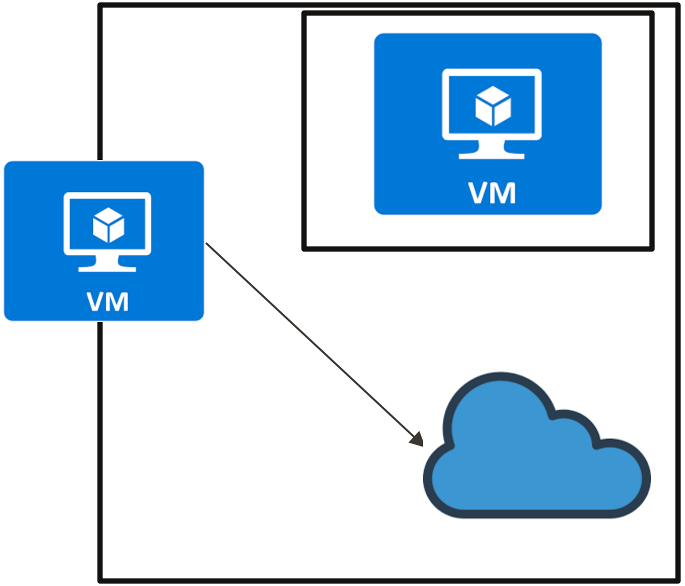
Vulnerable Software and OS Versions

Internal



Vulnerable Software and OS Versions

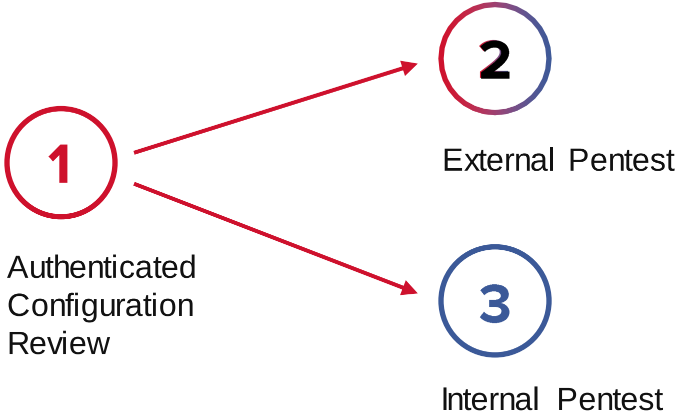
Remediation



CLOUD PENETRATION TESTING:

Methodology

3 PHASES OF TESTING PERFORMED CONCURRENTLY



GOALS

1 **IDENTIFY** Resources and Misconfigurations

2 **DEMONSTRATE** Impact Through Penetration Testing

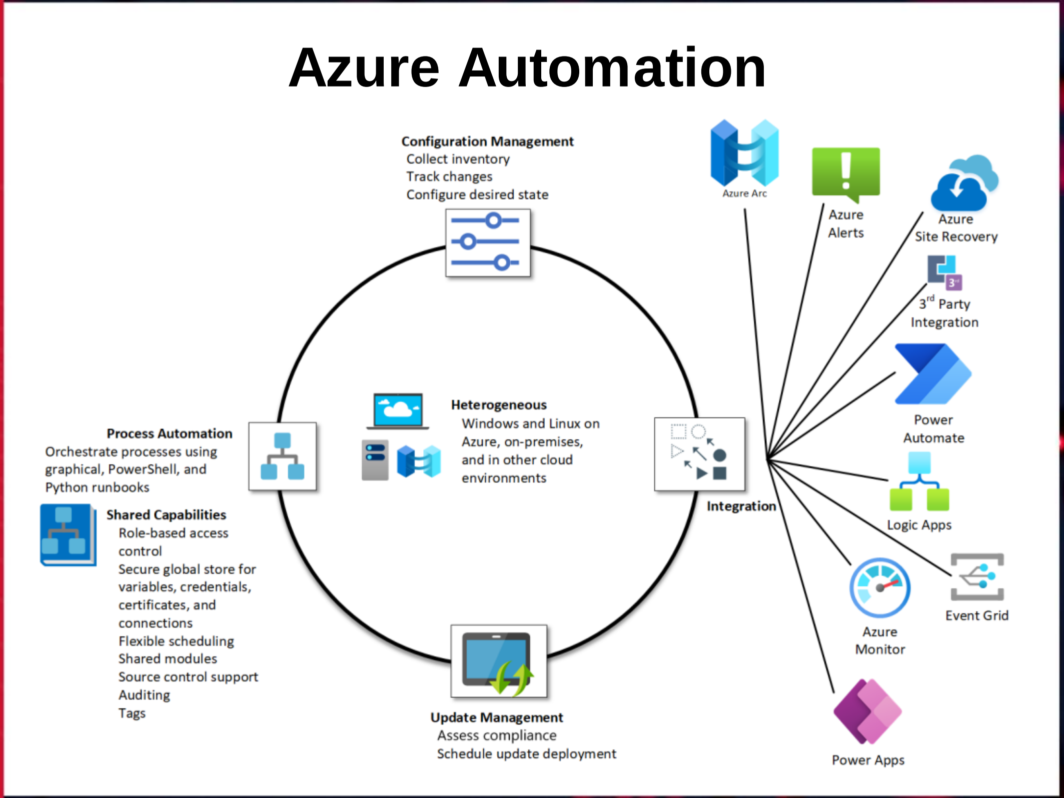
AZURE WAR STORY

Automation account contributor
to command execution
on every end user device

NETSPI®

Automation Accounts

What are they?



Azure Automation

Configuration Management
Collect inventory
Track changes
Configure desired state

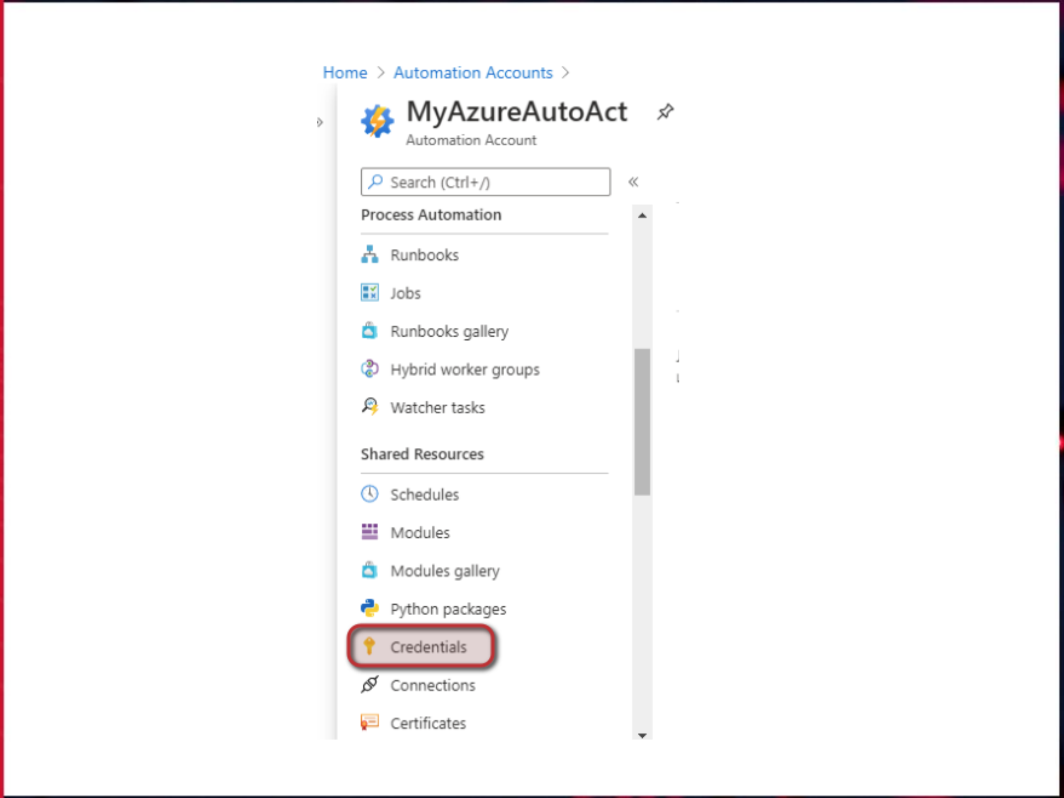
Process Automation
Orchestrate processes using graphical, PowerShell, and Python runbooks

