IAM Confused

Analyzing 8 Identity Breach Incidents

Maya Levine
Product Manager-Sysdig

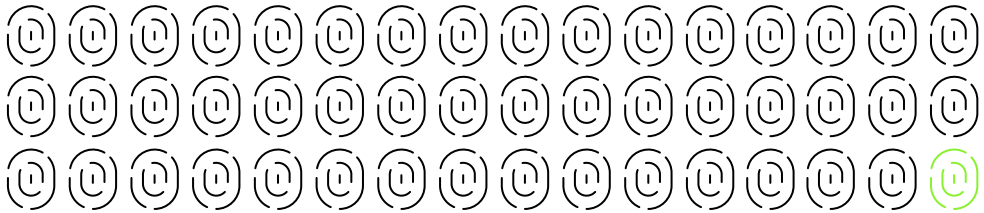


Identity management is the most overlooked cloud attack risk

Only 20% of CNAPP users are prioritizing CIEM.

Excessive permissions

98% Unused permissions



2% Granted permissions used



Ownership of identity posture b/w Dev, Ops, & Sec is often unclear


(Human/machine identity management)

Humans make mistakes

Social engineering accounts for 98% of all cyber-attacks



82% of breaches caused by human error

verizon

MFA Abuse through social engineering works

The Average Cloud Attack Takes **10 Minutes**



5 Seconds
Detect

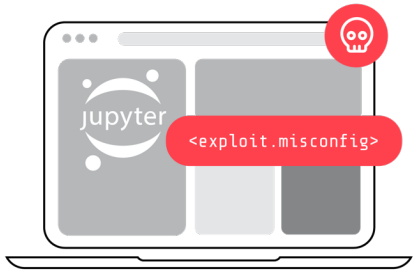
5 Minutes
Correlate

5 Minutes
Initiate response

Attack 1

Humans make mistakes – many easy things to miss in cloud

Initial Compromise | Execution/ Gather Information | Privilege Escalation/ Persistence



Exploit public facing web application

```
{
      “Sid”: “VisualEditor2”,
      “Effect”: “Deny”,
      “Action”: [
         “iam:CreateAccessKey”
      ],
      “Resource”: [
         “arn:aws:iam::078657857355:role/*”,
         “arn:aws:iam::078657857355:user/*admin*”
      ]
 }
```

