

SANS  
CLOUD  
SECURITY  
PRESENTS

# Finding Sherlock

Written by Shaun McCullough

[sans.org/posters](https://sans.org/posters)



**SHAUN  
MCCULLOUGH**  
CLOUD SECURITY ARCHITECT

- Cloud Security Architect with GitHub
- SANS Instructor and co-author of SEC541 Cloud Security Attacker Techniques, Monitoring & Threat Detection
- 20 years at the National Security Agency focused on cyber operations, red/blue/hunt, and software engineering



 cybergoof

 @thecybergooof

# ATTACK

**A story told in 6 parts**

**Maps to MITRE ATT&CK  
Fits AWS or Azure**

**Told in the world of  
Sherlock Holmes**

# DETECT

**Logs and Telemetry**

**Resource Groups  
Specific Log Types  
ATT&CK Detections**



**SEC541:** The poster reflects the content of SEC541.  
[sans.org/posters](https://sans.org/posters)

Special thanks to **David Garrison** for the awesome graphics.  
Our story begins with

**Sherlock Homes** in hiding...

## Initial Access

**ATTACKER:**  
**Culverton Smith -**  
**Serial Killer**





**TACTIC:** Initial Access

**RISK:** Long term Creds will get you in trouble

**DETECT:** SSO Logs shows login, cloud activity logs show activity in that cloud

**MITIGATE:** 2FA for all humans. Rotate Keys every 90 days. Move to cloud-native identity access. Watch out for artifacts in Git repos

