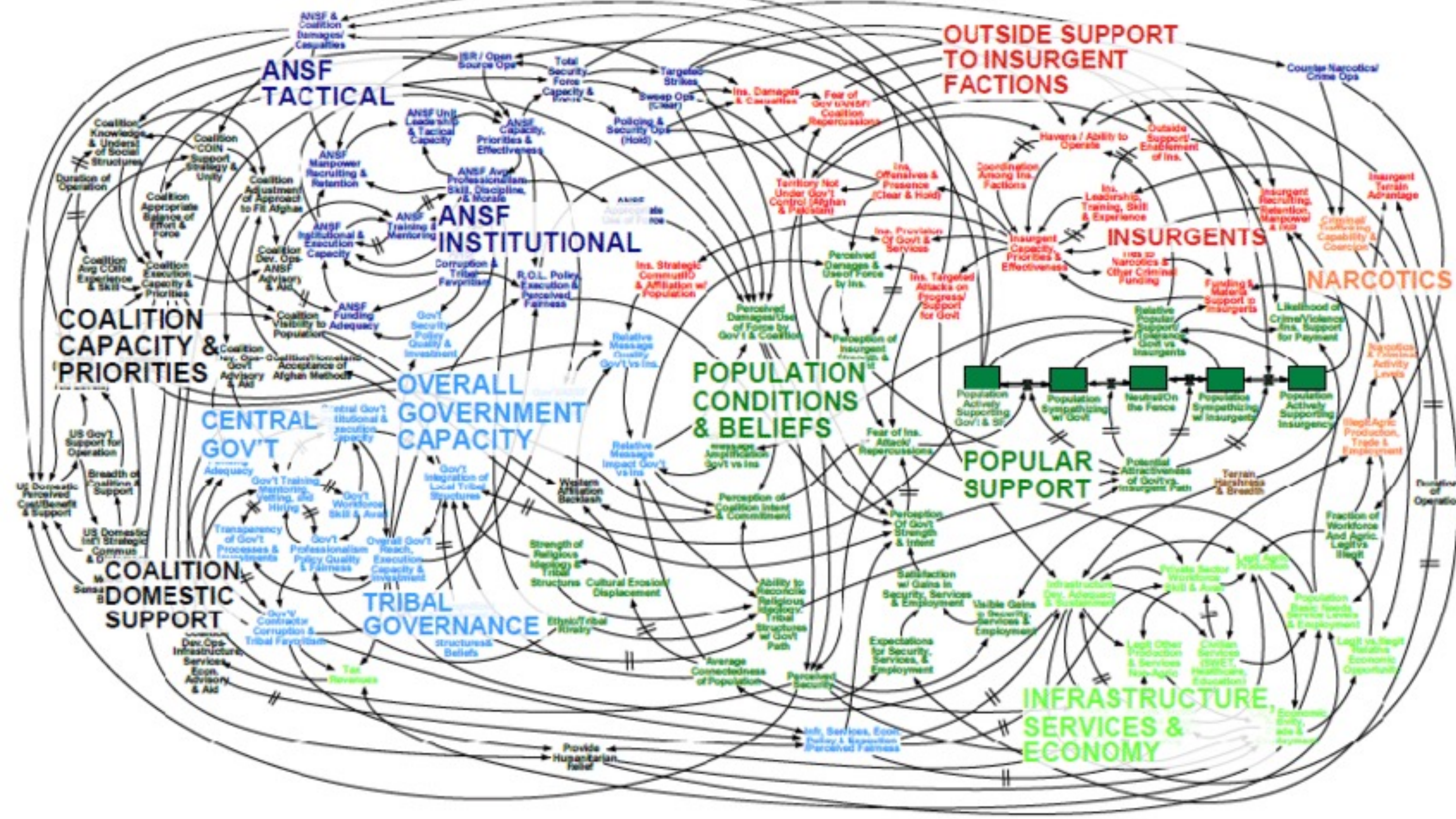
Complexity is the Enemy of Security Take it Out

