RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: CSV-T08

Break the Top 10 Cloud Attack Killchains

Rich Mogull

Analyst/Securosis

CISO/DisruptOps

@rmogull

Shawn Harris

Managing Principal Security Architect

Starbucks

@infotechwarrior

Kill Chains and ATT&CK's

- Lockheed Martin's Cyber Kill Chain represents a standard attack pattern from recon to action
- MITRE's ATT&CK framework is knowledge base of attack patterns in structured phases
- Both are to help you threat model and plan defenses
- This session includes *10 specific cloud kill chains* most commonly used (in our experience)

Objectives

Provide you with detailed information on the most common real world cloud attacks

AND

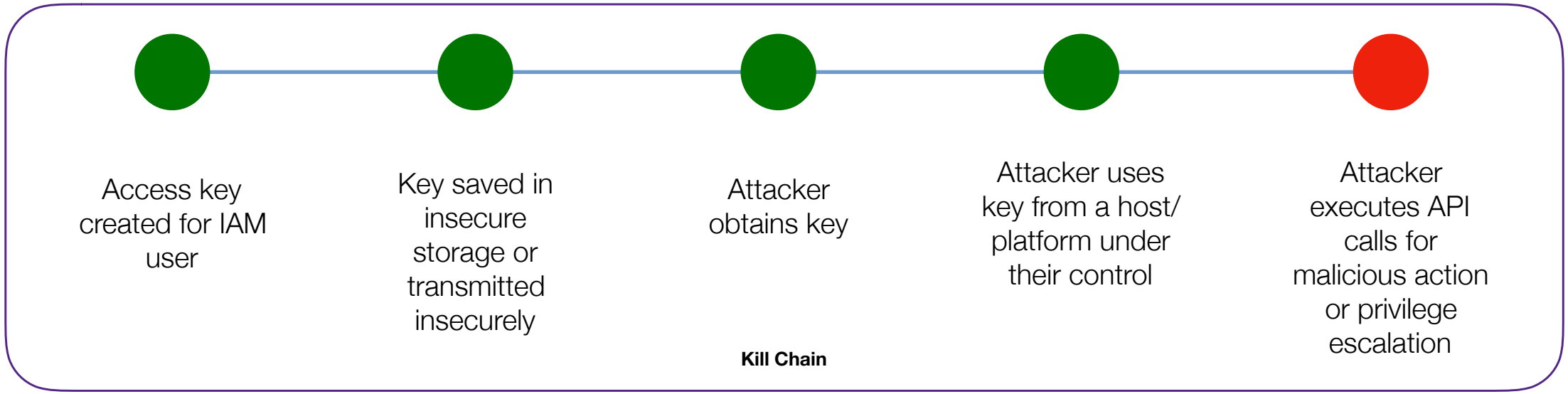
And the most effective ways to prevent them

RSAConference2020

Static API Credential Exposure to Account Hijack

Category	Attack (Scripted or Targeted)
Severity	High
Liklihood	High
Primary CSA Top Threat	4. Security Issue: Insufficient Identity, Credential, Access and Key Management 5.Security Issue: Account Hijacking
Primary Mitre ATT&CK	Valid Accounts

Static API Credential Exposure to Account Hijack



aws

Azure

Common sources of credential exposure

- GitHub/BitBucket ★
- Shared images
- Snapshots
- Compromised instance -> embedded code
- Compromised instance or dev/admin system - >
  - Shell history
  - Config/Credentials file
  - Local code

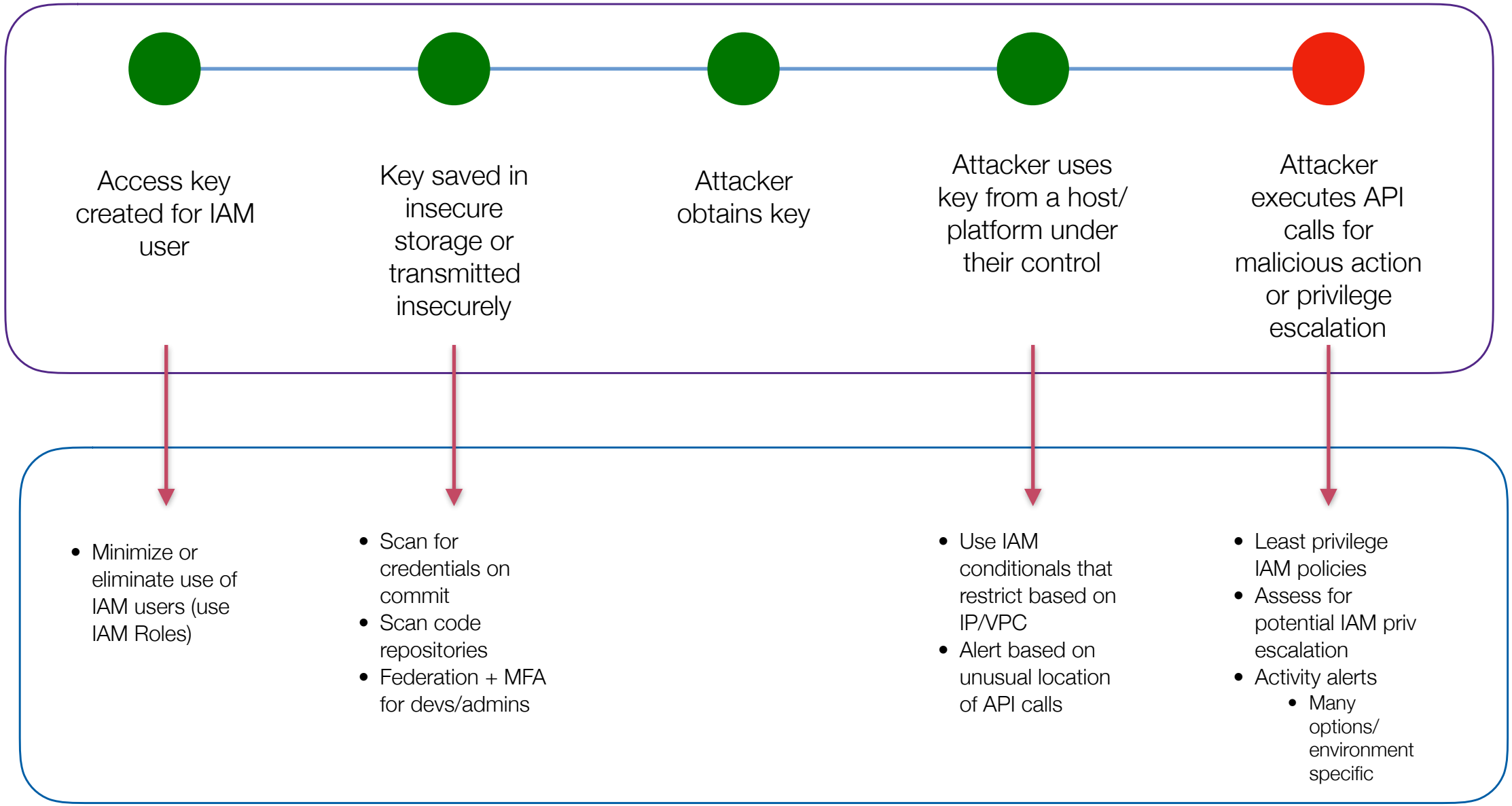

Data Centre ▸ Cloud

Hapless AWS engineer spilled passwords, keys, confidential internal training info, customer messages on public GitHub

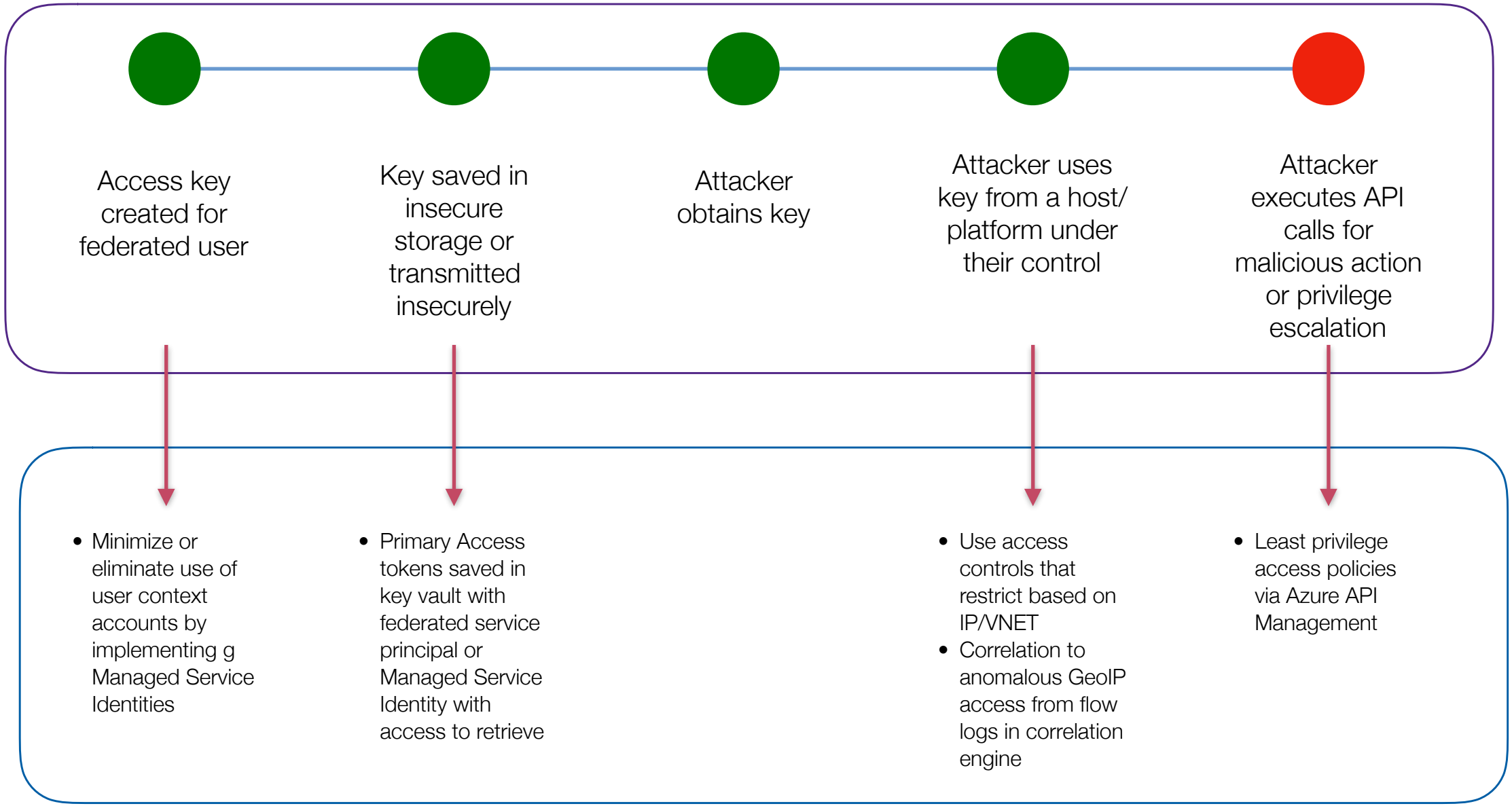
Only up for five hours, but that's plenty of time for the wrong person to spot it