**TECHNIQUES:** T11213 | T1078 | T1589



Discovery



**ATTACKER:**

**Henry Peter - Con Artist**

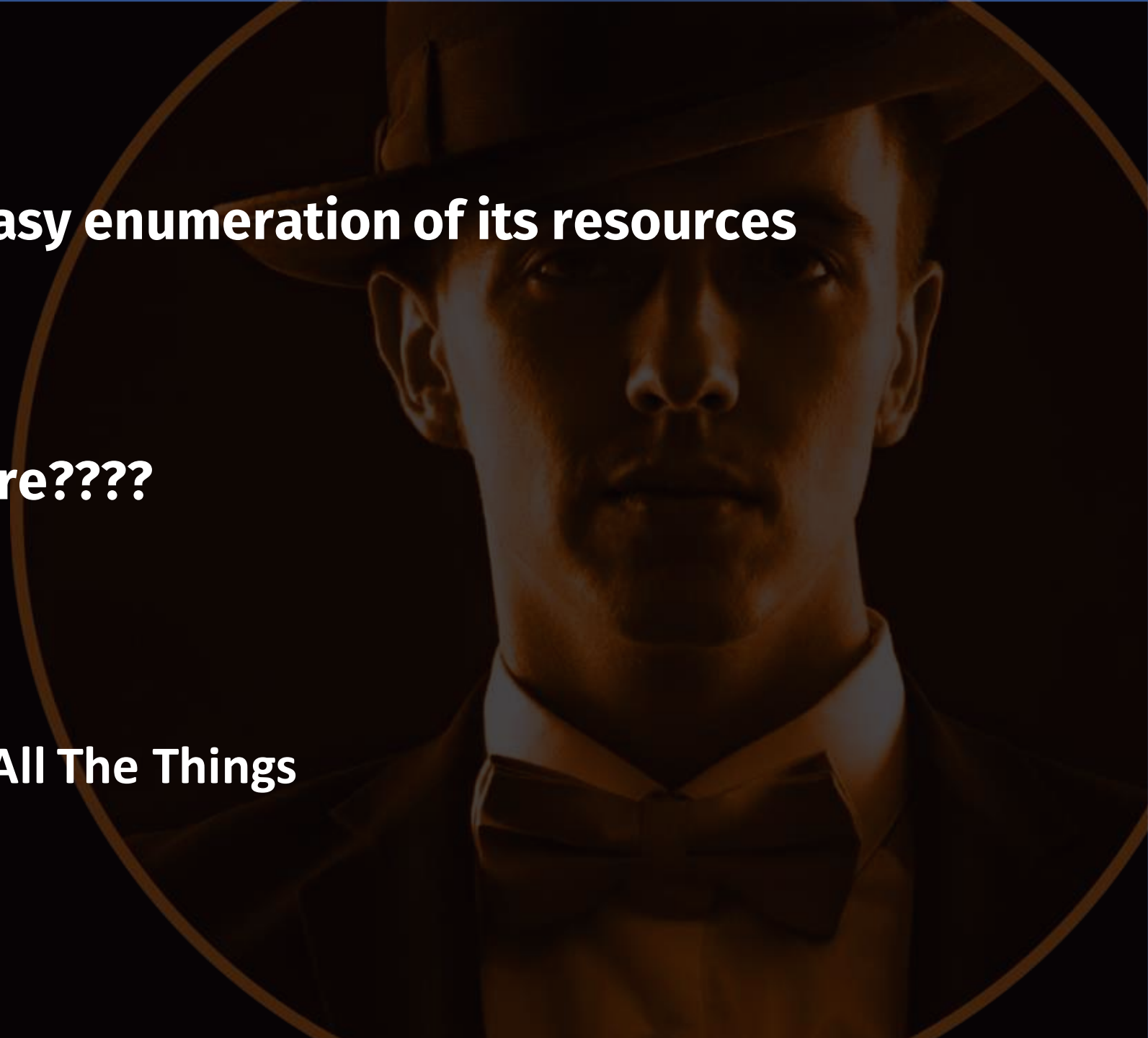
**TACTIC:** Discovery

**RISK:** The cloud offers easy enumeration of its resources

**DETECT:** AWS CloudTrail.  
What about Azure????