Steve Winterfeld
Advisory CISO
Akamai

Akamai
Experience the Edge

“Talent wins games, but teamwork and intelligence win championships.”
Michael Jordan


ANSF TACTICAL
ANSF INSTITUTIONAL
OUTSIDE SUPPORT TO INSURGENT FACTIONS
INSURGENTS
NARCOTICS
COALITION CAPACITY & PRIORITIES
OVERALL GOVERNMENT CAPACITY
CENTRAL GOV'T
POPULATION CONDITIONS & BELIEFS
POPULAR SUPPORT
COALITION DOMESTIC SUPPORT
TRIBAL GOVERNANCE
INFRASTRUCTURE, SERVICES & ECONOMY
ANSF & Coalition Damages/ Casualties
ISR / Open Source Ops
Targeted Strikes
Sweep Ops (Clear)
Policing & Security Ops (Hold)
Counter Narcotics/ Crime Ops
Havens / Ability to Operate
Insurgent Terrain Advantage
Population Actively Supporting Gov't & SF
Population Sympathizing w/ Gov't
Neutral/On the Fence
Population Sympathizing w/ Insurgents
Population Actively Supporting Insurgency
Perception of Coalition Intent & Commitment
Perceived Security
Provide Humanitarian Relief
Tax Revenues
Ethnic/Tribal Rivalry
Cultural Erosion/ Displacement

RSA 2023

599 Speakers

605 Vendors

76 ?

