



Cloud Breaches: Case Studies, Best Practices, and Pitfalls

SANS Cloud Security Summit 2020

Christopher Romano
Senior Consultant, Mandiant

Dylan Marcoux
Consultant, Mandiant

Agenda

- Introductions
- Cloud Threat Landscape Overview
- Frequent Attacker Methodologies
- Common Weaknesses & Root Causes
- Best Practices
- Case Studies



Christopher Romano



Senior Consultant at Mandiant

Over 14+ years of security experience

Based in USA

Interested in "Everything Cloud", DFIR, pentesting, Architecting things securely

Christopher.Romano@Mandiant.com

Dylan Marcoux



Consultant at Mandiant

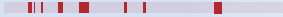
7+ years of security experience

Based in central Canada

Interested in malware analysis, DFIR, architecture/ops, pentesting, web apps, “the cloud”

Okay at Brazilian Jiu-Jitsu

Dylan.Marcoux@Mandiant.com



Case studies and examples are drawn from our experiences and activities working for a variety of customers, and do not represent our work for any one customer or set of customers. In many cases, facts have been changed to obscure the identity of our customers and individuals associated with our customers.

Current Threat Landscape

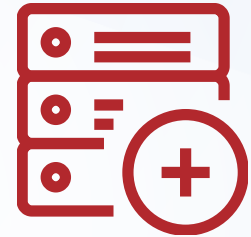
Rapid growth in
cloud adoption



Lack of awareness
of specific security
features



Misconfiguration of
tenant settings



Cloud Cybersecurity Statistics

24%

Of Organizations Have Hosts
Missing Critical Patches

95%

Of Cloud Security Failure Is The
Customer's Responsibility

84%

Of Organizations Say Traditional
Security Tech Doesn't Work In
Cloud

11%

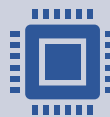
Of Mandiant IRs Have A Significant
Cloud Component



M-Trends 2020 Key Cloud Highlights^[1]



