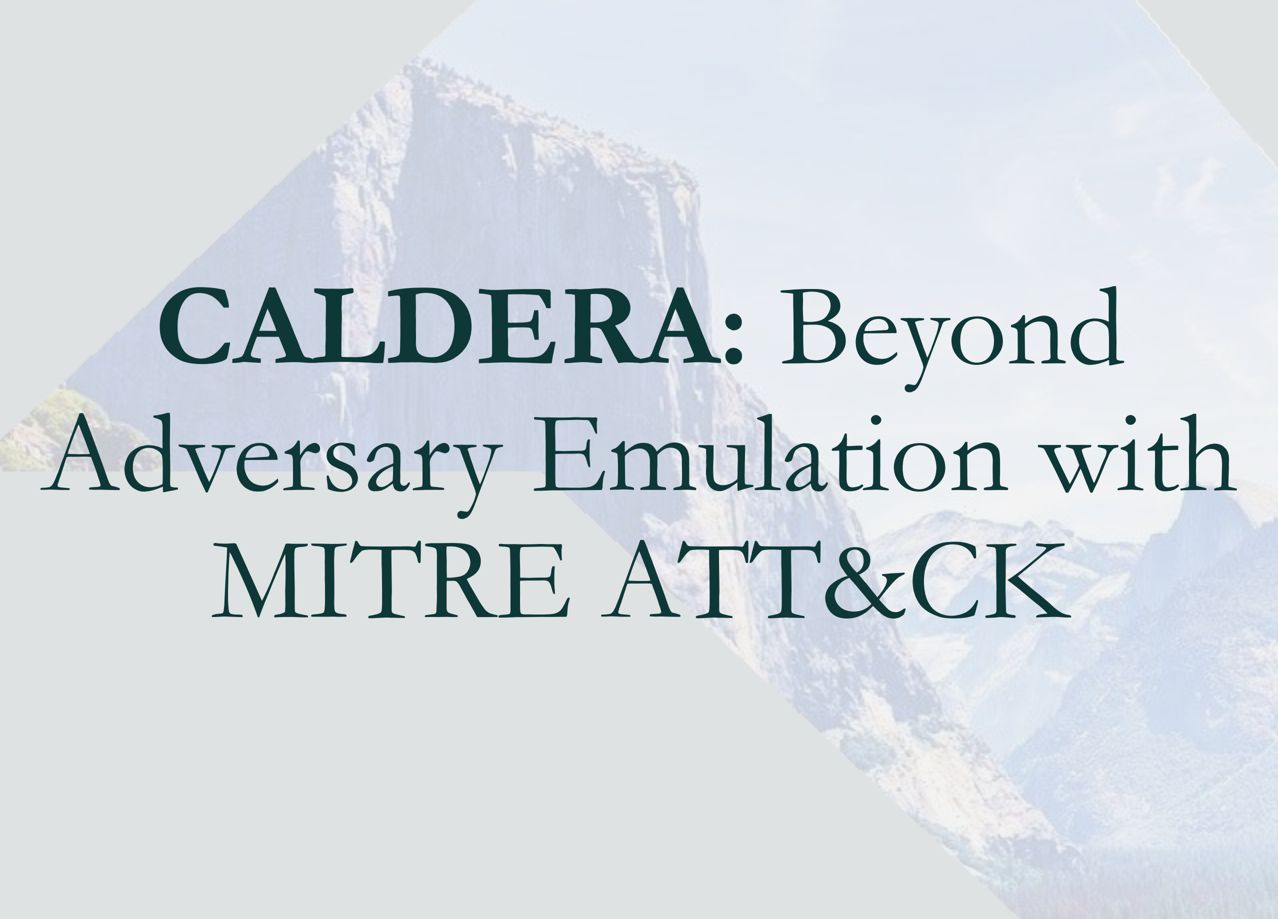
# **CALDERA:** Beyond Adversary Emulation with MITRE ATT&CK

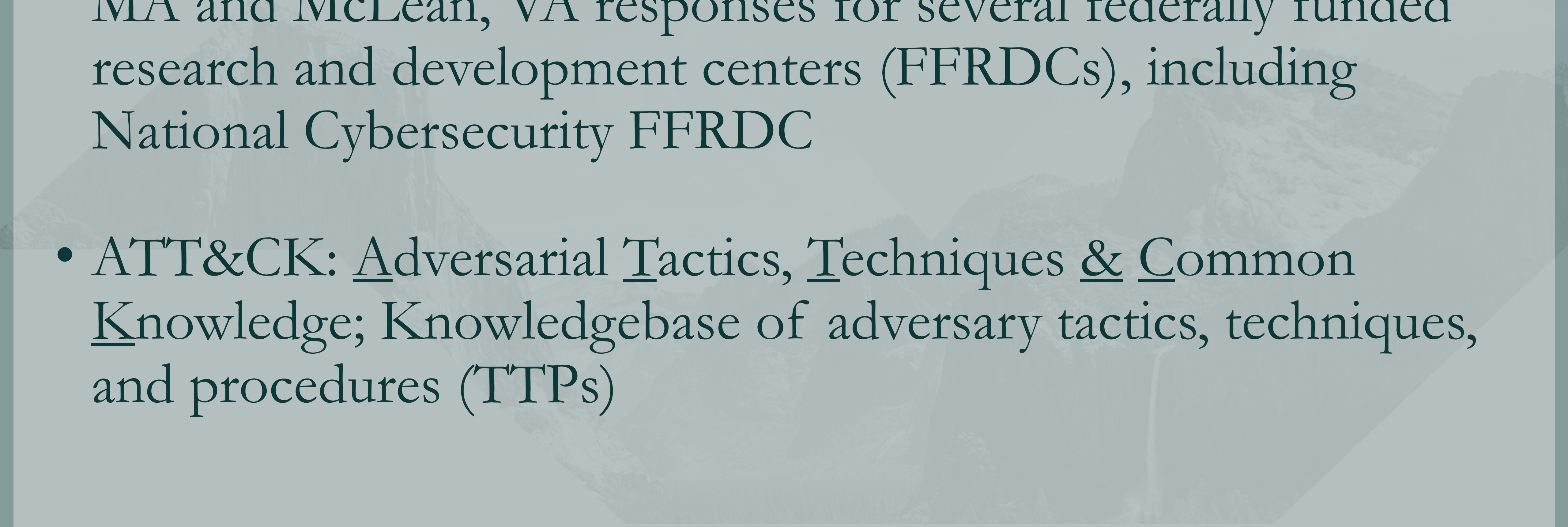


# Agenda

- ATT&CK
- CALDERA
- Collaboration

# ATT&CK

# Background and Context



- MITRE: Not-for-profit corporation with offices in Bedford, MA and McLean, VA responses for several federally funded research and development centers (FFRDCs), including National Cybersecurity FFRDC

