CYBERARK®

Workload

~~Application~~

Identity, Security & Governance

Dennis Mastin CISSP | CCSK

Agenda

- ✓Defining Application Identity
- ✓Understanding Application Identity Risks to the Business
- ✓Auditing DevOps Environments
- ✓Managing Application Identity Lifecycles
- ✓Q&A

Two Sides of the Same Coin

Bill

- Has a Defined Role
- Requires Access to Accomplish Role
- Activity Must be Audited
- Warm and friendly

Application Node WA113

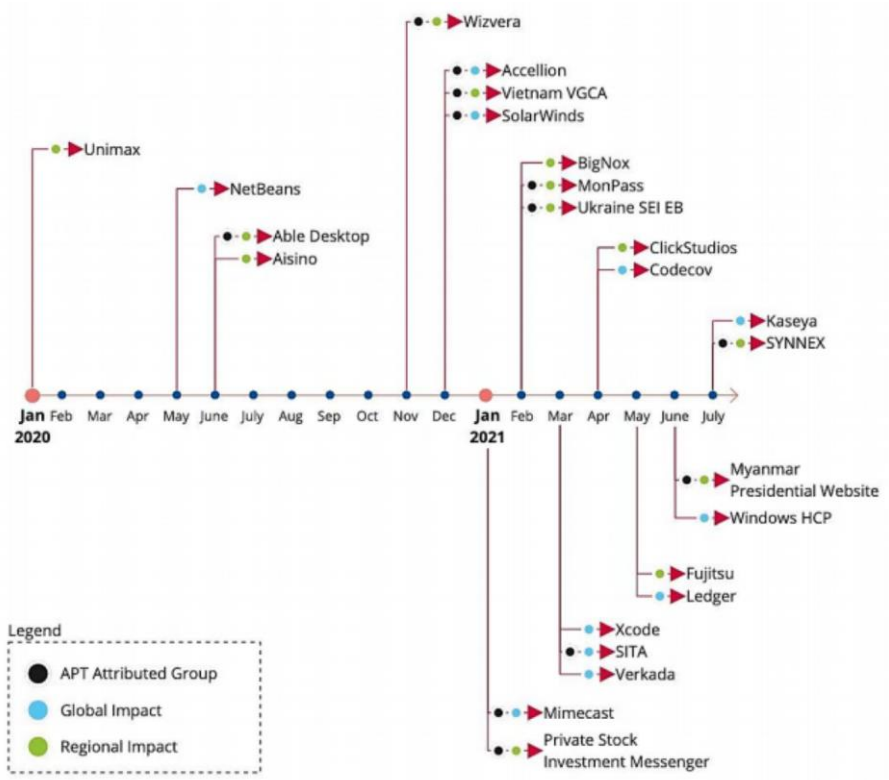
- (Should) Have a Defined Role
- Requires Access to Accomplish Role
- Activity Must be Audited
- Cold and unfeeling

Application Compromise Risks

- Loss of Company IP
- Injection of Malicious Source Code
- Loss of Client Data
- Hijacking of Operations

Common Link: All Impact the Organizational Supply Chain

The State of Software Supply Chain Attacks



71% Of organizations experienced an attack on their software supply chain in 2021

66% Of attacks in 2020-2021 compromised code

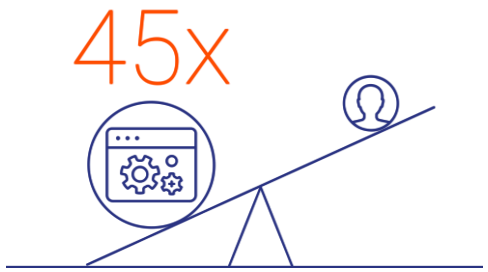
67% Of organizations have not done a formal assessment or education on software supply chain risk

