RSAConference2019

San Francisco | March 4–8 | Moscone Center

SESSION ID: IDY-T08

More than Vaulting: Adapting to New Privileged Access Threats

Lance Peterman

Enterprise Security Architect
Merck
@lpeterman

About Me

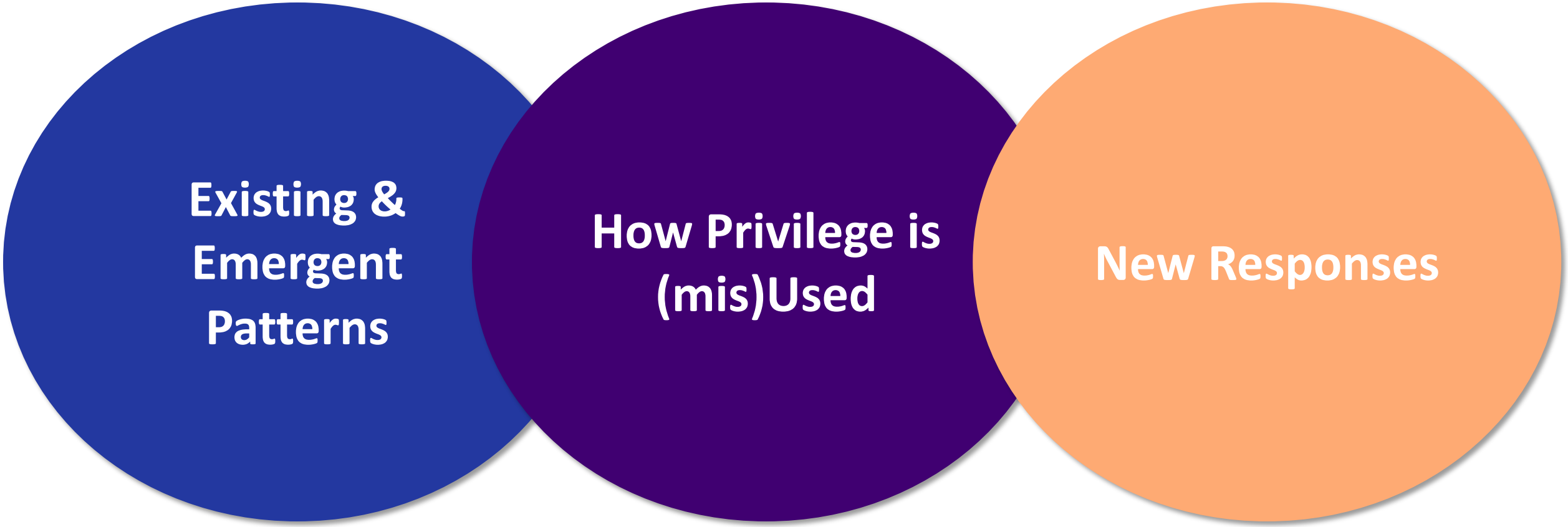
- Formerly IAM Strategy & Platform Lead at Merck
- Also, Teach Software Architecture & Design at UNC-Charlotte
- Also, Board & Founding member of IDPro
- Opinions are my own
- Twitter: @lpeterman