By Tim Anderson 23 Jan 2020 at 16:33 34 SHARE ▼

Static API Credential Exposure to Account Hijack



Static API Credential Exposure to Account Hijack



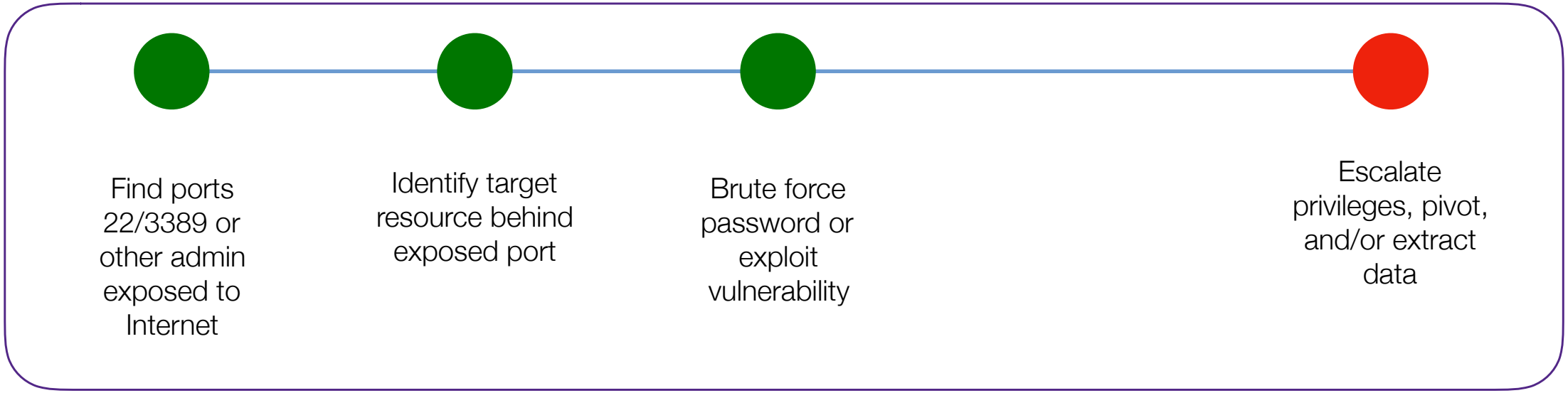
Azure

RSAConference2020

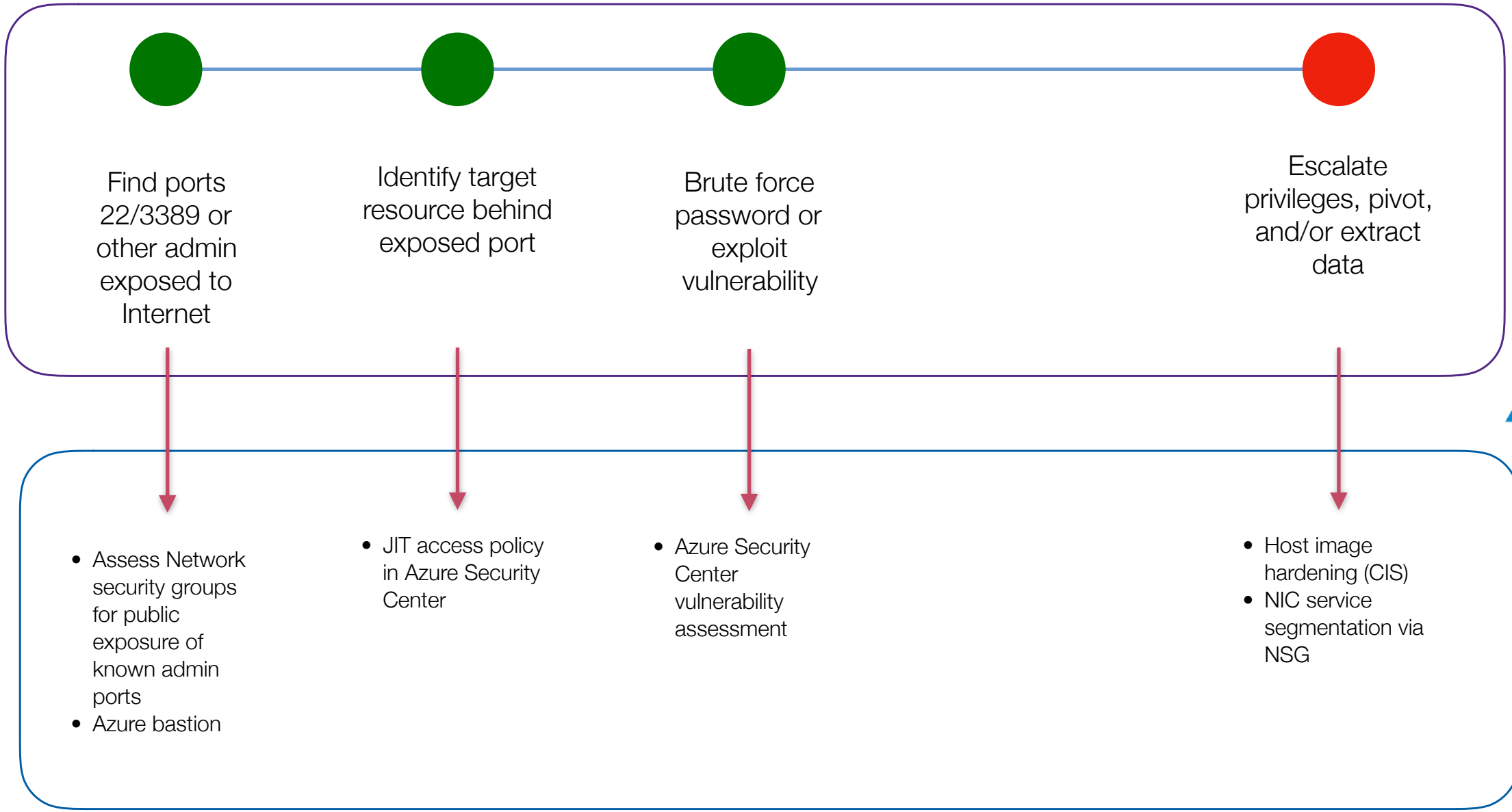
Compromised Server via Exposed SSH/RDP/Remote Access

Category	Misconfiguration (Common)
Severity	High
Liklihood	High
Primary CSA Top Threat	2: Misconfiguration and Inadequate Change Control
Primary Mitre ATT&CK	Exploit Public-Facing Application

