Google Cloud
Security

White paper

Beyond checking boxes: Unlocking the full potential of MITRE ATT&CK with Google

Table of Contents

Picture this: You're a security analyst facing a barrage of alerts signaling a potential breach. A familiar pattern emerges – spearphishing, suspicious logins, lateral movement. The adversary is already on your network. But you have a powerful tool at your disposal: the MITRE ATT&CK® framework. This knowledge base acts as your battle map in the cyber war, laying out the enemy's tactics and techniques. With ATT&CK, you can quickly identify the attacker's position, predict their next move, and deploy countermeasures.

Since 2013, this knowledge base has become the go-to resource for security teams worldwide. It provides a common language for understanding cyber threats, enabling defenders to proactively address vulnerabilities, and respond effectively to attacks.

But here's the catch, simply referencing the framework isn't enough. Many organizations struggle to translate ATT&CK's vast knowledge into actionable insights. They may map their controls to the framework, but then what? How do you prioritize threats? How do you protect what matters most?

In this white paper, we'll dive deep into the challenges SecOps teams face in truly harnessing the power of MITRE ATT&CK. And more importantly, we'll unveil Google's vision for a new era of ATT&CK optimization. Imagine a world where you can:

- **Move beyond basic mapping:** Translate ATT&CK knowledge into a tailored defense strategy that aligns with your organization's unique risk profile.
- **Prioritize threats strategically:** Focus on the most critical threats and allocate resources strategically.
- **Eliminate blind spots:** Proactively identify and address security gaps before attackers exploit them.
- **Optimize and streamline operations:** Improve efficiency and collaboration through automation and streamlined workflows.

Join us on a journey to redefine how SecOps teams leverage MITRE ATT&CK and build a more secure future.

MITRE ATT&CK: A Dynamic Cyber Threat Map

In today's complex threat landscape, SecOps teams need a reliable guide to navigate the ever-evolving world of cyberattacks. MITRE ATT&CK provides that guidance. Imagine a vast library, filled with meticulously detailed blueprints of every known cyberattack. That's essentially what MITRE ATT&CK offers to the security world. Developed by MITRE, a non-profit research organization, this framework provides a structured and comprehensive catalog of adversary tactics and techniques.

Think of it this way, each "blueprint" in this library outlines a specific attack technique, detailing the tools, procedures, and behaviors employed by malicious actors. Whether it's a phishing scam, malware deployment, or a sophisticated ransomware attack, ATT&CK breaks down the anatomy of these attacks, providing valuable insights into how they unfold.

But this library isn't static; it's constantly evolving, just like the threat landscape itself. When MITRE first opened its doors in 2013, it primarily focused on traditional enterprise environments - think Windows, macOS, and Linux systems. But as the world shifted towards the cloud, so did ATT&CK.

Recognizing the unique challenges of cloud security, MITRE expanded its library in 2019 to include blueprints for cloud-based attacks. This new wing of the library houses detailed schematics of attacks targeting cloud platforms like Google Cloud, AWS, and Microsoft Azure. It covers everything from SaaS applications to IaaS infrastructure, providing security teams with the knowledge they need to defend against cloud-specific threats.

This constant evolution is what makes ATT&CK so powerful. It's a living, breathing resource that empowers SecOps teams to:

- **Decipher attacker tactics:** By studying these blueprints, SecOps teams can gain a deeper understanding of attacker methodologies, predict their next moves, and proactively reinforce their defenses across all environments.
- **Develop countermeasures:** SecOps teams can leverage ATT&CK to identify vulnerabilities and implement effective security controls, whether on-premises or in the cloud.
- **Speak a common language:** ATT&CK provides a universal language for security professionals, fostering collaboration and knowledge sharing across the industry.
- **Build a proactive defense:** By understanding the tactics and techniques employed by attackers, security teams can shift from a reactive to a proactive security posture, anticipating threats before they materialize, regardless of where they strike.

In essence, MITRE ATT&CK is the SecOps professional's secret weapon. It's the key to unlocking a deeper understanding of the threat landscape, enabling organizations to build a robust and resilient security posture in an ever-changing digital world. We'll explore this more in the next section, but simply having access to this library is not enough. The true power lies in effectively leveraging its knowledge to optimize your security strategy.

The Challenges in Operationalizing MITRE ATT&CK

We've established that MITRE ATT&CK is a powerful tool, a vast library of adversary tactics and techniques. But even the most comprehensive library can have its limitations. Relying solely on the ATT&CK framework for effective security operations can lead to challenges.

The Illusion of 100% Coverage

The ATT&CK framework provides a broad overview of known attack techniques, but it doesn't account for every possible variation or emerging threat. It's like having a map that shows the main highways but omits the smaller roads and back alleys where attackers might lurk. Some security vendors claim "100% coverage" based on MITRE vendor tests, but these are often misleading. While these tests are useful for evaluating vendor performance against known attack scenarios, they don't guarantee complete protection in real-world environments.

