SNAPATTACK

Case Study

Leading Global Data Center Provider Accelerates SIEM Migration and Improves Threat Coverage

with SnapAttack

Content

TL;DR: In less than **30 days**, from the time we hooked up APIs for the client's SIEM migration:

- We had **746 detections deployed**.
- **509** were **validated**.
- **384** were **higher-highest confidence**.

About Our Customer

This SnapAttack customer is a digital infrastructure provider that connects leaders across industries, such as finance, manufacturing, retail, transportation, government, healthcare, and education. As a top 10 global data center provider, our customer is entrusted with the critical task of providing the foundational infrastructure upon which countless large enterprises rely.

The nature of their business makes this organization an exceptionally attractive target for a spectrum of threat actors, ranging from cybercriminals seeking financial gain to nation-state Advanced Persistent Threats (APTs) pursuing strategic objectives.

With a global presence spanning hundreds of locations worldwide, securing their infrastructure is a constant uphill battle – one that's challenging, complicated, and costly.

The Challenge

Protecting this organization's infrastructure is extremely difficult due to its complex network and diverse customer base. As both continue to evolve, that hurdle only grows higher, and the organization couldn't afford to stay restrained by legacy tooling. Their cybersecurity investment is, like all large enterprises, both financially and operationally significant to the entire organization, including their internal SOC used for threat detection and incident response.

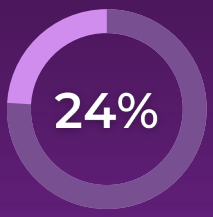
In short? Their legacy SIEM couldn't keep up - they needed to migrate their SIEM environment and fortify it with high-fidelity, behavioral detections, quickly.

Having familiarity with SnapAttack's ability to accelerate and simplify SIEM migration and optimization, the target SIEM's Customer Engineering team recommended the company engage SnapAttack for a solution to their challenge.

We needed to move fast.

"SIEM migrations are notoriously tedious and unclear: We needed to move fast but we also needed a clear picture of our coverage." ***– Security Engineering Leader at a Large Data Center Provider***

Industry Report: On average, most organizations still struggle to tailor threat detection to their unique, critical threat landscape.



OOTB security tools miss 76% of all MITRE ATT&CK techniques

182 Days

Security teams take an average of 182 days to identify breaches

of organizations need to be faster at actioning threat intelligence

Sources: Mandiant's Global Perspectives on Threat Intelligence; IBM's Cost of a Data Breach Report 2023

Financial:

Like most legacy SIEM platforms, this organization's existing platform became ever more costly over time due to a licensing model based upon the amount of data fed to the SIEM platform. And when cost and coverage don't complement one another, leadership and security teams experience friction: prioritizing finances leaves blindspots in security visibility, but more advanced sources of telemetry are just too expensive when security can't easily articulate the value of collecting it.

Technical:

The evolving nature of their network architecture posed a formidable technical challenge for not only the legacy SIEM platform, but for the technical team responsible for quickly and efficiently getting the new platform in place. SIEM platforms are versatile tools, but they require significant customization and configuration to address an organization's unique security needs. Like many enterprises, the company relied heavily on custom detection rules, alerts, and configurations tailored to their specific environment.

Timeline:
The organization needed to migrate from their legacy SIEM to the target SIEM on a tight timeline. If they couldn't meet that deadline, the security team would have had no choice but to renew the legacy SIEM's costly annual license while simultaneously managing a complicated migration.

The Customer's Goals

Rapid Migration:
With the legacy SIEM platform's license expiration looming, it was urgent that the data center expedited migration to avoid incurring additional licensing costs. Since a gap in coverage was a non-starter, failure to meet the deadline would mean the company would have to bear the cost of both platforms during a protracted migration – a common conundrum for teams migrating SIEMs.

MITRE ATT&CK Coverage:
Most companies struggle with a lack of visibility into their MITRE ATT&CK coverage, and even if they do have that visibility, it can be challenging to understand and operationalize. The company needed to expand and accurately measure MITRE ATT&CK coverage so they could provide leadership with comprehensive, actionable reporting of their security gaps.

Less Noise:
A noisy SOC is a risky SOC, and poorly-performing detection rules lead to alert fatigue, false negatives, and expensive incidents. The company needed to ensure the broadest possible coverage, while simultaneously minimizing the noise their analyst team would have to manage – and they needed to do it fast.

Enhanced Telemetry:
The data center needed to ensure they were ingesting the right set of telemetry to enable their threat detection team to achieve their goal of improving security while reducing overall cost. With a recent expansion into cloud-based applications, any gap in coverage over their significant cloud-based infrastructure would open the company to unacceptable risk.