**MITIGATE:** Least Privilege All The Things

**TECHNIQUES:** T1526 | T1580



# Escalation & Evasion

**ATTACKER:**  
**Irene Adler -**  
**Hacker for Hire**





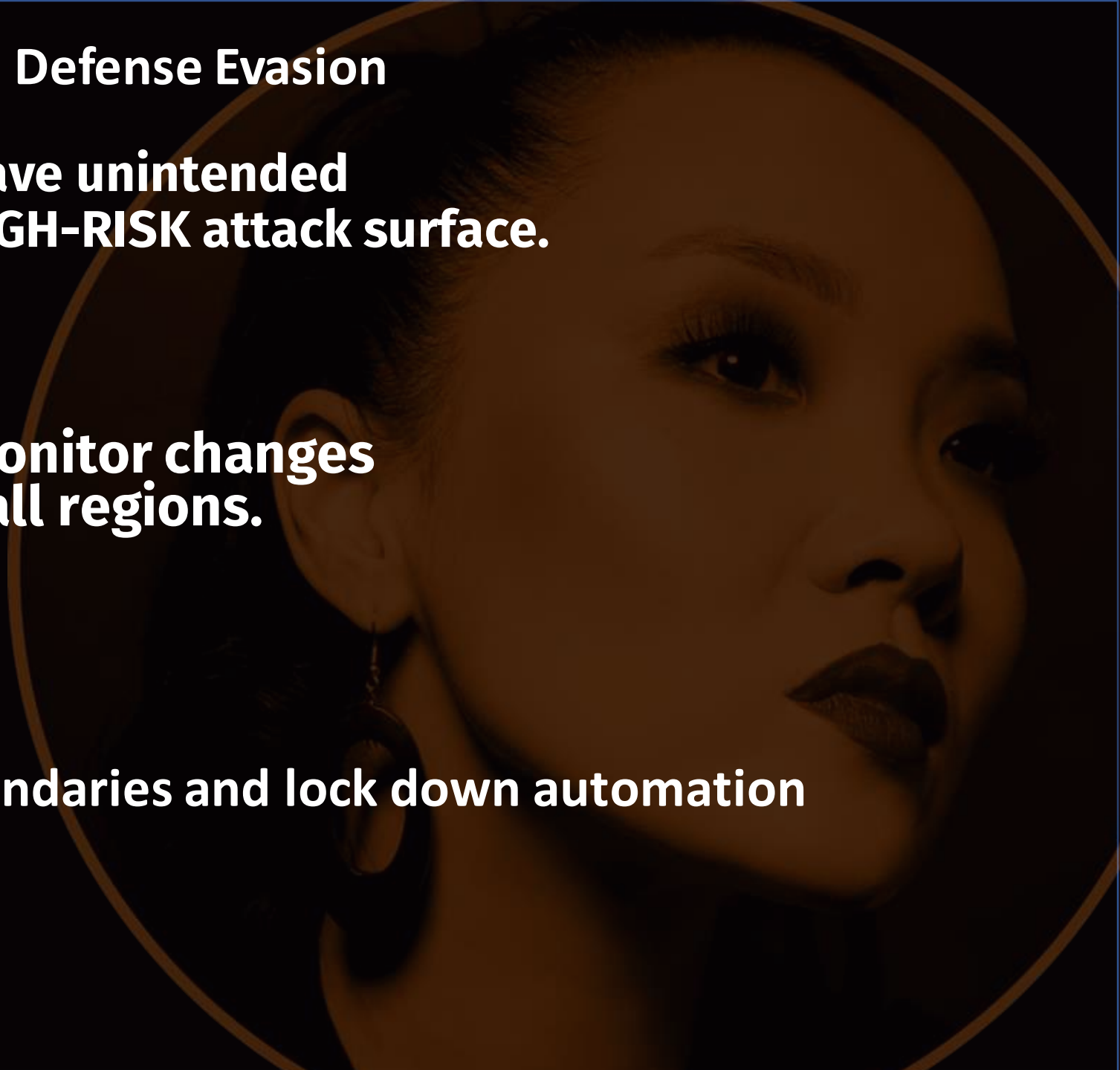
**TACTIC:** Privilege Escalation | Defense Evasion

