CYBERSECURITY AWARENESS MONTH

A People-Centric Approach to Breaking the Attack Chain

John C. Checco (C|CISO CISSP CCSK QTE)
Resident CISO, Financial Services

Bio

John C. Checco

C|CISO, CISSP, CCSK, QTE

Proofpoint:

- Former Resident CISO, Financial Services
- Board Certified QTE (Qualified Technology Expert)

Bank of America:

- Loaned Executive, US DHS CISA (fka NCCIC)
- Lead, Zero-Trust Strategy & Architecture
- SVP, Security Innovation Team
- BISO, Global Markets (Merrill Lynch)
- Head of Security Technology Assessment Team

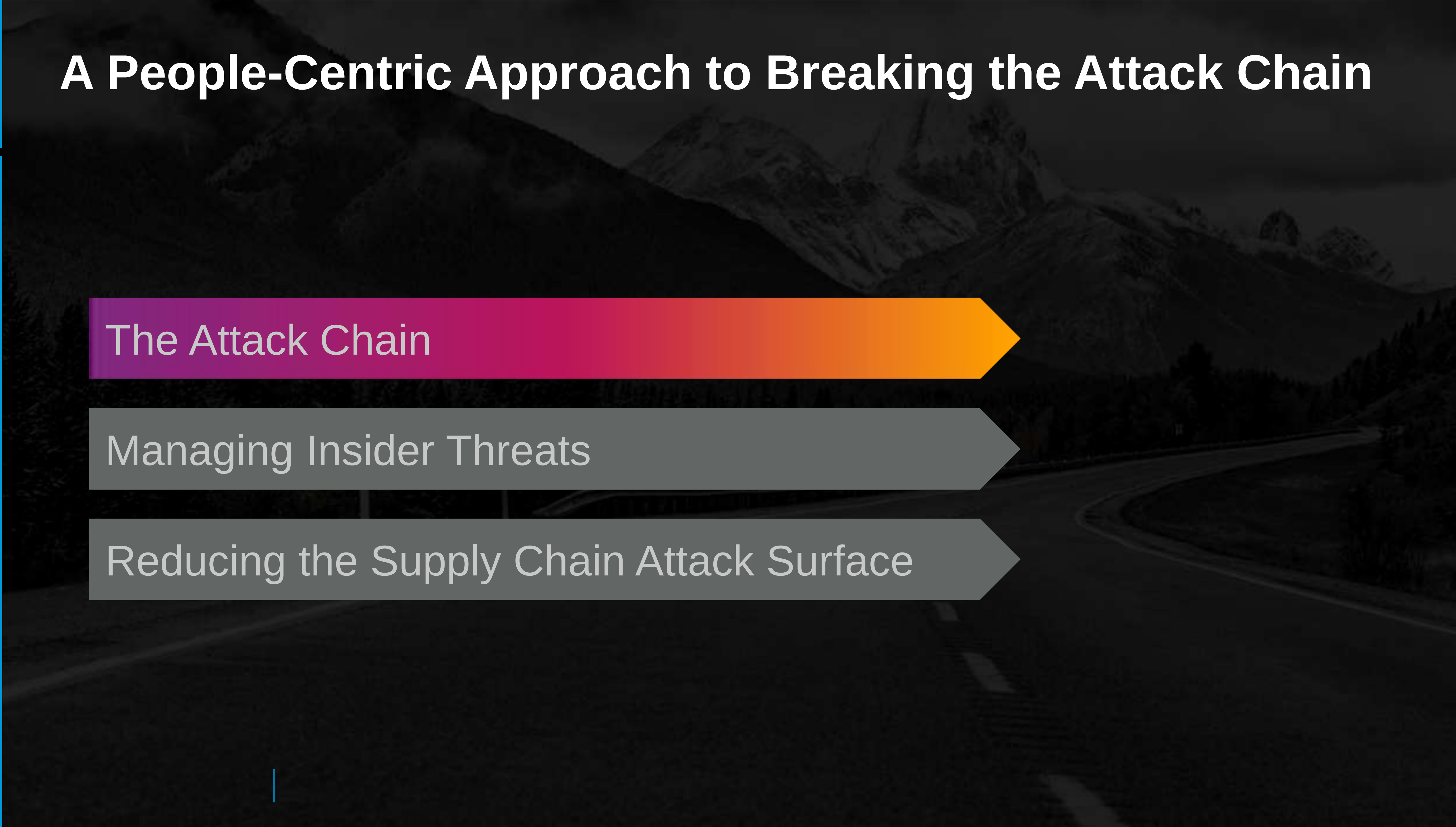
Bloomberg:

- CISO for BloombergBlack (Personal Wealth)
- Senior Security & Risk Executive

A People-Centric Approach to Breaking the Attack Chain

- The Attack Chain
- Managing Insider Threats
- Reducing the Supply Chain Attack Surface

A People-Centric Approach to Breaking the Attack Chain

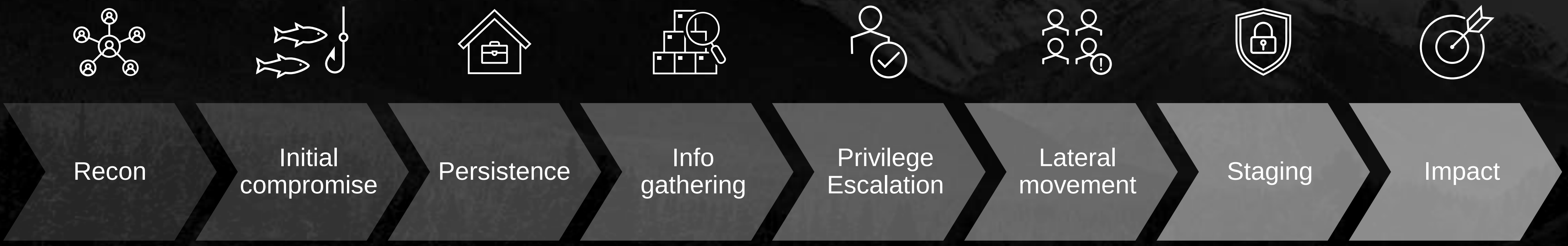


The Attack Chain

Managing Insider Threats

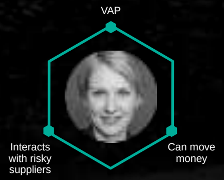
Reducing the Supply Chain Attack Surface

The Attack Chain …
… a People-Centric perspective



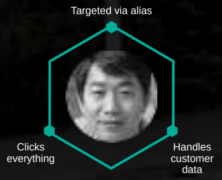
Recon → Initial compromise → Persistence → Info gathering → Privilege Escalation → Lateral movement → Staging → Impact