Heterogeneous
Windows and Linux on Azure, on-premises, and in other cloud environments

Shared Capabilities
Role-based access control
Secure global store for variables, credentials, certificates, and connections
Flexible scheduling
Shared modules
Source control support
Auditing
Tags

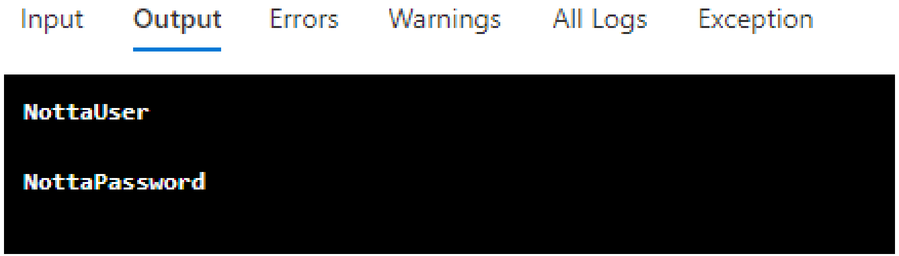
Update Management
Assess compliance
Schedule update deployment

Automation Account Credentials



Who has access?

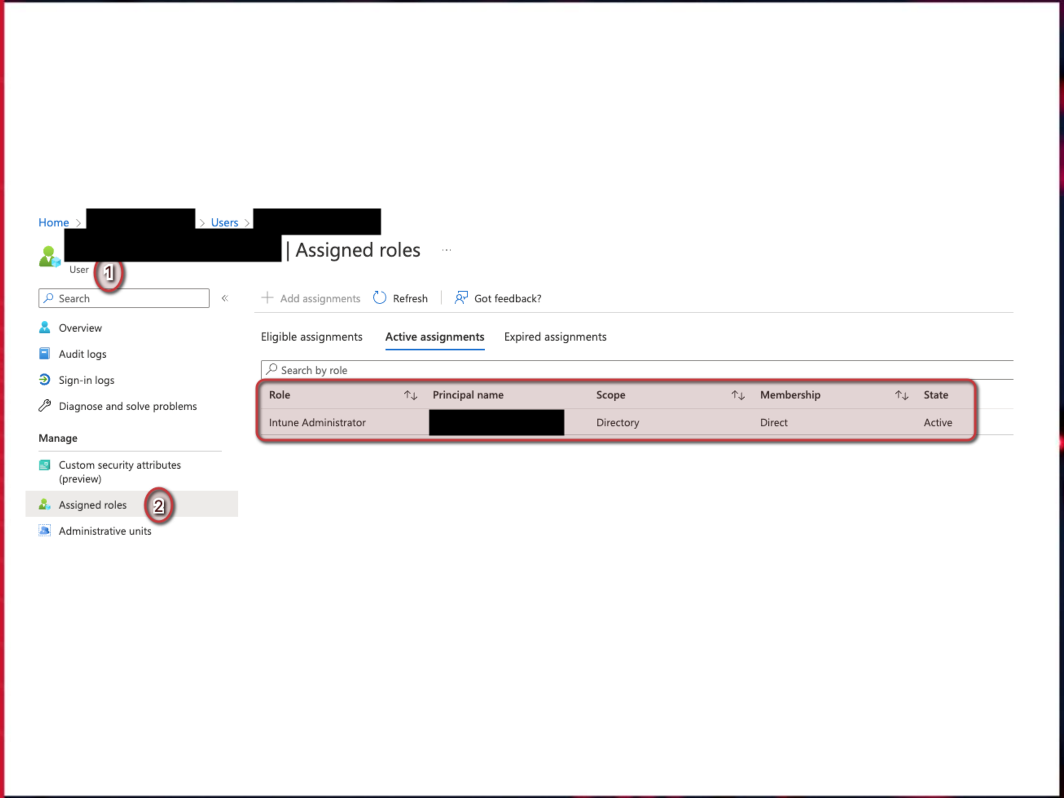
Get-AutomationPSCredential



```
NottaUser

NottaPassword
```