Compromised Server via Exposed SSH/RDP/Remote Access

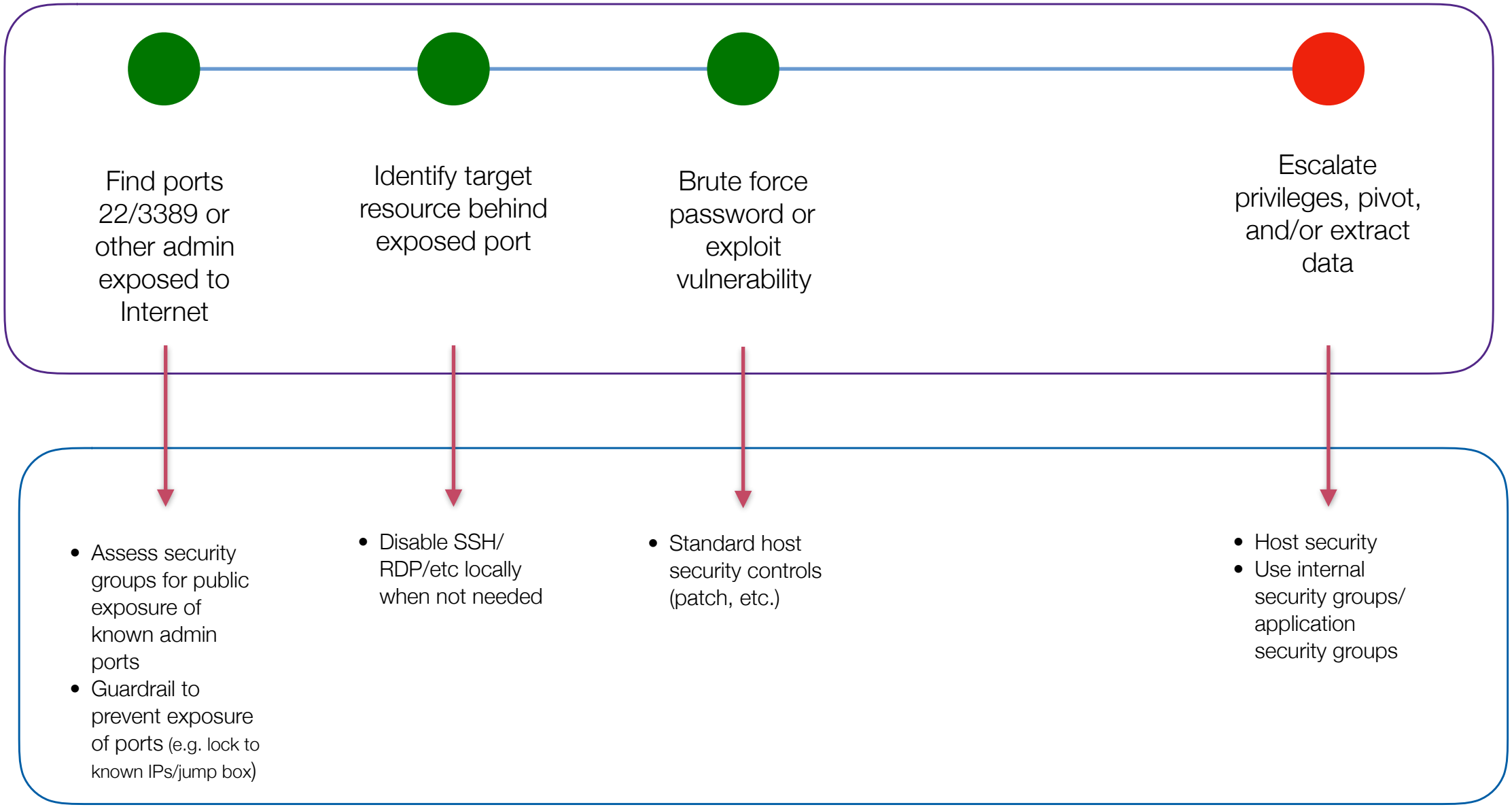


Compromised Server via Exposed SSH/RDP/Remote Access



Azure

Compromised Server via Exposed SSH/RDP/Remote Access



2 Million+!

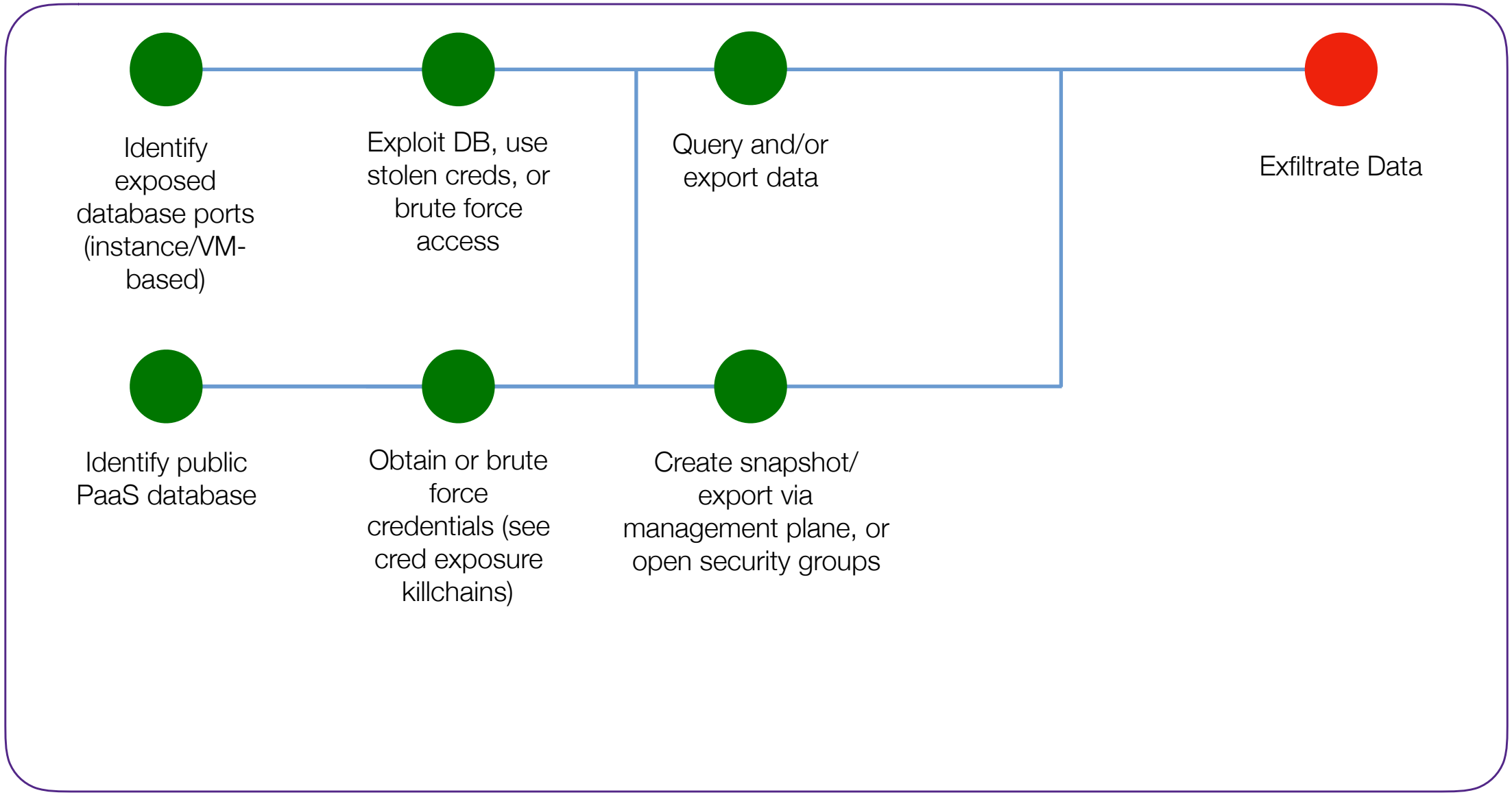

SHODAN
Pricing
ssh hostname:"amazonaws"
TOTAL RESULTS
2,913,172
TOP COUNTRIES
United States 1,794,808
Ireland 236,073
Germany 166,102
Japan 145,185
Singapore 121,402

RSAConference2020

Compromised Database via Inadvertent Exposure

Category	Misconfiguration (Common)
Severity	Medium
Liklihood	High
Primary CSA Top Threat	2: Misconfiguration and Inadequate Change Control
Primary Mitre ATT&CK	Exploit Public-Facing Application

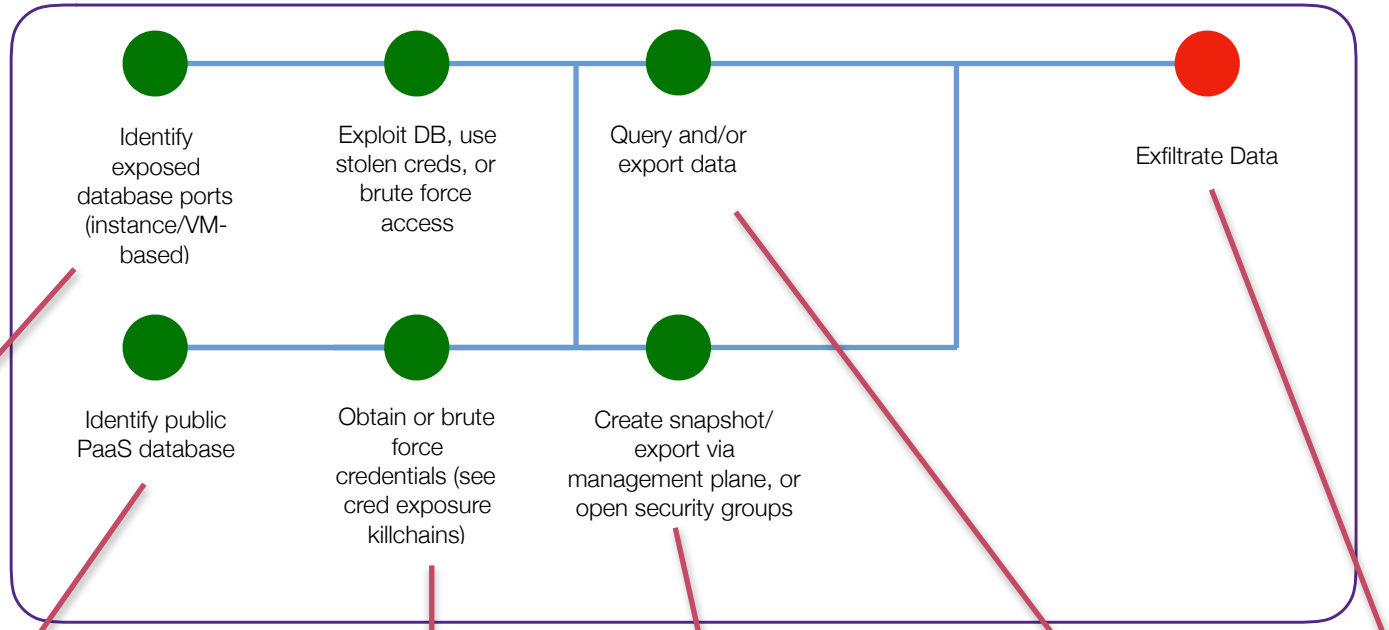
Compromised Database via Inadvertent Exposure



aws

Azure

Compromised Database via Inadvertent Exposure



- Security group rules
- Continuous assessment/ guardrails

- Continuous assessment/ guardrails
- SCPs/Policies

- Vulnerability management
- MFA

- Least privilege IAM
- IP/VPC restrictions on API call origins
- SCPs/Policy
- Guardrails

- DB least privilege
- Database Activity Monitoring

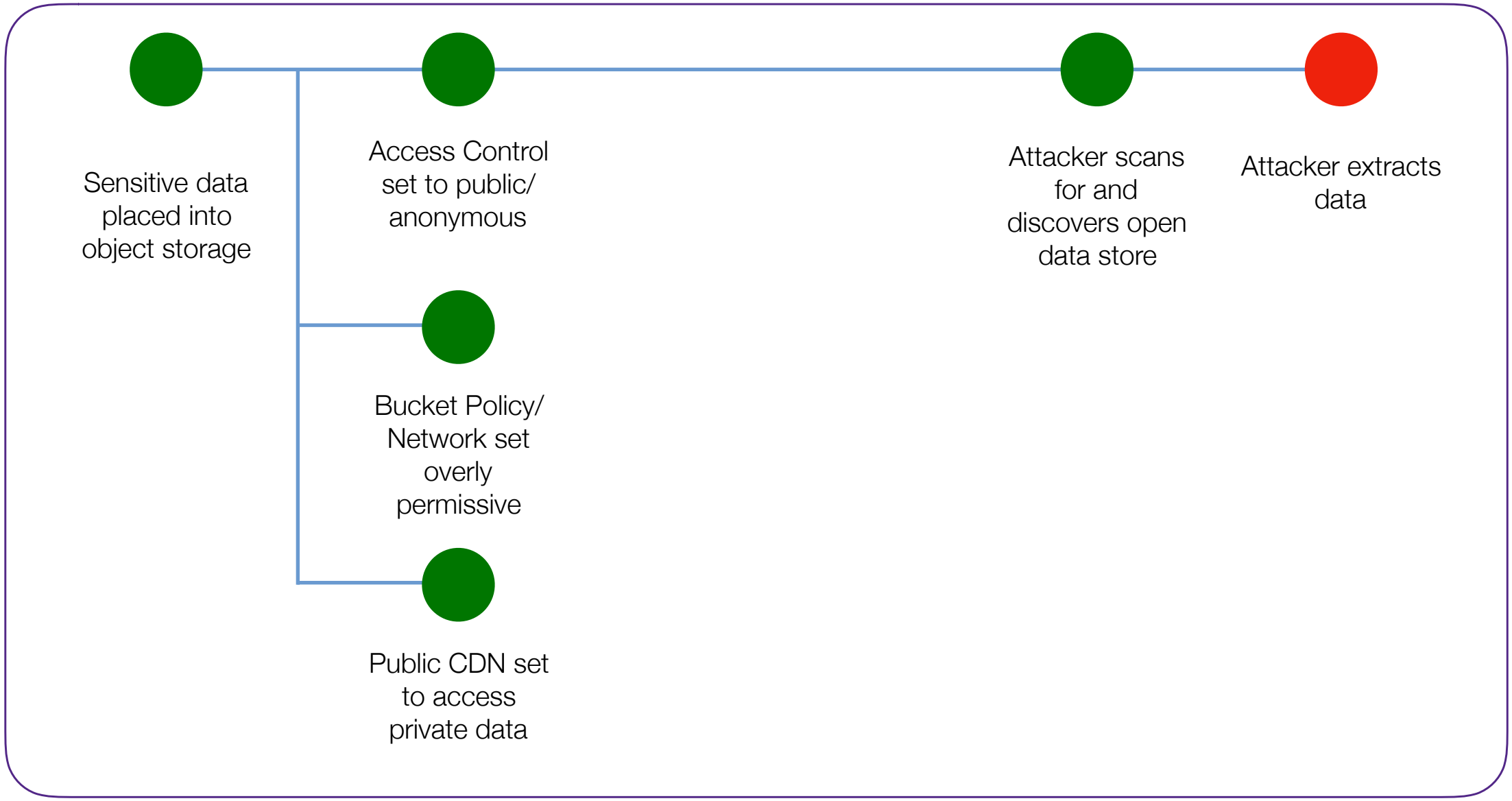
- Outbound network restrictions
- Cloud detection and response

RSAConference2020

Object Storage Public Data Exposure (S3, Azure Blob)

Category	Misconfiguration (Common)
Severity	High
Liklihood	High
Primary CSA Top Threat	2. Security Issue: Misconfiguration and Inadequate Change Control
Primary Mitre ATT&CK	Exploit Public-Facing Application

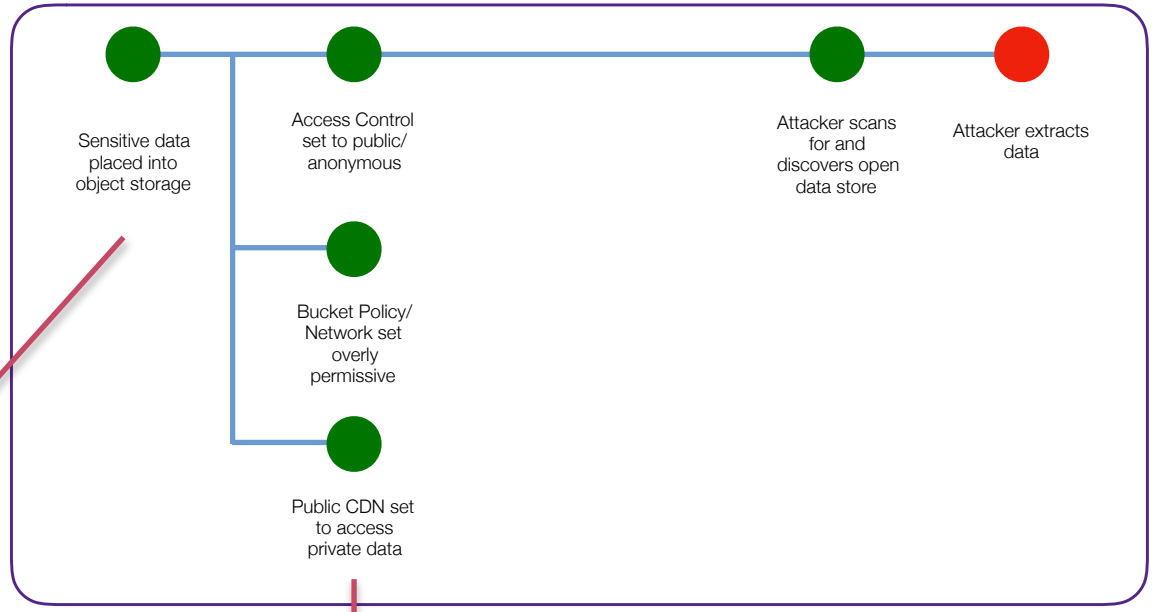
Object Storage *Public* Data Exposure (S3, Azure Blob)