**RISK:** IAM and automation have unintended consequences. CI/CD is a HIGH-RISK attack surface.

**DETECT:** Activity Logs to monitor changes to HIGH-RISK roles. Scan all regions.

**MITIGATE:** Build security boundaries and lock down automation

**TECHNIQUES:** T1535 | T1098



**ATTACKER:**  
**Violet Norbury -**  
**Leaker of Secrets**



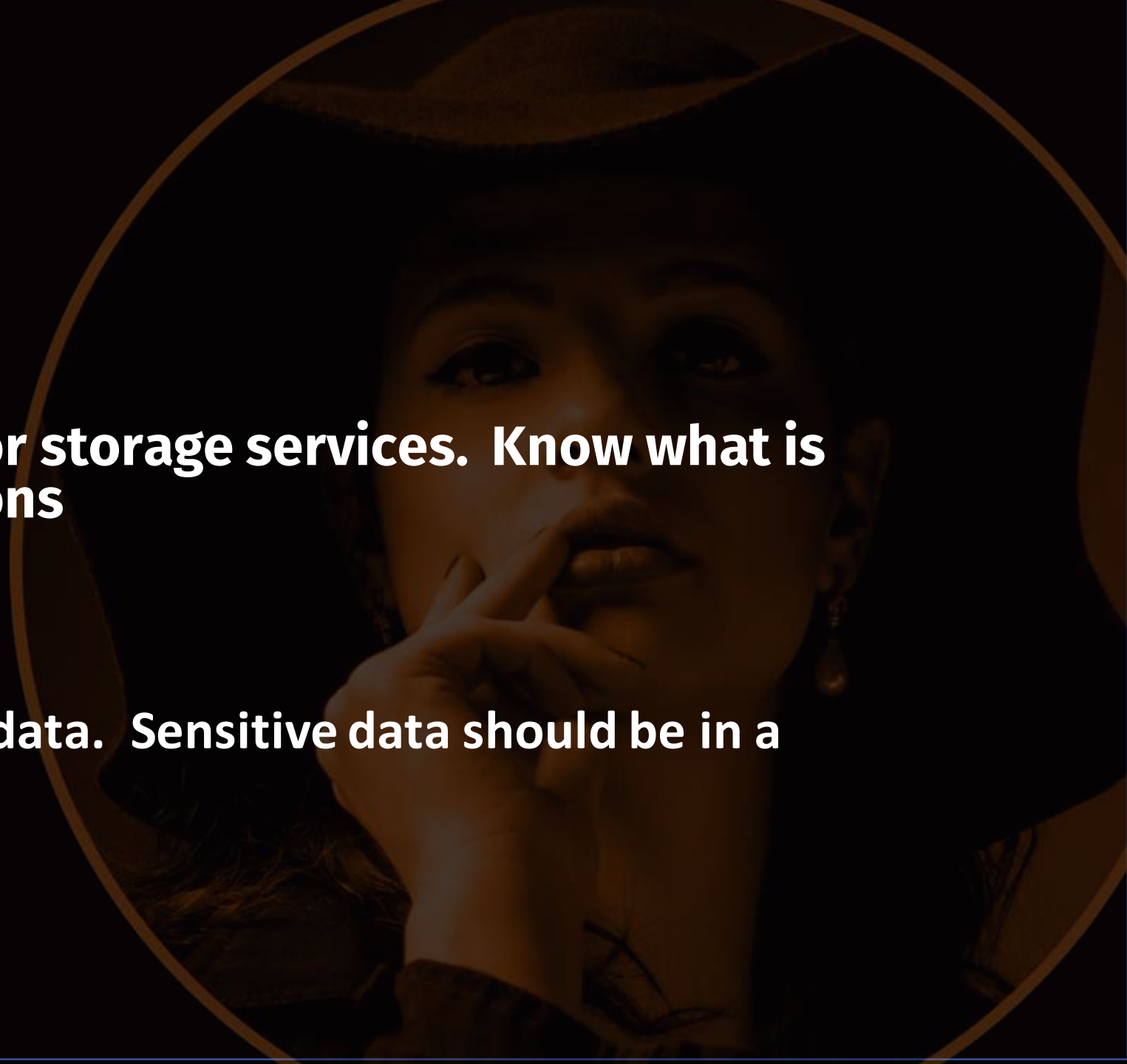
**TACTIC:** Collection

**RISK:** Sensitive data


**DETECT:** Turn on logging for storage services. Know what is sensitive and add detections

**MITIGATE:** Encrypt sensitive data. Sensitive data should be in a separate security boundary

**TECHNIQUES:** T1074 | T1530







**ATTACKER:**  
**Professor Moriarty -**  
**Mastermind**





```
moriarty> cat MINDPALACE.decrypt
```

Moriarty, it's always amusing to see you chase after me like a wild goose.  
But, I'm afraid your latest pursuit is nothing more than a red herring,  
a mere diversion that's led you astray.