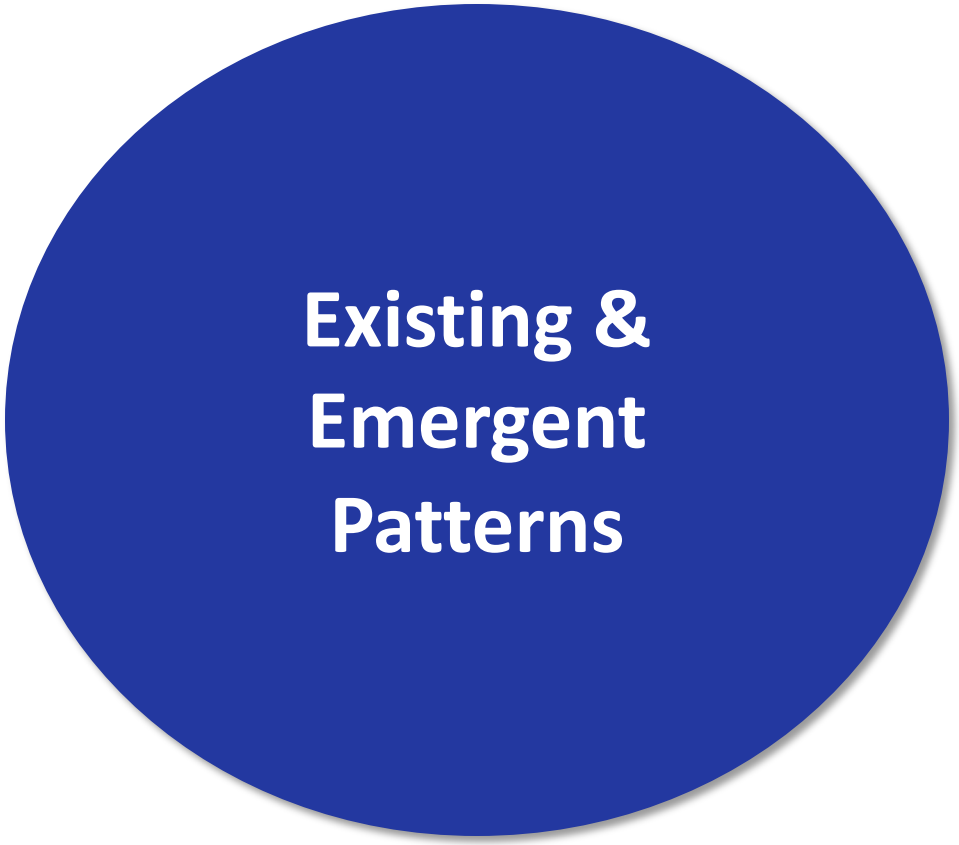
Why we can’t get a Perfect 10 in the Vault

