Attack Scenario Analytics

Based on MITRE ATT&CK® Framework

To help organizations improve their defenses against threats, CyberGRX uses a data-driven approach that combines third-party cyber risk management expertise with the MITRE ATT&CK framework. The attack scenario analytics data tool provides additional context to risk findings so enterprise customers and third parties can better understand gap recommendations in order to improve the overall defensibility of their ecosystem.

Leveraging the 13 MITRE tactics, an organization is able to have greater visibility and context how a well a third party is prepared in relation to common and recent attacks, highlighting areas that may need attention.

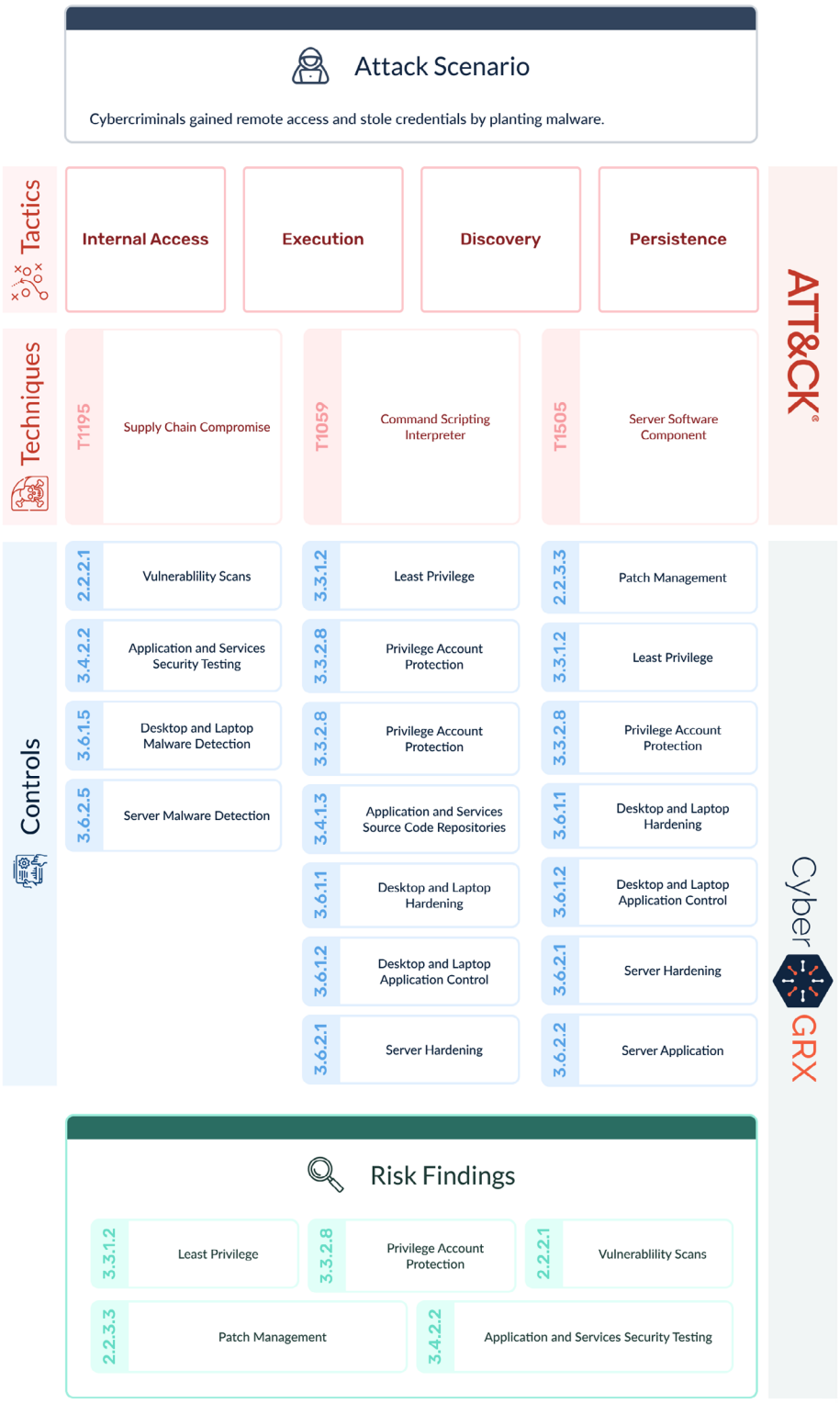
CyberGRX also uses MITRE techniques to create kill chains and uses cases which help uncover unreported gaps as well as inspect assessments in the context of attack post mortems.

Contextual Risk Analytics: Integrating MITRE ATT&CK Framework with CyberGRX Security Controls

The MITRE ATT&CK framework has become a global standard for analyzing tactics and techniques used by malicious actors. MITRE ATT&CK is the most comprehensive, granular and, widely adopted framework in the cybersecurity industry for attack/killchain modeling. CyberGRX is the only third-party cyber risk company to have mapped the entirety of their risk analytics platform with 150+ MITRE killchains based on the most impactful recent attacks.

Top Trending MITRE ATT&CK Use Cases

USE CASE	OUTCOME	SEVERITY	MITRE TECHNIQUES (ASSOCIATED TACTIC)
Government employee data exfiltration by nation-state actor	Data Loss	Very High	• T1078 Valid Accounts (Initial Access) • T1068 Exploitation for Privilege Escalation (Privilege Escalation) • T1078 Valid Accounts (Collection) • T1074 Data Staged (Command and Control) • T1071 Application Layer Protocol (Exfiltration)
Malware exfiltration attack via remote access on Retail credit card data	Data Loss	High	• T1078 Valid Accounts (Initial Access) • T1135 Network Share Discovery (Discovery) • T1078 Valid Accounts (Command and Control) • T1105 Ingres Tool Transfer (Command and Control) • T1571 Non-Standard Port (Collection)
Sensitive data stolen via phishing	Fraud	High	• T1566 Phishing (Initial Access) • T1078 Valid Accounts (Initial Access) • T1203 Exploitation for Client Execution (Execution) • T1057 Process Discovery (Discovery) • T1018 Remote System Discovery (Discovery)
Terminated employee gained access and concealed critical files	Disruption	Moderate	• T1078 Valid Accounts (Initial Access) • T1564 Hide Artifacts (Defense Evasion) • T1485 Data Destruction (Impact)
An internal user steals data from the CFO to use for insider trading	Data Loss	Low	• T1078 Valid Accounts (Initial Access) • T1005 Data from Local System (Collection) • T1114 Email Collection (Collection)



Benefits of using CyberGRX attack scenario risk analytics:

- Identify high-level techniques and tactic vulnerabilities that help identify gaps in reporting
- Allow for easier integration of CyberGRX risk outcomes and insights within internal risk and threat management programs
- Provide traceability for control gap selections
- Inspect assessments in the context of attack post mortems to help drive remediation efforts

Additional context on risk findings through improved visibility

- Increased credibility and defensibility of CyberGRX risk findings to support third-party decisions and relationships
- Additional exposure of threats and risk concerns enables improved third-party detection, monitoring and response to attacks

For more information on how the CyberGRX platform utilizes the MITRE framework please visit our website at:

www.CyberGRX.com

Cyber GRX