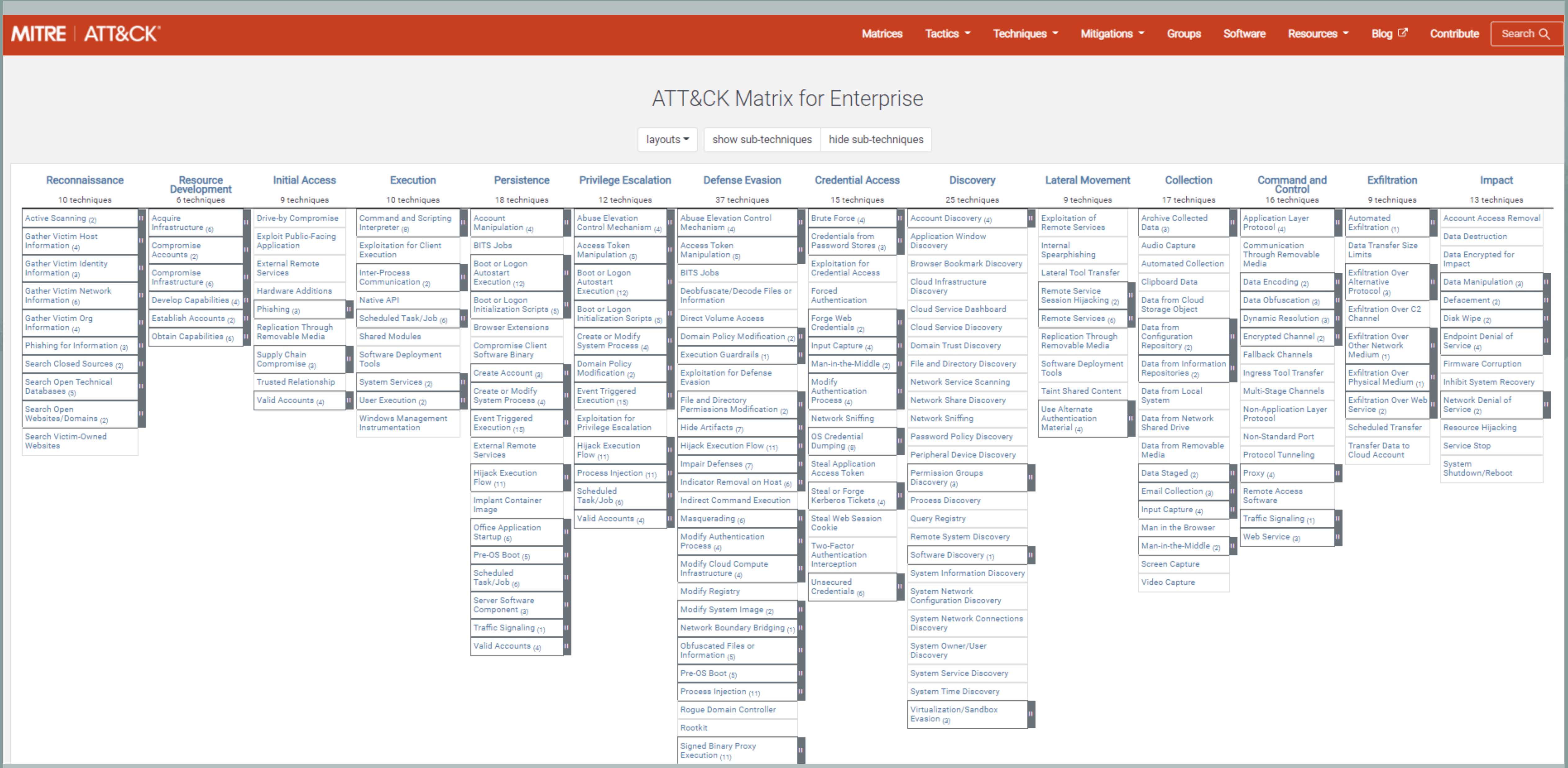
- ATT&CK: Adversarial Tactics, Techniques & Common Knowledge; Knowledgebase of adversary tactics, techniques, and procedures (TTPs)

# Background and Context

- Improved consistency of language used to describe malicious activities
- Focus on observable behaviors
- Knowledgebase includes explanations of TTPs, examples of uses, options for mitigation, options for detection, and references
- Separate matrices based on use cases/environment

Enterprise
PRE
Windows
macOS
Linux
Cloud
AWS
GCP
Azure
Office 365
Azure AD
SaaS
Network
Mobile
Android
iOS
ICS