2 years ago…

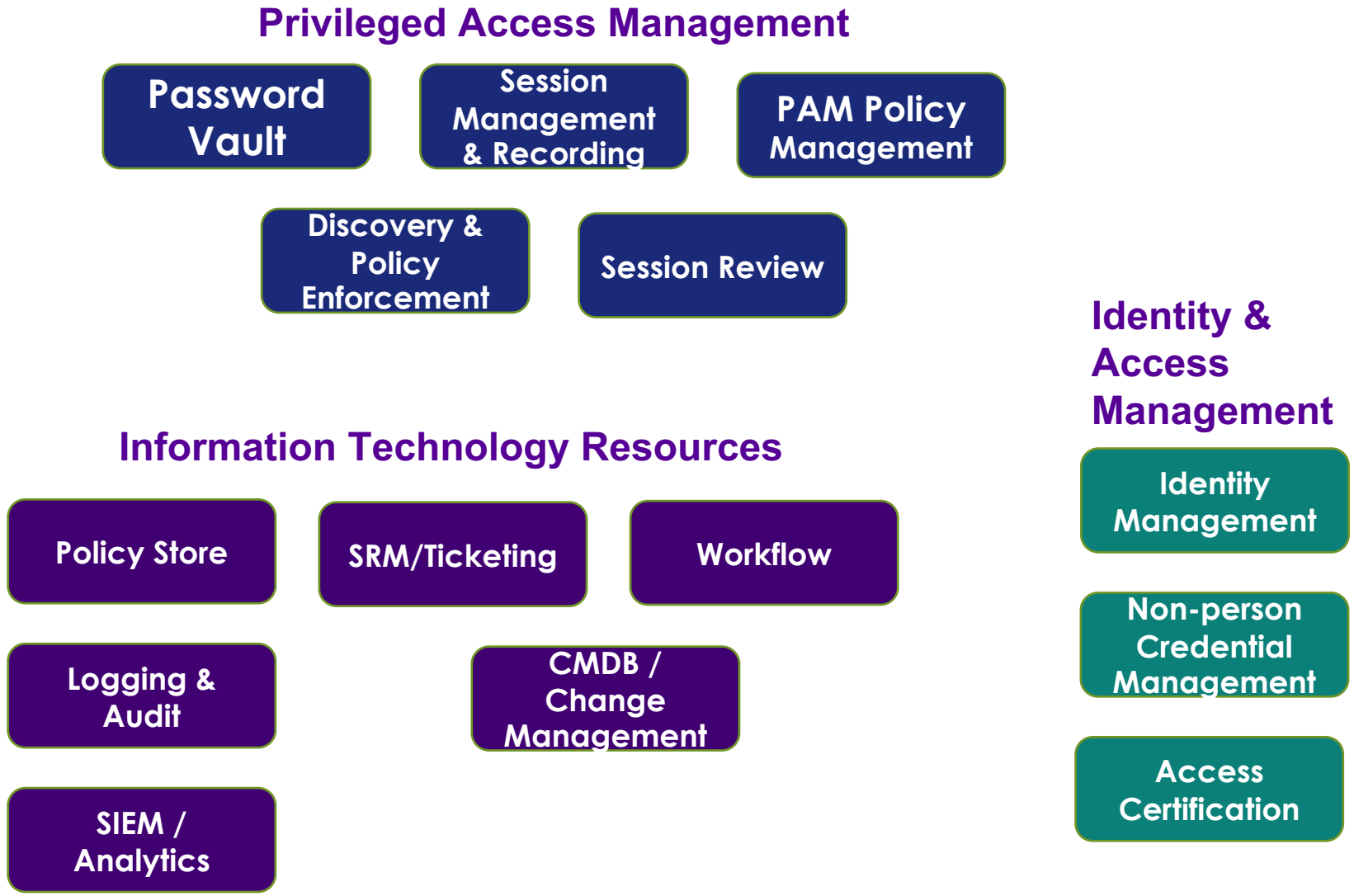

#RSAC
RSAConference2017
San Francisco | February 13 – 17 | Moscone Center
POWER OF OPPORTUNITY
SESSION ID: IDY-R10
Privileged Access Management: Unsticking Your PAM Program
Lance Peterman
Identity & Access Management Architect
Merck
@lpeterman

My use case…


Existing & Emergent Patterns
How Privilege is (mis)Used
New Responses


Existing &
Emergent
Patterns

PAM Reference Architecture (2015)



PAM Reference Architecture 2019

Privileged Access Management

- Just in Time Administration
- Credential Vault
- Session Management & Recording
- PAM Policy Management
- Discovery & Policy Enforcement
- Session Review
- Secret/Key Management

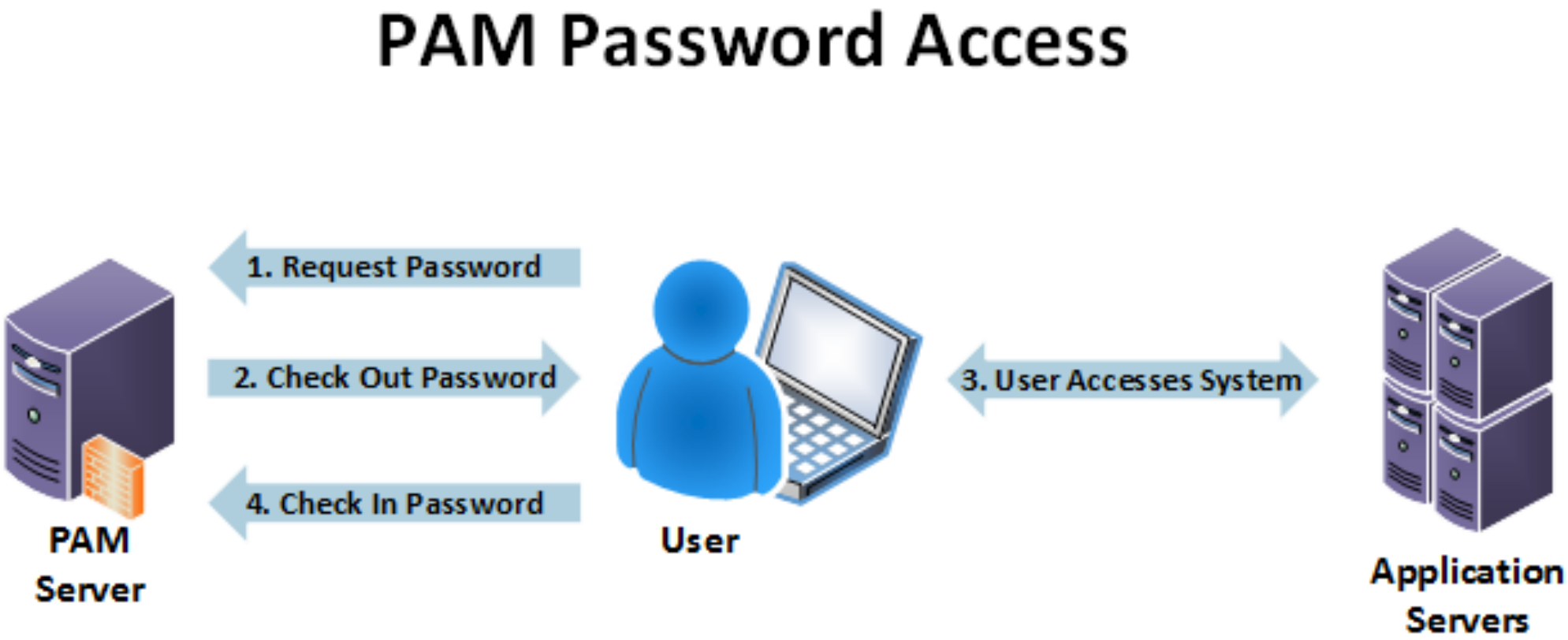
Information Technology & InfoSec Resources