MITRE itself emphasizes that evaluations offer insights into how solutions might address an organization's unique security needs against known adversaries. However, SecOps teams sometimes misinterpret this as a guarantee of comprehensive coverage within the vendor's stated domain. In reality, the devil is in the details. A closer look often reveals gaps in protection when applied to the specifics of a unique IT environment.

For instance, a vendor claiming complete detection of account manipulation techniques might fall short when faced with the specific operating systems or applications used within your organization. This creates a dangerous illusion of security, leaving critical vulnerabilities exposed. True comprehensive coverage remains an elusive goal due to the dynamic nature of cyber threats and the inherent complexities of diverse IT environments.

Checking Boxes vs. Assessing Risk

Treating the ATT&CK matrix as a simple checklist can be problematic. SecOps teams need to go beyond simply "checking boxes" and prioritize their defenses based on a thorough risk assessment. This includes identifying critical assets, understanding the threat actors most likely to target them, and tailoring their security controls accordingly.

Even with this approach, the sheer volume of techniques in the ATT&CK matrix can overwhelm resource-strapped teams. Trying to detect every single technique is impractical.

For example, evaluating vendor claims can be a minefield. A vendor might promise protection against account manipulation across operating systems and SaaS applications. But then, on closer inspection, you discover Linux isn't supported, and no vendor can cover every SaaS app. Without careful investigation, SecOps teams can be misled into a false sense of security.

The Static Nature of the Framework

While the ATT&CK framework is regularly updated, it can't always keep pace with the rapid evolution of cyberattacks. New techniques and tactics emerge constantly, and attackers often find creative ways to bypass known defenses.

Relying solely on the ATT&CK framework can create a false sense of security, as it may not capture the latest threats or account for the specific nuances of your environment.

The Missing Link: Automation and Integration

Finally, operationalizing the ATT&CK framework often requires manual effort, transferring insights from the matrix to other security tools and workflows. This lack of automation can lead to inefficiencies, errors, and delays in responding to threats. It's like having a map but needing to manually calculate distances and directions instead of using a GPS.

To truly optimize the use of ATT&CK, organizations need seamless integration and automated processes that translate its insights into actionable steps within their security operations.

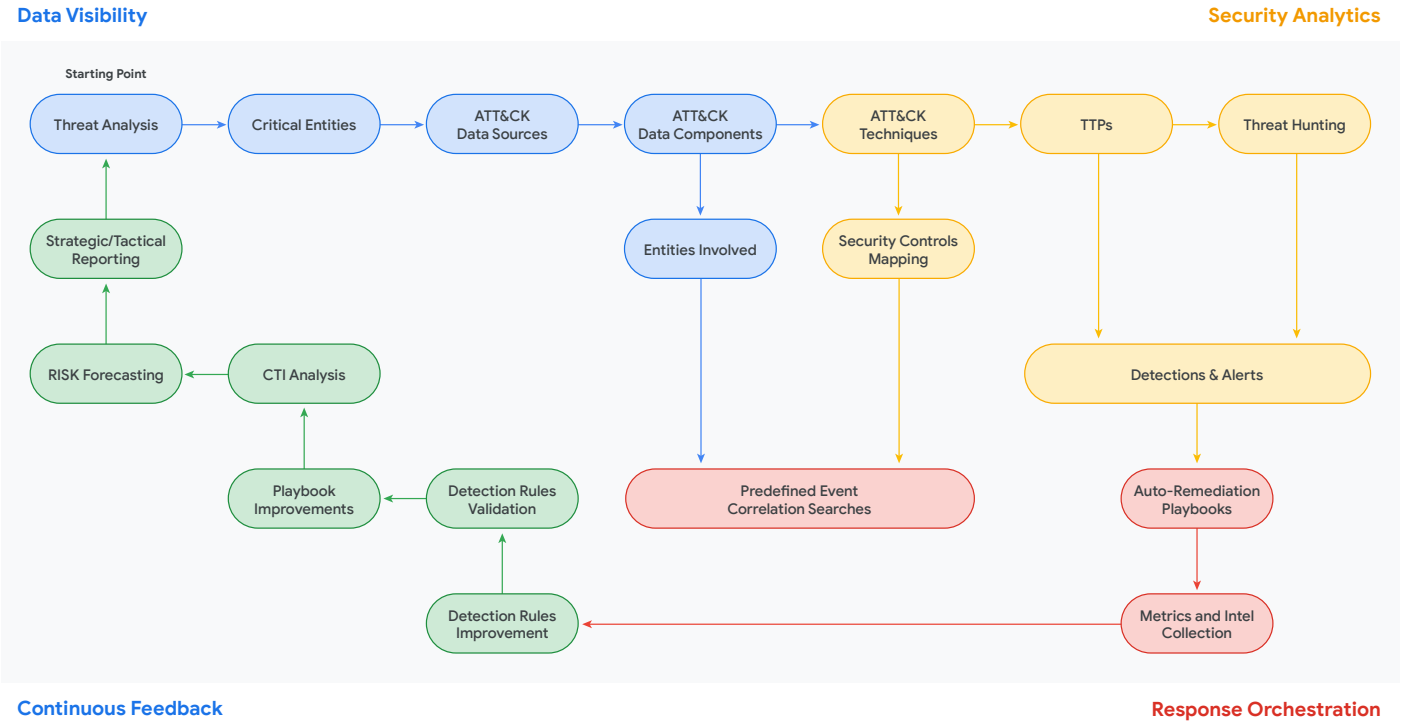
Google's Vision: A New Era of MITRE ATT&CK Optimization