Lack of cloud adoption for threat detection and response



Attackers utilizing hybrid environments



Credential management is paramount



Lack of granularity for policies and permissions

Frequent Attacker Methodologies



Rogue Devices and Shadow IT



UNAUTHORIZED
MACHINES



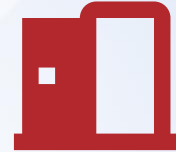
APPS LACKING
SECURITY



INTERNET FACING
REMOTE
MANAGEMENT

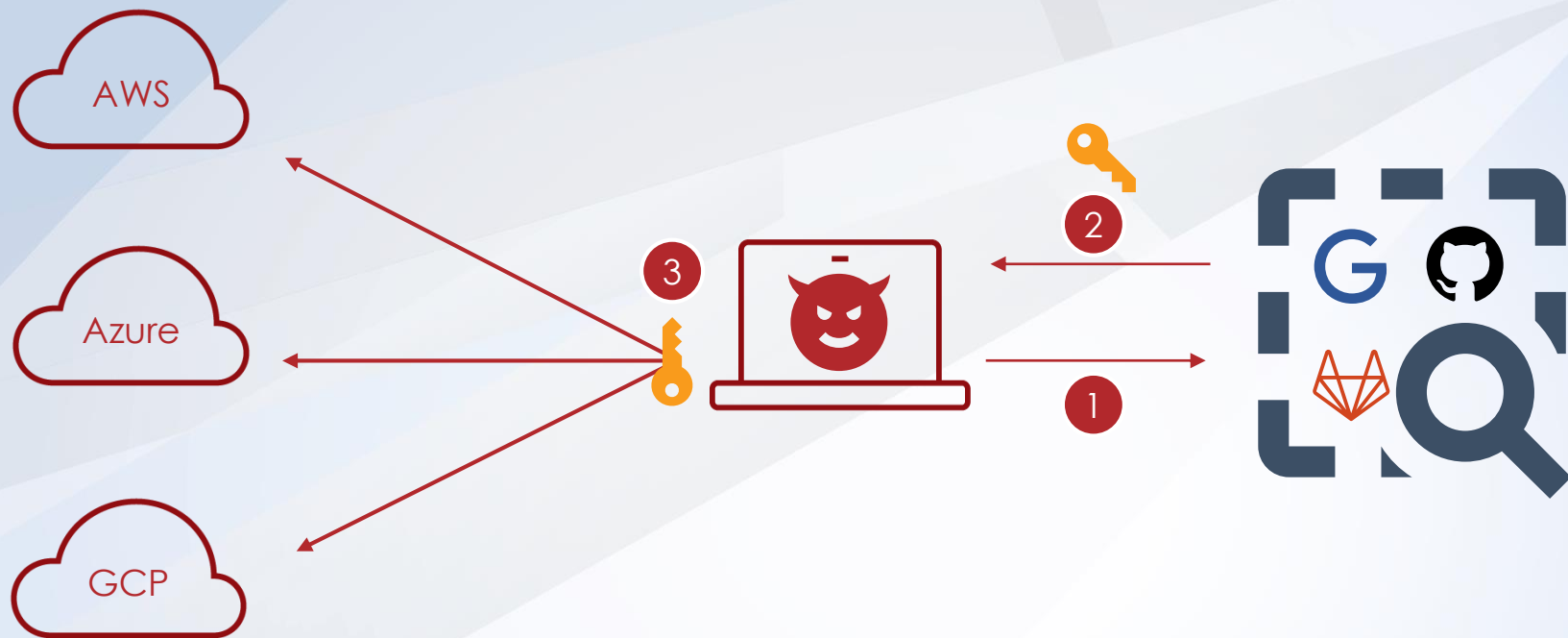


UNPATCHED
APPLICATIONS

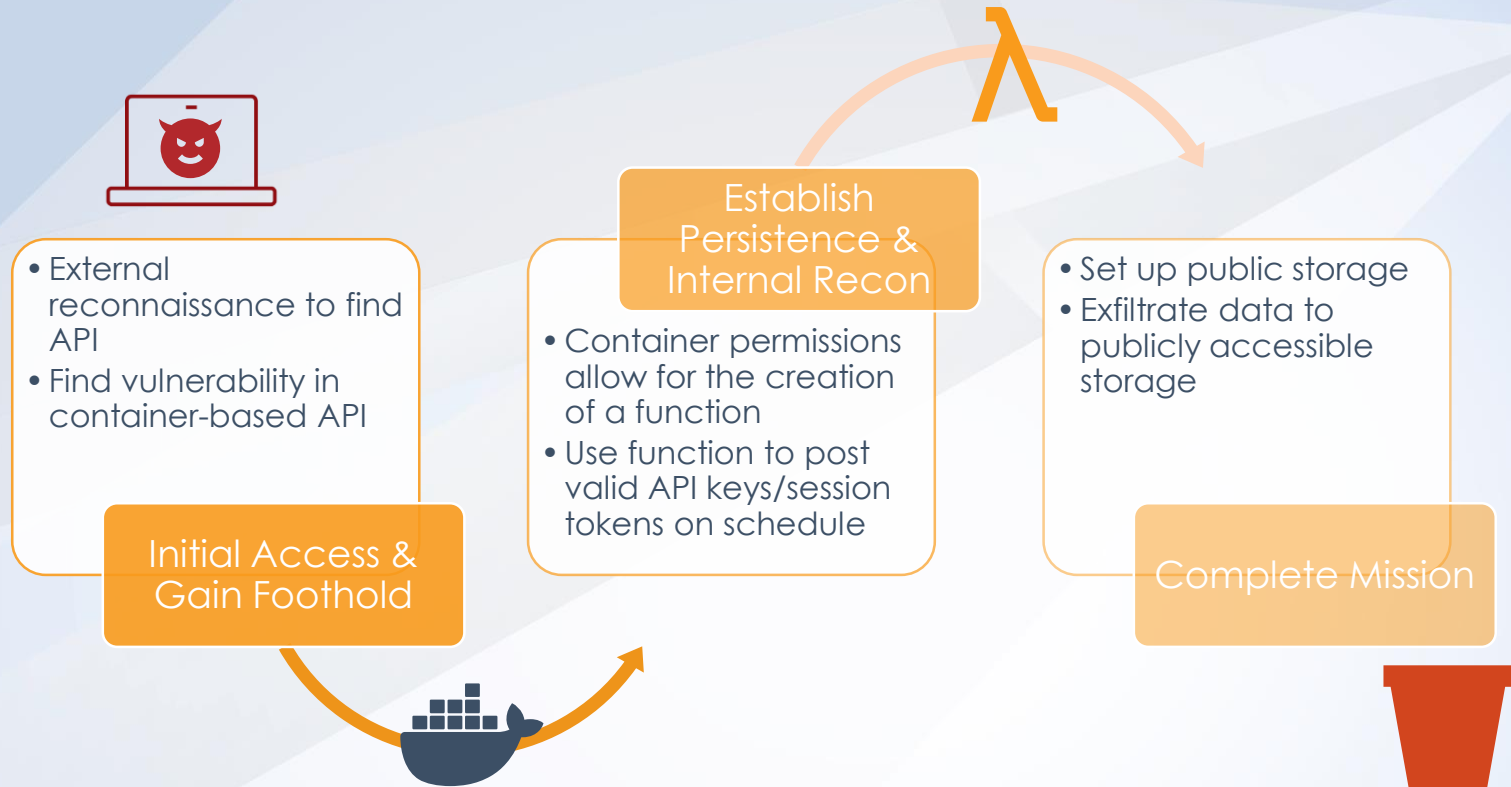


IT ADMIN
BACKDOOR

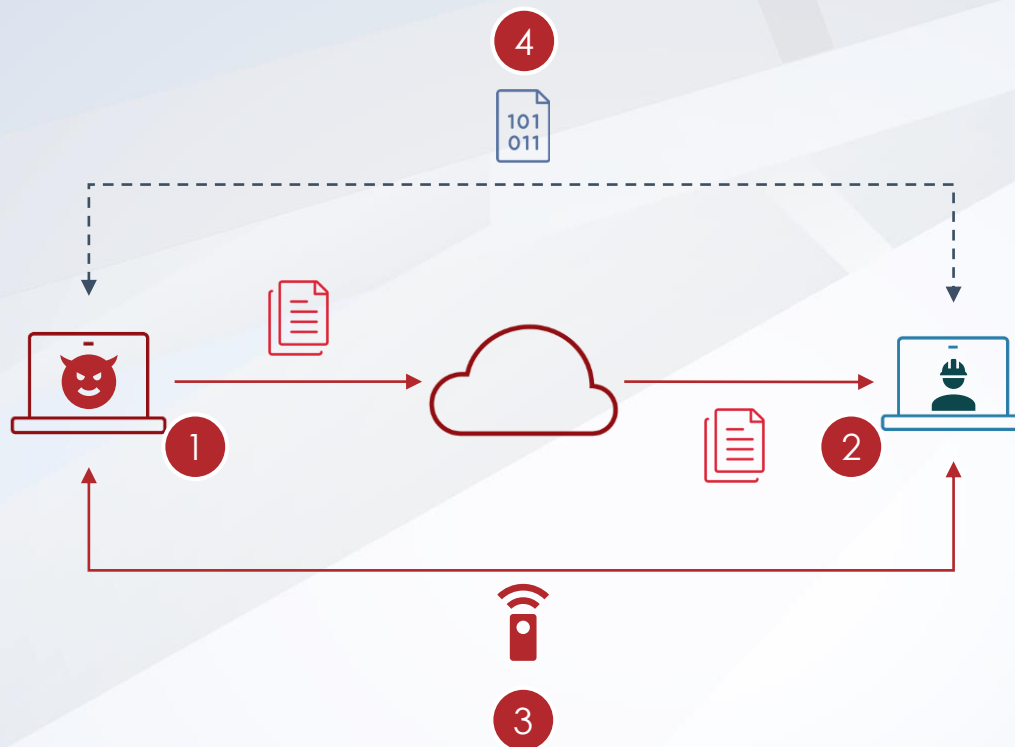
Credential Compromise via Public Exposure