- Policy Store
- SRM/Ticketing
- Workflow
- Logging & Audit
- CMDB / Change Management
- EPM & EDR
- SIEM
- **Analytics/ AI/ML
- SOC/ Incident Response

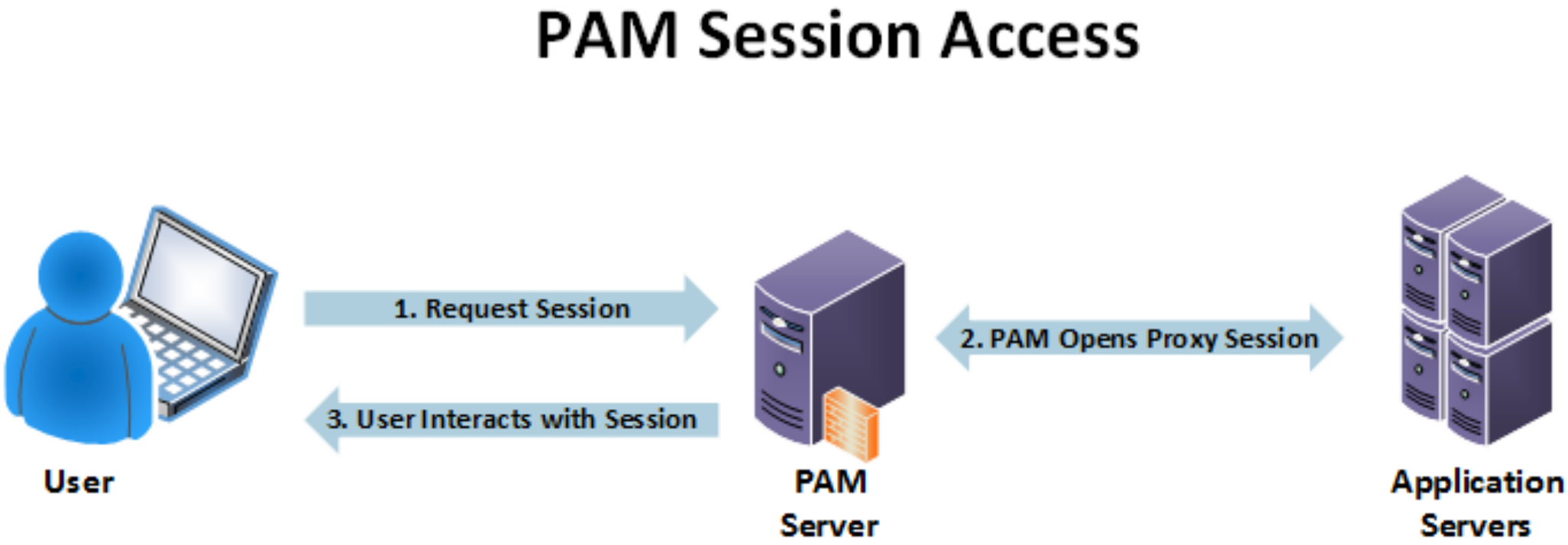
Identity Governance & Administration

- Identity Management
- Non-person Credential Management
- Access Certification

Vaulting


PAM Password Access
1. Request Password
2. Check Out Password
3. User Accesses System
4. Check In Password
PAM Server
User
Application Servers