aws

Azure

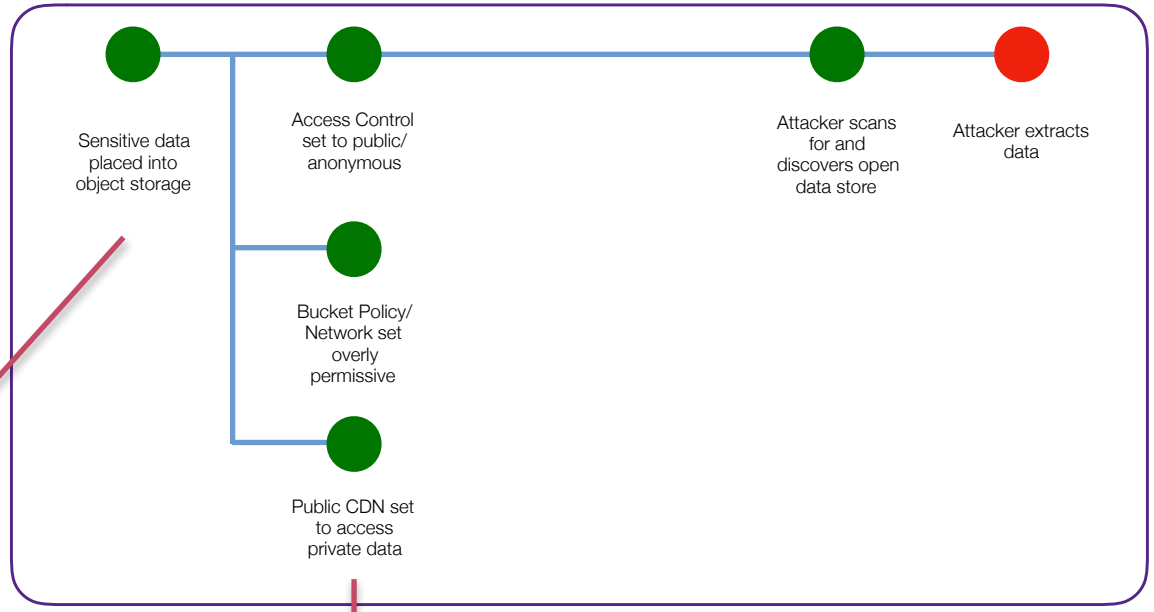
Object Storage *Public* Data Exposure (S3, Azure Blob)



- Cloud-based DLP (Macie/AIP) *Note: these are currently immature and of limited effectiveness*

- Continuous assessment
- Real time alerting on ACL and Bucket/Network policy changes
- Disable public access (CSP setting)
- Reactive Guardrail (FaaS or 3rd party)

Object Storage *Public* Data Exposure (S3, Azure Storage)



- MCAS Microsoft Cloud Application Security (CASB)

Verify with Trull

- Azure Advanced Threat Protection for storage accounts
- Azure Storage Firewall configured to disable public access

Oops, my bad...

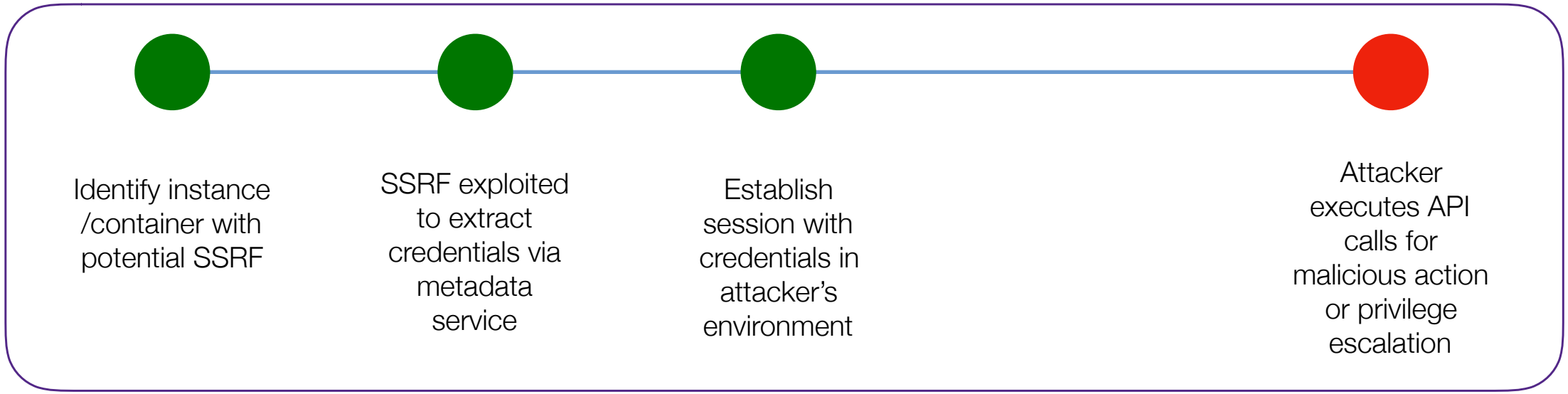
		Public	US West (Oregon)
		Public	US East (Ohio)
		Public	US West (Oregon)
	51-us-west-2	Objects can be public	US West (Oregon)
		Objects can be public	US East (N. Virginia)
		Objects can be public	US West (Oregon)
		Public	US West (Oregon)

RSAConference2020

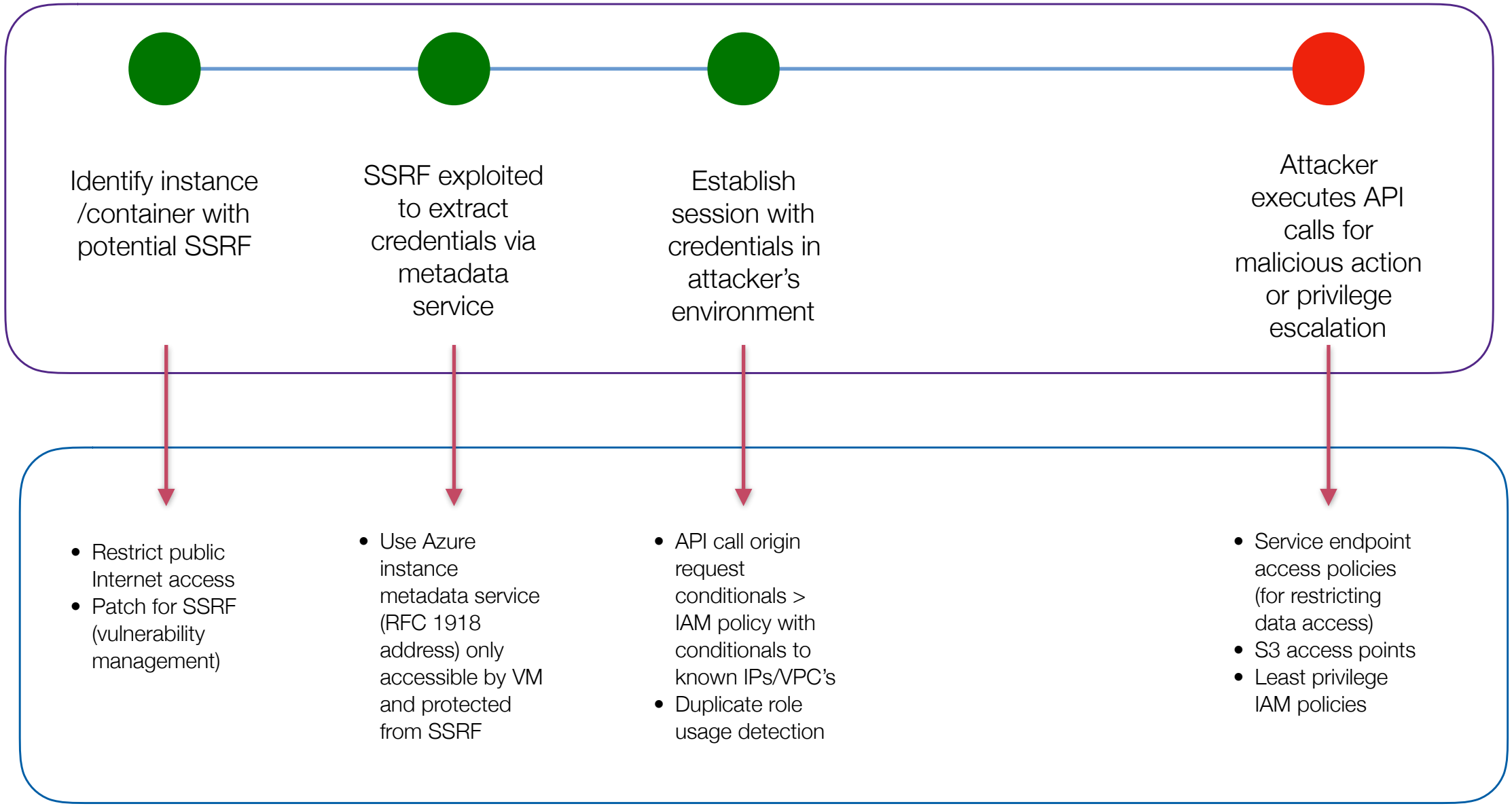
Server Side Request Forgery -> Credential Abuse

Category	Attack (Scripted or Targeted)
Severity	Medium
Liklihood	High
Primary CSA Top Threat	1. Data Breaches
Primary Mitre ATT&CK	Exploit Public Facing Application, Cloud Instance Metadata API

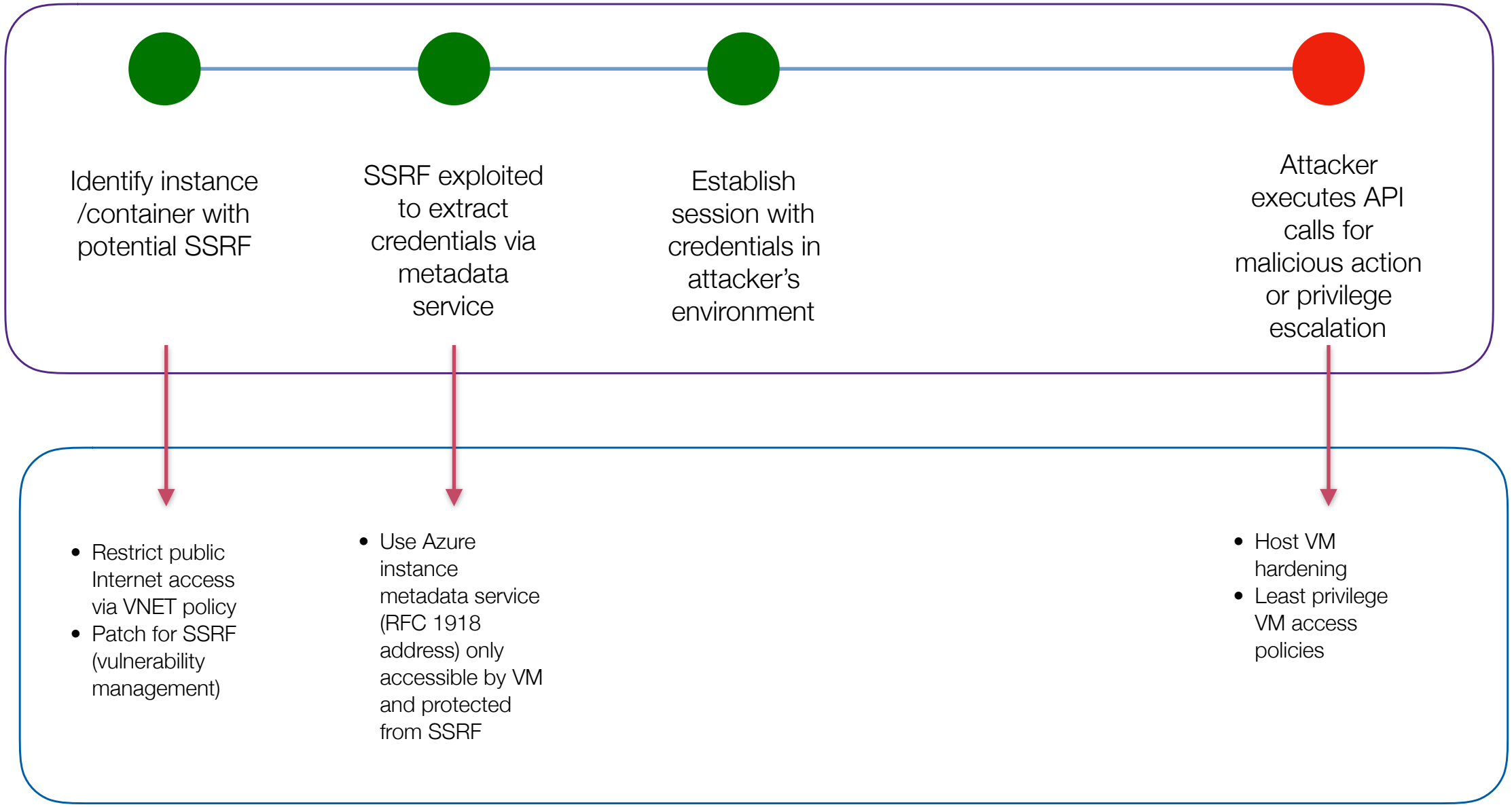
Server Side Request Forgery -> Credential Abuse