RSAConference2023

San Francisco | April 24 – 27 | Moscone Center

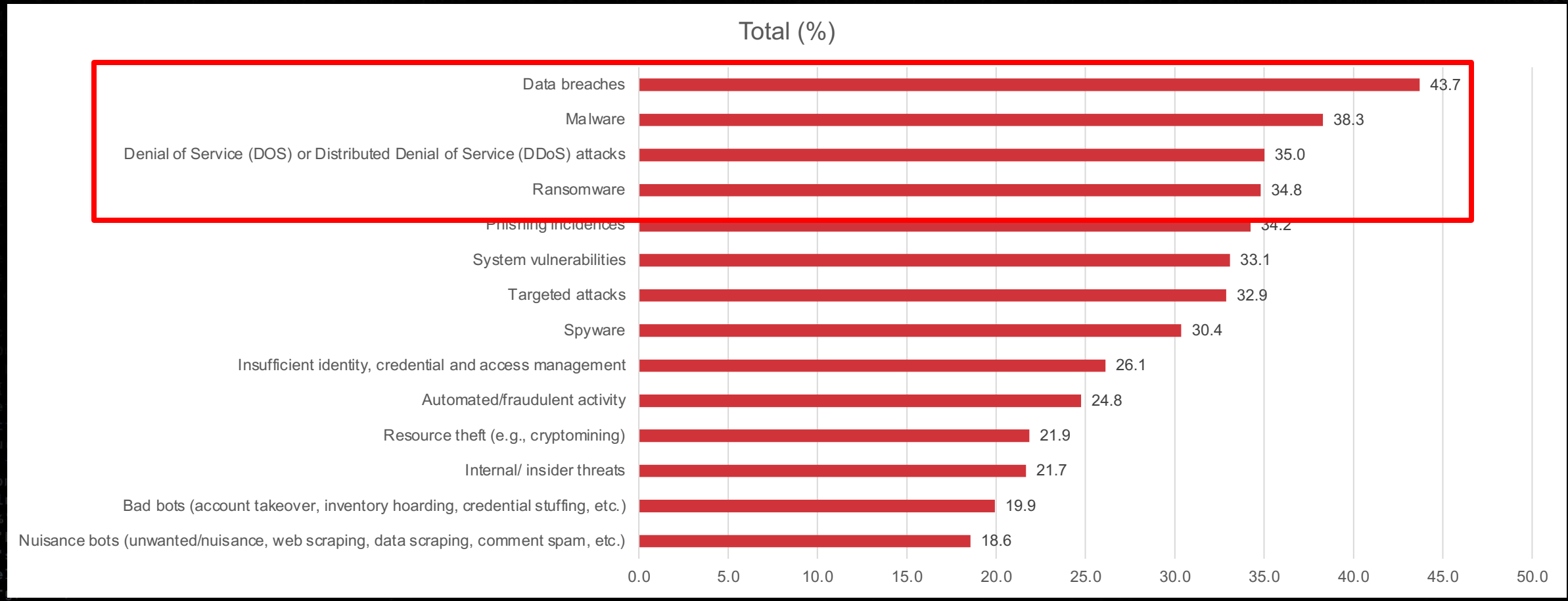
1/19/2023

SOUTH EXPO

Goals for Transformation

- Faster
- Better
- Cheaper
- Secure

Triple Extortion Threat
Immediate Impacts

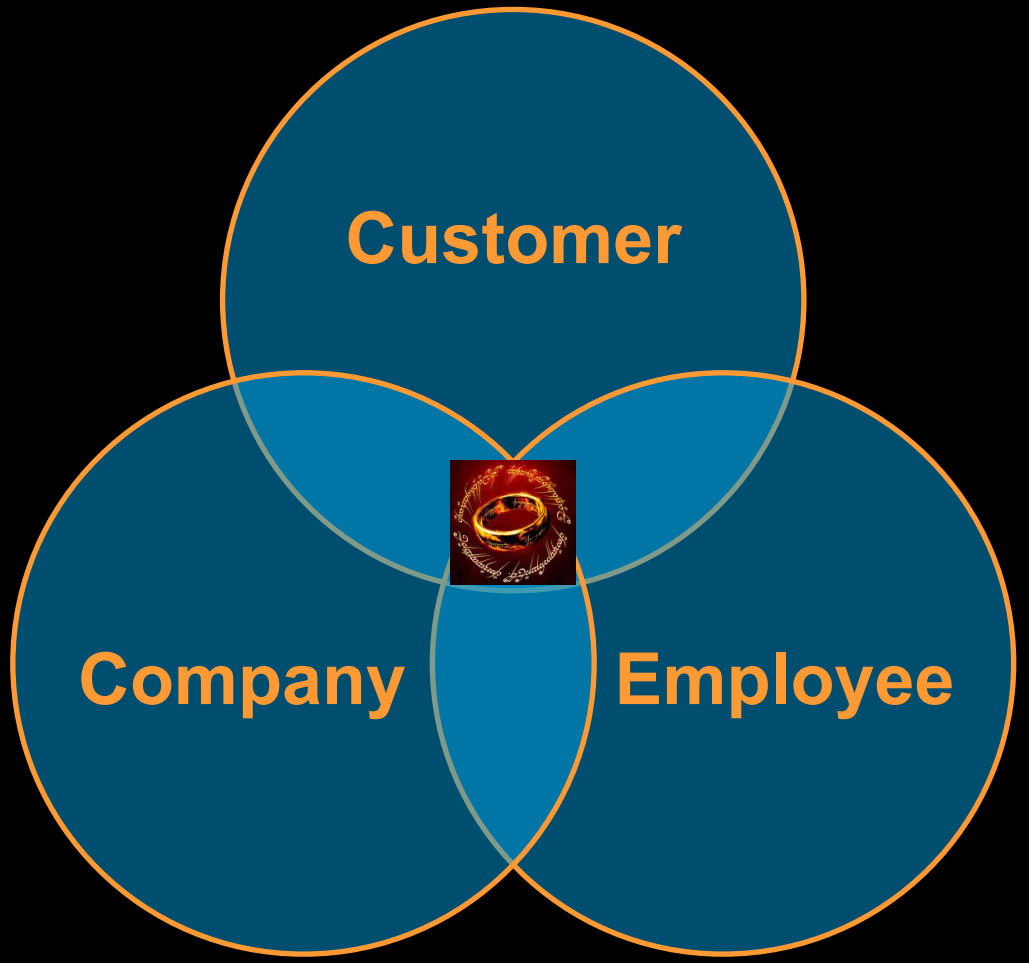


Source: Global – Outsourced Cybersecurity Services (MSS, MDR, DDoS) Survey, IDC, December, 2021

