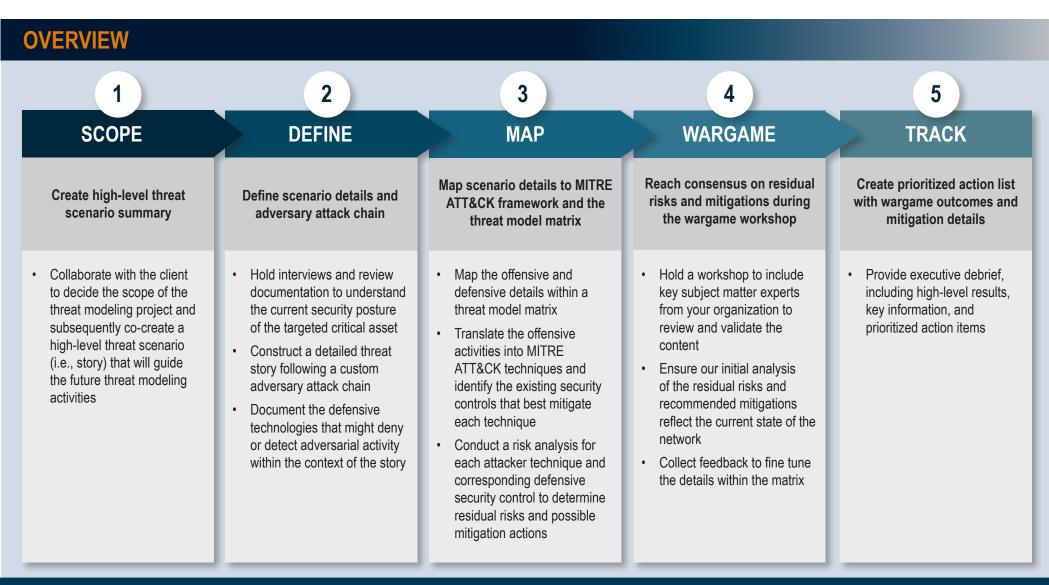
# **Threat Modeling**



CrossCountry's approach is based on the attack chain principle and incorporates industry best practices to include the MITRE ATT&CK framework, NIST 800-53, and Lockheed Martin's Cyber Kill Chain. The outcomes of threat modeling, via collective wargaming, are evidence-based actions that strengthen the organizational security posture. Given the need to keep up with the ever-changing threat landscape, we train your staff throughout your project to sustain this capability for routine assessments.





## **OUTPUT EXAMPLES**

# 2 DEFINE

A realistic 12-part attack scenario based on the twelve MITRE ATT&CK techniques, CrossCountry's threat intelligence program, and CrossCountry's adversary emulation experience.



#### 3 MAP

A threat model matrix, containing the modeled adversary's tactics and techniques, current client countermeasures, and level of residual risk.



### 5 TRACK

A high-level executive summary, prioritizing the attacker tactics with high levels of residual risk and those where additional mitigating actions could significantly lower those levels of risk.

Adversar     Model da	ioud Data Ware g: Nation APT de: Dec 21, 202 de: Dec 21, 202	the i ther give	W. &. Co. defense-in-depth would very likely detect the adversarial attack within the linital foothold or network propagation phase of the attack chain. However, there are a total origit (8) control areas than end to be further investigated given their effectivenes is currently unknown or high risk. These controls of concern span the entire adversary statistic chain.			er, activist group had identified a disgruntled W & Co. employee sympathetic to	
	· · · · · ·		Unknown	High Residual Risks and Pla	n of Mitigating	Actions	
# Priority to Fix	Residual Risk	ATT&CK Tactic	ATT&CK Technique	Mitigating Action	Current Security	Comment	
1	High	Discovery (#6 ATAC)	T1083 File and Directory Discovery	Create preventative and detective controls	NAC	Enhance ACL and network segmentation for identified service accounts that have access to cloud data warehouse using a static password. Use central password storage solution to avoid using static password.	
2	Unknown	Credential Access (#8 ATAC)	T1212 Exploit for Credential Access	Validate prevention and detection controls	Cloud Native Securit Capabilities	y Explore and tune native security capabilities within cloud data warehouse for this scenario context.	
3	Unknown	Collection (#10 ATAC)	T1075 Data Staged - Local	Validate prevention and detection controls	Cloud Native Securit Capabilities	<ul> <li>Explore app, server resource, and network monitoring alerts in this scenario.</li> </ul>	
4	Unknown	Collection (#10 ATAC)	T1075 Data Staged - Local	Validate prevention and detection controls	SIEM	Explore app, server resource, and network monitoring alerts in this scenario.	
5	Unknown	Collection (#10 ATAC)	T1560 Archive Collected Data	Validate prevention and detection controls	SIEM	Further explore detection of encryption and compression activities in this scenario context.	
6	High	Initial Access (#1 ATAC)	T1199 Trusted Relationship	Create preventative and detective controls	None	Create formal insider threat program. Strategically align to organization recent IT strategy document.	
7	High	Initial Access (#1 ATAC)	T1199 Trusted Relationship	Revise intelligence requirements and collections	None	Update intelligence requirements and subsequent collections to detect for insider threat activity with open and dark/deep net.	
8	Unknown	Collection (#10 ATAC)	NA	Validate prevention and detection controls	None	Validate and create alerting on manipulation of PII in cloud data warehouse using current capabilities. Use data labeling and data taggin	

#### **MEET OUR TEAM**



CAMERON OVER
Cyber & Privacy Partner Lead
cover@crosscountry-consulting.com



ERIC EAMES
Advanced Cyber Risk Lead
eeames@crosscountry-consulting.com