# Background and Context



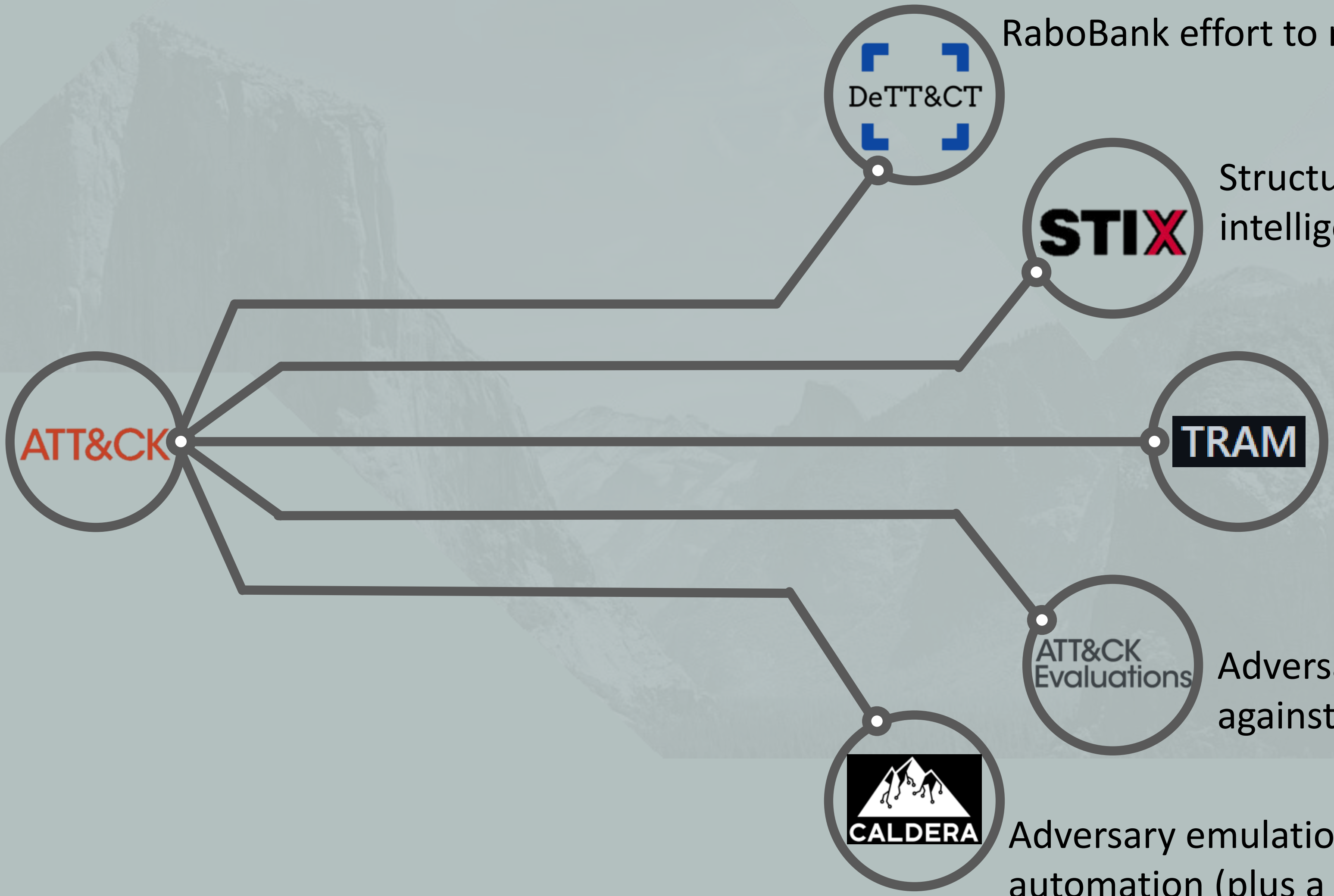
ATT&CK Matrix for Enterprise

| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 techniques | 6 techniques | 9 techniques | 10 techniques | 18 techniques | 12 techniques | 37 techniques | 15 techniques | 25 techniques | 9 techniques | 17 techniques | 16 techniques | 9 techniques | 13 techniques |
| Active Scanning (2) | Acquire Infrastructure (6) | Drive-by Compromise | Command and Scripting Interpreter (8) | Account Manipulation (4) | Abuse Elevation Control Mechanism (4) | Abuse Elevation Control Mechanism (4) | Brute Force (4) | Account Discovery (4) | Exploitation of Remote Services | Archive Collected Data (3) | Application Layer Protocol (4) | Automated Exfiltration (1) | Account Access Removal |
| Gather Victim Host Information (4) | Compromise Accounts (2) | Exploit Public-Facing Application | Exploitation for Client Execution | BITS Jobs | Access Token Manipulation (5) | Access Token Manipulation (5) | Credentials from Password Stores (3) | Application Window Discovery | Internal Spearphishing | Audio Capture | Communication Through Removable Media | Data Transfer Size Limits | Data Destruction |
| Gather Victim Identity Information (3) | Compromise Infrastructure (6) | External Remote Services | Inter-Process Communication (2) | Boot or Logon Autostart Execution (12) | Boot or Logon Autostart Execution (12) | BITS Jobs | Exploitation for Credential Access | Browser Bookmark Discovery | Lateral Tool Transfer | Automated Collection | Data Encoding (2) | Exfiltration Over Alternative Protocol (3) | Data Encrypted for Impact |
| Gather Victim Network Information (6) | Develop Capabilities (4) | Hardware Additions | Native API | Boot or Logon Initialization Scripts (5) | Boot or Logon Initialization Scripts (5) | Deobfuscate/Decode Files or Information | Forced Authentication | Cloud Infrastructure Discovery | Remote Service Session Hijacking (2) | Clipboard Data | Data Obfuscation (3) | Exfiltration Over C2 Channel | Data Manipulation (3) |
| Gather Victim Org Information (4) | Establish Accounts (2) | Phishing (3) | Scheduled Task/Job (6) | Browser Extensions | Create or Modify System Process (4) | Direct Volume Access | Forge Web Credentials (2) | Cloud Service Dashboard | Remote Services (6) | Data from Cloud Storage Object | Dynamic Resolution (3) | Exfiltration Over Other Network Medium (1) | Defacement (2) |
| Phishing for Information (3) | Obtain Capabilities (6) | Replication Through Removable Media | Shared Modules | Compromise Client Software Binary | Domain Policy Modification (2) | Domain Policy Modification (2) | Input Capture (4) | Cloud Service Discovery | Replication Through Removable Media | Data from Configuration Repository (2) | Encrypted Channel (2) | Exfiltration Over Physical Medium (1) | Disk Wipe (2) |
| Search Closed Sources (2) | | Supply Chain Compromise (3) | Software Deployment Tools | Create Account (3) | Event Triggered Execution (15) | Execution Guardrails (1) | Man-in-the-Middle (2) | Domain Trust Discovery | Software Deployment Tools | Data from Information Repositories (2) | Fallback Channels | Exfiltration Over Web Service (2) | Endpoint Denial of Service (4) |
| Search Open Technical Databases (5) | | Trusted Relationship | System Services (2) | Create or Modify System Process (4) | Exploitation for Privilege Escalation | Exploitation for Defense Evasion | Modify Authentication Process (4) | File and Directory Discovery | Taint Shared Content | Data from Local System | Ingress Tool Transfer | Scheduled Transfer | Firmware Corruption |
| Search Open Websites/Domains (2) | | Valid Accounts (4) | User Execution (2) | Event Triggered Execution (15) | Hijack Execution Flow (11) | File and Directory Permissions Modification (2) | Network Sniffing | Network Service Scanning | Use Alternate Authentication Material (4) | Data from Network Shared Drive | Multi-Stage Channels | Transfer Data to Cloud Account | Inhibit System Recovery |
| Search Victim-Owned Websites | | | Windows Management Instrumentation | External Remote Services | Process Injection (11) | Hide Artifacts (7) | OS Credential Dumping (8) | Network Share Discovery | | Data from Removable Media | Non-Application Layer Protocol | | Network Denial of Service (2) |
| | | | | Hijack Execution Flow (11) | Scheduled Task/Job (6) | Hijack Execution Flow (11) | Steal Application Access Token | Network Sniffing | | Data Staged (2) | Non-Standard Port | | Resource Hijacking |
| | | | | Implant Container Image | Valid Accounts (4) | Impair Defenses (7) | Steal or Forge Kerberos Tickets (4) | Password Policy Discovery | | Email Collection (3) | Protocol Tunneling | | Service Stop |
| | | | | Office Application Startup (6) | | Indicator Removal on Host (6) | Steal Web Session Cookie | Peripheral Device Discovery | | Input Capture (4) | Proxy (4) | | System Shutdown/Reboot |
| | | | | Pre-OS Boot (5) | | Indirect Command Execution | Two-Factor Authentication Interception | Permission Groups Discovery (3) | | Man in the Browser | Remote Access Software | | |
| | | | | Scheduled Task/Job (6) | | Masquerading (6) | Unsecured Credentials (6) | Process Discovery | | Man-in-the-Middle (2) | Traffic Signaling (1) | | |
| | | | | Server Software Component (3) | | Modify Authentication Process (4) | | Query Registry | | Screen Capture | Web Service (3) | | |
| | | | | Traffic Signaling (1) | | Modify Cloud Compute Infrastructure (4) | | Remote System Discovery | | Video Capture | | | |
| | | | | Valid Accounts (4) | | Modify Registry | | Software Discovery (1) | | | | | |
| | | | | | | Modify System Image (2) | | System Information Discovery | | | | | |
| | | | | | | Network Boundary Bridging (1) | | System Network Configuration Discovery | | | | | |
| | | | | | | Obfuscated Files or Information (5) | | System Network Connections Discovery | | | | | |
| | | | | | | Pre-OS Boot (5) | | System Owner/User Discovery | | | | | |
| | | | | | | Process Injection (11) | | System Service Discovery | | | | | |
| | | | | | | Rogue Domain Controller | | System Time Discovery | | | | | |
| | | | | | | Rootkit | | Virtualization/Sandbox Evasion (3) | | | | | |
| | | | | | | Signed Binary Proxy Execution (11) | | | | | | | |