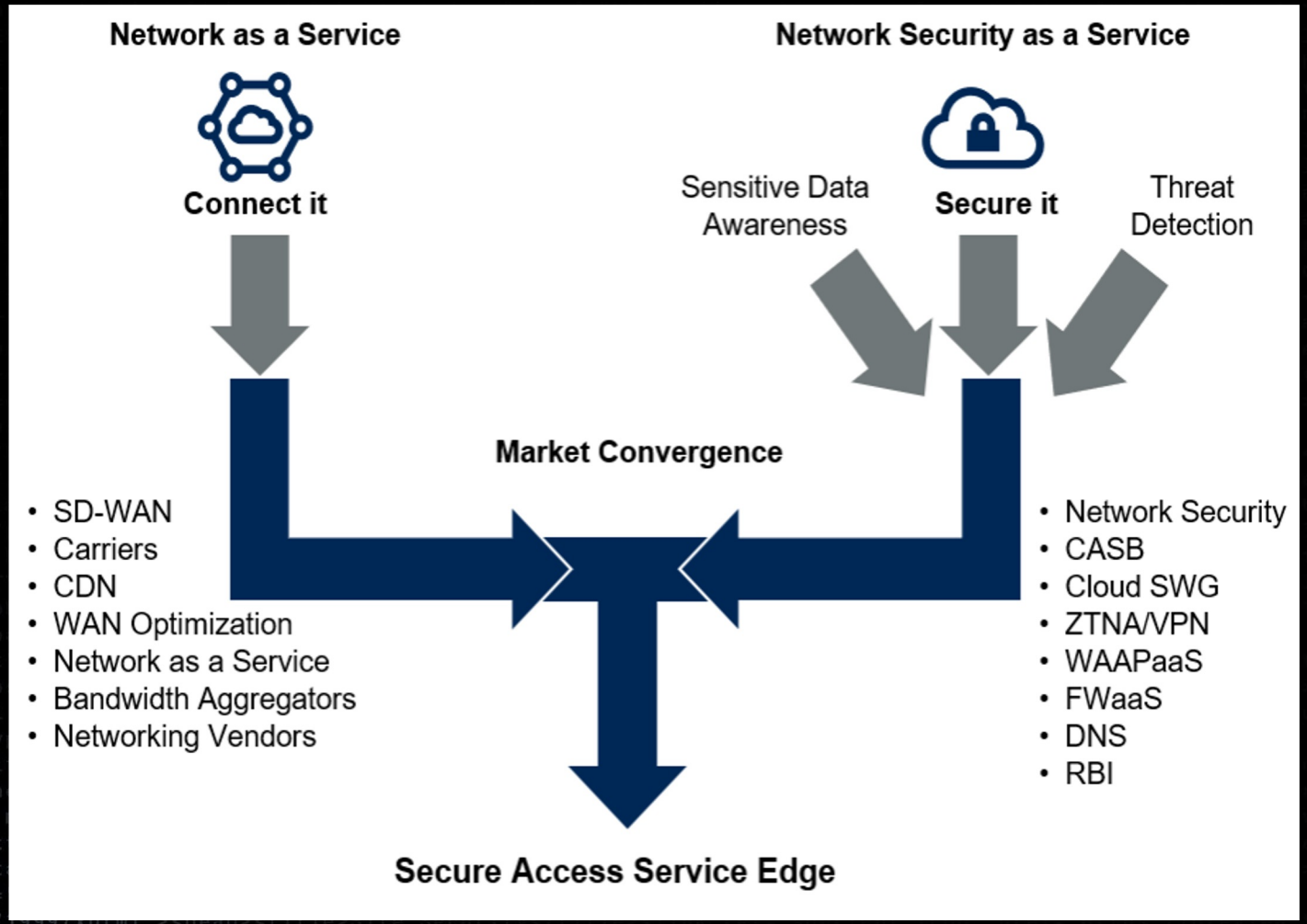
Environment components

North-South

East-West