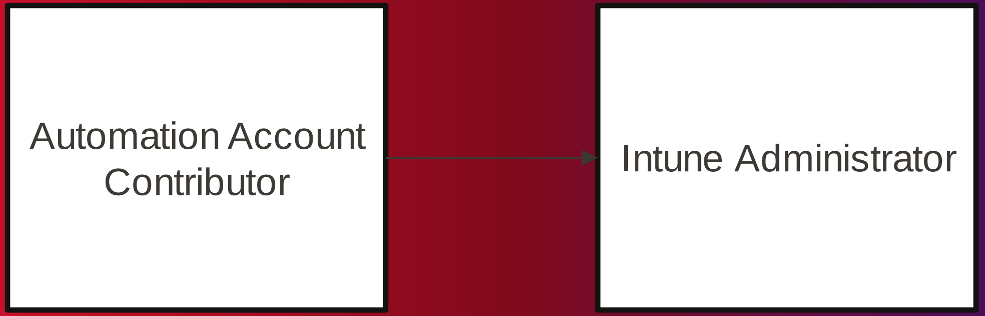
Why is this bad?



Role	Principal name	Scope	Membership	State
Intune Administrator	[redacted]	Directory	Direct	Active

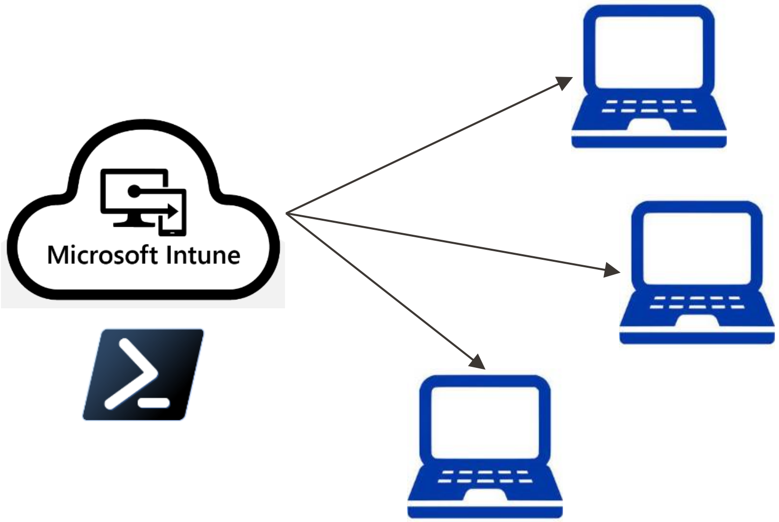
AZURE WAR STORY

Why is This Bad?



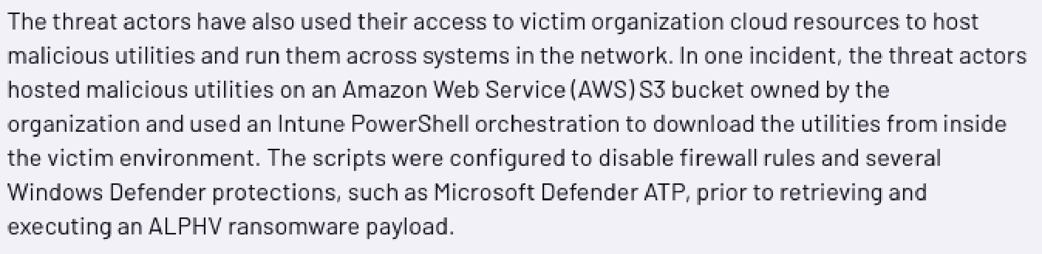
Why is this bad?