ROLE:
Finance



ROLE:
Research Scientist

ROLE:
Support Contractor



- Service Accounts
- Local Admin Accounts
- Shadow Admin Accounts

- Exposed Credentials & Cloud Tokens
- Legacy App Accounts
- Open RDP Sessions

CARELESS USER

COMPROMISED USER

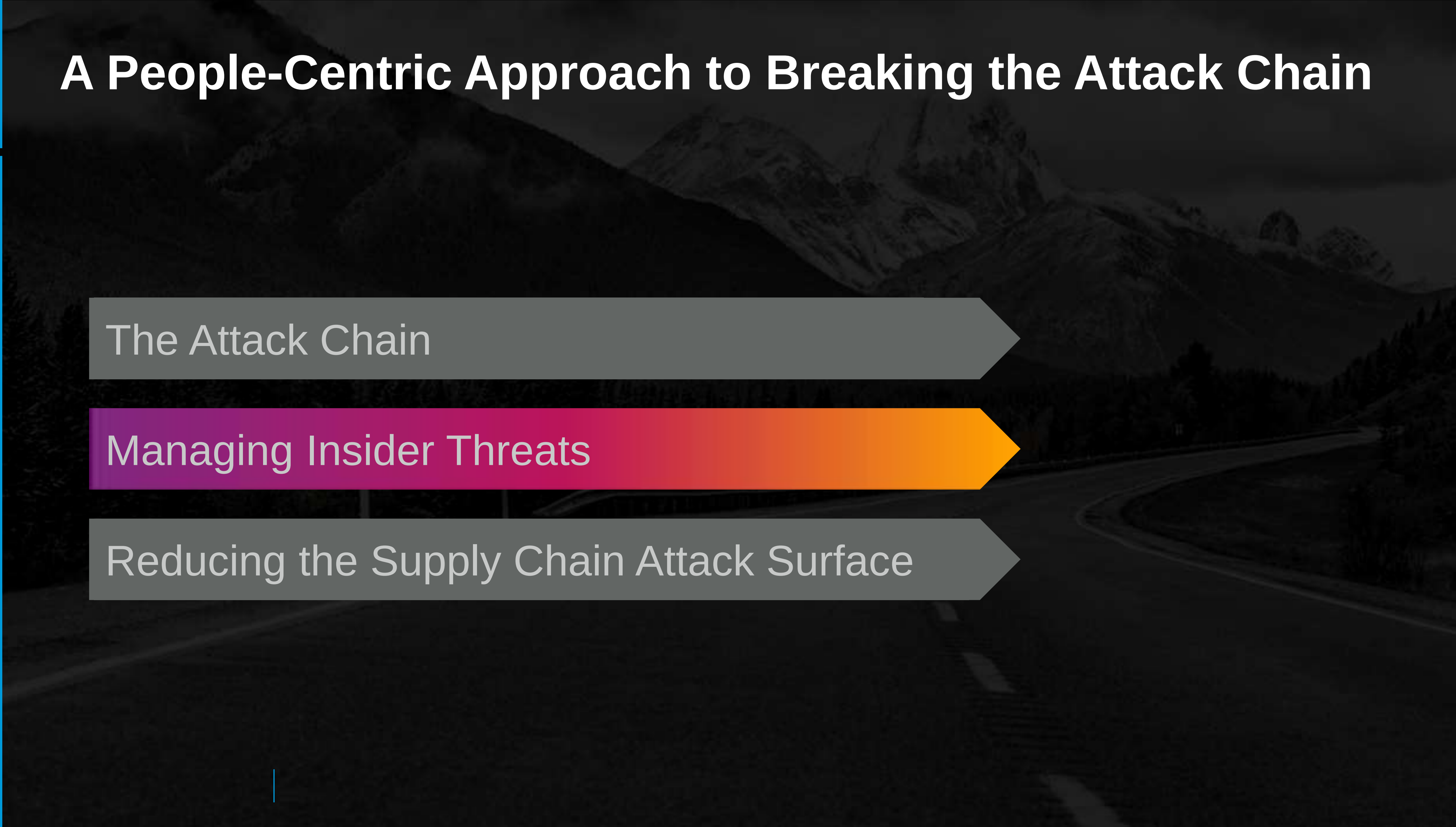
MALICIOUS USER

Threat Prevention

Access Detection + Response

Information Protection

A People-Centric Approach to Breaking the Attack Chain



- The Attack Chain
- Managing Insider Threats
- Reducing the Supply Chain Attack Surface

Data Doesn’t Lose Itself … There’s Always a Person Behind a Loss

CARELESS USER

Misconfiguration, wrong recipients, mistaken file attachments, or inadvertent over-sharing.

58% of all insider-related incidents.

- Well intentioned but accidentally takes sensitive information or inadvertently shares credit card information externally

COMPROMISED USER

Often have privileged and/or elevated access to information.

- **17% of insider-related incidents.**
- Credentials could be compromised by threat actors looking to access company systems

MALICIOUS USER

- Motivated by personal gain and a sense of entitlement.
- **25% of insider-related incidents.**
- Examples include exfiltrating trade secrets or destroying sensitive data

Insider Threat: The Careless User (58%)

Persistence
Info gathering
Impact

Shadow Admin Accounts

Exposed Credentials & Cloud Tokens

Legacy App Accounts

Open RDP Sessions

CARELESS USER

COMPROMISED USER

MALICIOUS USER

Threat Prevention

Access Detection + Response

Information Protection

Insider Threat: The Malicious User (25%)