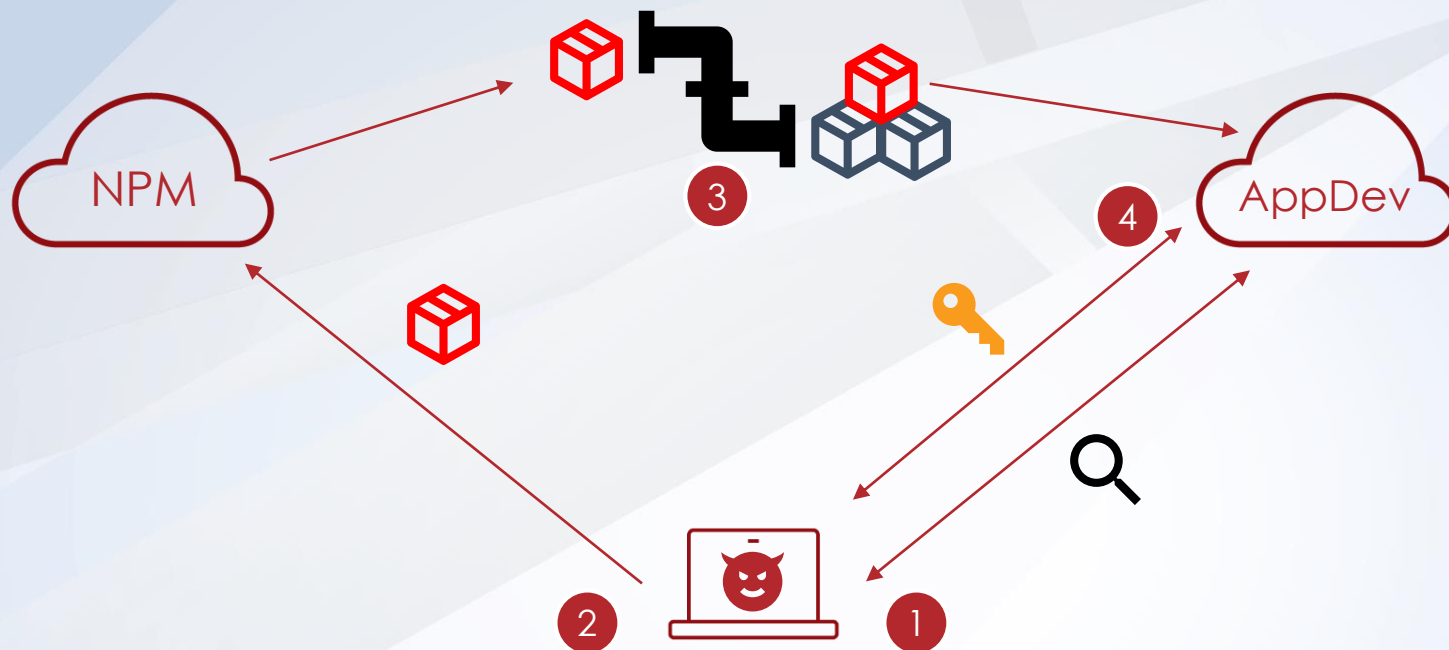
Cloud Platform Service Attacking



Hybrid-Cloud Lateral Movement via Cloud App



Third-Party Library Supply Chain Attack

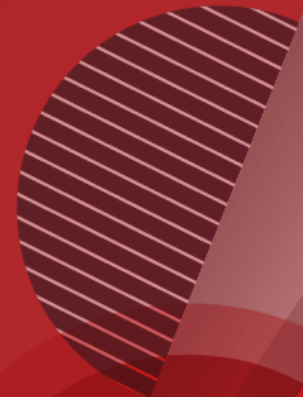


And Many More...