Future of Network Security Is in the Cloud

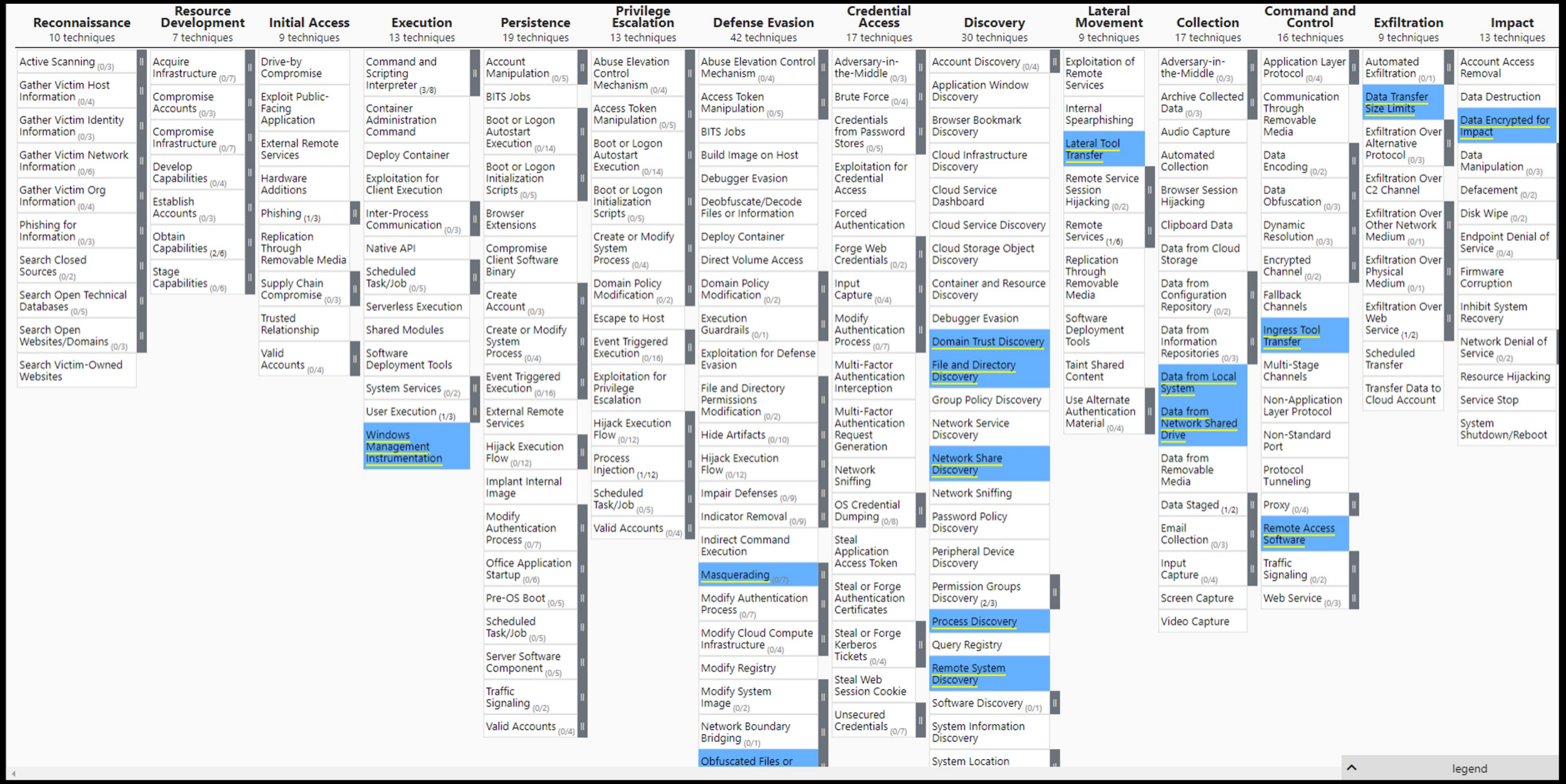


Benefits:

- Reduce complexity
- Simplify vendor management

Zero Trust Edge

MITRE ATT&CK


Reconnaissance
10 techniques
Active Scanning (0/3)
Gather Victim Host Information (0/4)
Gather Victim Identity Information (0/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (0/3)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/3)
Search Victim-Owned Websites
Resource Development
7 techniques
Acquire Infrastructure (0/7)
Compromise Accounts (0/3)
Compromise Infrastructure (0/7)
Develop Capabilities (0/4)
Establish Accounts (0/3)
Obtain Capabilities (2/6)
Stage Capabilities (0/6)
Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (1/3)
Replication Through Removable Media
Supply Chain Compromise (0/3)
Trusted Relationship
Valid Accounts (0/4)
Execution
13 techniques
Command and Scripting Interpreter (3/8)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (0/3)
Native API
Scheduled Task/Job (0/5)
Serverless Execution
Shared Modules
Software Deployment Tools
System Services (0/2)
User Execution (1/3)
Windows Management Instrumentation
Persistence
19 techniques
Account Manipulation (0/5)
BITS Jobs
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Browser Extensions
Compromise Client Software Binary
Create Account (0/3)
Create or Modify System Process (0/4)
Event Triggered Execution (0/16)
External Remote Services
Hijack Execution Flow (0/12)
Implant Internal Image
Modify Authentication Process (0/7)
Office Application Startup (0/6)
Pre-OS Boot (0/5)
Scheduled Task/Job (0/5)
Server Software Component (0/5)
Traffic Signaling (0/2)
Valid Accounts (0/4)
Privilege Escalation
13 techniques
Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Create or Modify System Process (0/4)
Domain Policy Modification (0/2)
Escape to Host
Event Triggered Execution (0/16)
Exploitation for Privilege Escalation
Hijack Execution Flow (0/12)
Process Injection (1/12)
Scheduled Task/Job (0/5)
Valid Accounts (0/4)
Defense Evasion
42 techniques
Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (0/2)
Execution Guardrails (0/1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Hide Artifacts (0/10)
Hijack Execution Flow (0/12)
Impair Defenses (0/9)
Indicator Removal (0/9)
Indirect Command Execution
Masquerading (0/7)
Modify Authentication Process (0/7)
Modify Cloud Compute Infrastructure (0/4)
Modify Registry
Modify System Image (0/2)
Network Boundary Bridging (0/1)
Obfuscated Files or
Credential Access
17 techniques
Adversary-in-the-Middle (0/3)
Brute Force (0/4)
Credentials from Password Stores (0/5)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (0/2)
Input Capture (0/4)
Modify Authentication Process (0/7)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (0/8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (0/4)
Steal Web Session Cookie
Unsecured Credentials (0/7)
Discovery
30 techniques
Account Discovery (0/4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (2/3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (0/1)
System Information Discovery
System Location
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (0/2)
Remote Services (1/6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (0/4)
Collection
17 techniques
Adversary-in-the-Middle (0/3)
Archive Collected Data (0/3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (0/2)
Data from Information Repositories (0/3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (1/2)
Email Collection (0/3)
Input Capture (0/4)
Screen Capture
Video Capture
Command and Control
16 techniques
Application Layer Protocol (0/4)
Communication Through Removable Media
Data Encoding (0/2)
Data Obfuscation (0/3)
Dynamic Resolution (0/3)
Encrypted Channel (0/2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (0/4)
Remote Access Software
Traffic Signaling (0/2)
Web Service (0/3)
Exfiltration
9 techniques
Automated Exfiltration (0/1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (0/3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (0/1)
Exfiltration Over Physical Medium (0/1)
Exfiltration Over Web Service (1/2)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
13 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (0/3)
Defacement (0/2)
Disk Wipe (0/2)
Endpoint Denial of Service (0/4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (0/2)
Resource Hijacking
Service Stop
System Shutdown/Reboot
legend