Server Side Request Forgery -> Credential Abuse

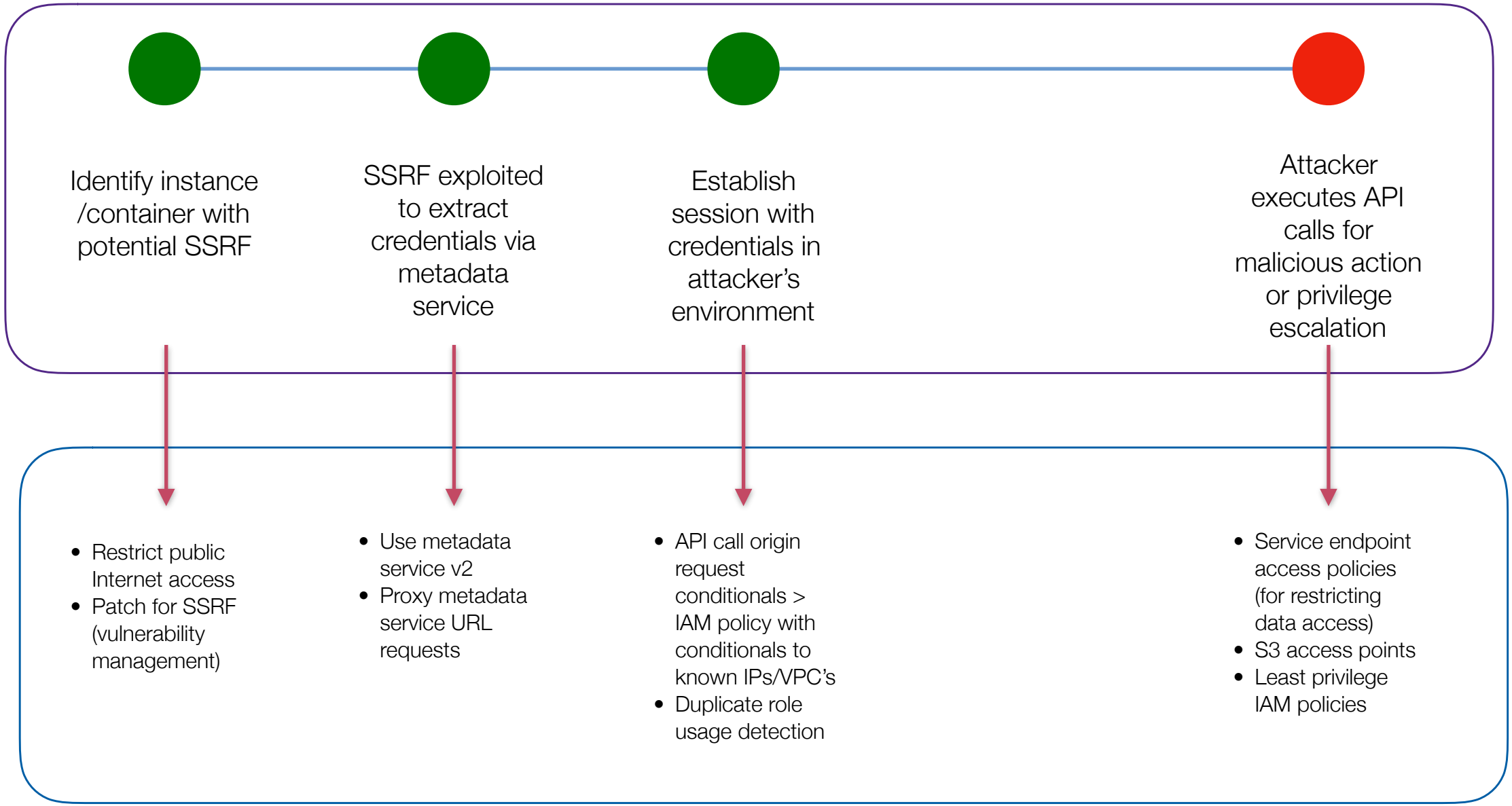


Server Side Request Forgery -> Credential Abuse



Azure

Server Side Request Forgery -> Credential Abuse



Demo

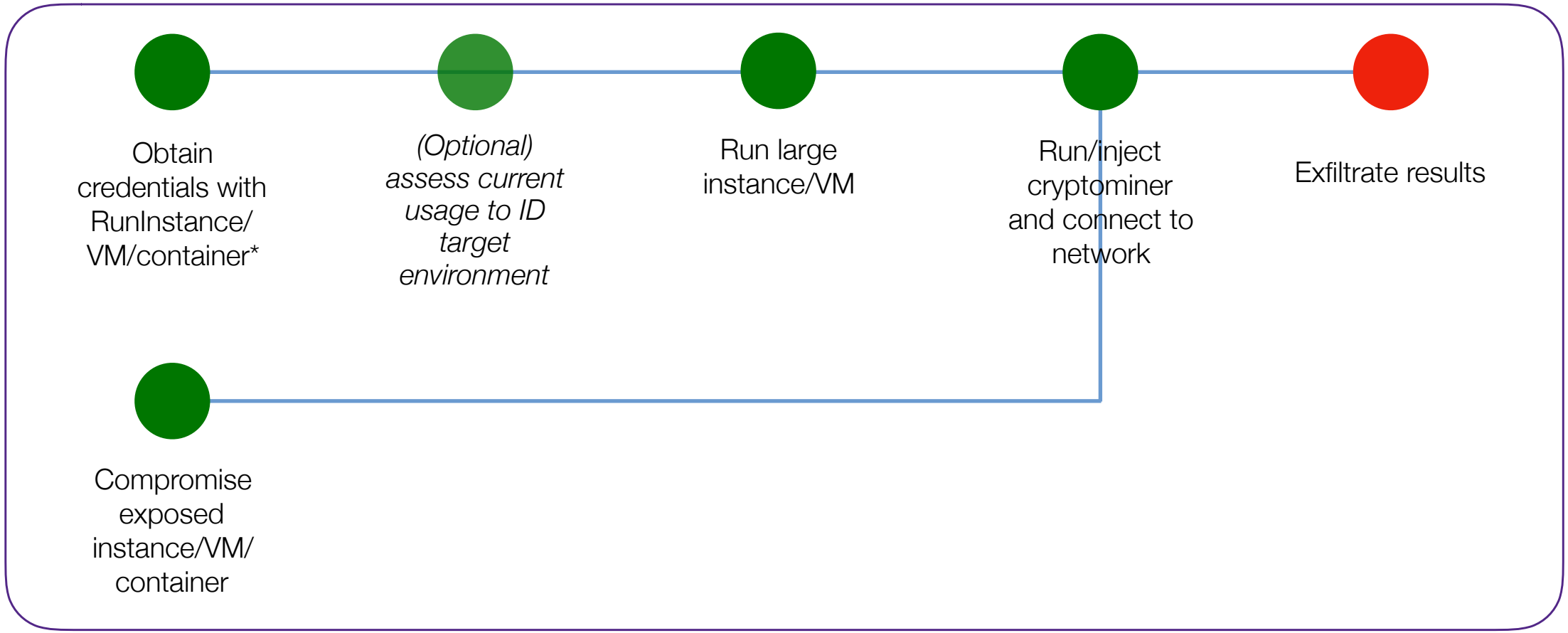
```
~ — ec2-user@ip-172-31-27-252:~ — ssh -i mykey.pem ec2-user@52.42.196.113 ...   ~ — ec2-user@ip-172-31-28-218:~ — ssh -i mykey.pem ec2-user@34.219.163.255
Last login: Sat Jul 27 02:03:50 on ttys001
MacBook-Pro:~ rmogull$ ssh -i mykey.pem ec2-user@34.219.163.255
The authenticity of host '34.219.163.255 (34.219.163.255)' can't be established.
ECDSA key fingerprint is SHA256:ihAVUzVRInoHIFXAJk5MXOTW7gszBzi/7NJeCo0ADC0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '34.219.163.255' (ECDSA) to the list of known hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
3 package(s) needed for security, out of 8 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-28-218 ~]$
```

RSA Conference2020

Cryptomining

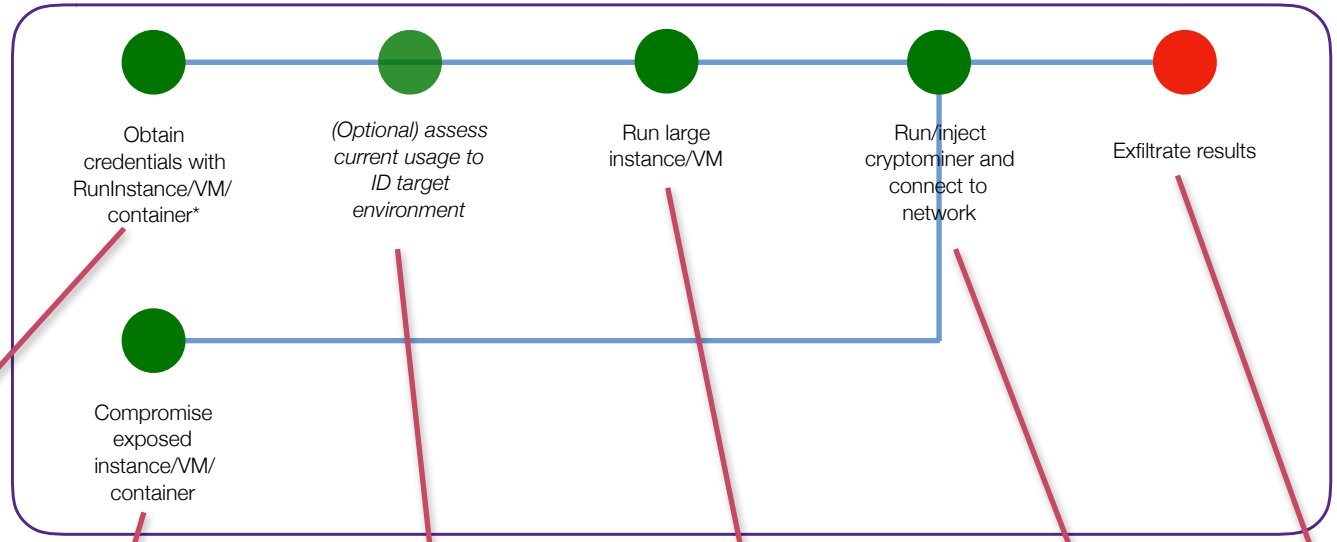
Category	Attack (Scripted or Targeted)
Severity	Low
Liklihood	High
Primary CSA Top Threat	11. Security Issue: Abuse and Nefarious Use of Cloud Services
Primary Mitre ATT&CK	Resource Hijacking, Unused/Unsupported Cloud Regions