Session Management



Local Admin Management/EPM

Secrets/Key Management

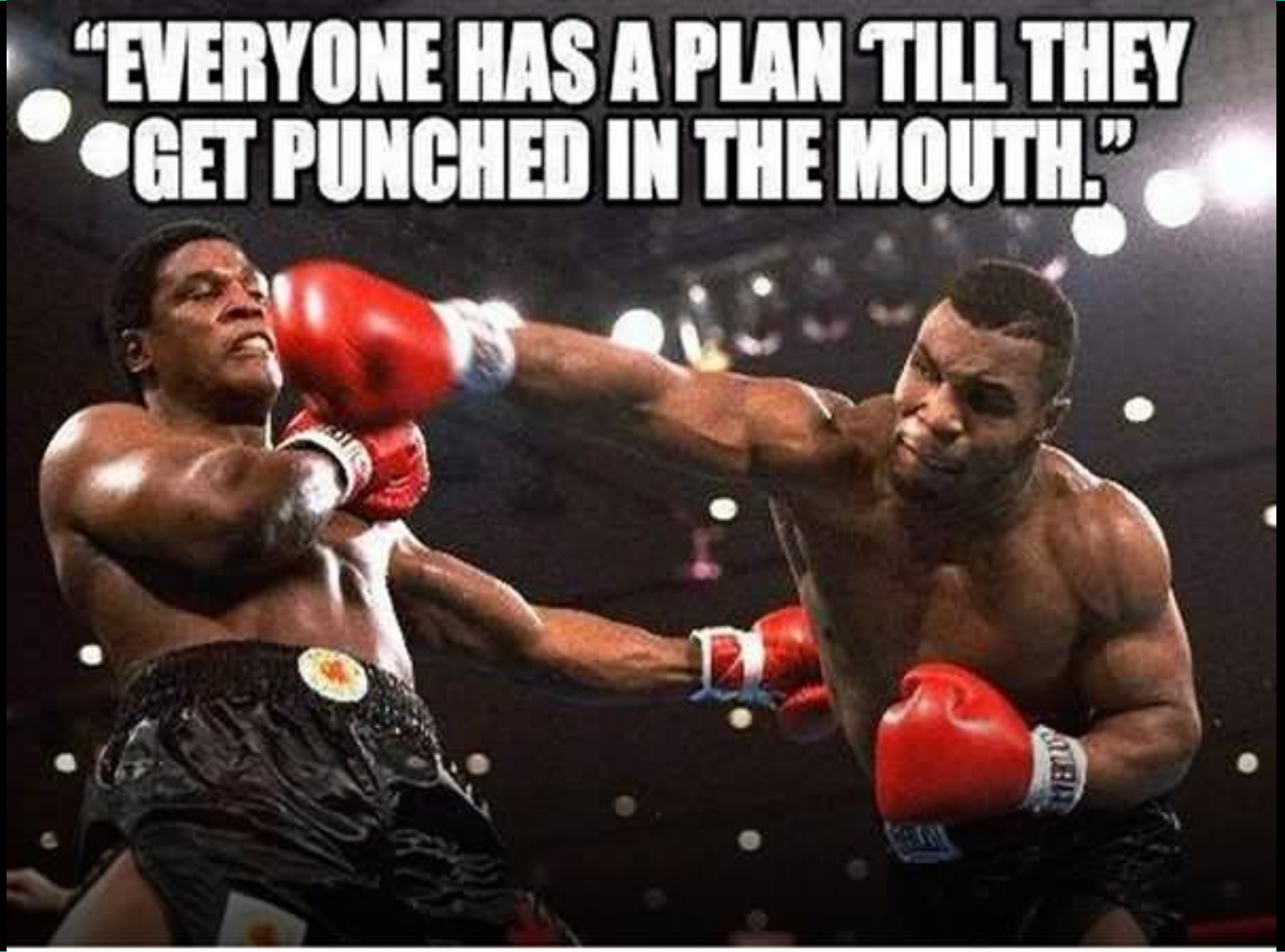
- Market is fragmented here – AWS, Ansible, Chef, Vault, CyberArk…lots more
- Does this belong in IAM? Similar challenge with CIAM & API management for many enterprises
- DevSecOps emergence is helping generate momentum for this, but cultural challenges remain…

Secrets / Key Management

Other Patterns/Approaches

- Just in Time Administration - Elevation vs. Vaulting for person & non-person accounts
- Analytics…got a minute, or 90?
- AI/ML – Lots of potential here, but can you get the right (and all) of the data for training
- SOC & Incident Response – How fast can you shut down privilege abuse/misuse?

How Privilege is (mis)Used


"EVERYONE HAS A PLAN 'TILL THEY
GET PUNCHED IN THE MOUTH."