Attack 1

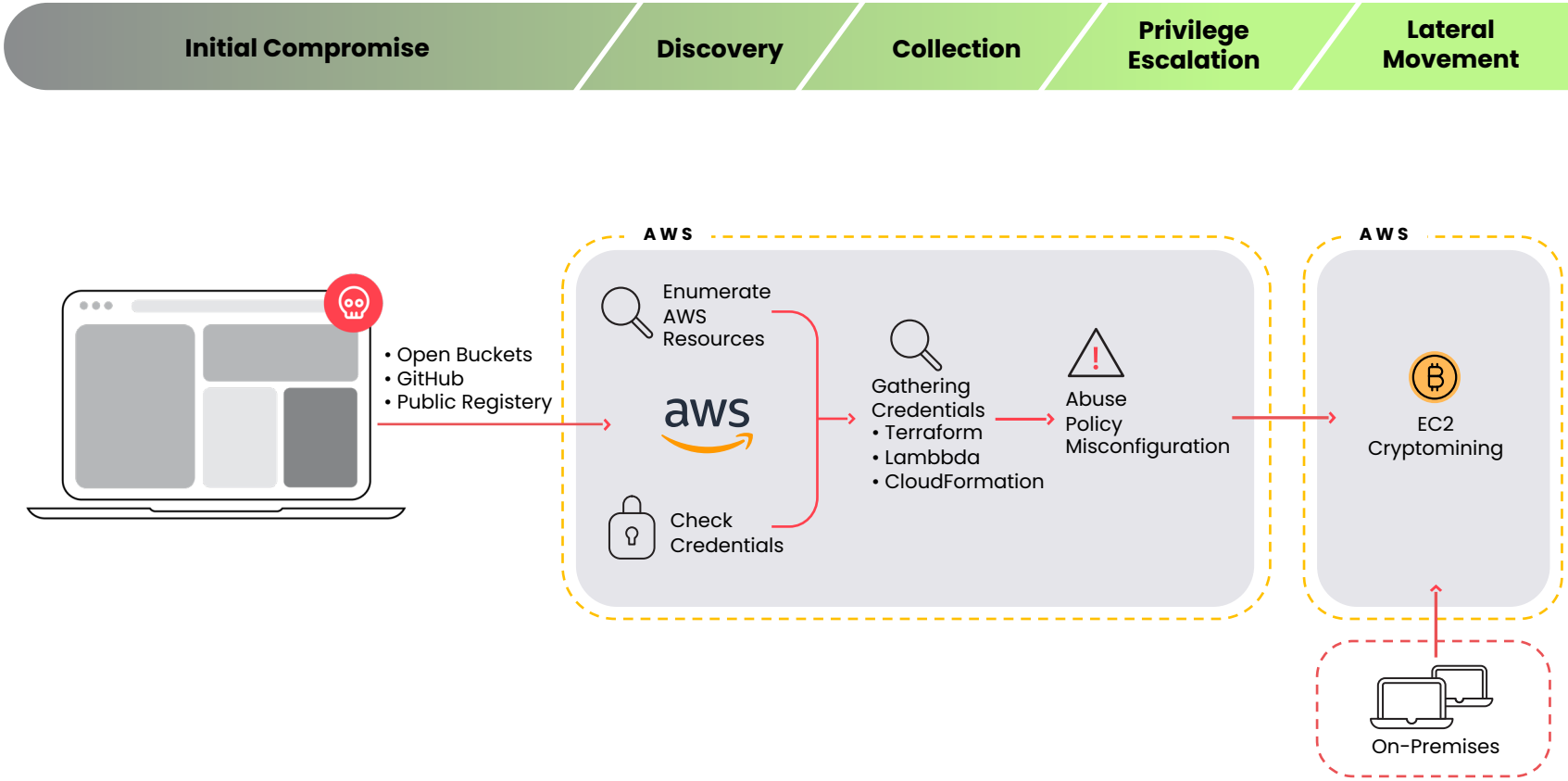


Least Permissive is not just buzz words

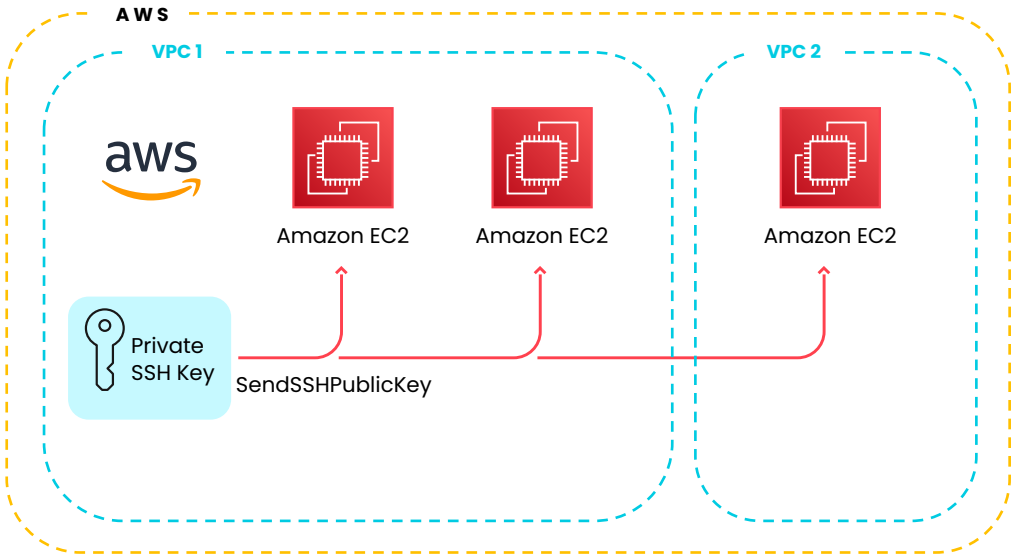
Watch out for **case sensitive mistakes**