Better luck next time, old boy!

```
moriarty> █
```

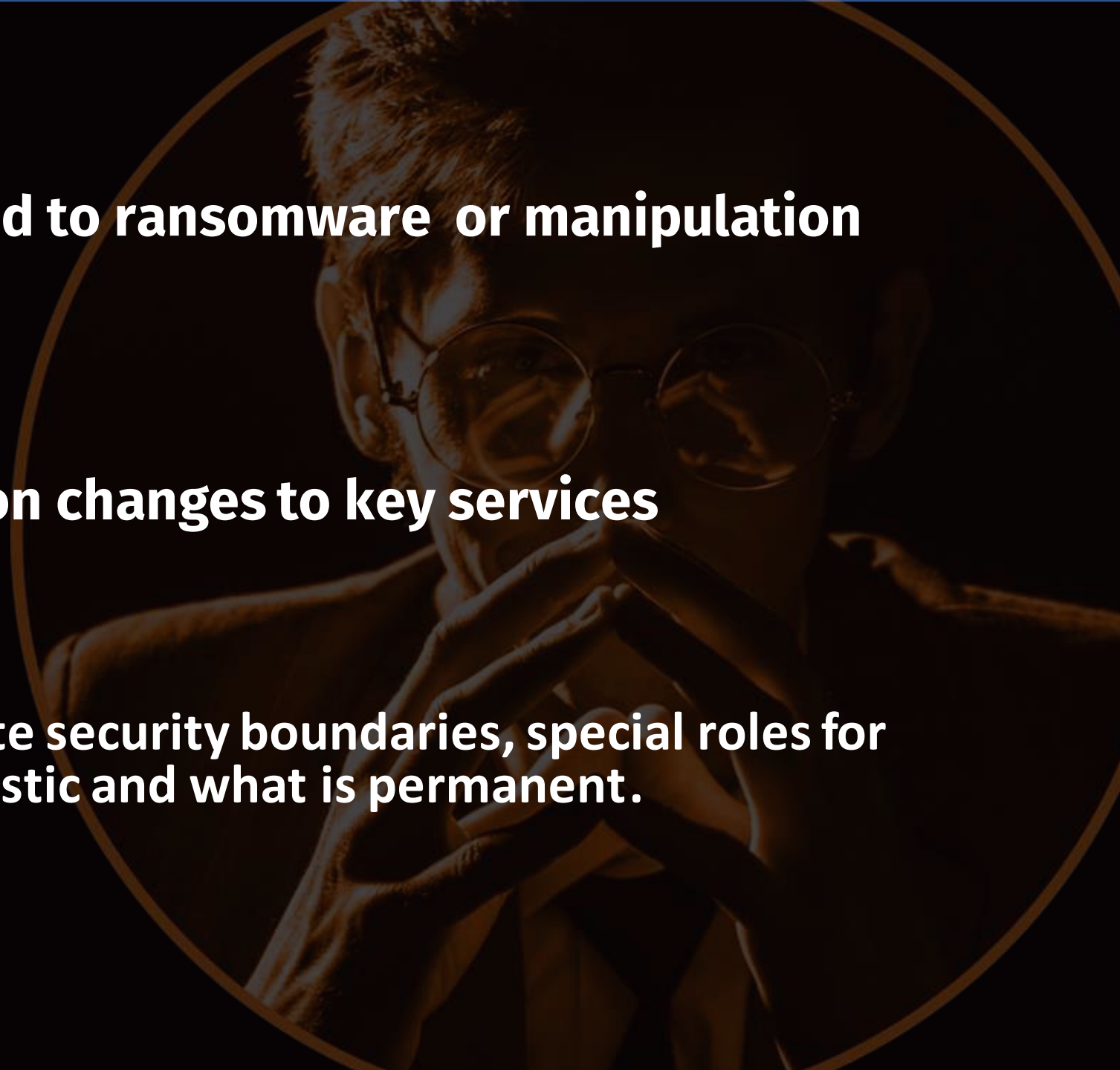
**TACTIC:** Impact

**RISK:** Admin access can lead to ransomware or manipulation

**DETECT:** Activity Log alert on changes to key services

**MITIGATE:** Backups in separate security boundaries, special roles for destruction, know what is elastic and what is permanent.

**TECHNIQUES:** T1485 | T1491





**John H. Watson, M.D.**





# **SEC541: Cloud Security Attacker Techniques, Monitoring, and Threat Detection**



**SANSFIRE 2023**  
July 10 – 14  
Shaun McCullough

**SANS OnDemand**  
Anytime  
Shaun McCullough

**Cyber Security Central**  
May 1 - 5  
Ryan Nicholson

**Cloud Singapore**  
May 22-31  
Alex Braulik

[sans.org/sec541](https://sans.org/sec541) | [giac.org/gctd](https://giac.org/gctd)

SANS  
CLOUD  
SECURITY  
PRESENTS

Thank You

# Finding Sherlock

Written by Shaun McCullough

[sans.org/posters](https://sans.org/posters)