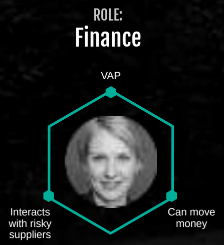
Persistence

Info gathering

Lateral movement

Staging

Impact



Local Admin Accounts

Shadow Admin Accounts

Legacy App Accounts

CARELESS USER

COMPROMISED USER

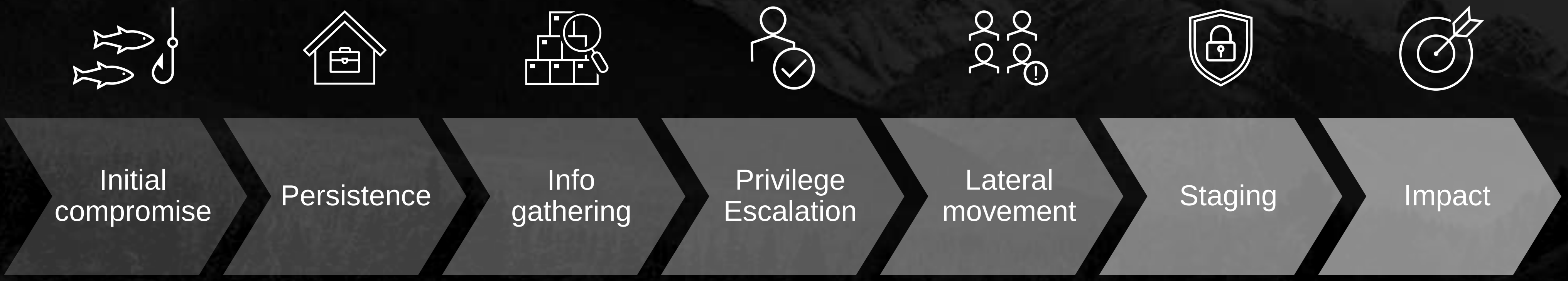
MALICIOUS USER

Threat Prevention

Access Detection + Response

Information Protection

Insider Threat: The Compromised User (17%)

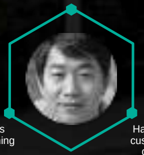


Initial compromise → Persistence → Info gathering → Privilege Escalation → Lateral movement → Staging → Impact

ROLE:

Support Contractor

Targeted via alias



Clicks everything

Handles customer data

Local Admin Accounts

Shadow Admin Accounts

Legacy App Accounts

CARELESS USER

COMPROMISED USER

MALICIOUS USER

Threat Prevention

Access Detection + Response

Information Protection

#TrueStories: Unique Insider Threat Cases

The Arrogant CEO

- How one executive decision to ignore an audit finding cost the company its largest contract, and ultimately its business.

ITM / Archive Collaboration

- How lookback with Archive and context through eDiscovery team augmented an Insider Threat investigation to stop a larger systemic poaching operation.

The Overzealous Reporter

- The news division that caused a lawsuit by their information gathering techniques.

Front-Running as an SDLC

- Developers were found using production data to not only test applications but make trades on pre-public information.

What's Mine is Yours…Maybe

- NFT trading representatives found using their personal digital wallets to manage client NFTs.

The Attack Surface Prerequisite

- Product Team creates thick client apps requiring Python on desktop, which also runs ".py" files from the web.