Building on the foundational power of MITRE ATT&CK, explored in previous sections, Google envisions a future that transcends the framework's conventional limitations. We believe that by integrating ATT&CK with other cybersecurity best practices and leveraging cutting-edge technologies, SecOps teams can overcome existing challenges and unlock a new era of operational efficiency, building a truly proactive and resilient security posture.

Five Key Strategies for SecOps Teams

1. **From Coverage to Posture:** As we discussed earlier, simply checking boxes on the ATT&CK matrix is not enough. To truly defend your enterprise IT environment, SecOps teams need to shift their focus from mere coverage to a continuous assessment and refinement of their security posture. This involves several crucial steps:

    - **Threat profiling:** Generate detailed threat profiles based on known adversary behaviors prevalent in your industry and geographic area.
    - **Posture assessment:** Evaluate the strength of your security posture against these threat profiles, identifying the Tactics, Techniques, and Procedures (TTPs) that require prioritization.
    - **Crown jewels first:** Identify your high-value assets ("crown jewels") and combine this knowledge with TTP prioritization to determine the most critical areas for defense.
    - **Gap analysis:** Filter your findings against existing ATT&CK coverage to uncover any security gaps.
    - **Control enhancement:** Develop or enhance security controls to address identified gaps and bolster your overall security posture.
    - **Continuous testing:** Use pre-configured templates designed around specific techniques or chains of techniques to test the effectiveness of your security controls. These templates can be expanded over time to incorporate new procedures and ensure comprehensive testing.
    - **Integration and measurement:** Map each use case to the MITRE ATT&CK framework and integrate detection logic to quantify measurable enhancements to your detection and remediation capabilities.



2. **Prioritization is Key:** In the dynamic world of cyberattacks, not all threats are created equal. Real-time threat intelligence enables you to prioritize your responses based on the threats most likely to impact your mission-critical systems. This includes:

    - **Analyzing threat actor activity:** Observe threat actor activity within your enterprise environment through the lens of ATT&CK, identifying where threat activity is concentrated and what malicious internal and external actors are doing.
    - **Identifying misalignments:** Detect misalignments between your rule portfolio and observed threat actor activity. This will highlight areas of the ATT&CK map where rule density is disproportionate to the level of threat activity, allowing you to prioritize the implementation of new detection rules.
    - **Developing threat profiles:** Create detailed threat profiles that accurately describe your company and generate a prioritized list of ATT&CK techniques to focus on. This helps you identify and defend against the threats that are most likely to target your organization.

3. **Harnessing the Power of Inference:** Imagine a tool that can predict an attacker's next move based on their current tactics. The Technique Inference Engine, developed by the Center for Threat Informed Defense, does just that. By leveraging machine learning and threat intelligence, this engine empowers SecOps teams to:

    - **Prioritize threat hunting:** Focus on the most likely intrusion methods during cyber triage events.
    - **Enhance incident analysis:** Improve post-mortem analysis of security incidents.
    - **Identify gaps:** Highlight potential sensing, detection, and reporting gaps in your security posture.

- **Discover related attacks:** Identify similar or related attack vectors.
- **Plan for adversary emulation:** Create effective adversary emulation plans for testing and improving your defenses.

The inference engine uses a machine learning model trained on cyber threat intelligence to recommend likely TTPs based on known input TTPs. As new activity is detected, the model can be retrained to incorporate previously unseen adversary TTPs, ensuring that your security team stays ahead of the curve.

4. **Embracing the Cloud Matrix:** As organizations increasingly migrate to the cloud, the need for a cloud-specific approach to ATT&CK becomes paramount. Traditional security tools often struggle with the volume of cloud logs and the dynamic nature of cloud environments. The cloud matrix provides a comprehensive view of tactics and techniques employed in cloud-based attacks, addressing these challenges and offering guidance on mitigating cloud-specific threats.