# Expansion and Growth

- Rapidly expanded adoption
- Additional MITRE-sponsored projects
- ATT&CKCon and Power Hour presentations
- Expanded matrix/knowledgebase
- Increased depth of detail and correlation to threat actors

# Adjacent Efforts



RaboBank effort to measure and improve detection

Structured language for cyber threat intelligence

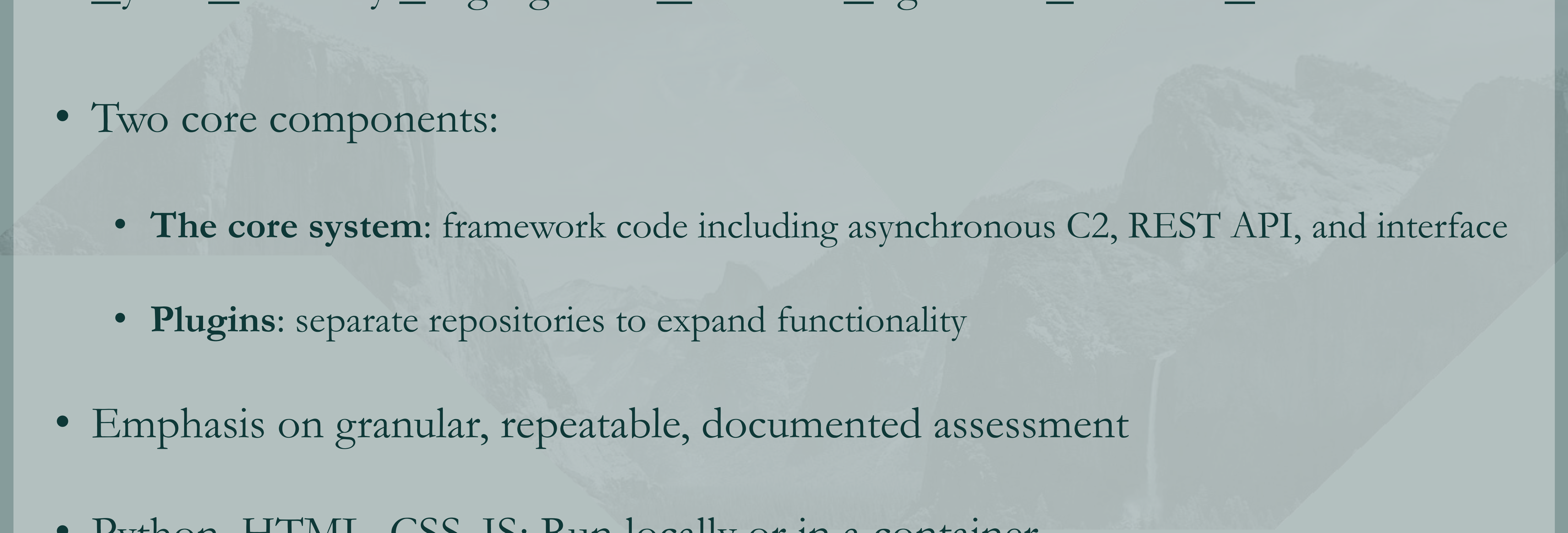
Threat Report ATT&CK Mapping

Adversary emulation campaigns against security products

Adversary emulation and red team automation (plus a LOT more)

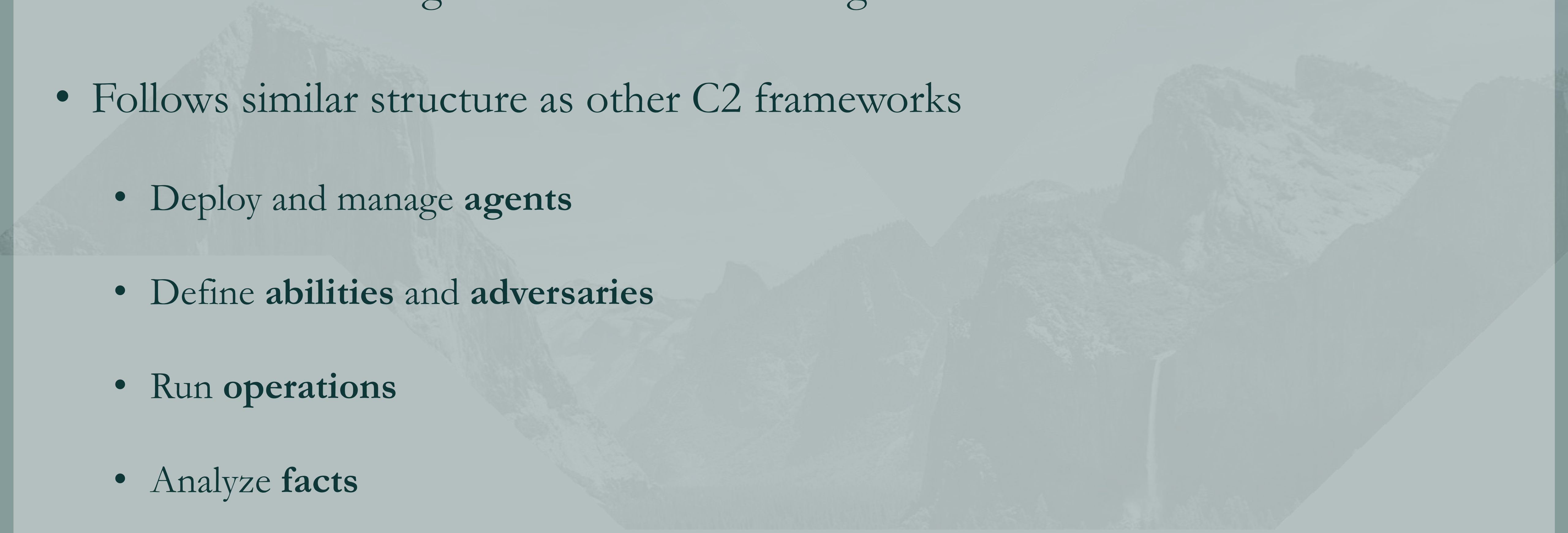
# CALDERA

# Concepts



- Cyber Adversary Language and Detection Engine for Red team Automation
- Two core components:
  - **The core system**: framework code including asynchronous C2, REST API, and interface
  - **Plugins**: separate repositories to expand functionality
- Emphasis on granular, repeatable, documented assessment
- Python, HTML, CSS, JS; Run locally or in a container