June 27, 2017 6am EDT

NotPetya


ROSNEFT


MAERSK


FedEx


Mondelēz
International


NUANCE

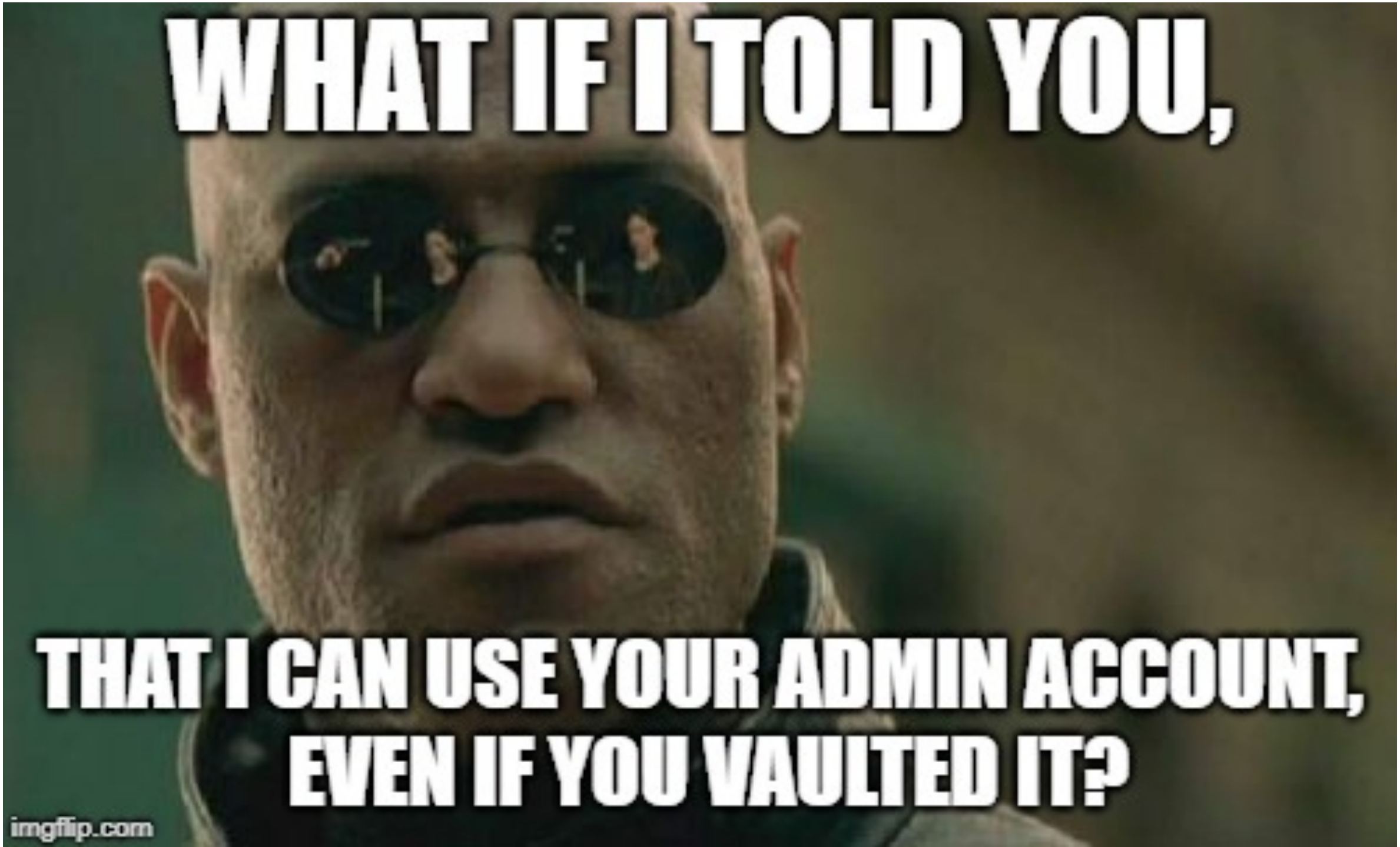

rb
Reckitt
Benckiser


SAINT-GOBAIN

MimiKatz “cute kitten”

- “Swiss army knife” (or multi-tool) of Windows credentials created by Benjamin Delpy (@gentilkiwi)
- Needs **local admin** for ‘most’ functions
- Leverages weaknesses/features in:
  - LSASS - Local Security Authority Subsystem Service – credentials stored in memory after use
- Can leverage credentials stored as (depending on OS level):
  - Kerberos tickets
  - NTLM password hashes
  - LM password hashes
  - Clear-text passwords
- GREAT Resource for understanding MimiKatz – ADSecurity.org

```
Authentication Id : 0 ; 2858340 (00000000:002b9d64)
Session           : Service from 0
User Name         : svc-SQLDBEngine01
Domain            : ADSECLAB
SID               : S-1-5-21-1473643419-774954089-2222329127-1607
        msv :
         [00000003] Primary
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * NTLM     : d0abfc0cb689f4cdc8959a1411499096
         * SHA1     : 467f0516e6155eed60668827b0a4dab5eecefacd
        tspkg :
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * Password : ThisIsAGoodPassword99!
        wdigest :
         * Username : svc-SQLDBEngine01
         * Domain   : ADSECLAB
         * Password : ThisIsAGoodPassword99!
        kerberos :
         * Username : svc-SQLDBEngine01
         * Domain   : LAB.ADSECURITY.ORG
         * Password : ThisIsAGoodPassword99!
        ssp :
        credman :
```