- Datastores without access control
 - E.g., Open AWS S3 Buckets
- Credential compromise
 - E.g., Through an infected endpoint or phishing
- Third-party application
 - E.g., Phishing that asks for malicious OAuth application approval, malicious application download from Apple's AppStore or Google's Play Store



Root Causes and Common Observations



Common Root Causes



Insufficient protection of
critical assets



Insufficient incident
detection and response

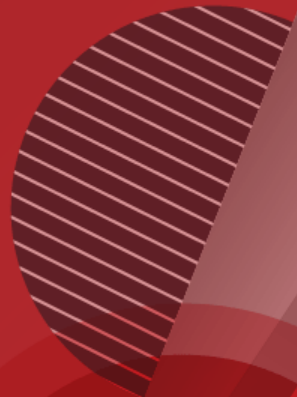


Poor identity and access
management / privilege
management



Lack of understanding about
the environment

Top O365 and Azure Observations



Identity and Access Management



Legacy authentication protocols enabled



Not using MFA



Too many privileged accounts

Hardening of Administration



Remote PowerShell typically enabled for all users



Privileged access workstations rarely used



Misuse of administrative credentials

Service Hardening and Logging



Minimal control of access to services



Poor hygiene of cloud networking configuration



No integration into current security detection and response



Lack of log monitoring and threat hunting

Top AWS Observations



Identity & Access Management



AWS Managed Policies are known to be overly permissive



Not using MFA for both Console or Command-line Interface



IAM policies are given wild card access on AWS resources



Permission Boundaries and Service Control Policies not being used



Lack of rotating IAM Access Keys



Long-lived credentials being used

Hardening of Administration



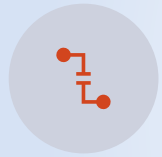
Hardened jump hosts or
PAWs not utilized to
access AWS
environments



Shared SSH keys across
EC2 instances



Misconfigured IAM
policy that permits
privilege escalation

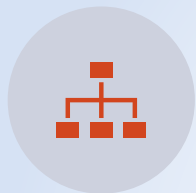


Abuse of AWS services
and attached roles
(e.g., CloudFormation,
Lambda, SSM)

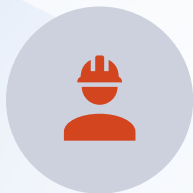


Misuse of administrative
credentials

Service Hardening and Logging



No control over services or regions



Permit users to pass any role to any given service (e.g., EC2, Lambda)



No integration into current security detection and response



Lack of knowledge on advanced logging features



Lack of log monitoring and threat hunting

Top GCP Observations



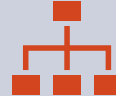
Identity & Access Management



Service accounts being used for daily tasks



Overly-permissive IAM roles



Lack of structure or governance for projects and folders within organization



Lack of rotating user-managed service account keys

Hardening of Administration



Bastion hosts or networks
not utilized to access GCP
environments



Misconfigured IAM
policies that permits
privilege escalation



Lack of MFA enforcement
across accounts



Super administrator and
administrative accounts
used for day-to-day
activities

Service Hardening and Logging



No use of GCP-native tools such as Cloud Security Command Center



Storage buckets with unrestricted permissions or the ability to set IAM policies



No integration into current security detection and response



Lack of knowledge on advance logging features such as collecting Admin Read events



Lack of log monitoring and threat hunting

The background features a complex geometric design. On the left, there are overlapping shapes in various shades of blue, including a circle and a rectangle with diagonal lines. These transition into larger, solid blue triangular and polygonal shapes that fill the rest of the frame. The text 'Best Practices' is centered in the lower-left area of this large blue field.