Intune Administrator



AZURE WAR STORY

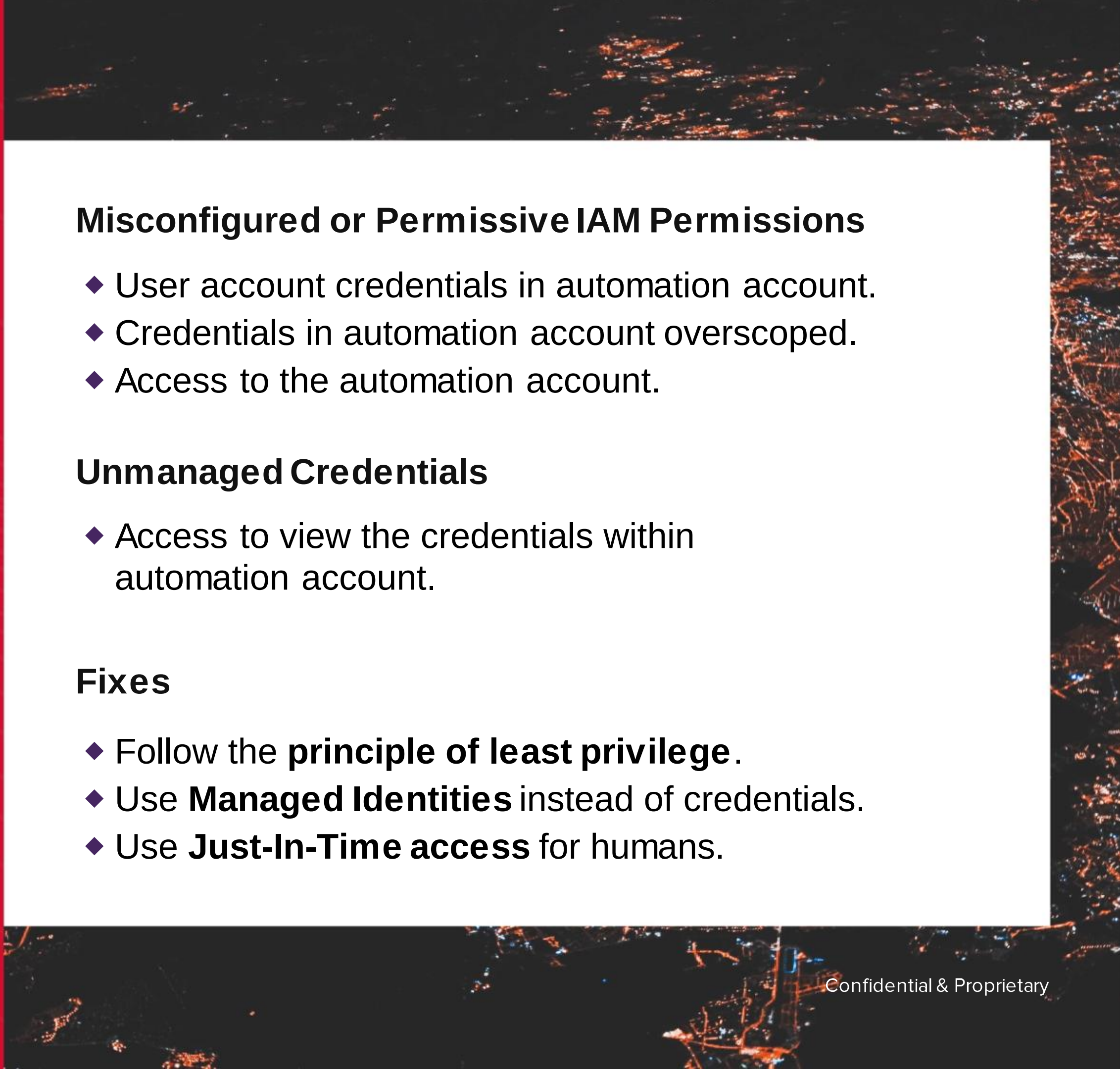
Why is This Bad?



The threat actors have also used their access to victim organization cloud resources to host malicious utilities and run them across systems in the network. In one incident, the threat actors hosted malicious utilities on an Amazon Web Service (AWS) S3 bucket owned by the organization and used an Intune PowerShell orchestration to download the utilities from inside the victim environment. The scripts were configured to disable firewall rules and several Windows Defender protections, such as Microsoft Defender ATP, prior to retrieving and executing an ALPHV ransomware payload.

https://www.mandiant.com/resources/blog/unc3944-sms-phishing-sim-swapping-ransomware

Linking back to most common vulnerabilities



Misconfigured or Permissive IAM Permissions

- User account credentials in automation account.
- Credentials in automation account overscoped.
- Access to the automation account.

Unmanaged Credentials

- Access to view the credentials within automation account.

