TheChertoffGroup
Enabling A More Secure World

Building Effective Cybersecurity Programs with MITRE ATT&CK

THE CHERTOFF GROUP APPROACH

Adaptive threats, heightened regulatory expectations and rapidly changing business drivers are significantly increasing enterprise cyber risks. Many organizations are struggling to understand whether their security measures provide effective coverage against cyber threats. The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework is an authoritative knowledge-base and model for cyber threat behavior, and the Chertoff Group applies it to drive defensive planning and validation activities.

The ATT&CK framework comprehensively defines major threat actor groups and maps them to their known tactics, techniques and procedures (TTPs) and their targets. The Chertoff Group uses ATT&CK to enable:

- Smarter, risk-based defensive countermeasure planning
- Risk-informed processes around buying and optimizing tools
- Greater precision in testing to validate that countermeasures are operating as intended

MITRE | ATT&CK™

MITRE'S ATT&CK FRAMEWORK – A PRIMER

ATT&CK is a unique approach that applies offense-informed defense to understand adversary behavior and defend against it. We leverage ATT&CK because:

- It is both **practical and powerful**, reflecting tactics and techniques that have actually been used.
- It allows defenders to lay out a comprehensive mapping of TTPs to defensive countermeasures and **identify blind spots** in their defensive strategy.
- It goes deeper than indicators like hash values, IP addresses, domains, **orienting defenses around TTPs**, which are harder for an adversary to adjust.

HOW TCG LEVERAGES ATT&CK TO HELP CLIENTS ACHIEVE SECURITY EFFECTIVENESS:

1

More precise risk assessments. TCG uses the ATT&CK framework to tailor risk assessments to the specific business profiles of our clients. We start an assessment by evaluating how attractive a client's business is to reasonably sophisticated threat actors. Because ATT&CK maps threat actor groups to associated techniques, this mapping is used to compare threat adversary TTPs to defensive measures, identify gaps and make recommendations on risk-reducing countermeasures. Findings can be mapped to authoritative frameworks (e.g., NIST Cybersecurity Framework, ISO, CIS 20 Critical Security Controls).

2

Smarter risk mitigation processes—using ATT&CK to prioritize defensive countermeasures, inform buying decisions and optimizing tools. We use the MITRE knowledge-base to help clients prioritize and phase-in security investments based on risk reduction value. TCG uses the MITRE ATT&CK framework to develop coverage maps that help organizations justify and prioritize purchasing decisions, building credibility in the budgeting process.

Likewise, we also use the ATT&CK framework to advance resiliency capabilities by prioritizing response-oriented measures, categorizing incidents with a higher level of fidelity, and informing realistic cybersecurity exercise scenarios.

3

Risk-based testing strategies. Many organizations struggle to effectively implement security tools and thus live with a false sense of security. TCG leverages pre-built ATT&CK testing scripts to help clients validate and hone defenses. Testing projects can also generate more focused insights into how to prioritize remediation, as well as meaningful translation of such efforts into risk reduction benefit.

BOTTOM LINE – DRIVING TOWARD AN OFFENSE INFORMED PROGRAM:

The Chertoff Group's approach is grounded in the belief that risk elimination is impossible and that organizations should focus security around assets that matter most through programs that are risk-based, intuitive and trusted. Combining TCG's expertise with the power of MITRE's ATT&CK framework helps ensure that clients derive maximum risk reduction value from their security strategy, build confidence in program effectiveness, and achieve resilience, all while streamlining organizational resources towards top priorities.

THE CHERTOFF GROUP | 1399 NEW YORK AVE. NW | SUITE 1100 | WASHINGTON, DC 20005 | 202.552.5280 | CHERTOFFGROUP.COM