Cryptomining



* See credential exposure kill chain for details

Cryptomining



- See credential exposure kill chain and SSRF kill chain
- Least privilege

- Vulnerability assessment
- Network security

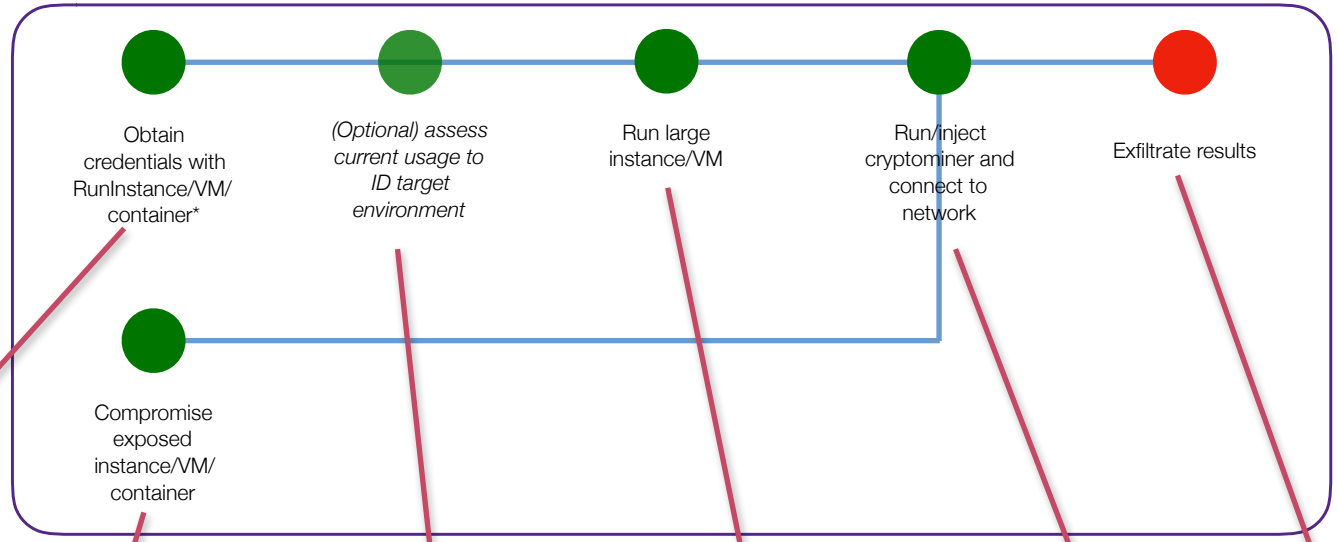
- Lock down unused regions
- API call (CloudTrail/ Activity Log) monitoring for excess Describe call usage

- Restrict AMIs/VMs to only pre-approved
- Least privilege
- Billing alerts

- GuardDuty/Azure Security Center
- Flow logs

- Flow log monitoring and alerting
- Outbound traffic restrictions

Cryptomining



- See credential exposure kill chain and SSRF kill chain
- Least privilege

- Vulnerability assessment
- Network security

- Azure Policy
- Activity logs alerted via SIEM correlation to identify increased usage
- Azure monitor configured for threshold cost controls

- Azure policy to restrict VM images
- Azure monitor configured for threshold cost controls

- Azure Security Center
- Flow logs
- Egress traffic monitored via Azure Firewalll

- Flow log monitoring and alerting
- Outbound traffic restrictions

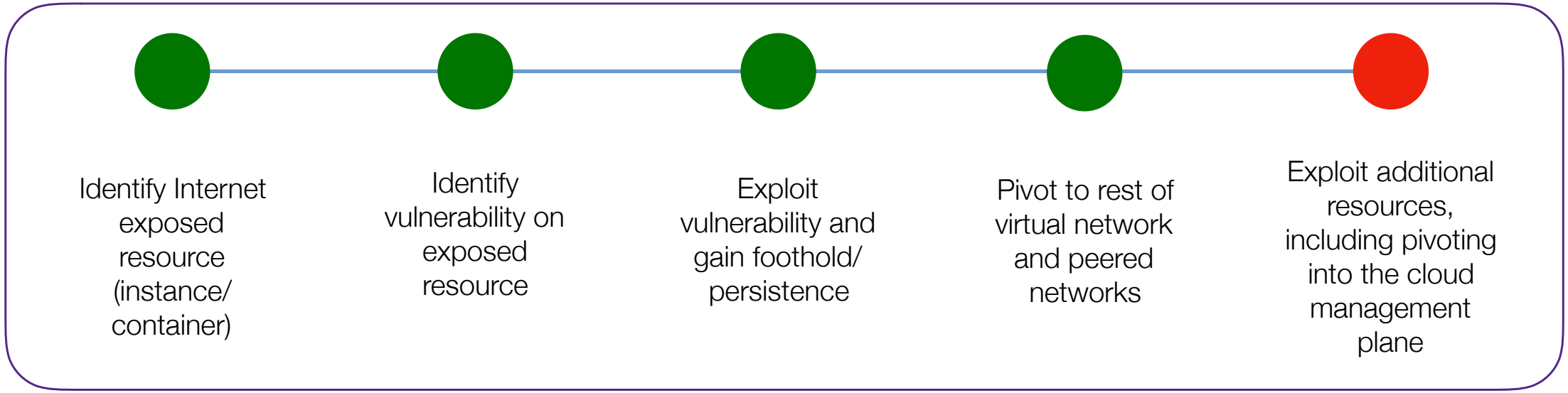
Azure

RSAConference2020

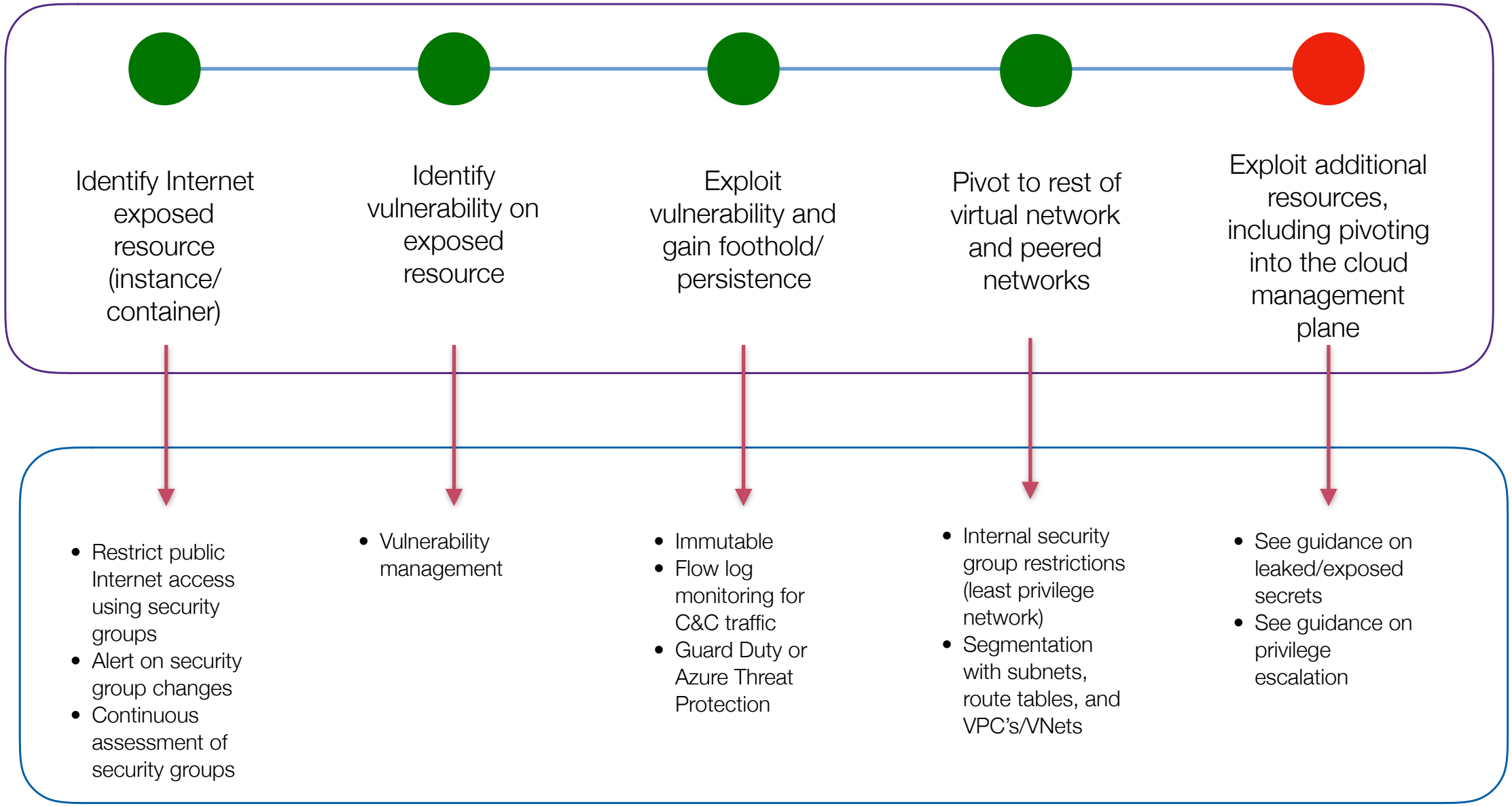
Network Attack

Category	Attack (Scripted or Targeted)
Severity	High
Liklihood	Medium
Primary CSA Top Threat	10. Security Issue: Limited Cloud Usage Visibility
Primary Mitre ATT&CK	Network Service Scanning, Remote System Discovery