Attack 2

Patterns of attacker playbooks are being seen by Threat Research


Initial Compromise
Discovery
Collection
Privilege Escalation
Lateral Movement
• Open Buckets
• GitHub
• Public Registery
AWS
Enumerate AWS Resources
aws
Check Credentials
Gathering Credentials
• Terraform
• Lambbda
• CloudFormation
Abuse Policy Misconfiguration
AWS
EC2 Cryptomining
On-Premises

Lateral Movement



Attack 2



Don’t assume **On Premise vs Cloud is Isolated**

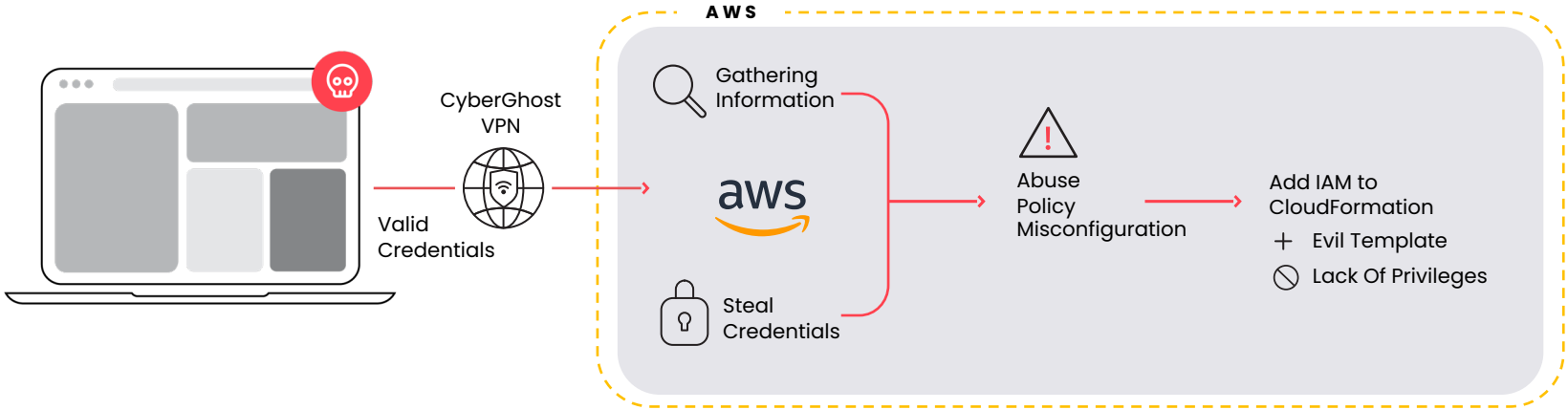
Employ **Secrets Management Systems**

CSPM Solution

Attack 3

The danger of overly permissive for IAC services

Initial Access | Discovery | Lateral Movement | Privilege Escalation



Attack 3



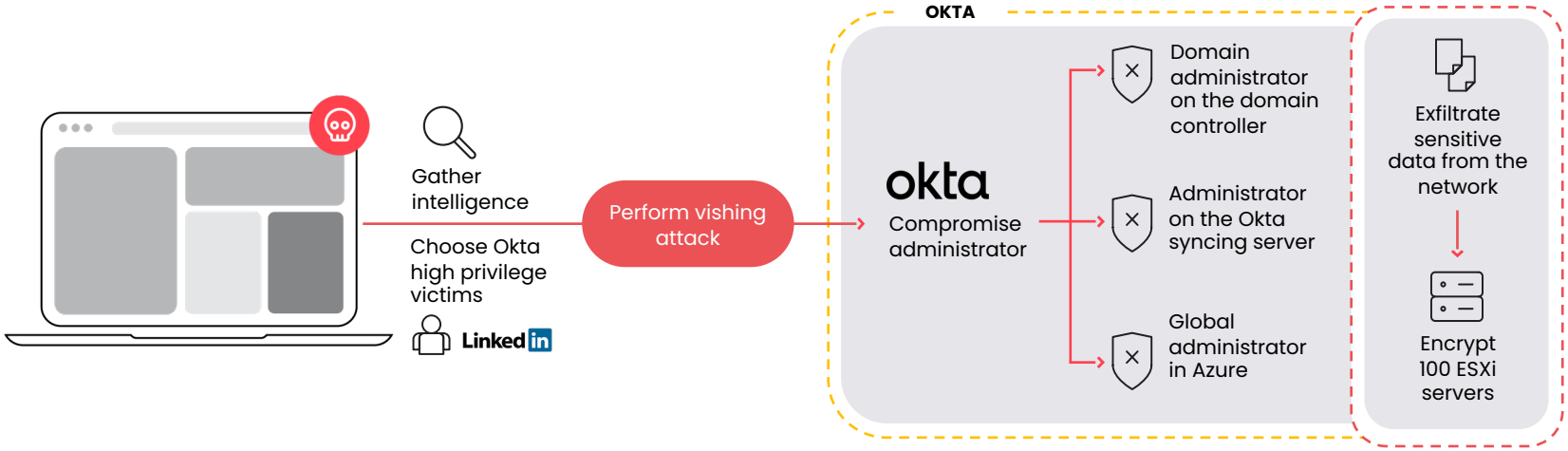
Visibility - Inventory

Real time Threat Detection across runtime workloads and cloud

Attack 4

Social Engineering at it's finest

Reconnaissance | Establish Foothold | Persistence | Impact



Attack 4



Synchronizing credentials between on-premise and cloud resources opens attack vectors