Millions Of organizations affected

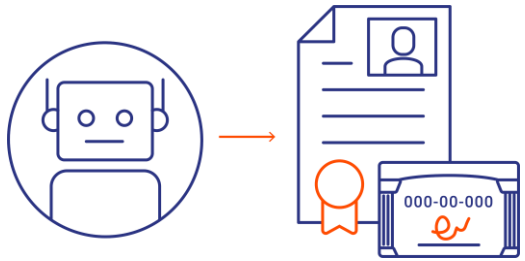
CyberArk, 2022 Identity Security Threat Landscape Report
ENISA, Threat Landscape of Software Supply Chain attacks
PWC, 2022 Global Digital Trust Insights

CyberArk 2022 IdSec Threat Landscape – Key Trends

The average staff member accesses more than 30 applications and accounts



Machine identities outnumber human identities by a factor of 45x



68% of non-humans or bots have access to sensitive data and assets

52% of organizations' workforces have access to sensitive corporate data

RANSOMWARE

>70%

of organizations experienced a ransomware attack in the past year

Average number of attacks among healthcare organizations **2**

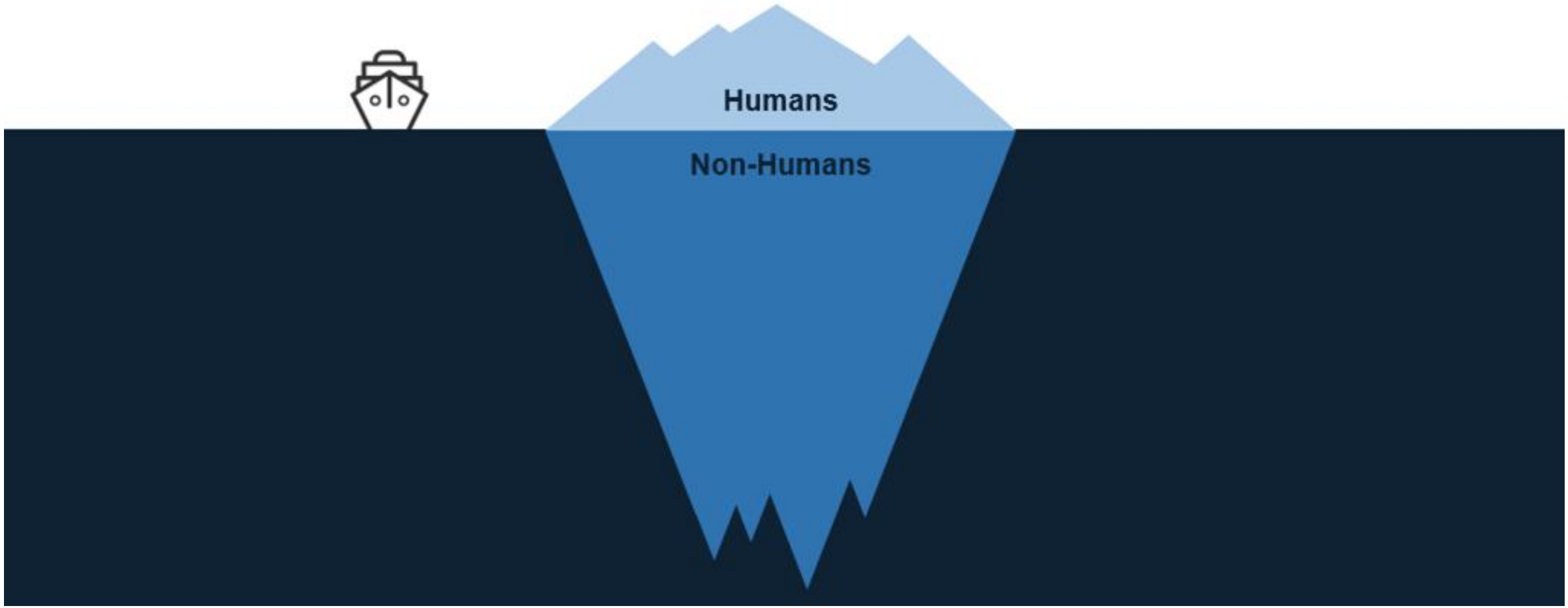
SOFTWARE SUPPLY CHAIN

>71%

of organizations suffered a software supply chain-related attack resulting in data loss or compromised asset