WHAT IF I TOLD YOU,
THAT I CAN USE YOUR ADMIN ACCOUNT,
EVEN IF YOU VAULTED IT?
imgflip.com

Other Windows OS/protocol threats

- Kerberoasting
- Vulnerabilities in Kerberos (UN)Constrained Delegation (KCD)
- GPO Permissions
- Deeply Nested AD Groups - Do you really know where your privileges are…
- Notice that little of this is explicitly identity related? Or is it?

Other Vectors

- (I)IoT – Mirai showed us what default admin passwords can do
- SaaS & IaaS accounts (ie. O365 & ec2 user) – How well do you know your privileged accounts not tied to central IDP?
- Network – Much is shifting to layer 7, where are your privileges now?

Secrets Revealed

22K OPEN, VULNERABLE CONTAINERS FOUND EXPOSED ON THE NET

by Tara Seals

June 18, 2018 , 12:19 pm

More than 22,000 container orchestration and API management systems are unprotected or publicly available on the internet – highlighting the reality of the risks of operating workloads in the cloud.

According to research from Lacework, the containers (Kubernetes, Mesos, Docker Swarms and more) suffer from poorly configured resources, lack of credentials and the use of non-secure protocols. As a result, attackers can remotely access the

IOT Exploits

Someone Is Taking Over Insecure Cameras and Spying on Device Owners

By Catalin Cimpanu June 22, 2018 06:50 AM 1

Many brands of webcams, security cameras, pet and baby monitors, use a woefully insecure cloud-based remote control system that can allow hackers to take over devices by performing Internet scans,

Insider threat is still a thing…

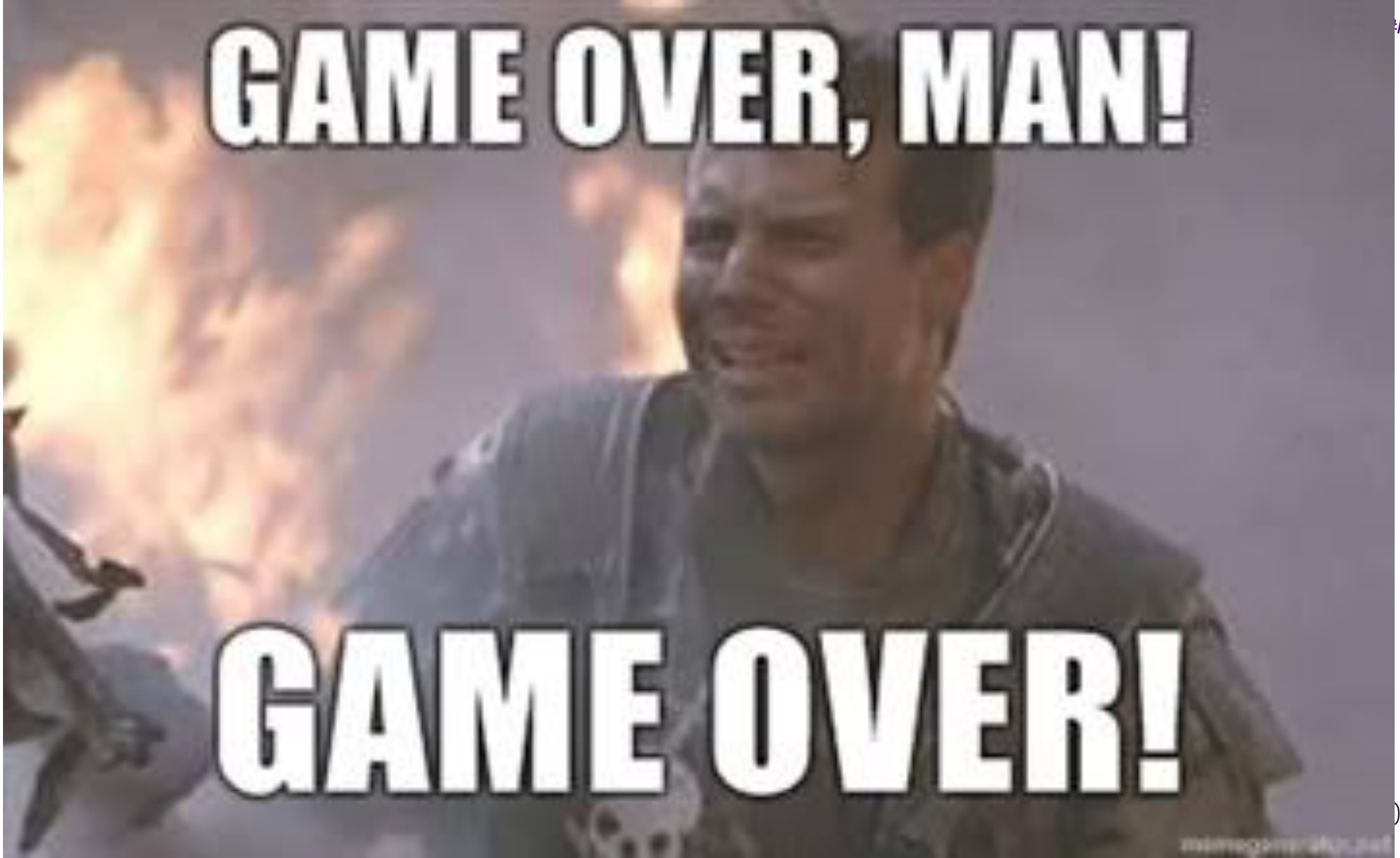
Tesla Breach: Malicious Insider Revenge or Whistleblowing?