Network Attack



Network Attack

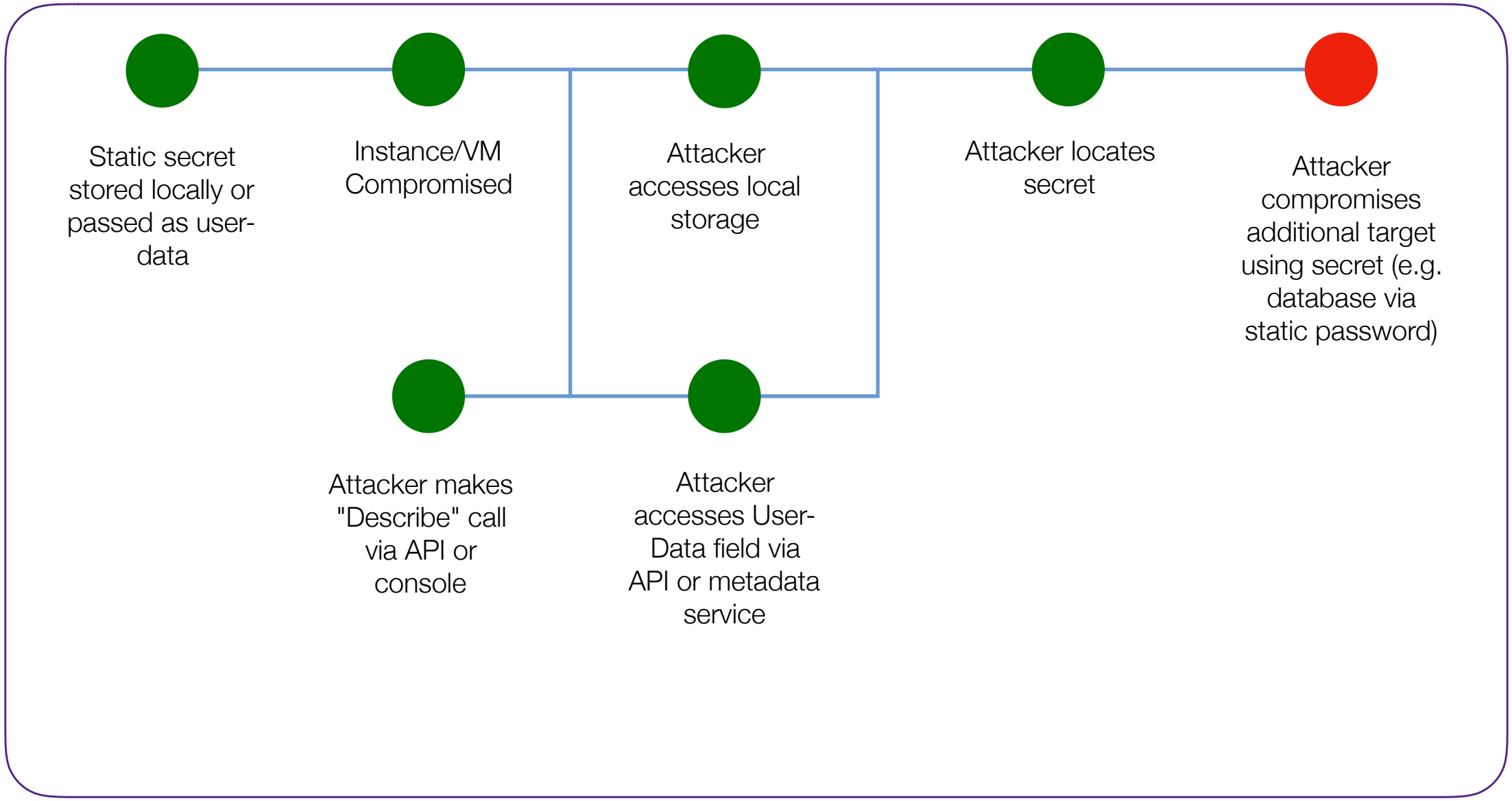


RSAConference2020

Compromised Secrets (Instance/VM)

Category	Attack (Scripted or Targeted)
Severity	High
Liklihood	High
Primary CSA Top Threat	4. Security Issue: Insufficient Identity, Credential, Access and Key Management 5.Security Issue: Account Hijacking
Primary Mitre ATT&CK	Valid Accounts, Credentials in Files

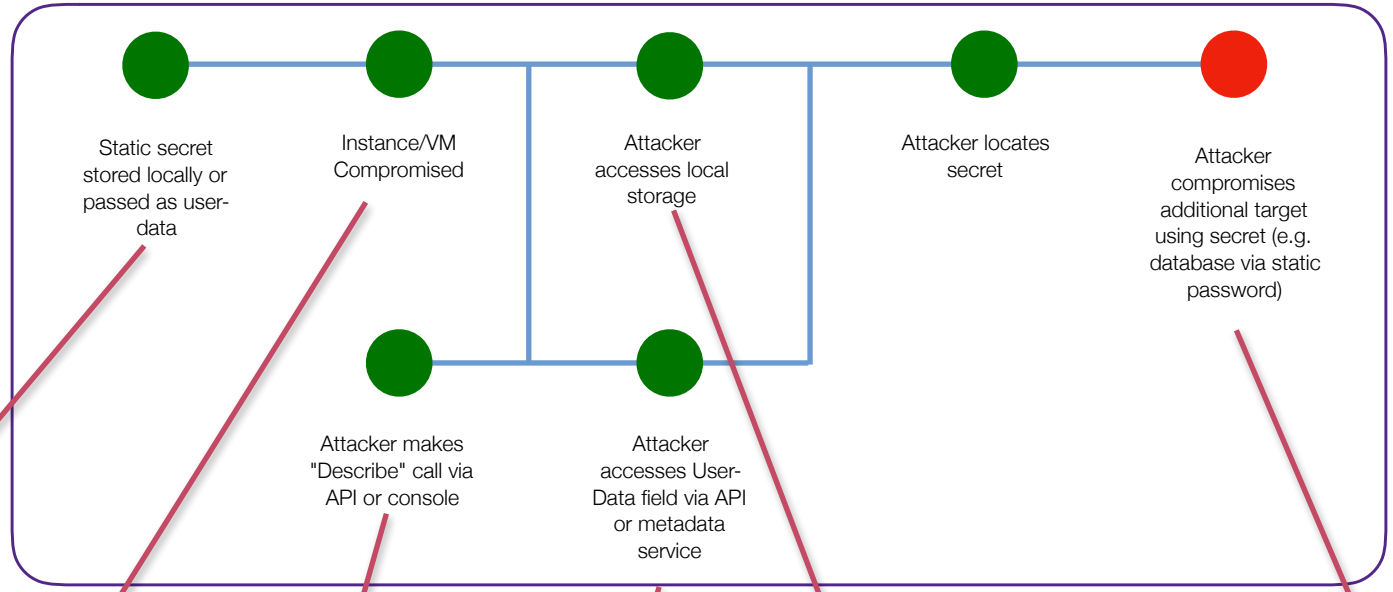
Compromised Secrets (Instance/VM)



aws

Azure

Compromised Secrets (Instance/VM)



- Never pass in a secret as user-data
- Use a secrets manager tool

- Vulnerability management

- Use resource restrictions on IAM/RBAC for read/describe access
- Limit read access to sensitive resources

- Use metadata defenses as listed in other killchains

- Limit secrets to specific process/ user access

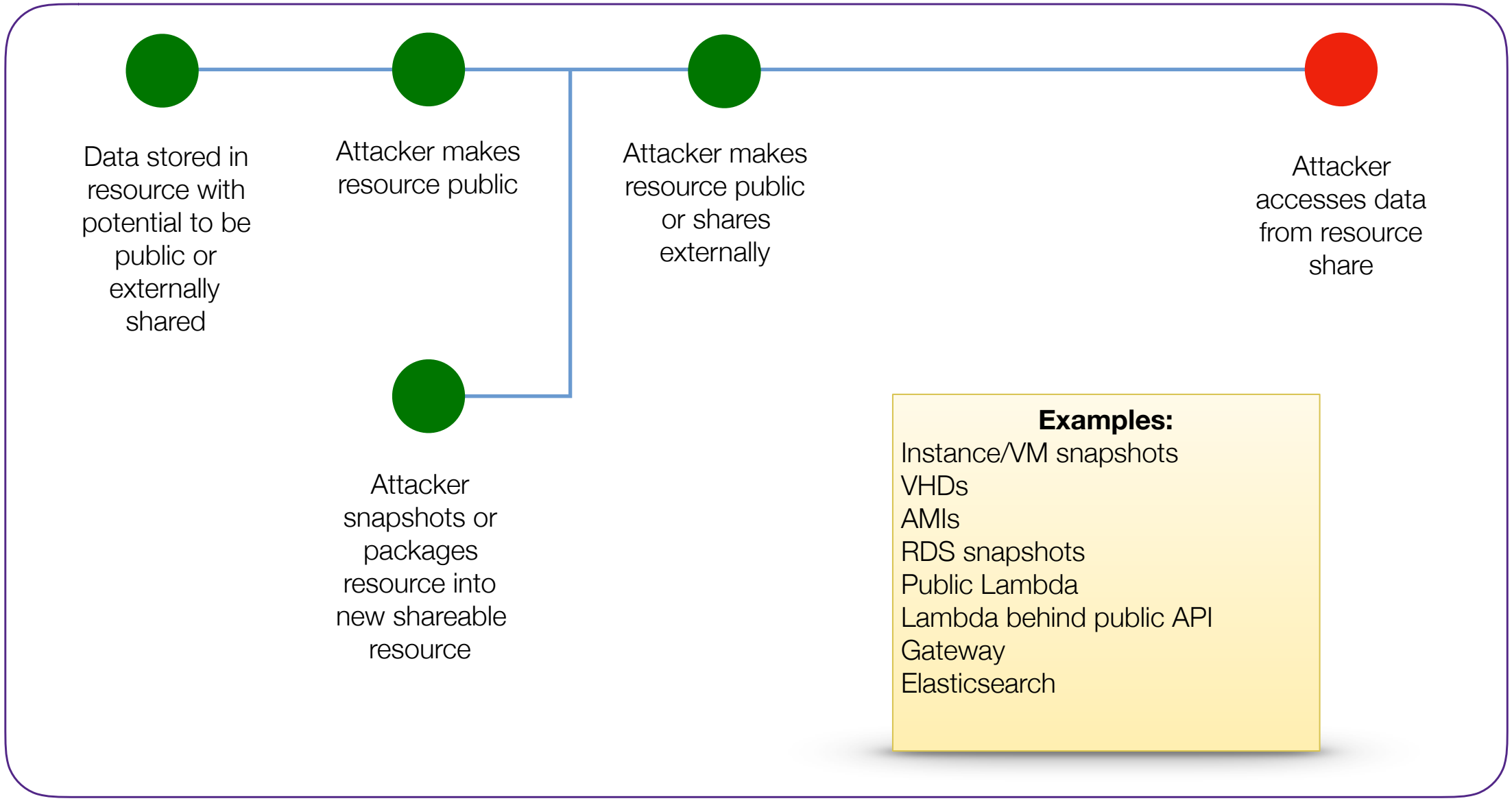
- Network/source restrictions may limit attack if attacker tries to use secret from external location

RSAConference2020

Novel Cloud Data Exposure and Exfiltration

Category	Misconfiguration
Severity	High
Liklihood	Medium
Primary CSA Top Threat	9. Metastreucture and Applistructure Failures
Primary Mitre ATT&CK	Account Manipulation, Transfer Data to Cloud Account

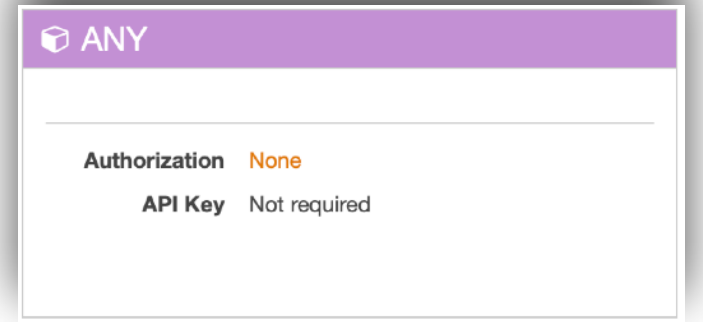
Novel Cloud Data Exposure and Exfiltration