IdP administrator accounts should be managed with scrutiny

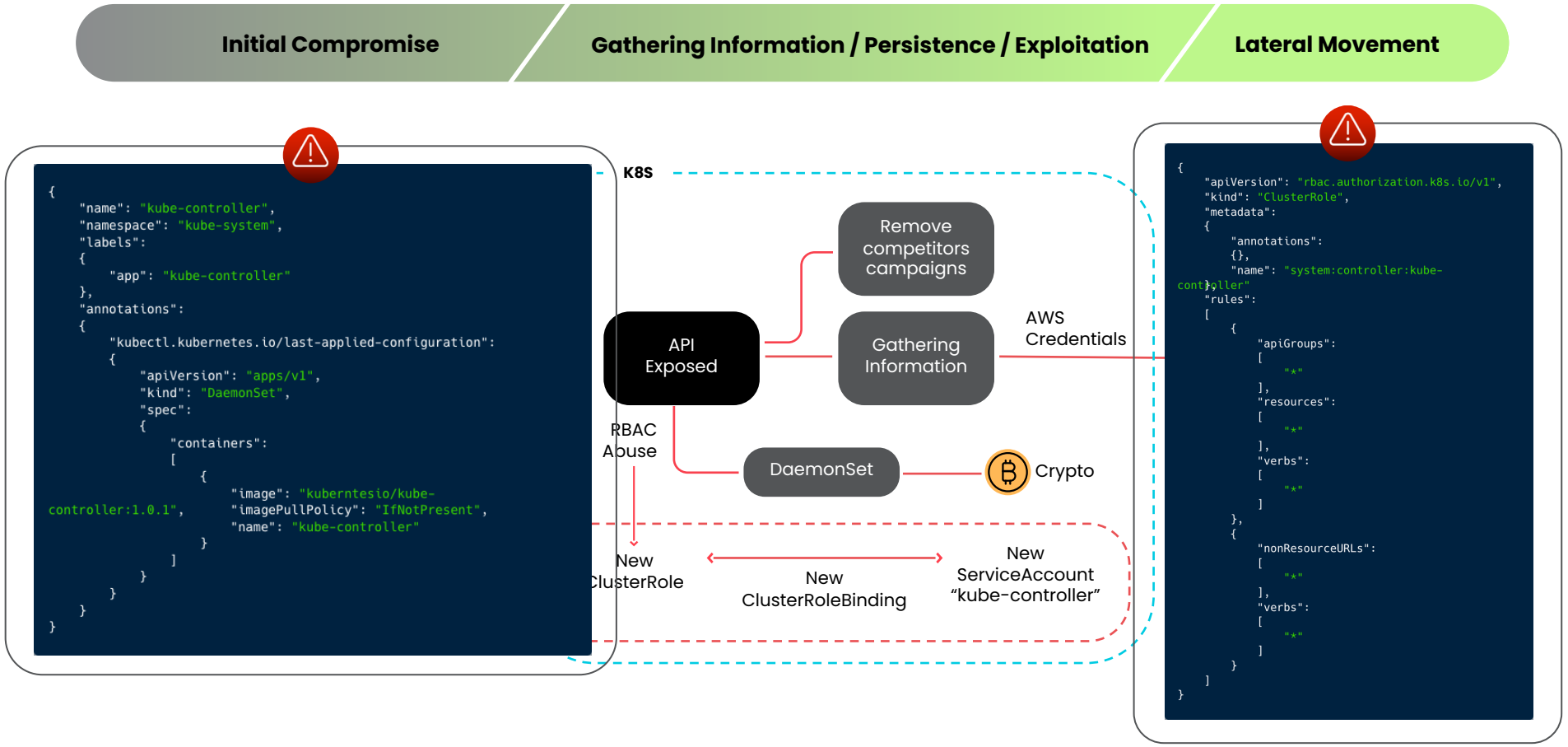
RaaS is a big business

MFA Device Reset - Limit to specific phone number

Require **multiple authorizations** for critical actions

Attack 5

Establishing Persistence while blending in


Initial Compromise
Gathering Information / Persistence / Exploitation
Lateral Movement
{
"name": "kube-controller",
"namespace": "kube-system",
"labels":
{
"app": "kube-controller"
},
"annotations":
{
"kubectl.kubernetes.io/last-applied-configuration":
{
"apiVersion": "apps/v1",
"kind": "DaemonSet",
"spec":
{
"containers":
[
{
"image": "kubernetesio/kube-controller:1.0.1",
"imagePullPolicy": "IfNotPresent",
"name": "kube-controller"
}
]
}
}
}
}
K8S
API Exposed
Remove competitors campaigns
Gathering Information
AWS Credentials
RBAC Abuse
DaemonSet
Crypto
New ClusterRole
New ClusterRoleBinding
New ServiceAccount "kube-controller"
{
"apiVersion": "rbac.authorization.k8s.io/v1",
"kind": "ClusterRole",
"metadata":
{
"annotations":
{},
"name": "system:controller:kube-controller"
},
"rules":
[
{
"apiGroups":
[
"*"
],
"resources":
[
"*"
],
"verbs":
[
"*"
]
},
{
"nonResourceURLs":
[
"*"
],
"verbs":
[
"*"
]
}
]
}