Fixes

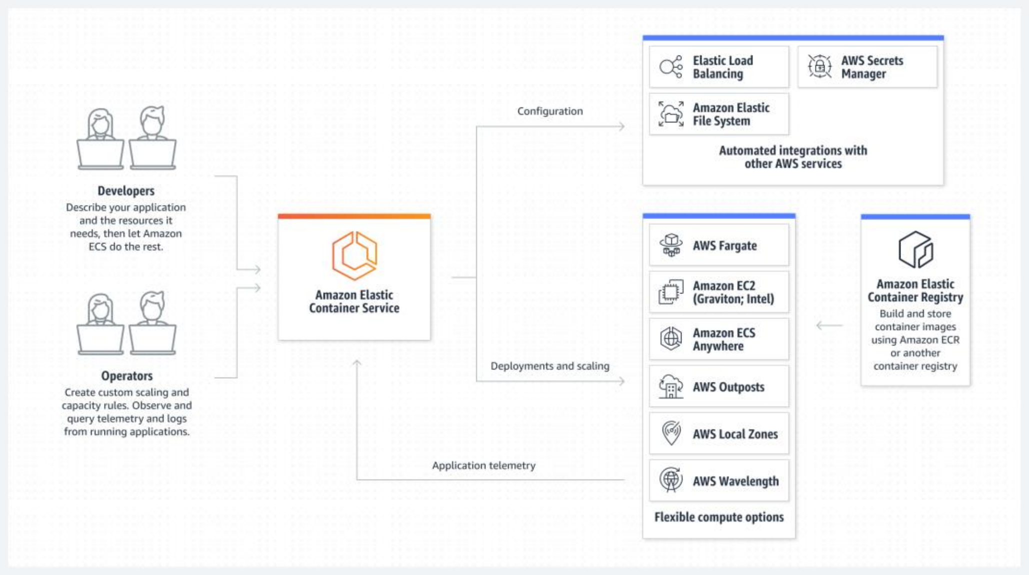
- Follow the **principle of least privilege**.
- Use **Managed Identities** instead of credentials.
- Use **Just-In-Time access** for humans.

AWS WAR STORY

Read only access to full administrator access privilege escalation

AWS WAR STORY

Elastic Container Service (ECS)


Developers
Describe your application and the resources it needs, then let Amazon ECS do the rest.
Operators
Create custom scaling and capacity rules. Observe and query telemetry and logs from running applications.
Amazon Elastic Container Service
Configuration
Deployments and scaling
Application telemetry
Elastic Load Balancing
AWS Secrets Manager
Amazon Elastic File System
Automated integrations with other AWS services
AWS Fargate
Amazon EC2 (Graviton; Intel)
Amazon ECS Anywhere
AWS Outposts
AWS Local Zones
AWS Wavelength
Flexible compute options
Amazon Elastic Container Registry
Build and store container images using Amazon ECR or another container registry

AWS WAR STORY

Elastic Container Service (ECS)