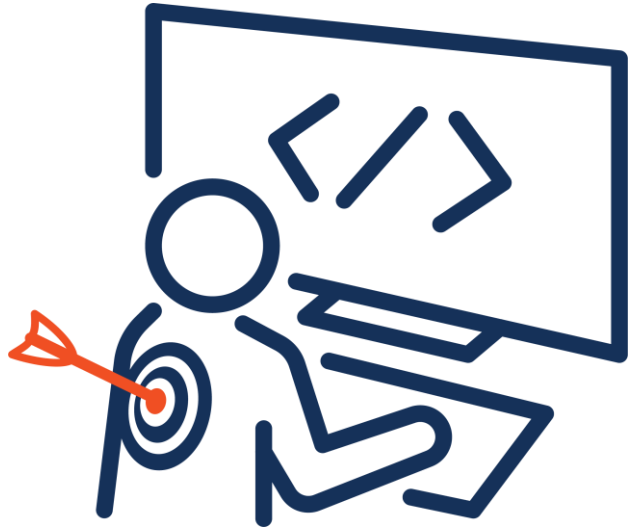
88% of energy and utilities companies suffered a successful software supply chain-related attack

Human Access vs. Non-human Access



Devs - The Modern Power User

- ✓Heart of the Software Supply Chain
- ✓Requires a diverse range of privileged and sensitive access across many disparate toolsets and environments
- ✓Operationally driven, immensely sensitive to slowdowns
- ✓Focused on delivery and empowered to overcome obstacles
- ✓Typically, the last user type that organizations secure



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its

Draft (2nd) NIST Special Publication 800-161
Revision 1

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

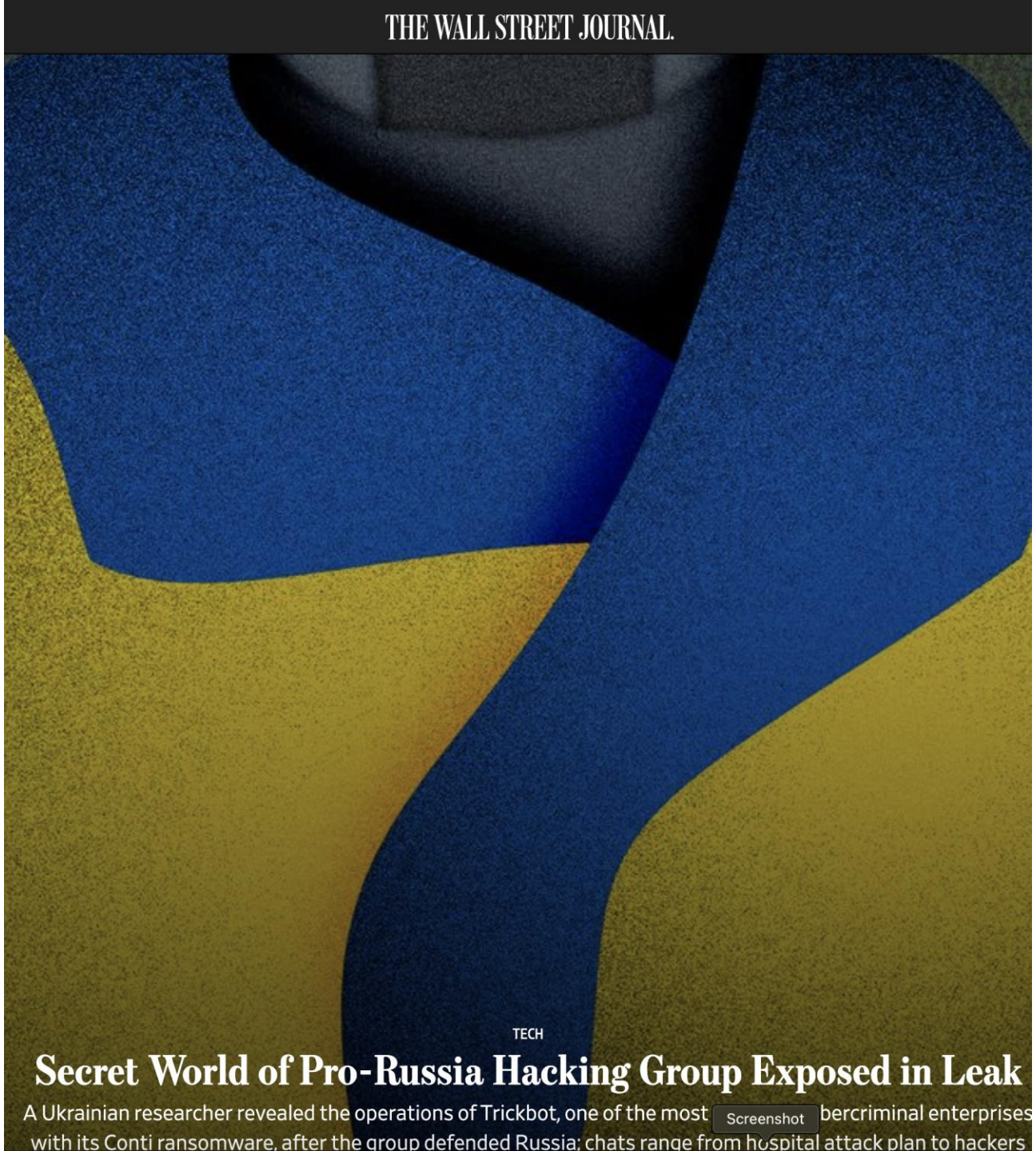
Jon Boyens
Angela Smith
Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-161r1-draft2