Attack 5



Overly Permissive

Kubernetes Audit

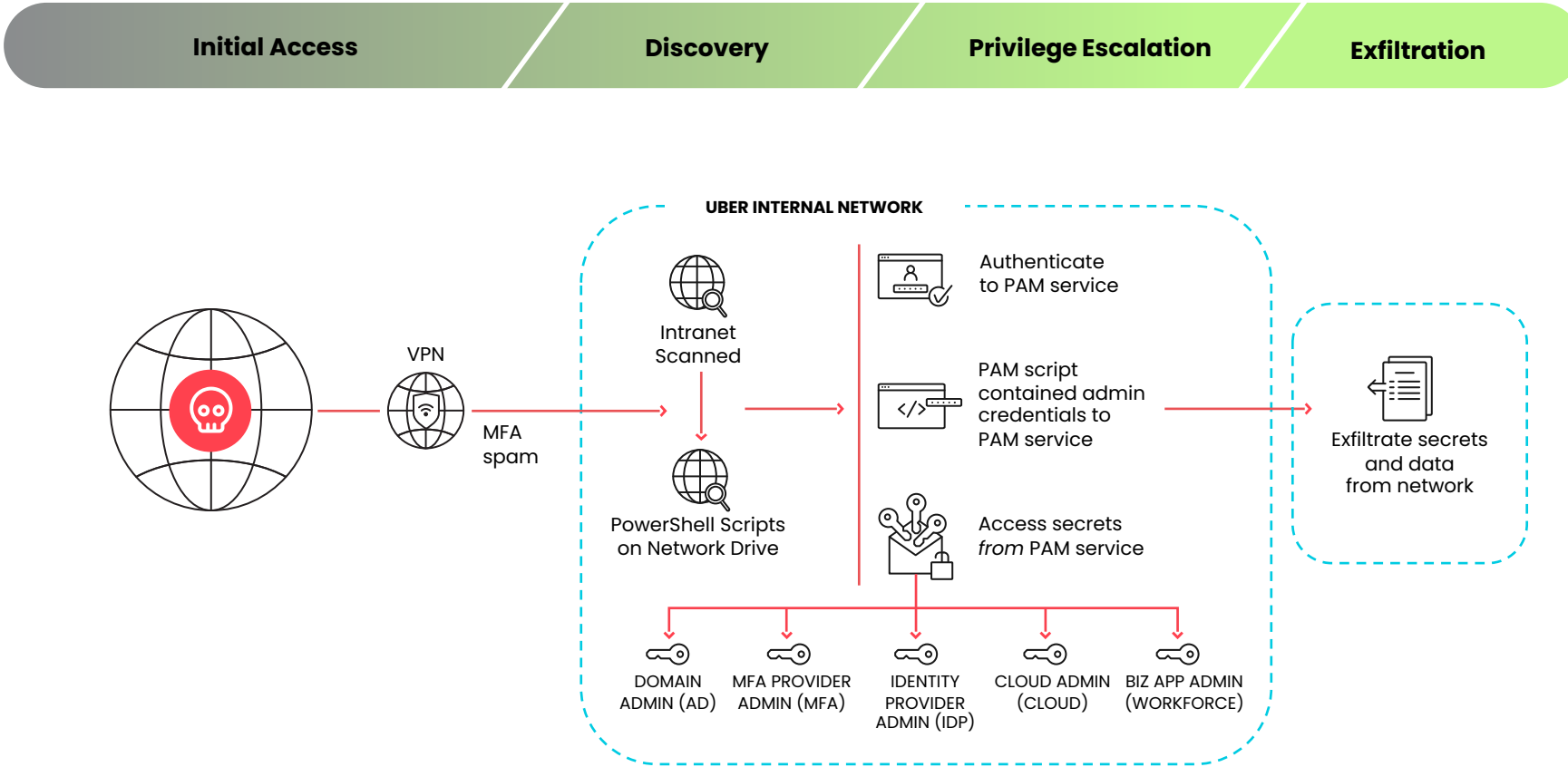
- New cluster role creation
- Cluster role binding

Runtime Analysis with Machine Learning

- CPU, Memory, Network activity
- Can still detect without cryptomining name from known mining pool,

Attack 6

Hard coded credentials can be a gold mine for attackers


Initial Access
Discovery
Privilege Escalation
Exfiltration
UBER INTERNAL NETWORK
VPN
MFA spam
Intranet Scanned
PowerShell Scripts on Network Drive