By Kevin Townsend on June 22, 2018

Share G+ Tweet Recommend 0 RSS

Just before midnight last Sunday evening (June 17, 2018), Elon Musk sent an email to all staff. He was dismayed, he said, to learn about a Tesla employee "making direct code changes to the Tesla Manufacturing Operating System under false usernames and exporting large amounts of highly sensitive Tesla data to unknown third parties."

This was a mainstream malicious insider attack -- but there may be more to it than meets the eye. The motive, according to Musk, was revenge: "he wanted a promotion that he did not receive." But this incident goes way beyond simple revenge sabotage, and includes the


GAME OVER, MAN!
GAME OVER!

New Responses

Technology Arrows

- Use EPM or similar tools to reduce/eliminate local admin privileges wherever possible
- If you don’t have secrets/key management, explore the need. Talk to your vendors.
- Have an IoT platform? Find out, explore gateways for segmentation
- Consider automated tools for privileged account discovery

More Technology ‘Arrows’

- Reduce privilege ‘scale’ through segmentation (ex. AD Red Forest)
- Eliminate credential caching where possible
- MFA for sensitive internal apps, even regular users
- Consider analytics for privilege abuse use cases but make sure you get the data

Process ‘Arrows’

- Reduce privilege ‘scale’ through segmentation (ex: SCCM admins), including number of admins per server
- Consider software updates a threat vector (supply chain attack)
- Leverage Least Privilege (LPM)wherever possible (see people arrows)
- Defense in depth should be a mindset, look beyond Layer 7 for solutions

More Process ‘Arrows’

- Embed security & identity in your SDLC (Push Left, thanks Tanya Janca @shehackspurple)
- Same for Change Management (CMDB is your most important identity asset)
- If you use Policy, leverage it to the hilt for privileged access compliance

People ‘Arrows’

- Partner with Developers on Secrets & Local Admin
- Partner with InfoSec on expanding privilege analysis, focus on LPM, and Defense in Depth
- Partner with the business on identifying your high value assets (HVA), know what you’re protecting and why
- Partner with everyone on MFA – pierce the veil on how it can be used and reduce friction
- Prioritize activities based on risk

This is a LOT, where do I start?

- Use the reference architecture (revise if needed!)
- Partner with the Business, Security, & Risk to start to understand your risks & current capabilities
- Pick an activity – Ready!
- Pick an arrow – Focus on Risk Mitigation – Aim!
- Execute – Fire!
- Measure your results!


IDPRO
founding member

Resources

- 2017 Talk - https://youtu.be/1HA2N_4c2jw
- Local Admin rights blog post - https://identitybytes.com/index.php/2018/03/20/applying-a-rheostat-to-local-admin-rights/
- Secrets compromised - https://threatpost.com/22k-open-vulnerable-containers-found-exposed-on-the-net/132898/
- IoT compromised - https://www.bleepingcomputer.com/news/security/someone-is-taking-over-insecure-cameras-and-spying-on-device-owners/
- MimiKatz - https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/
- ADSecurity.org Guide to MimiKatz - https://adsecurity.org/?page_id=1821
- ”Push Left” – Tanya Janca - https://code.likeagirl.io/pushing-left-like-a-boss-part-1-80f1f007da95
- Photo credits – Natalie Peterman

Thank You!!!