# Core Functionality

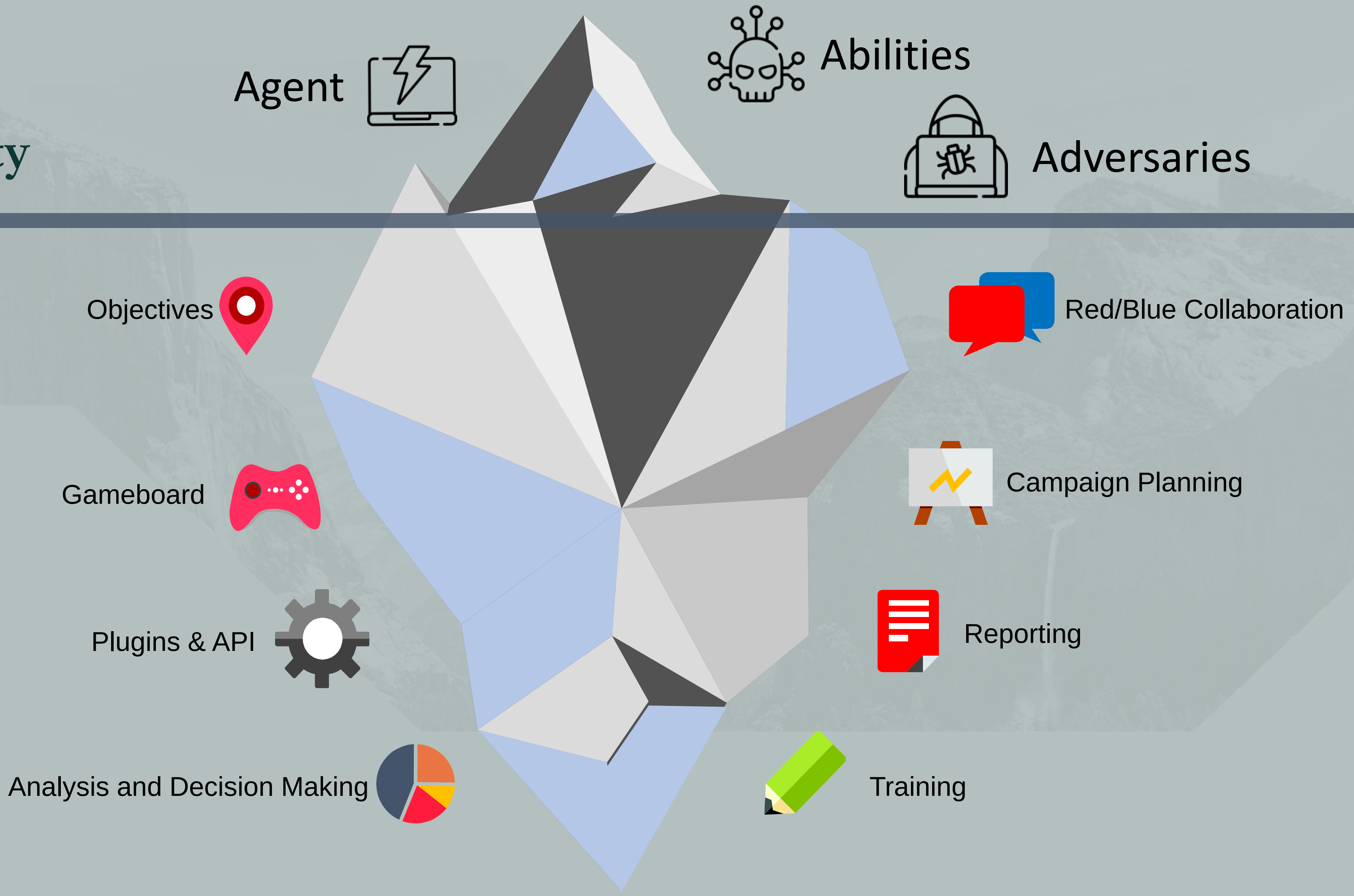


- C2 framework for granular offensive testing
- Follows similar structure as other C2 frameworks
  - Deploy and manage **agents**
  - Define **abilities** and **adversaries**
  - Run **operations**
  - Analyze **facts**