- **Google's commitment:** When MITRE first introduced the cloud matrices in 2019, Google immediately recognized its importance and sponsored a project to map Google Cloud Platform security controls to ATT&CK. This collaborative effort with the Center for Threat Informed Defense (CTID), a MITRE Engenuity organization, has resulted in comprehensive mappings of cloud techniques to AWS, Azure, and GCP security controls.
- **Unique cloud threats:** Using the ATT&CK cloud framework is vital because cloud vulnerabilities often differ from traditional on-premises vulnerabilities and may not be included in databases like CVE. The cloud matrices provide visibility into a wide range of cloud-specific attacks, including:

  i. Initial account access
  ii. Execution commands
  iii. Persistence to manipulate accounts
  iv. Privilege escalation
  v. Defense evasion
  vi. Credential access
  vii. Discovery of services and accounts
  viii. Lateral movement
  ix. Data and email collection
  x. Data exfiltration
  xi. Data destruction
  xii. Encrypted data attacks
  xiii. Denial of service
  xiv. Financial theft
  xv. Resource hijacking

- **Visibility and dynamic environments:** The cloud matrix addresses the critical challenge of visibility in cloud environments where traditional tools may be less effective. By mapping specific log sources and security controls to ATT&CK, you gain a clearer understanding of your cloud security posture. This is especially important in dynamic cloud environments with DevOps practices, where development environments may be more vulnerable to attacks. The cloud matrix provides guidance on mitigating these unique threats.

5. **Collaboration and Information Sharing:** In the fight against cybercrime, information is power. By fostering collaboration both internally and with industry peers, SecOps teams can gain a broader perspective on the threat landscape and share best practices for defense.

    - **Internal collaboration:** Involve stakeholders from every department in discussions about security strategies, fostering a culture of shared responsibility and open communication.
    - **Breaking down silos:** Encourage the use of common security tools and automate processes to eliminate workflow silos and reduce the burden on your SecOps team.
    - **External collaboration:** Leverage resources like ISAC (Information Sharing and Analysis Centers) and CTID (Center for Threat Informed Defense) to gain insights into industry-specific threats and collaborate with peers on defense strategies.

The Benefits of Google's Approach

By embracing Google's vision for ATT&CK optimization, SecOps teams can:

- **Move beyond a reactive security posture** and proactively identify and mitigate threats before they materialize.
- **Gain a deeper understanding of adversary tactics** and tailor their defenses to their organization's unique risk profile.
- **Prioritize their responses** based on real-time threat intelligence and focus on the threats that pose the greatest danger.
- **Improve operational efficiency** through automation and streamlined workflows.
- **Foster collaboration and information sharing** to build a stronger collective defense against cyberattacks.

Elevate Your Security Posture with Google's Vision for MITRE ATT&CK

Throughout this white paper, we've journeyed through the intricacies of the MITRE ATT&CK framework, exploring its strengths and limitations. We've seen how it empowers security teams to understand adversary tactics, predict their next moves, and build a proactive defense. But we've also uncovered the challenges – the limitations of static frameworks, the illusion of 100% coverage, and the critical need for prioritization and automation.

Now, it's time to take the next step.

Imagine a world where you can seamlessly integrate ATT&CK into your security operations, transforming it from a reference guide into a dynamic weapon against cyber threats. This is the vision Google is pioneering.

Key Takeaways

- **Move beyond basic mapping:** Don't just check boxes. Translate ATT&CK knowledge into a tailored defense strategy, prioritizing threats based on your unique risk profile and focusing on your "crown jewels" – your most critical assets.

- **Prioritize like a pro**: Leverage real-time threat intelligence and the power of the Technique Inference Engine to anticipate attacker actions and allocate resources strategically.
- **Embrace the cloud matrix:** Navigate the unique challenges of cloud security with ATT&CK's cloud-specific framework, gaining visibility and control in dynamic cloud environments.
- **Collaborate and conquer:** Break down silos, foster information sharing, and build a stronger collective defense through internal and external collaboration.

The Google Advantage

Google's approach to ATT&CK optimization empowers you to:

- **Proactively mitigate threats** before they disrupt your business.
- **Gain a deeper understanding of adversary tactics** and tailor your defenses accordingly.
- **Improve operational efficiency** through automation and streamlined workflows.
- **Build a more resilient security posture** through continuous assessment and improvement.

Ready to unlock the full potential of MITRE ATT&CK and transform your security operations? Contact the Google Cloud Security team today to learn more about our innovative solutions and embark on a journey towards a more secure future. Together, let's turn the tide against cyberattacks.