TASK DEFINITIONS

- Docker image to use
- IAM role to use
- Launch type
- Metadata

AWS WAR STORY

Secrets in ECS Task Definitions

TASK DEFINITIONS

- Read access required
- Iam:PassRole *
- Ec2:RunInstances *

NETSPI®

AWS WAR STORY

Permissions Explanation

Ec2:RunInstances *

- Allows attacker to create ec2 instances

Iam:PassRole *

- Allows attacker to assign permissions to resources

AWS WAR STORY

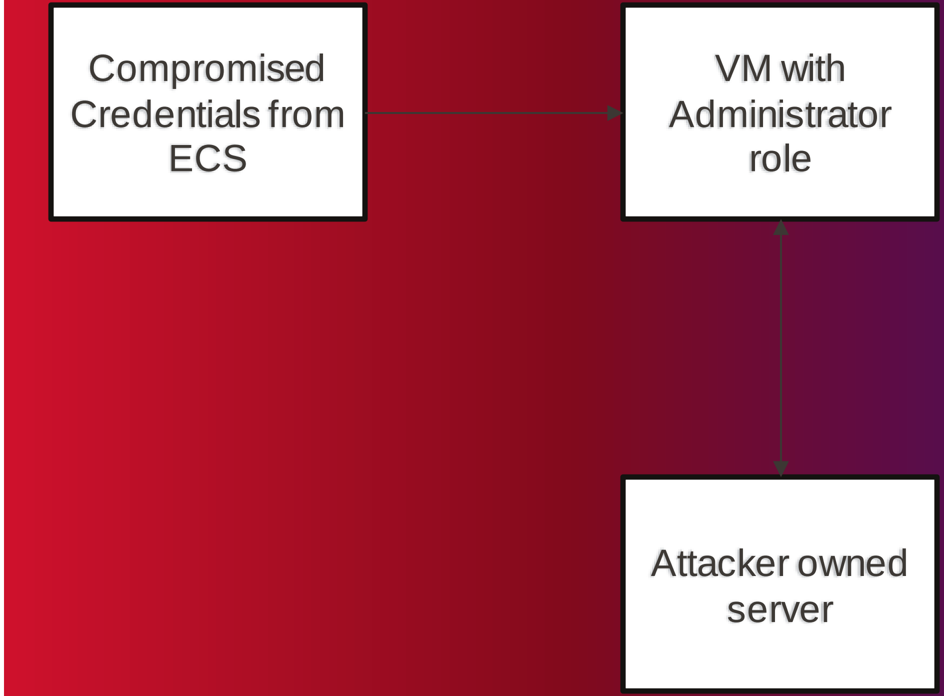
Getting Access

- Host listener for reverse shell on attacker owned machine
- Startup script on ec2

NETSPI®

AWS WAR STORY

Getting Access

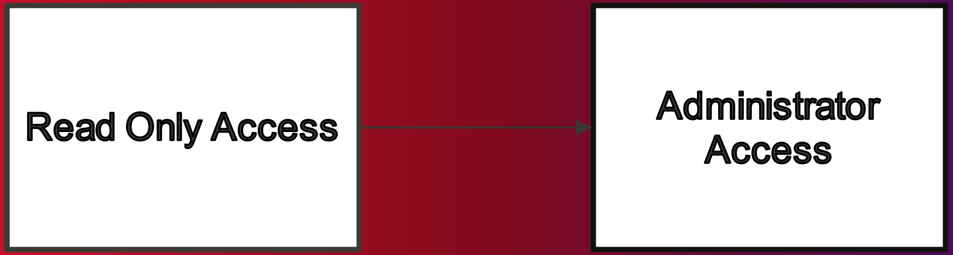


NETSPI®

AWS WAR STORY

Why is This Bad?

- EC2 instance created with full AWS administrator privileges
- Attacker can send commands to EC2 instance remotely



NETSPI®

AWS WAR STORY

Linking Back to the Most Common Vulnerabilities

CLEARTEXT CREDENTIALS STORAGE

- AWS key in ECS task definition

MISCONFIGURED OR PERMISSIVE IAM PERMISSIONS

- Leaked AWS key overscoped

NETSPI®

AWS WAR STORY

Remediation

- Do not store keys in ECS task definitions
- Follow principle of least privilege when defining roles

The NetSPI Cloud Penetration Testing Difference

NETSPI'S APPROACH AND INDUSTRY CONTRIBUTIONS

Emphasis on research to deliver cutting edge value to our customers

- NetSPI dedicates time and resources to research
- Result: research directly delivers value to our customers
- Public Research and Vulnerability Disclosures on the Technical Blog
  - https://www.netspi.com/blog/technical/cloud-penetration-testing/azure-function-apps/
  - https://www.netspi.com/blog/technical/vulnerability-research/azure-service-bus-power-platform/

Track record of community tooling, publications, and talks

- Open-source tooling
  - https://github.com/NetSPI/MicroBurst
- The Azure Penetration Testing book
  - https://www.amazon.com/Penetration-Testing-Azure-Ethical-Hackers/dp/1839212934
- DefCon Cloud Village 2022 Talk - *Automating Insecurity in Azure* - Karl Fosaaen
- DefCon Cloud Village 2023 Talk - *What the Function: A Deep Dive into Azure Function App Security*

NETSPI®

KEY TAKEAWAYS

- Configuration review is not enough to offer a full picture of security posture in an environment.
- Be very aware of shared responsibility model when making security decisions.
- Store secrets in appropriate services and regularly scan for exposed secrets (internal and external)
- Follow principle of least privilege when creating or assigning IAM roles

NETSPI™

Q & A

NETSPI™

NETSPI®