# Core Functionality

## Core Functionality

## True Capabilities



Agent

Abilities

Adversaries

Objectives

Red/Blue Collaboration

Gameboard

Campaign Planning

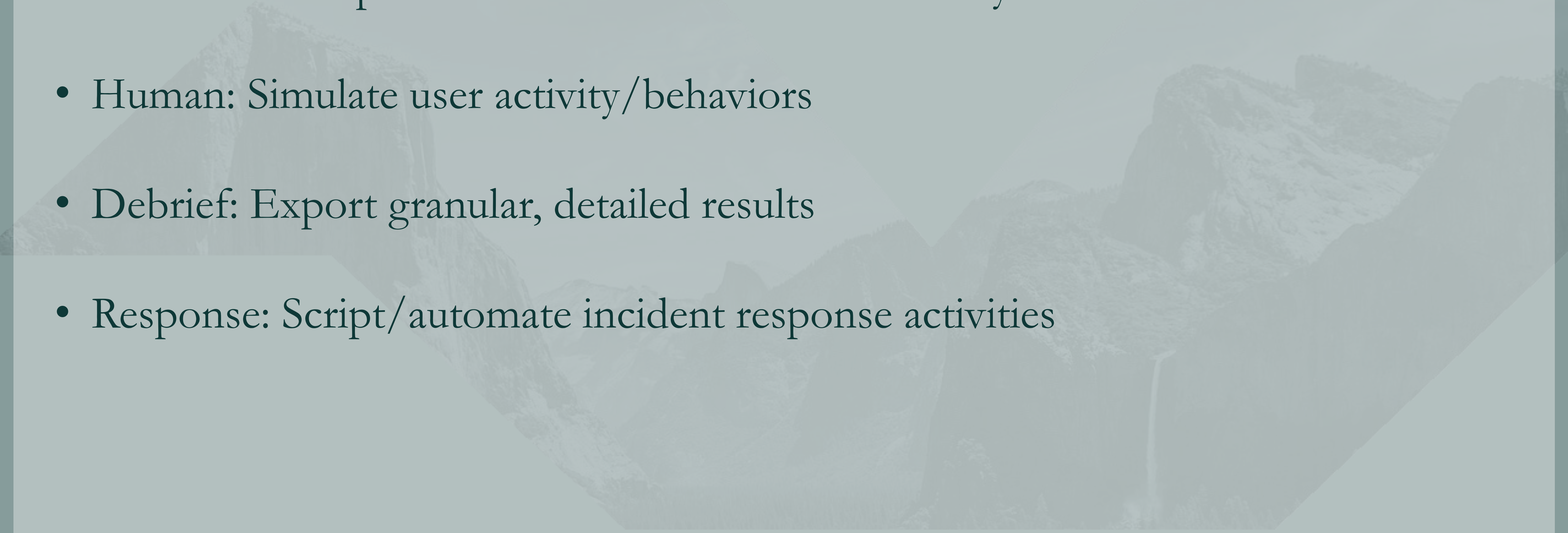
Plugins & API

Reporting

Analysis and Decision Making

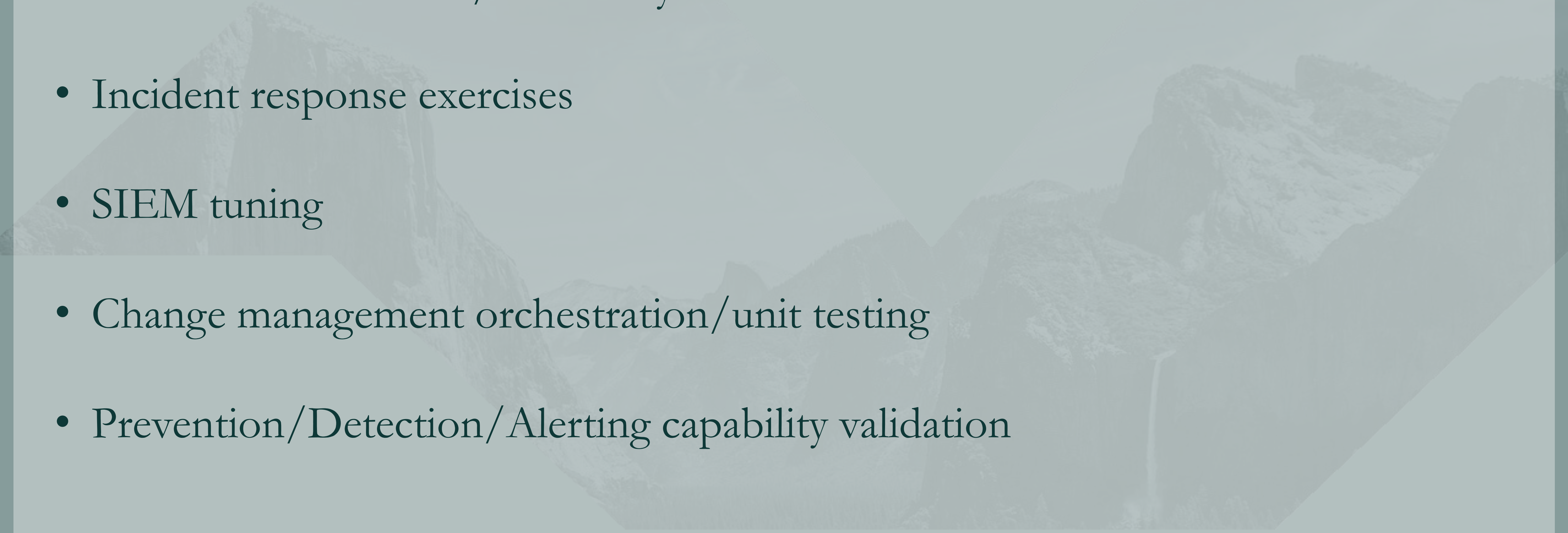
Training

# Plugins



- Pathfinder: Map vulnerabilities and define adversary abilities
- Human: Simulate user activity/behaviors
- Debrief: Export granular, detailed results
- Response: Script/automate incident response activities

# Applicability and Use Cases



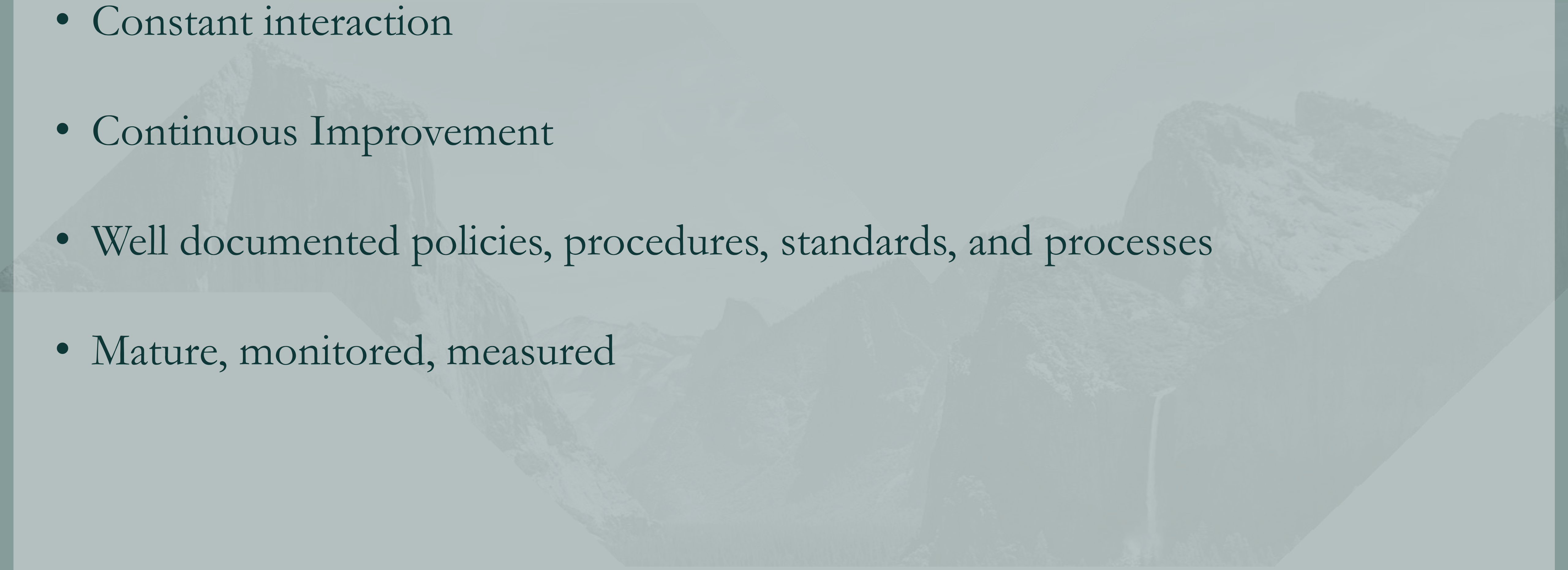
- Red team automation/Adversary emulation
- Incident response exercises
- SIEM tuning
- Change management orchestration/unit testing
- Prevention/Detection/Alerting capability validation