Best Practices

Best Practices

Identity and Access Management

- Require multi-factor for console, CLI access, and roaming users
- Utilize principle of least privilege for IAM permissions assignment
- Restrict number of privileged accounts
- Utilize temporary credentials or Just-in-Time access when possible
- Use dedicated admin accounts
- Implement privileged access workstations

Governance, Risk and Compliance

- Implement account guard rails to ensure proper Governance
- Understand shared responsibility for each service in the cloud
- Understand the terms of contracts with any cloud service providers
- Determine compliance requirements for organization and understand how the cloud service provider controls apply

Configuration Management

- Restrict usage of legacy authentication protocols
- Restrict console and CLI to trusted source IP addresses/ranges
- Audit for overly permissive network security rules
- Back-ups and disaster recovery
- Building resilient services

Best Practices continued

Application Security and DevOps

- Prevent credentials from being committed to Code repositories
- Scan Infrastructure as Code templates to look for misconfigurations
- Scan code and third-party libraries for vulnerabilities
- Utilize dummy data in development
- Implement test-driven security

Secrets and Data Protection

- Rotate access keys frequently
- Monitor for secret leakage
- Have a plan to revoke and rotate secrets
- Leverage resource tags to control access to resources and alerting
- Encrypt data in motion and at rest
- Apply data classification standards across cloud resources

Threat Detection and Response

- Ensure logging and security measures are extended to the cloud
- Enable advanced logging features for sensitive resources
- Aggregate log sources to SIEM
- Enhance SIEM alerts to include cloud-focused alerts
- Apply cloud security practices to incident response plans and playbooks

Summary/Key Take Away

The Solution



NEED FOR ROBUST
IAM SOLUTION
"THE GATE KEEPER"



ASSESS CLOUD
INFRASTRUCTURE EXISTING
CONTROLS
"PUT IN GUARD RAILS"



THREAT DETECTION
AND RESPONSE
"NIGHT WATCH"

■ The challenge:

- Attackers following data to the Cloud
- Lack of Cloud security expertise
- Insecure default settings

Case Studies

The background is a dark blue gradient with several large, light blue geometric shapes. On the right side, there is a stylized representation of a globe or sphere, composed of various shades of blue and white, with some internal lines suggesting a grid or latitude/longitude.

Mandiant Incident Response Case Studies: Insider Threat Timeline

Opportunity for prevention!

Access not terminated

Opportunity for detection!

Sensitive object storage accessed outside of working hours

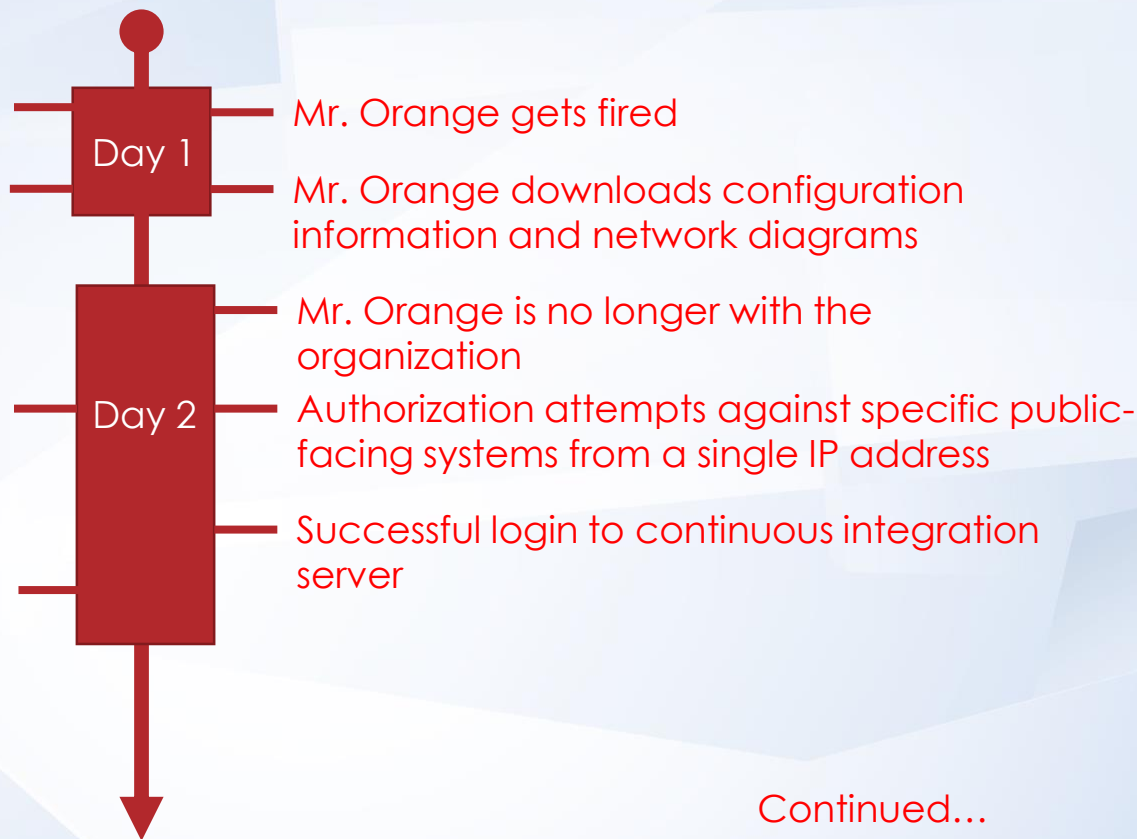
Opportunity for prevention!