Authenticate to PAM service
PAM script contained admin credentials to PAM service
Access secrets *from* PAM service
Exfiltrate secrets and data from network
DOMAIN ADMIN (AD)
MFA PROVIDER ADMIN (MFA)
IDENTITY PROVIDER ADMIN (IDP)
CLOUD ADMIN (CLOUD)
BIZ APP ADMIN (WORKFORCE)

Attack 6



MFA is required, **but it might not be enough**

Hard Coded and Embedded Credentials Pose Huge Risk

Hire Bounty Hunters to Help

Employee Education

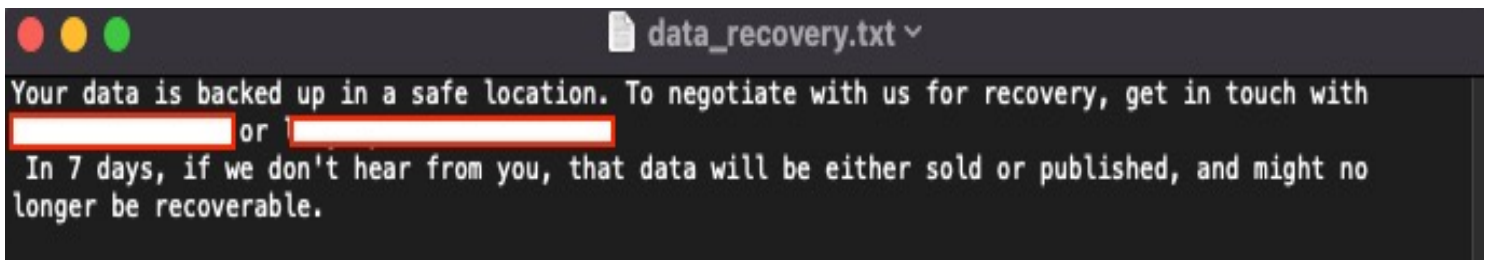
Identity Hygiene – Rotate your access keys!