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

…and a few example controls

- (AC-5) Separation of Duties
- (AC-6) Least Privilege
- (AU-2) Event Logging
- (AU-3) Content of Audit Records
- (AU-10) Non-Repudiation
- (CM-7) Least Functionality
- (CM-8) System Component Inventory
- (IA-2) Identifies and Authenticates Users (or processes on behalf of users)
- (IA-3) Device ID and authN
- (IA-4) Identifier Management
- (IA-5) Authenticator Management, chain of custody
- (PM-5) System Inventory
- (PM-23) Data Governance
- (PM-31) Continuous Monitoring
- (SA-3) System Development Lifecycle
- (SA-8) Security Engineering Principles
- (SA-10) Developer Configuration Management
- (SA-15) Standardized Tools and Processes
- (SI-4) Monitoring, Centralized Logging

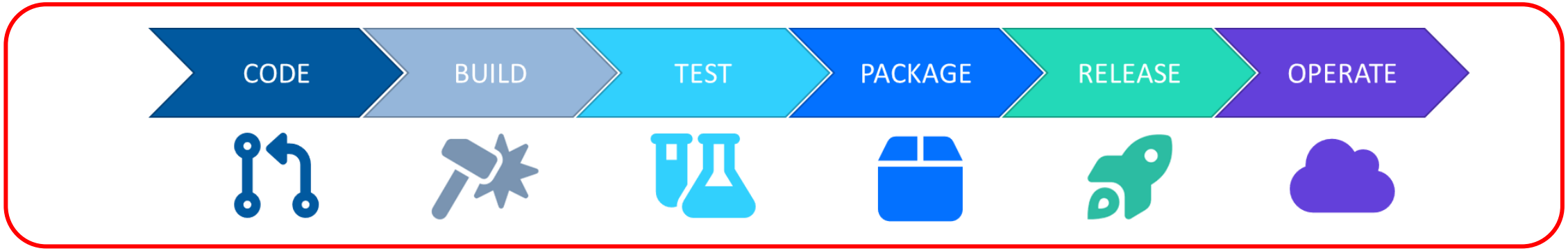

THE WALL STREET JOURNAL.
TECH
Secret World of Pro-Russia Hacking Group Exposed in Leak
A Ukrainian researcher revealed the operations of Trickbot, one of the most
bercriminal enterprises
with its Conti ransomware, after the group defended Russia; chats range from hospital attack plan to hackers

Screenshot

Software Supply Chain – The Risks

- Exposed Credentials
- Compromised OSS
- Code Injection, Theft, and Tampering
- Malicious Use of Interactive Access