# Basic Walkthrough

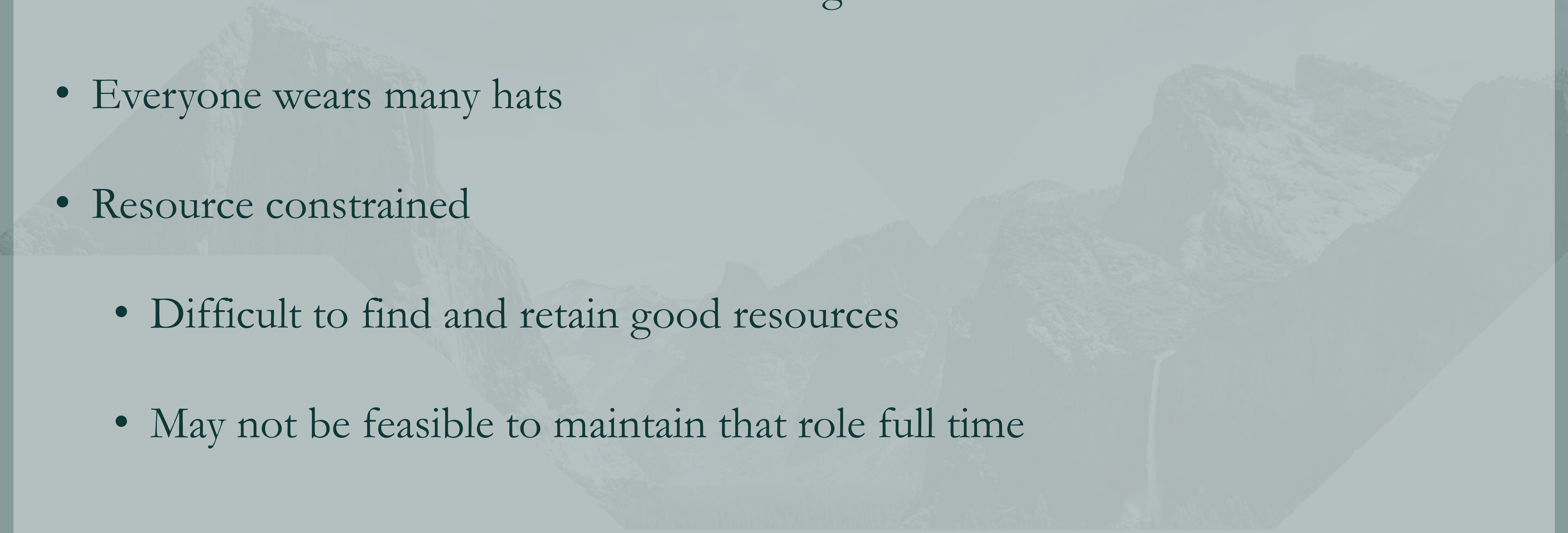
# Collaboration

# Ideals and Best Practices

- Constant interaction
- Continuous Improvement
- Well documented policies, procedures, standards, and processes
- Mature, monitored, measured

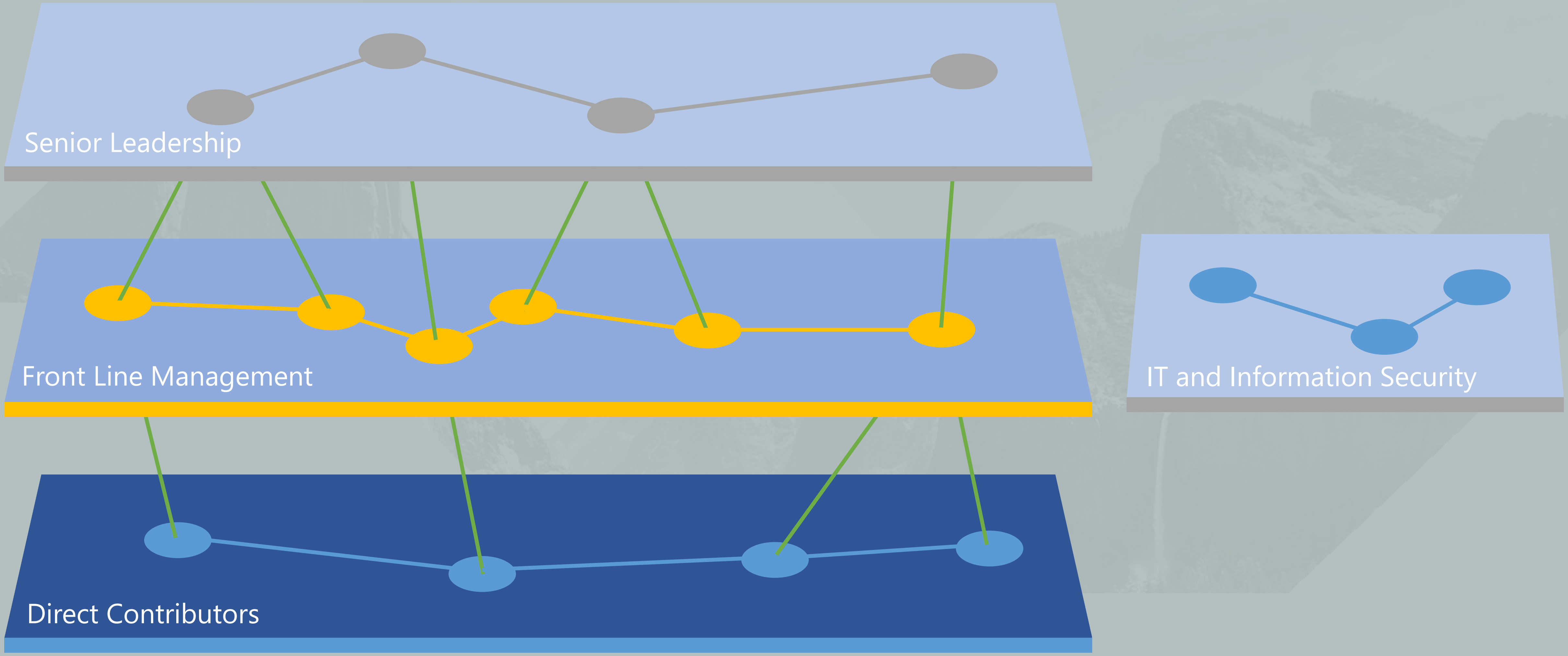


# Mid-size Organizations



- Focus on differentiation vice risk advantage
- Everyone wears many hats
- Resource constrained
    - Difficult to find and retain good resources
    - May not be feasible to maintain that role full time

