

Go Beyond Checking Boxes: Unlock the Full Potential of MITRE ATT&CK with Google

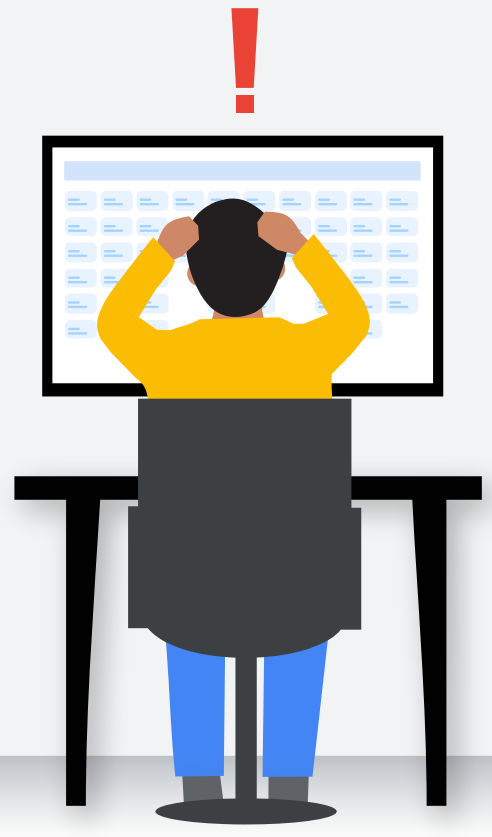
MITRE ATT&CK: A Powerful Tool, But Not a Silver Bullet

The MITRE ATT&CK matrices empower security teams to better understand adversary tactics, predict their next moves, and build a proactive defense.

But here's the catch: simply referencing the framework isn't enough.

Mapping controls to the MITRE framework is an important step. But then what? How do you prioritize threats? How do you protect what matters most? The key is translating the vast ATT&CK knowledge base into actionable insights.

To help tackle this challenge, Google has pioneered a new vision to transcend the MITRE framework's conventional limitations. We developed a set of best practices to accurately identify security gaps and prioritize where to focus your mitigation efforts.



5 Best Practices for SecOps Teams to Leverage the MITRE ATT&CK Matrices

1

Shift from coverage to posture

Shift from a focus on mere coverage to a continuous refinement of your security posture. This involves threat profiling, posture assessment, identifying high-value assets, gap analysis, control enhancement, and continuous testing.

2

Prioritize threats

Use real-time intelligence to prioritize responses based on the threats most likely to impact your mission-critical systems. This includes analyzing threat actor activity, identifying misalignments, and developing threat profiles.

3

Harness the power of inference

Predict an attacker's next move by leveraging the **Technique Inference Engine**. The engine uses machine learning to prioritize threat hunting, enhance incident analysis, identify gaps, discover related attacks, and plan for adversary emulation.

4

Embrace the MITRE cloud matrices

View tactics and techniques employed in cloud-based attacks by tapping into the MITRE cloud matrices. Along with comprehensive mappings of cloud techniques to AWS, Azure, and GCP security controls, you also receive guidance for mitigating cloud-specific threats.

5

Collaborate and share

Gain a broad perspective on the threat landscape and share best practices for defense by fostering collaboration internally and with industry peers through organizations like **ISAC** and **CTID**. Involve all stakeholders in security strategies to establish a culture of shared responsibility while breaking down workflow silos.

The Google Advantage

SecOps teams must move beyond simply referencing the vast knowledge of the MITRE ATT&CK framework to translate the information gleaned from the matrices into actionable insights. Checking the boxes for coverage is not enough.

Adopting the Google approach to optimizing the MITRE ATT&CK matrices empowers you to...

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

Learn more about the Google vision for how to apply the MITRE ATT&CK framework to your security workflows [in this whitepaper](#).

<https://cloud.google.com/security/products/security-operations>