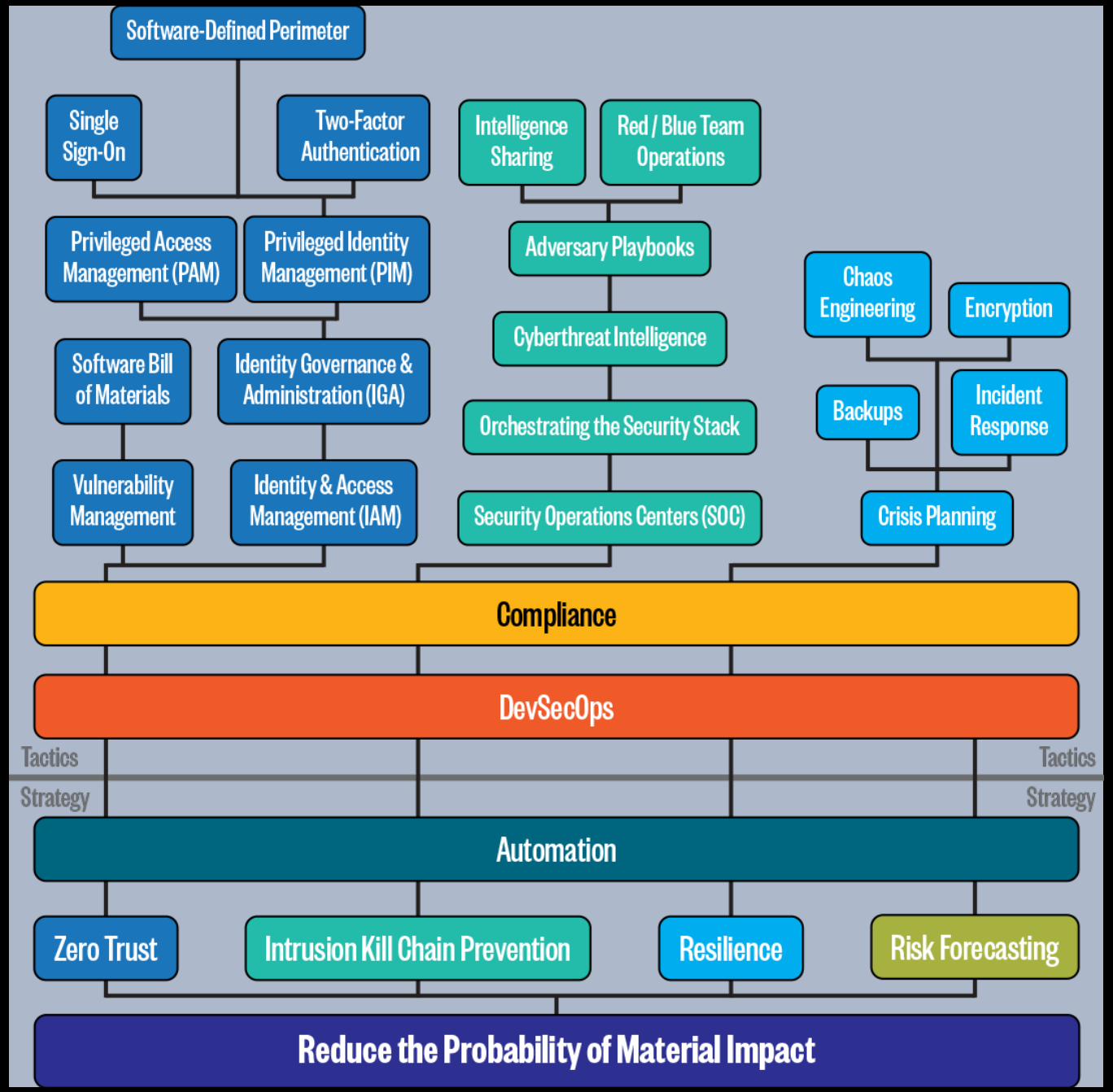
What are the risks and impacts

- Operational
- Brand / Trust
- Compliance
- Revenue

Focus on material impacts

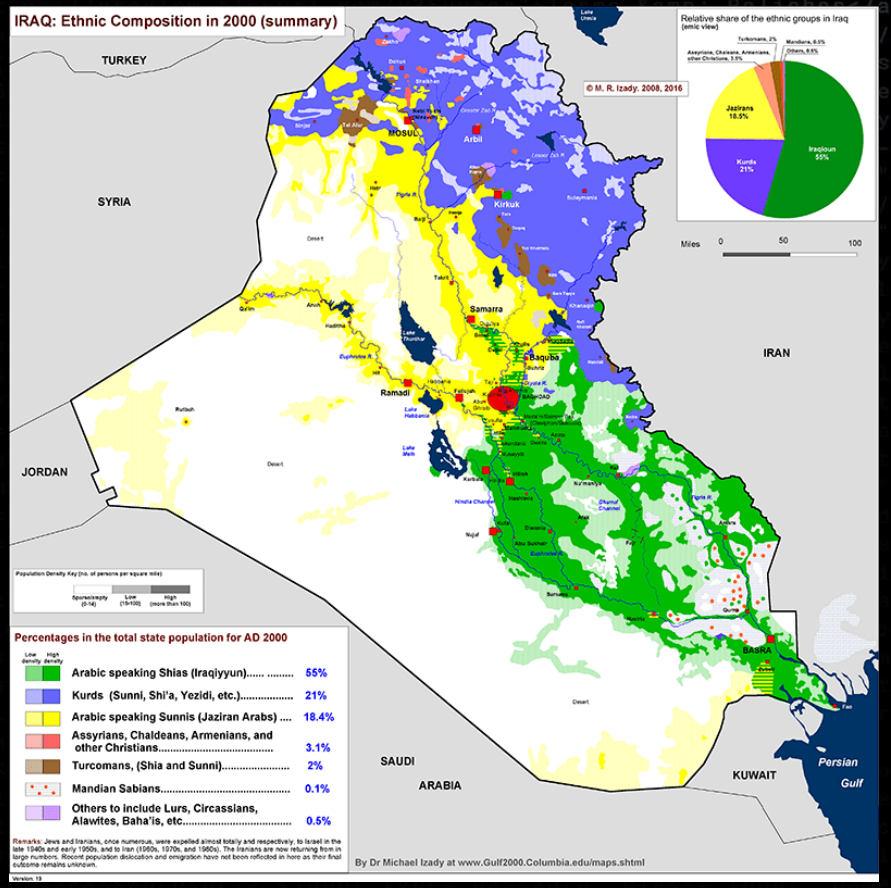
Reduce the probability of material impact due to a cyber event over the next three years

From: Cyber First Principles



The journey

- Framework vs Guiding Principle
- Culture (in house vs managed)
- Reduce tools + tech dept > automate
- Compliance (byproduct)



KISS (keep it simple stupid)

Next steps

- Consolidate tools
- Optimize current capabilities
- Solve with current partners
- Buy tools that play well with others

Tech / Process / People

Akamai Threat Hub:

www.akamai.com/our-thinking/threat-research


Akamai
Power and protect
life online

Notes

- Mindset What is next step
- Exercise
- Why does is happen – entropy
- Use case – M&A
- Models hide complexity