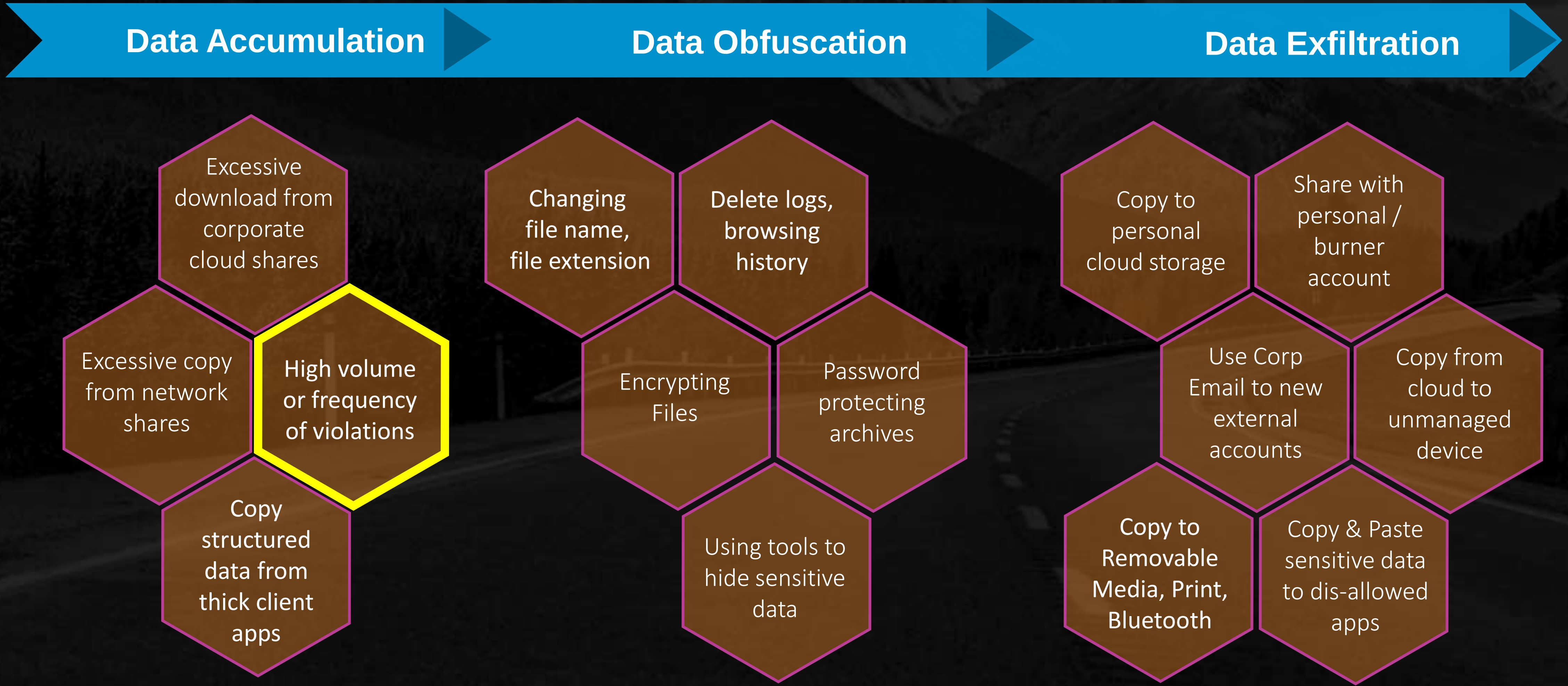
Jumping the PAM Shark

- Trading team using the privileged access management security tool to bypass named seat licensing for a financial market data terminal.

Insider Threats:
Tools and Technologies

	FinServ	Overall
Data Loss Prevention (DLP)	69%	64%
Endpoint Detection and Response (EDR)	65%	50%
Privileged Access Management (PAM)	65%	60%
Security Information and Event Management (SIEM)	58%	53%
User and Entity Behavior Analytics (UEBA)	51%	57%
Insider Threat Management (ITM)	49%	41%

Insider Threats:
Simple Rules for Managing 98% of Insider Data Loss Incidents



Data Accumulation

- Excessive download from corporate cloud shares
- Excessive copy from network shares
- High volume or frequency of violations
- Copy structured data from thick client apps