- Stolen Access Keys
- Hijacked Compute/Resources
- Exposed Data
- Stolen IP



CI/CD

- Weak authentication
- Authentication fatigue
- Lack of credential rotation
- Lack of audit
- Over-permissioning

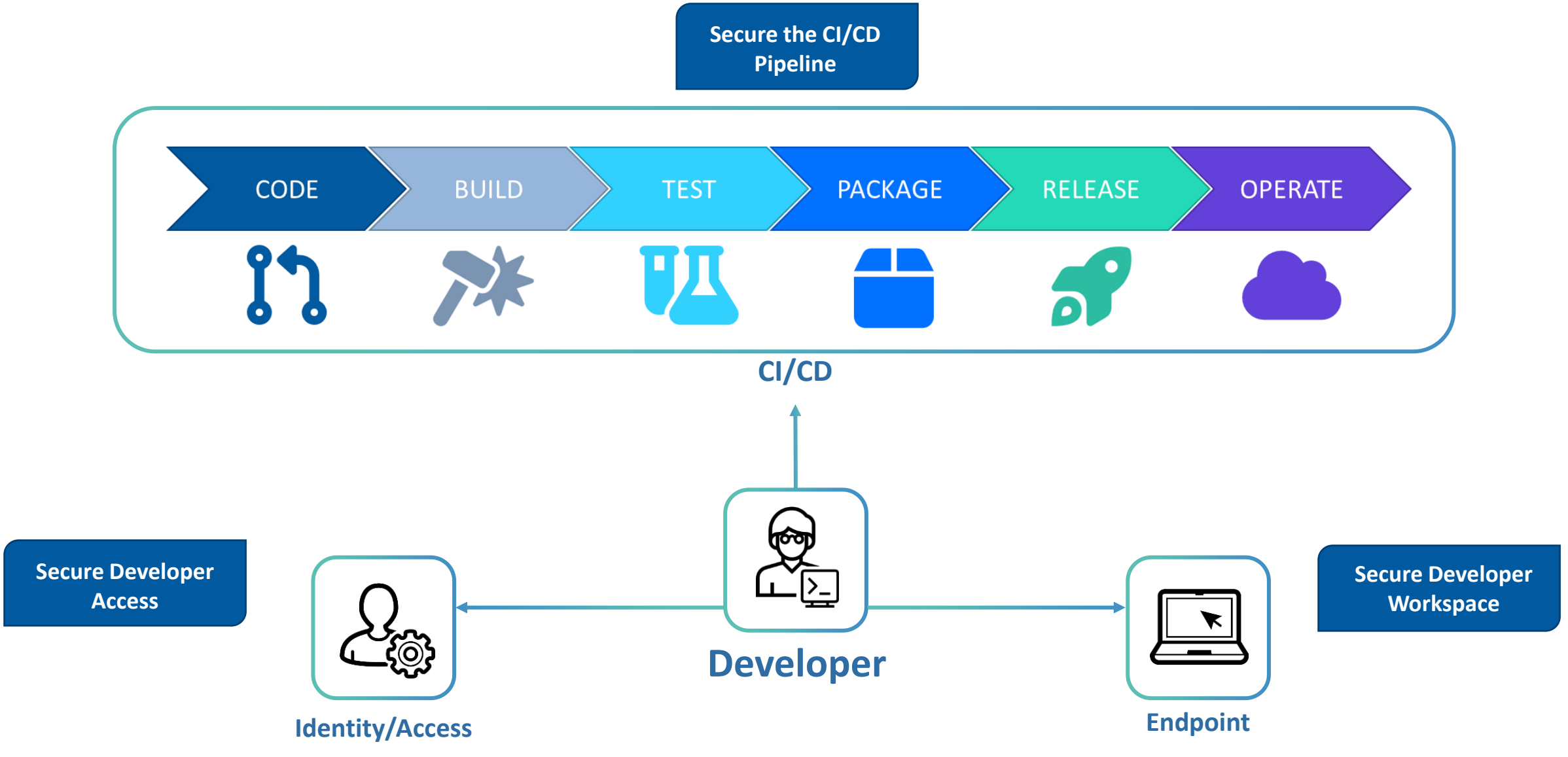
Identity/Access

Developer

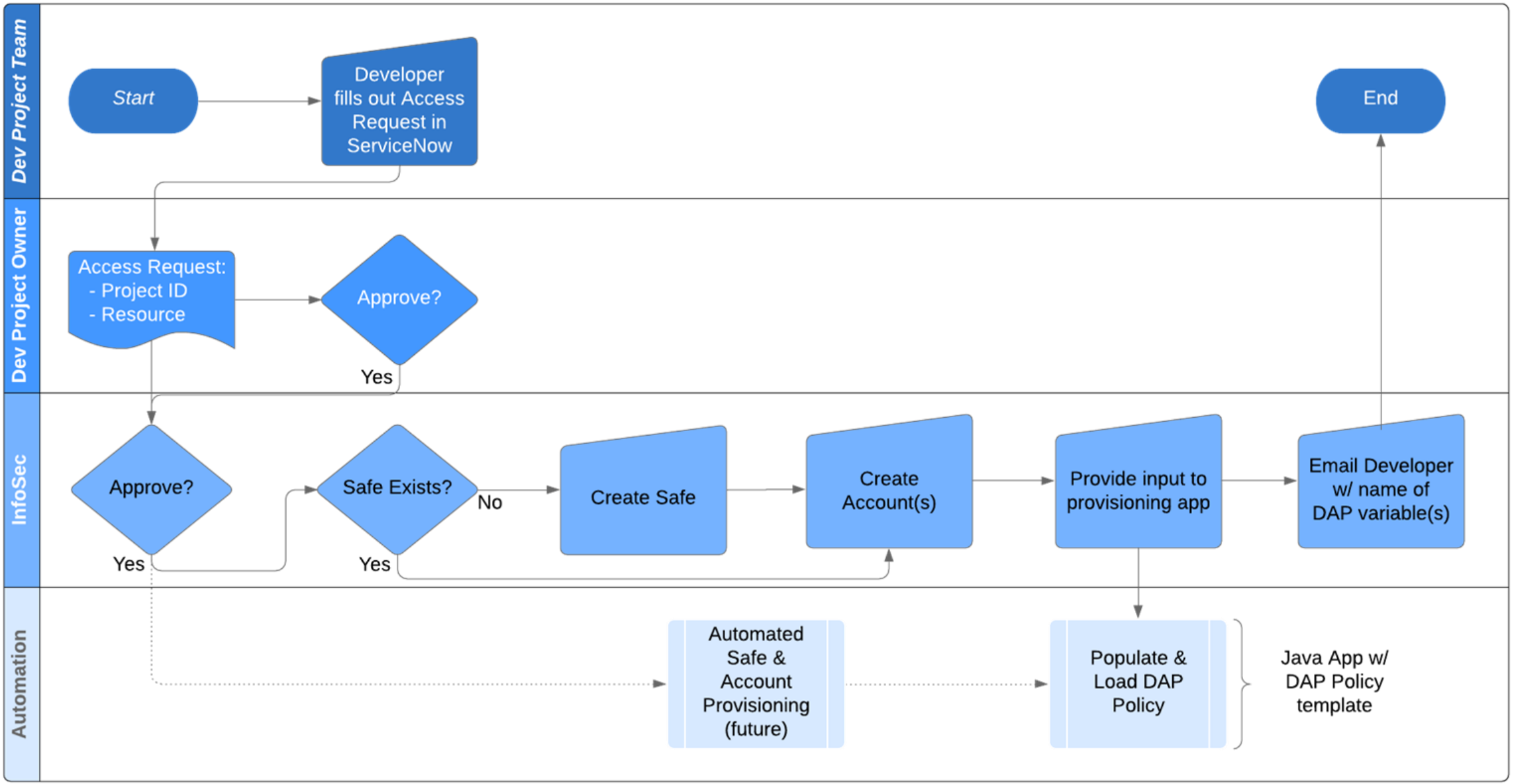
Endpoint

- Local admin rights
- Credential theft risk
- High variability of unknown applications
- Relaxed security policy