Attack 7

What makes Storage Resources more vulnerable to ransomware attacks and data exfiltration?

Initial Compromise | Reconnaissance | Persistence | Exfiltration | Impact

AWS



Files deleted
Ransom note uploaded in S3 bucket

username: ses-smtp-user.<date-time>

exfiltrated

Attack 7



Utilize Cloudtail

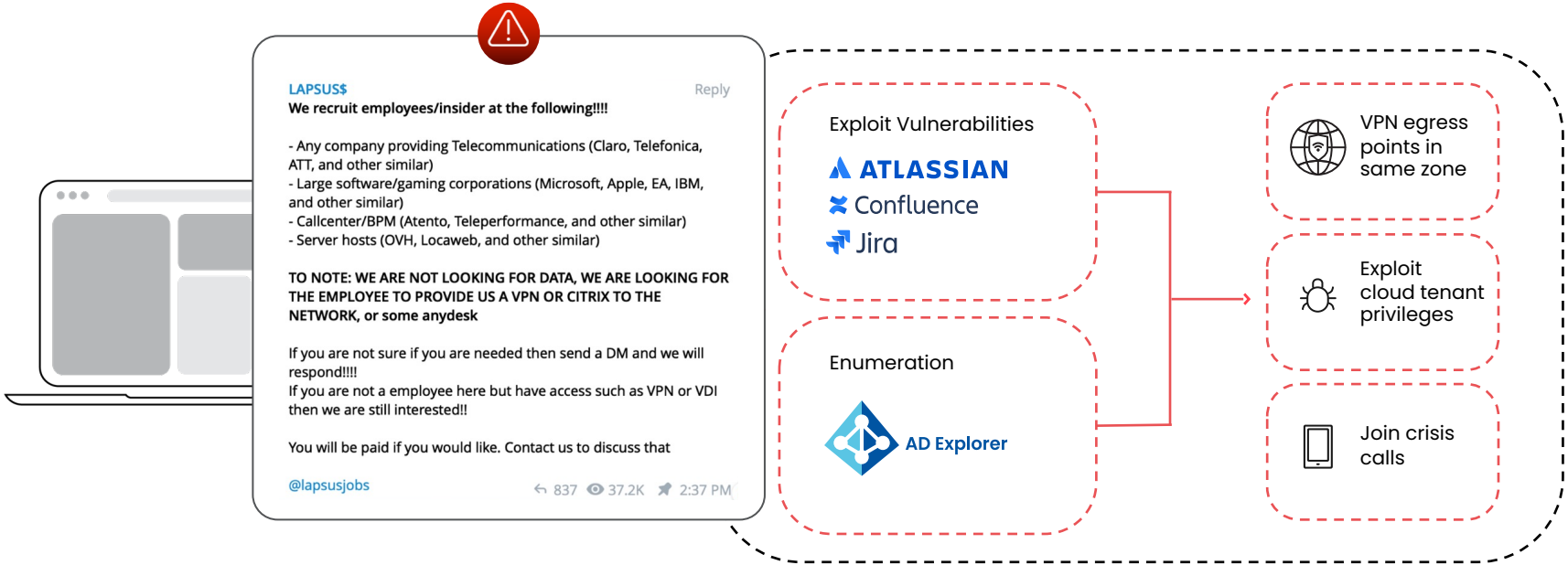
Consider IAM over Long Term Access Keys

Enable MFA for bucket versioning and delete

Attack 8

Attackers are creative

Initial Compromise | **Reconnaissance/Privilege Escalation** | **Exfiltration, Extortion**