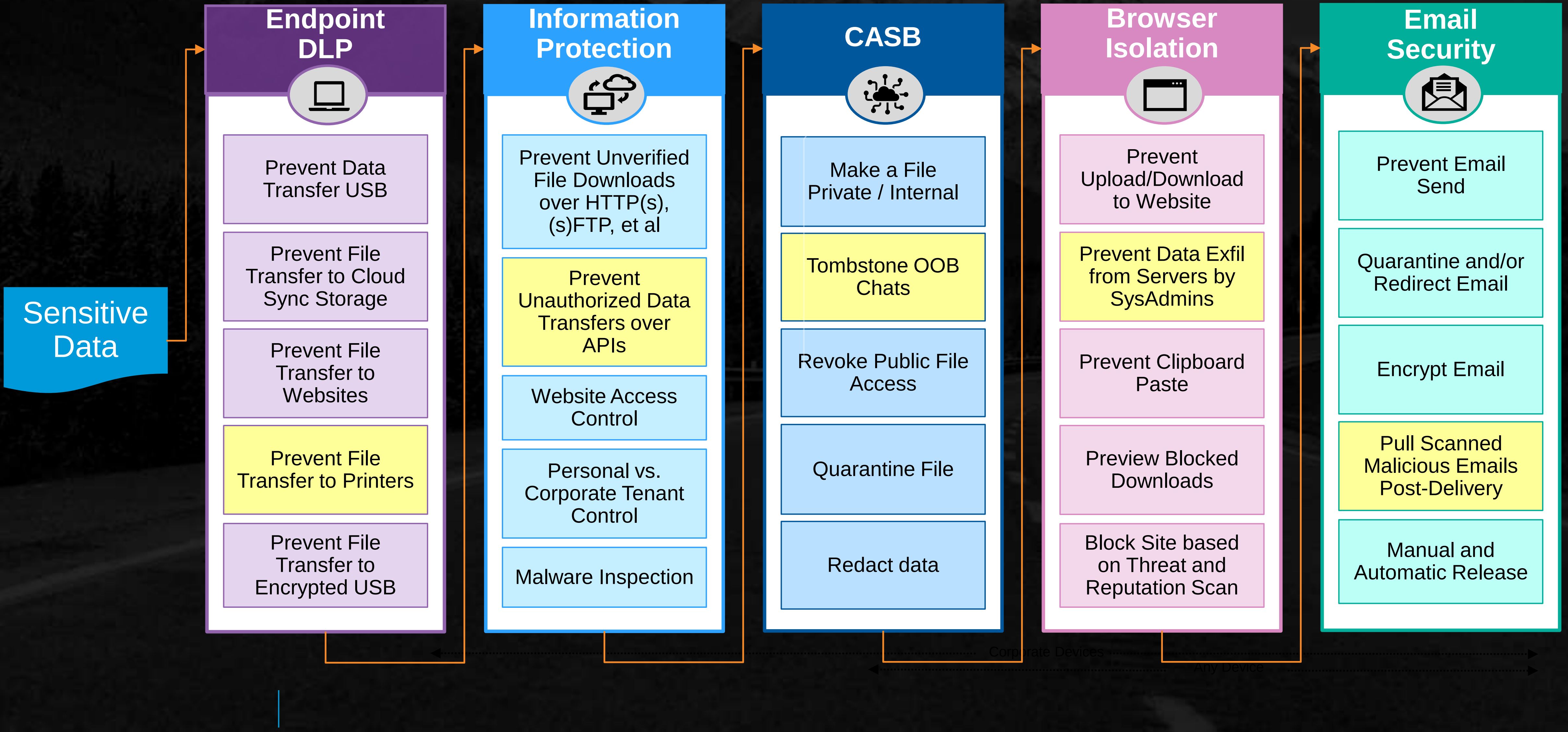
Data Obfuscation

- Changing file name, file extension
- Delete logs, browsing history
- Encrypting Files
- Password protecting archives
- Using tools to hide sensitive data

Data Exfiltration

- Copy to personal cloud storage
- Share with personal / burner account
- Use Corp Email to new external accounts
- Copy from cloud to unmanaged device
- Copy to Removable Media, Print, Bluetooth
- Copy & Paste sensitive data to dis-allowed apps

Insider Threats:
Amplify Capabilities by Layering Defenses



Sensitive Data

Endpoint DLP

- Prevent Data Transfer USB
- Prevent File Transfer to Cloud Sync Storage
- Prevent File Transfer to Websites
- Prevent File Transfer to Printers
- Prevent File Transfer to Encrypted USB

Information Protection

- Prevent Unverified File Downloads over HTTP(s), (s)FTP, et al
- Prevent Unauthorized Data Transfers over APIs
- Website Access Control
- Personal vs. Corporate Tenant Control
- Malware Inspection

CASB

- Make a File Private / Internal
- Tombstone OOB Chats
- Revoke Public File Access
- Quarantine File
- Redact data

Browser Isolation

- Prevent Upload/Download to Website
- Prevent Data Exfil from Servers by SysAdmins
- Prevent Clipboard Paste
- Preview Blocked Downloads
- Block Site based on Threat and Reputation Scan

Email Security

- Prevent Email Send
- Quarantine and/or Redirect Email
- Encrypt Email
- Pull Scanned Malicious Emails Post-Delivery
- Manual and Automatic Release