Securing the Software Supply Chain

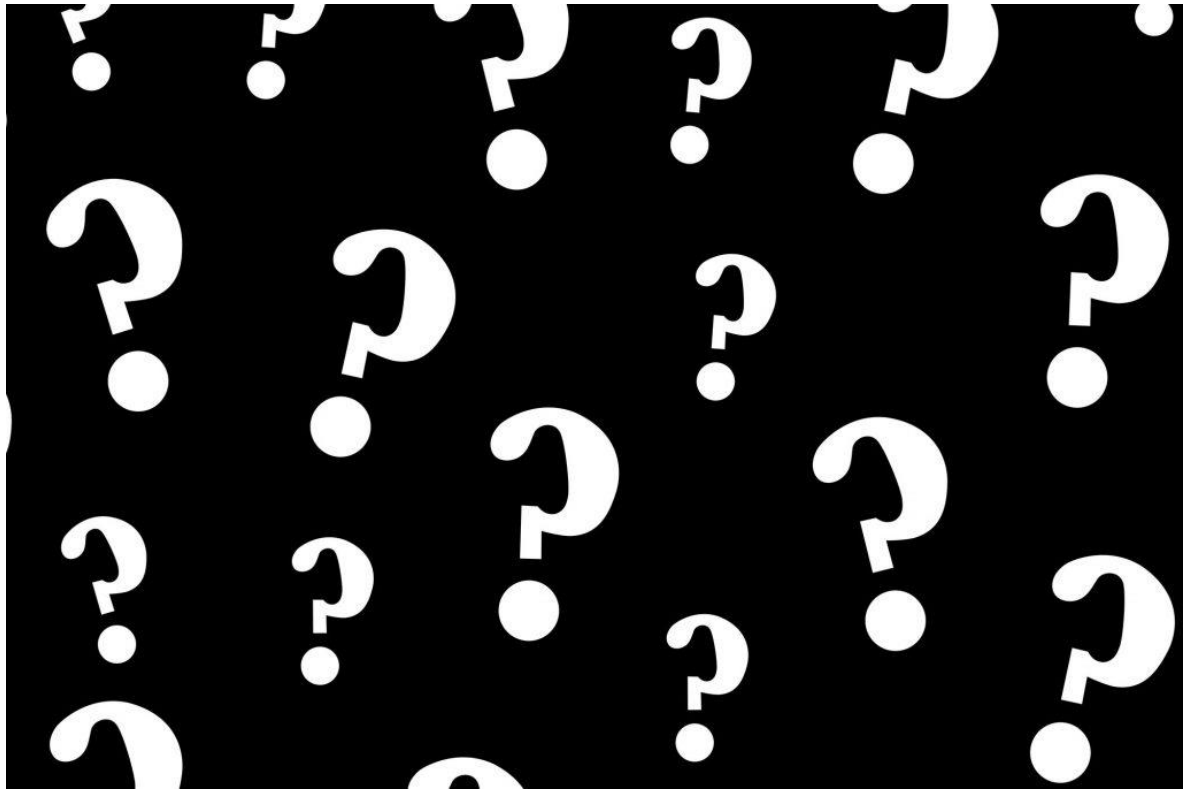


Example: Security-owned Provisioning Workflow



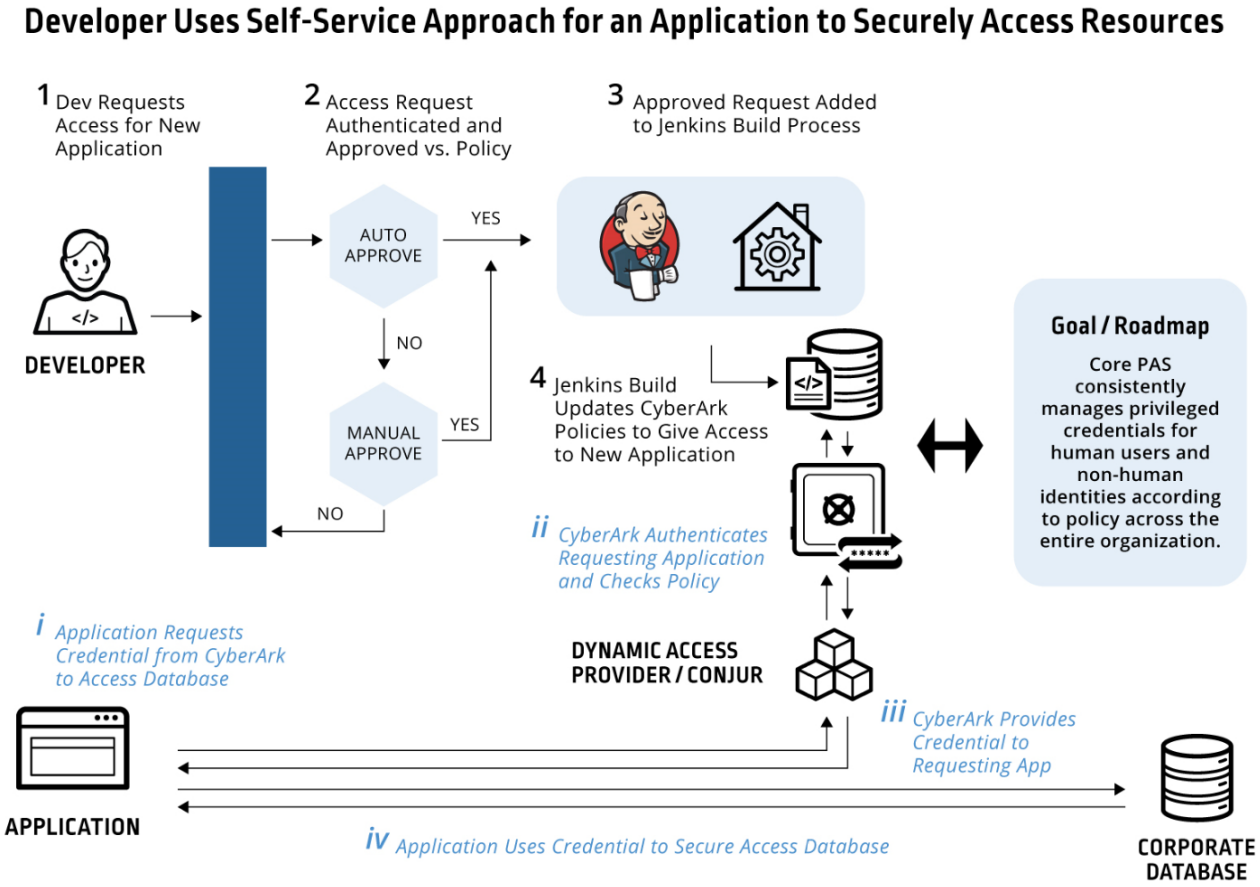
So What Are a Few Questions to Ask?

- Where are the Application Credentials Stored?
- If a secrets management type solution is utilized, who owns it? (Development, Security, Ops) SOD?
- How Is Access to the Secrets Managed?
- How is Access limited across the organization?
- How Do The Applications Authenticate to Retrieve the Secrets?
- How Frequently are the credentials rotated? If the credentials are dynamic what is the Time To Live?
- How is credential retrieval and change audited?



Leading Big Box Retailer

Security works with developers on self-service for secure app access to databases



- **Objective**
  - Shrink attack surface and meet rigorous audit requirements imposed after prior breach
  - Establish an enterprise-wide solution for human and non-human credentials
  - Enable lean security team's approval process to scale for thousands of developers
- **Approach**
  - Enable self-service provisioning for typical requests and route exceptions to the security team.
  - Automatically update secrets manager policies to give apps secure access to resources
  - Leverage PAM to protect human credentials
- **Result/Outcome**
  - Successfully rolling out across org.

Two Sides of the Same Coin (Revisited)

Bill

- Has a Defined Role
- Requires Access to Accomplish Role
- Activity Must be Audited
- Warm and friendly

Application Node WA113

- Have a Defined Role
- Requires Access to Accomplish Role
- Activity Must be Audited
- Warm and Friendly

Q&A