Attack 8



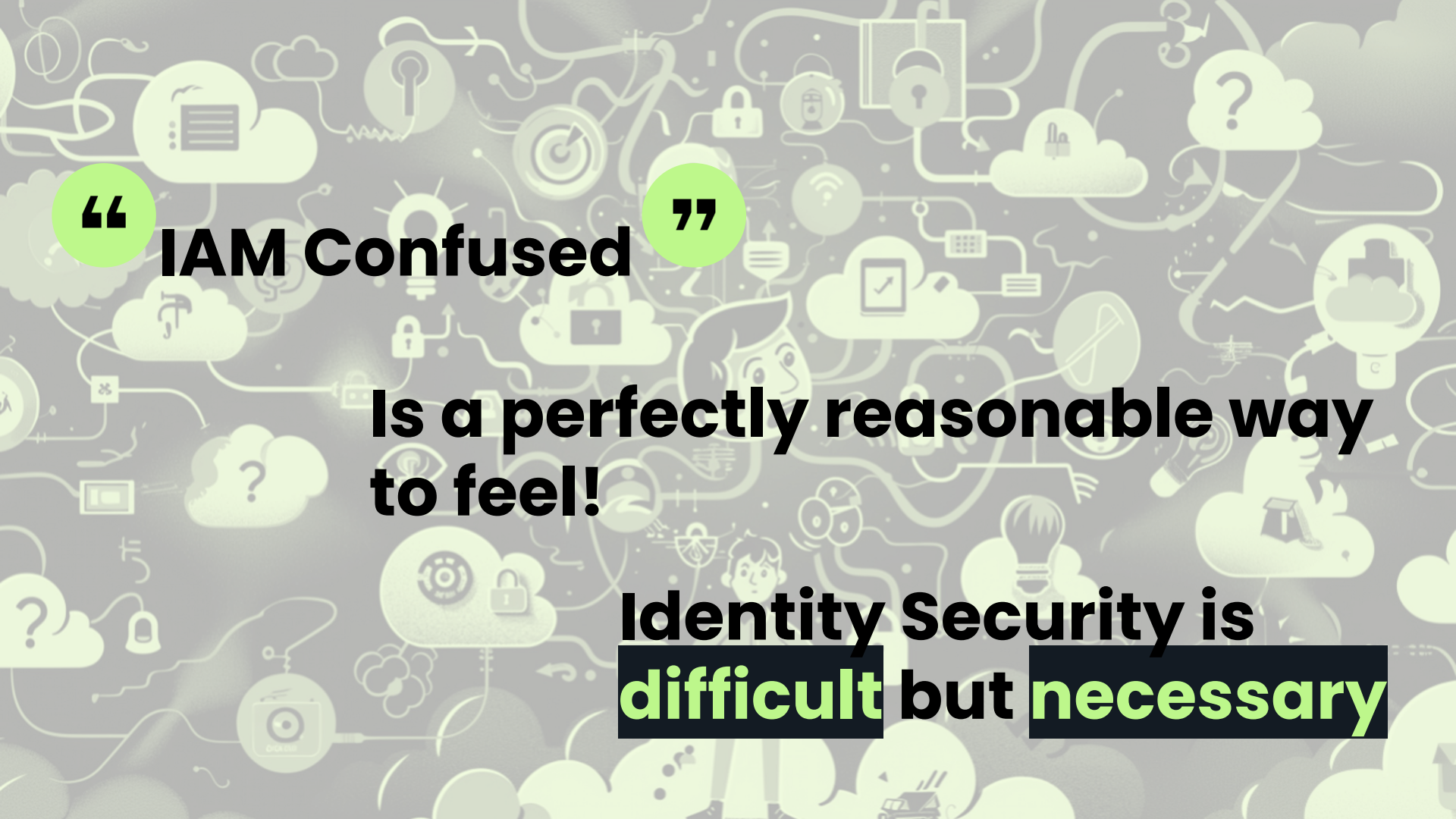
Require **Trusted Endpoints**

Leverage Modern
Authentication for VPNs

Establish Operational
Security **Processes**

In Summary

- Credential hunting- pay bounties on discovery of credentials
- Education, training, secrets management
- Correlate threat detection signals on SaaS & IAM logs
- Shorten session length for admin accounts in big SaaS apps
- Improve MFA
- Network Segmentation


“IAM Confused”
Is a perfectly reasonable way to feel!
Identity Security is difficult but necessary


sysdig
SECURE
EVERY
SECOND