Unknown Internet-facing systems without strong authentication

Opportunity for detection!

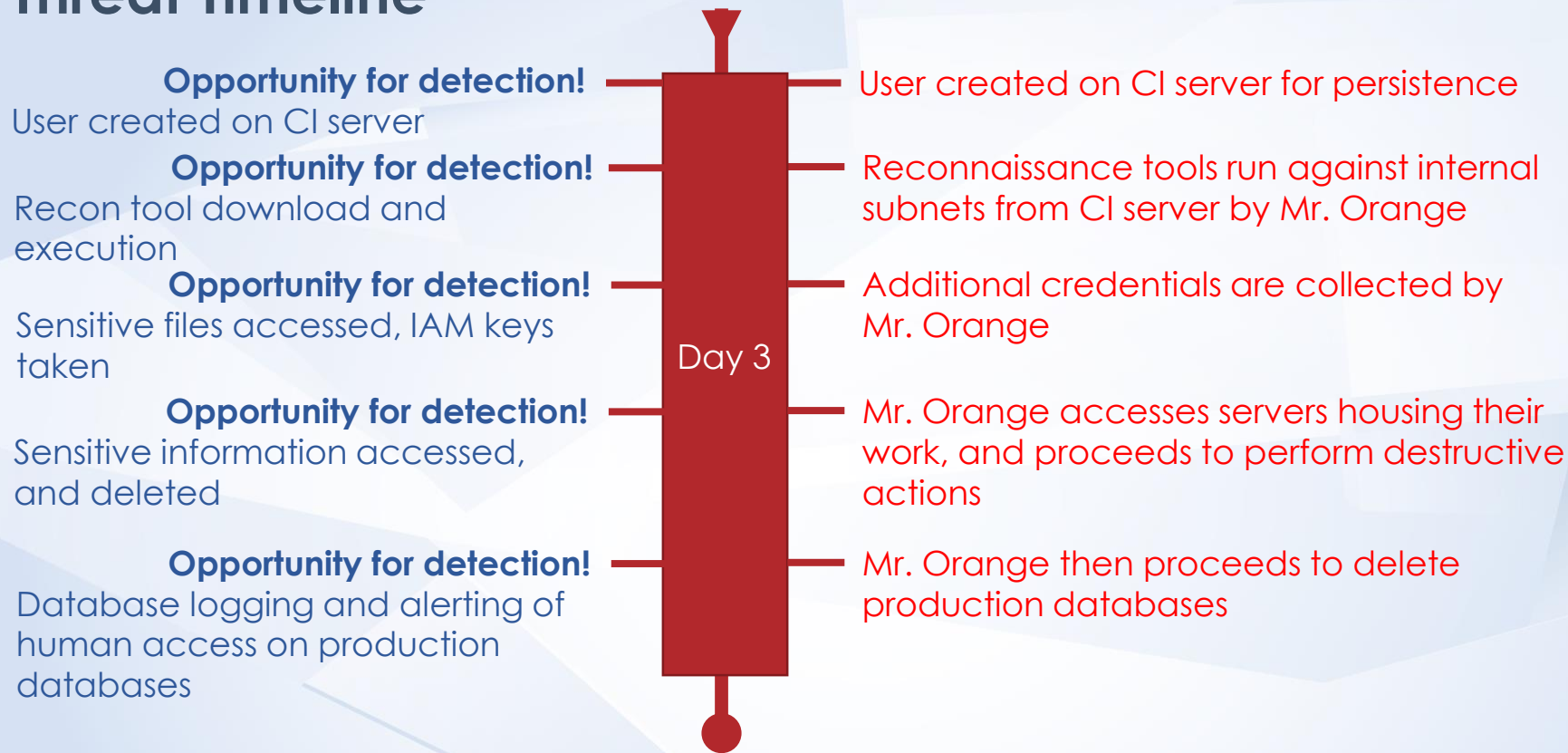
Activity analytics:

- Anomalous amount of API activity and anomalous API calls
- New IP logging in to CI system



Continued...

Mandiant Incident Response Case Studies: Insider Threat Timeline



Mandiant Incident Response Case Studies: A Tale of Two DBs

ACME, Inc.



- Some things in common...
- Threat prevention opportunities:
 - Integration of security in application design
 - Integration of security in development pipelines
 - Cloud Service Provider logs (e.g., CloudTrail) centralized and monitored
 - Developers with permissions not aligned with their scope of duties
 - Weak database authentication and authorization

ACMO, Inc.



Mandiant Incident Response Case Studies: A Tale of Two DBs

ACME, Inc.



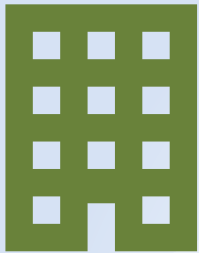
- More things in common...
- Threat detection opportunities:
 - Automated enforcement of rules/policies to remove weak security group rules (e.g., AWS Config)
 - CSP-native tools to detect and alert on misconfigurations (e.g., Trusted Advisor)
 - Custom or open-source tools to enable continuous validation
 - Detection on suspicious or anomalous connections
 - Database logs monitored for sensitive commands

ACMO, Inc.

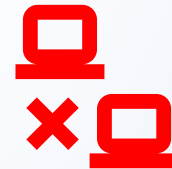
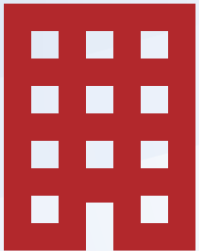


Mandiant Incident Response Case Studies: A Tale of Two DBs

ACME, Inc.

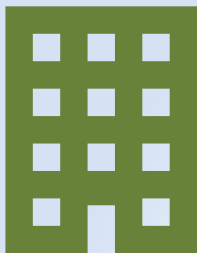


ACMO, Inc.



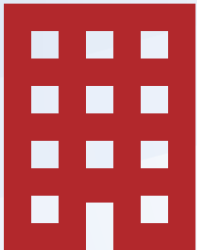
Mandiant Incident Response Case Studies: A Tale of Two DBs

ACME, Inc.



- No things in common...
- Threat response:
 - Ensure all resources are configured to log based on threat model
 - Ensure all cloud logging is sent to centralized system
 - Cloud-focused alerting (based on captured logs) and standard operating procedures
 - Update and adapt workflows, processes or technical components
 - Practice, practice, practice

ACMO, Inc.



Questions?

Christopher.Romano@Mandiant.com

Dylan.Marcoux@Mandiant.com