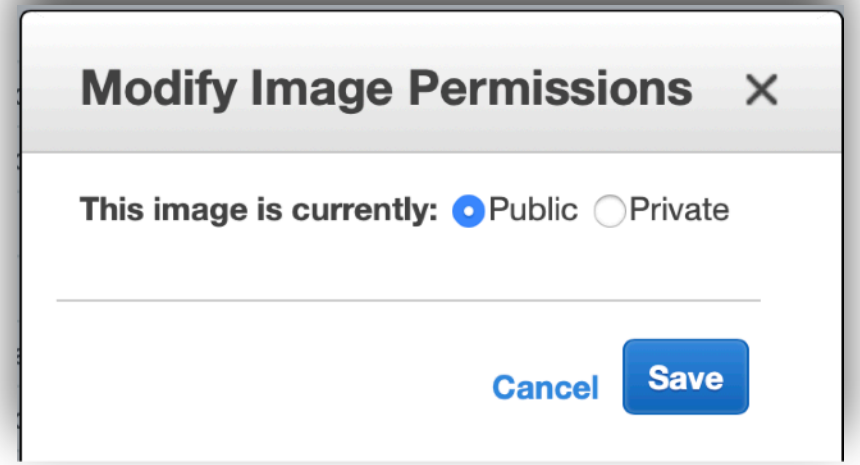


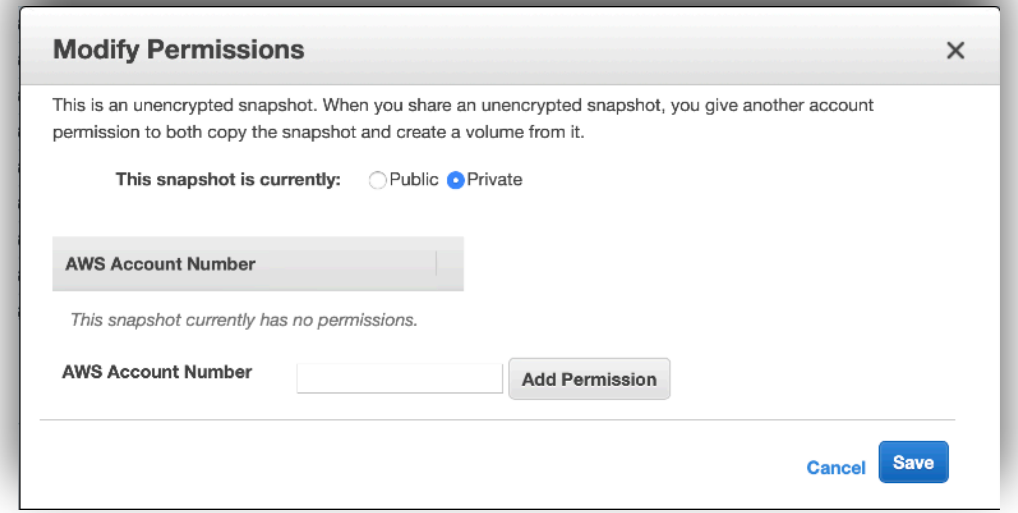
aws

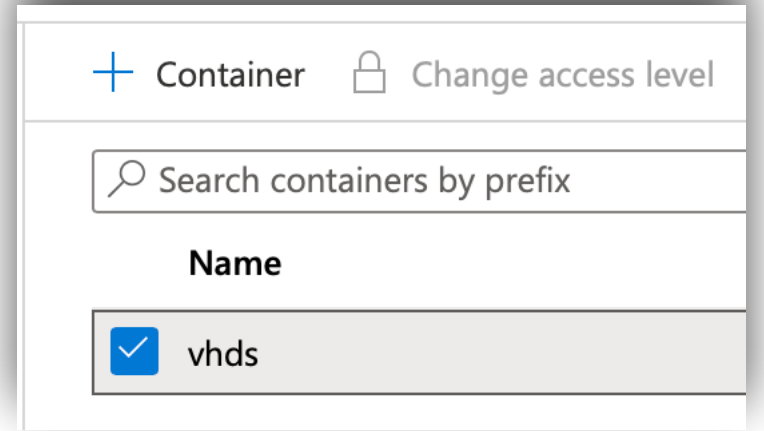
Azure

I see public EVERYWHERE!

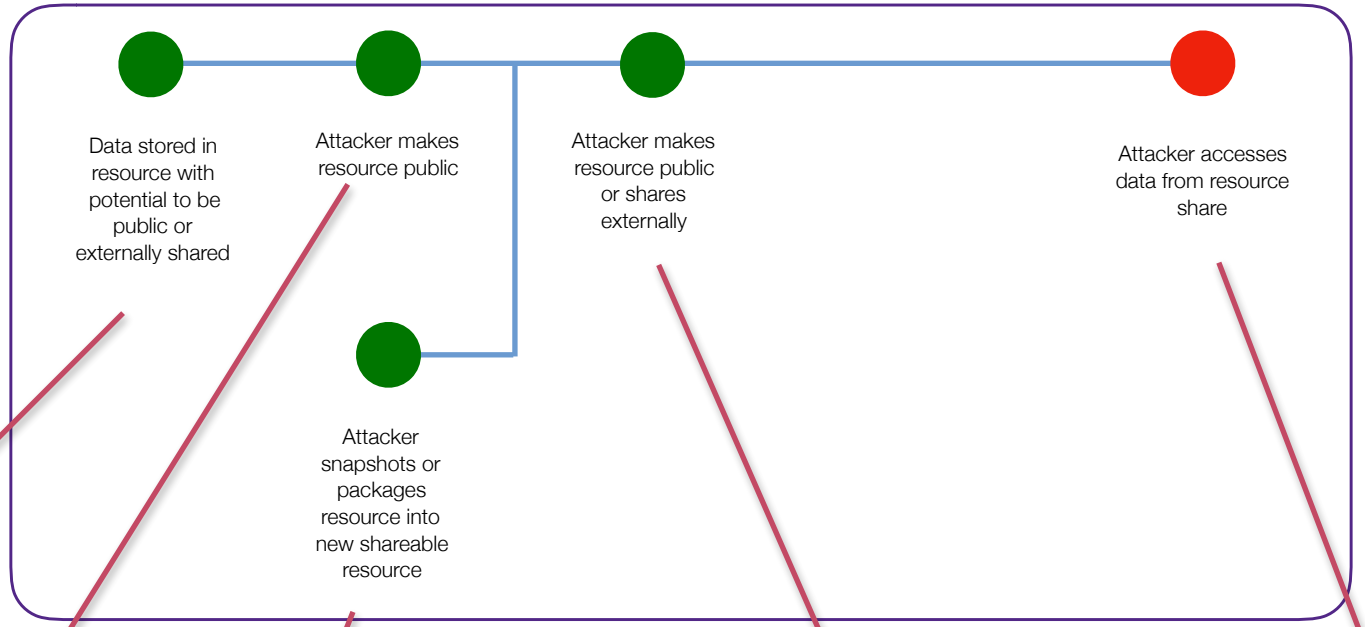








Novel Cloud Data Exposure and Exfiltration



- Data governance

- SCP's/Policies
- IAM restrictions
- Continuous assessment
- Reactive Guardrails

- SCP's/Policies
- IAM restrictions
- Continuous assessment
- Reactive Guardrails
- Encryption (KMS/ Key Vault)

- SCP's/Policies
- IAM restrictions
- Continuous assessment
- Reactive Guardrails
- Encryption (KMS/ Key Vault)

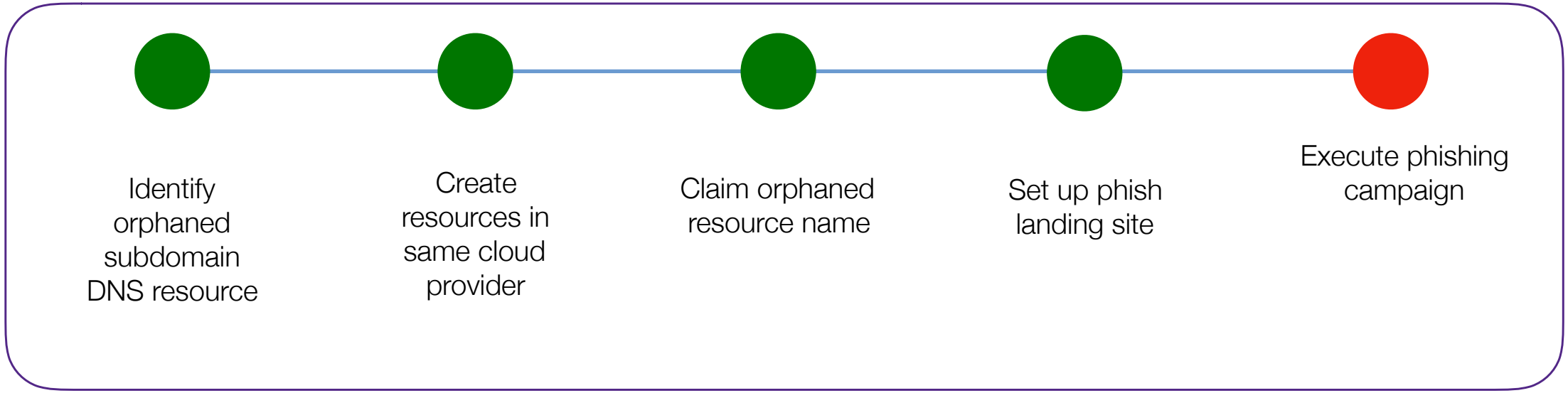
- Resource policies/Access controls
- Network origin restrictions

RSAConference2020

Subdomain Takeover

Category	Attack (Scripted or Targeted)
Severity	Medium
Liklihood	High
Primary CSA Top Threat	10. Limited Cloud Usage Visibility
Primary Mitre ATT&CK	Resource Hijacking

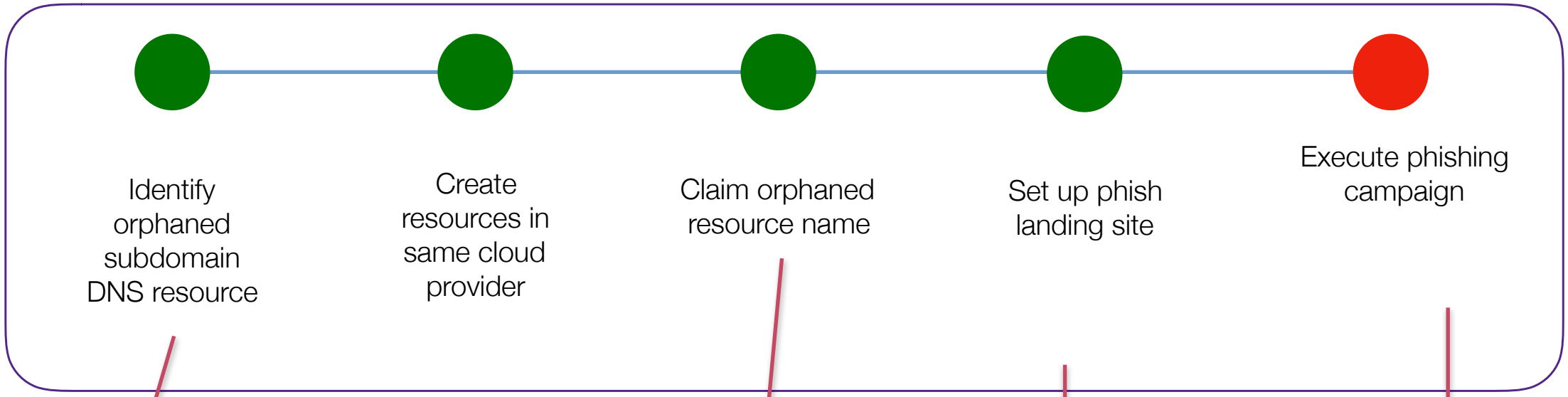
Subdomain Takeover



aws

Azure

Subdomain Takeover



aws

Azure

- Keep placeholder resources In place to avoid subdomain orphans
- Add a task to existing automation management jobs to ensure any service with custom domains have a delete resource lock.
- Create a serverless function that monitors provider events that would alert/take action on the deletion of a service with a custom domain name

- Reduce TTL in granted subdomain records
- Build automation to detect and takeover your own teams subdomains!

- Implement resource monitoring for cloud subscriptions to understand if/when new resources are being deployed

- Implement anomalous traffic detection to identify unauthorized resource usage

Non-Killchain Related Issues

- Privilege escalation
  - e.g. RunInstance + PassRole without resource restriction
- Pre-signed URLs
  - Any API call in AWS can be a pre-signed URL, not just S3
- 3rd Party Cross Account Access
  - Can be abused; especially if External ID's are not randomized
- Azure "public by default" VNets and services
  - All VM resources have *outbound* Internet access by default (NAT)
  - Some services require public inbound and *do not respect defined Network Security Group rules*

Contributing Factors

- Excessive permissions
- Scale
- Use of “traditional” architectures (e.g. network sprawl)
- Segregation
- Ineffective monitoring and inadequate logging

Apply

- Prioritize the killchains based on your:
  - Cloud providers
  - Deployment architectures
  - Sensitivity/risk profile of environments
- Identify overlapping controls that break each killchain
  - Hints- least privilege IAM, continuous monitoring and enforcement
- Implement defenses in prioritized layers
  - Place at least one control in place for each killchain
  - Then layer in additional controls

RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: CSV-T08

Break the Top 10 Cloud Attack Killchains

Rich Mogull

Analyst/Securosis

CISO/DisruptOps

@rmogull

Shawn Harris

Managing Principal Security Architect

Starbucks

@infotechwarrior