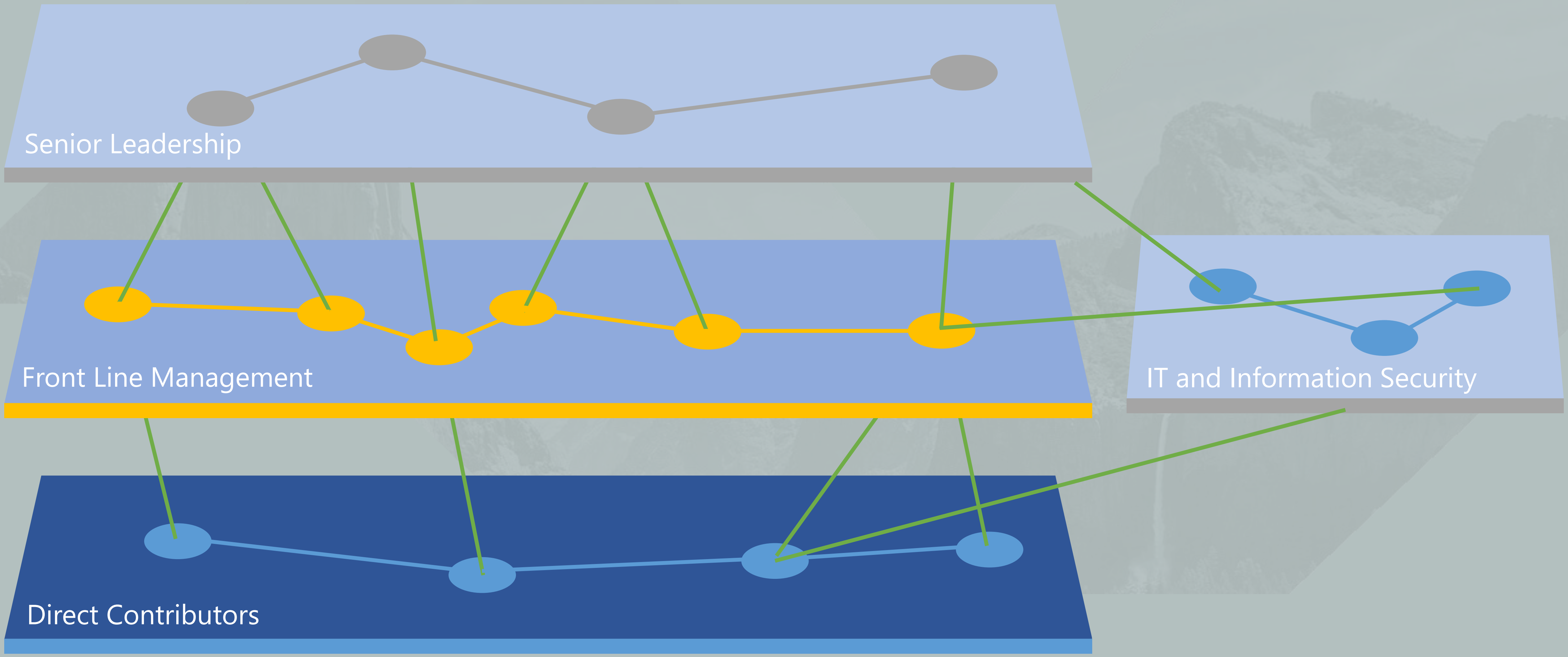
# Organizational Structure



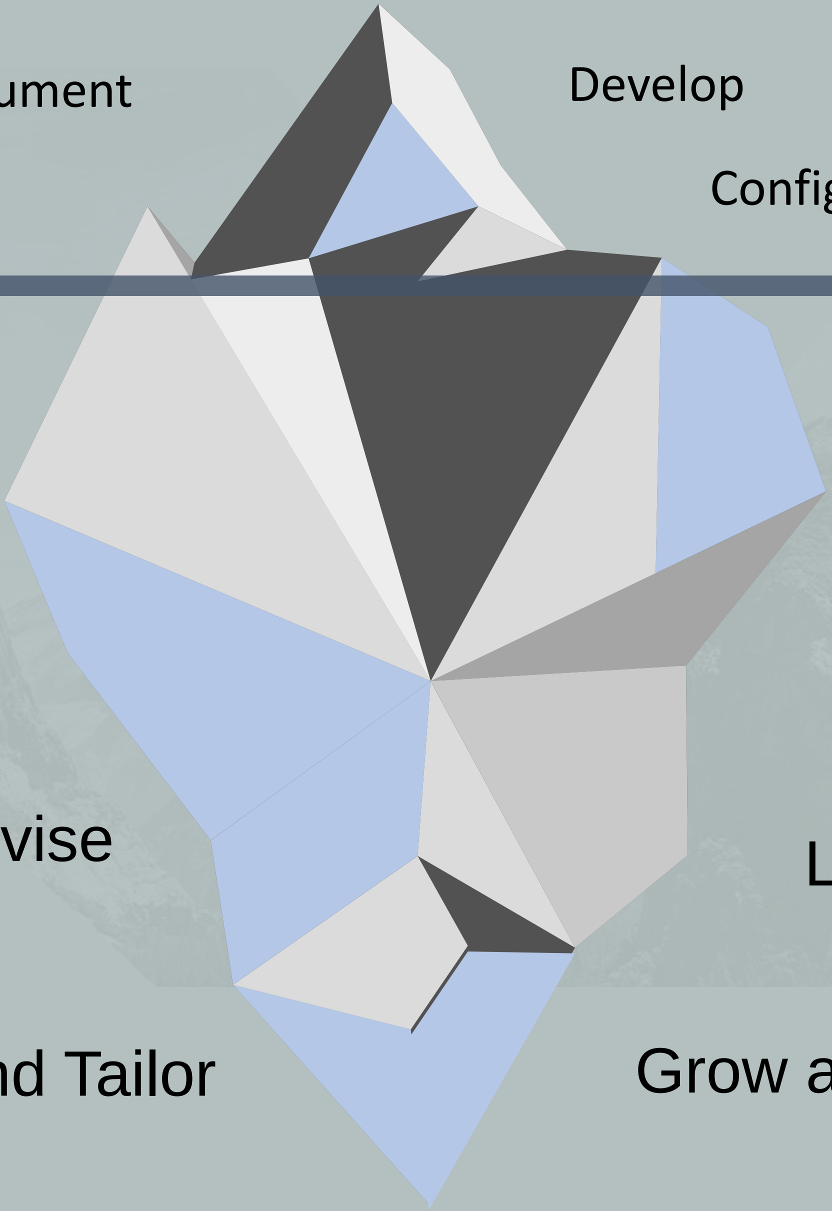
# Realities of IT and Security Operations

- For most mid-size businesses, availability is highest priority
- Investments need to generate revenue; speed of time to market is prioritized
- Security considerations are based on regulatory or statutory requirements
- IT team is expected to handle information security risk management
- Book value != cash flow

# The Matrix Role



# Bridging Gaps



## Core Job Role

Document

Develop

Report

Configure

## True Capabilities

Collaborate

Make and Build

Connect

Understand and Improve

Support and Advise

Lead AND Follow

Customize and Tailor

Grow and Progress

# Conclusion

# Jon King

MBA, CISSP, CISM, CISA, MCSE, ITIL, VCA-DCV, CMMC RP

**@shoveleejoe**

**linkedin.com/in/jrkingitpro**