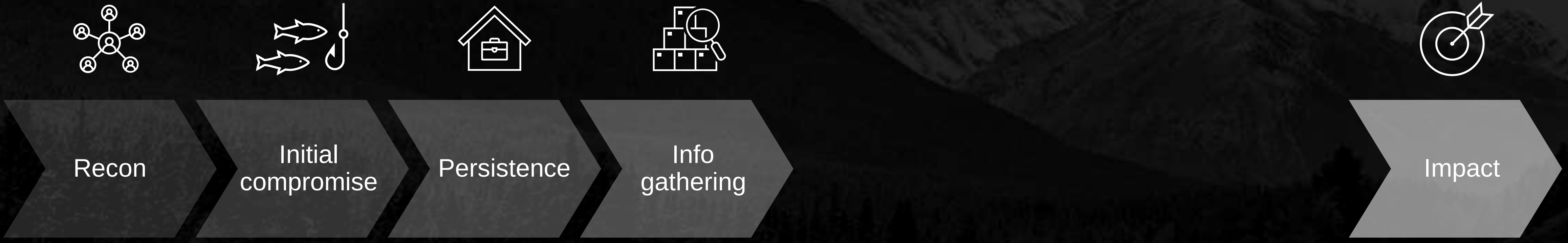
A People-Centric Approach to Breaking the Attack Chain

The Attack Chain

Managing Insider Threats

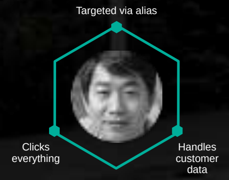
Reducing the Supply Chain Attack Surface

Supply Chain Compromise



ROLE:
Research Scientist

ROLE:
Support Contractor



Service Accounts

⚠ Exposed Credentials & Cloud Tokens

Open RDP Sessions

CARELESS USER

COMPROMISED USER

MALICIOUS USER

Threat Prevention

Access Detection + Response

Information Protection

#TrueStories: Unique Supply Chain Cases

Using Data to Identify Leaks

- How one company used document management dynamically-generated fake data tracers to identify external sources of data leaks.

The Rogue Cell

- How a test failure with a compliance solution identified an entire office of rogue operators rerouting encryption technology to restricted countries.

Blood is Thicker than Business

- Contract win falls through during its celebration because owner’s sibling needed money.

Email Fraud in the Supply Chain

- Monitor suppliers’ domains for domain twisting, impersonation and/or account takeover (ATO).

Supply Chain:
Detection & Prevention by Converging Event Data

Legacy Approach		Modern Approach
Data centric detection and prevention without necessary context	»	People centric that correlates data, threats and user behavior
Siloed products for each data loss channel and critical application	»	Unified platform for monitoring, detection, prevention and response across all channels
Heavyweight, hard to maintain and on-premise architecture	»	Cloud-native, scalable, and lightweight architecture

Platform Consolidation = Reduced Supply Chain Risk

RISK	POINT SOLUTIONS		CONSOLIDATED PLATFORM
VENDOR SECURITY	**Difficult to Protect:** • Disparate Data Stores • Encryption Key Management Nightmare • Multiple Access Points / Attack Surfaces • Multiple Exposures of Internal Directories	→	**Reduced Attack Surface:** • Single Data Store • Simplified Encryption Key Management • Single Access Control Point • Single Exposure of Internal Directories
SECURITY OPERATIONS	**Inability to Meet Objectives:** • Disconnected Intelligence • Inadequate Reporting • Untenable Noise-to-Signal Ratio for SOC	→	**Optimal Defense Operations:** • Shared Intelligence Across Solutions • Contextually Complete Reporting • Highly Efficient SOC Operations
SECURITY COVERAGE	**Composite Topology:** • Feature Overlap = Wasted $$$ • Unknown Gaps = Immeasurable Exposure	→	**Comprehensive Topology:** • Tight Integration = Optimal ROI • Known Gaps = Manageable Exposure
SUPPLY CHAIN	**Complex Vendor Management:** • Unaligned License Renewal Cadence • Multiple Support Teams	→	**Simple Vendor Management:** • Simplified License Renewal Process • Single Point-of-Contact

CYBERSECURITY AWARENESS MONTH