How SnapAttack Helped

Pre-Curated Detections:

SnapAttack's extensive detection library, comprising thousands of pre-built detection rules, can be easily translated into the query language of the target SIEM platform. Customers can quickly expand their threat coverage without the need for extensive time and resource investments typically associated with developing such content – a process that often requires specialized expertise and can span months.

Threat-Informed Defense:

SnapAttack’s detection library's exceptional power stems from its threat-informed foundation. We start with the most comprehensive threat intelligence available and go beyond intelligence analysis by emulating thousands of real-world threats within our controlled sandbox environment. Powered by machine learning, we identify the most effective detection strategies for threats spanning the MITRE ATT&CK framework, and through detection-as-code and advanced API integrations, we make the curation and deployment of threat content simple.

Machine Learning:

SnapAttack applies machine learning to automate validation and benchmark the performance of every piece of detection content, proving the efficacy of detection strategies against specific threats. This means that security teams can leverage SnapAttack’s extensive content library with confidence, enabling that rapid transition between SIEM platforms our customer needed while not only maintaining but significantly enhancing their threat coverage.

SnapAttack makes threat hunting and detection engineering fast, efficient, reliable, and comprehensive.

Enhance Reliability

Use **Detection-As-Code** and **Attack-As-Code** to validate real-world detection performance, purple team style.

Increase Speed & Efficiency

Detects threats **75% faster** and more efficiently across your technology stack.

Boost Technique Coverage

Cover **>84% of ATT&CK Techniques** with pre-built detections that can be deployed or hunted with a few clicks.

Results

Velocity:

Within 30 days of the company's implementation of SnapAttack and – critically – within the deadline of their cutover initiative, their security team had successfully deployed hundreds of validated, high-fidelity rules from our platform, providing the coverage necessary for the organization to confidently cut security threat detection over to the new SIEM. This milestone, which might otherwise have taken a year or more of continuous effort, underscores the effectiveness of SnapAttack's approach.

Threat Detection:

Our seamless integration with the target SIEM further simplified the curation and deployment of this extensive set of detection content. Setting up our API integration takes less than 15 minutes, and once integrated, deploying detection rules becomes a matter of a few simple clicks. This streamlined process significantly accelerates the transition period, making it an achievable task even within the tightest timelines.

Measurement:

SnapAttack goes beyond threat detection content deployment; we also empower organizations to measure and prove their coverage. Through our Validation Engine, we simulate real-world attacks using thousands of pre-curated attack plans designed to trigger the related detection rules, allowing security teams to validate their coverage effectively. This validation process instilled confidence among both the security team and leadership that the cutover would be successful, even in the face of the stringent timeline that the company had to contend with.

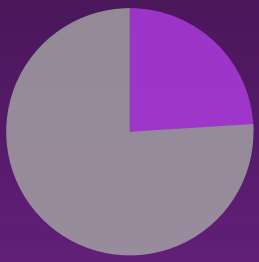
Time to migrate from legacy SIEM:

SnapAttack's comprehensive detection library enables rapid SIEM migration while simultaneously improving coverage across the MITRE ATT&CK framework.

Conclusion

With a dedication to our customer's tight deadline and the proactive threat detection content to support it, SnapAttack revolutionized the SIEM migration process by offering a vast and threat-informed detection library, simplified integration with the target SIEM, and automated validation capabilities. This comprehensive approach empowers organizations to rapidly transition between SIEM platforms, enhance their threat coverage, and validate their security posture, all within a fraction of the time typically required for such endeavors.

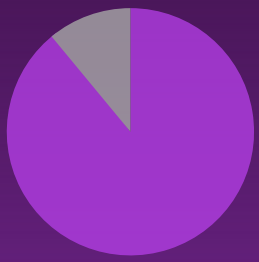
Average OOTB SIEM Coverage



24% of MITRE ATT&CK framework covered

VS

SIEM Coverage with SnapAttack



89% of MITRE ATT&CK framework covered

Whether you're planning or are right in the middle of a **SIEM migration** project, reach out to **sales@snapattack.com** today to learn how SnapAttack can **shorten the timeline** and effort, **improve your coverage,** and **give you confidence** in your security.

We're more confident in our ability to detect relevant threats than ever.

"SnapAttack's detection library simplified our SIEM process and helped us get up and running in our new platform quickly, with better coverage than we had in the old platform. We also used the platform to benchmark our detections against the MITRE ATT&CK framework so we are now able to easily report on coverage and prioritize detection engineering and threat hunting. We're more confident in our ability to detect relevant threats than ever — and we finally have the visibility in our coverage to back that confidence up." ***– Security Engineering Leader at a Large Data Center Provider***

About SnapAttack

SnapAttack is a threat management platform built by threat hunters, CISOs, and SOC leaders, and threat hunters for threat hunters, CISOs, and SOC leaders. SnapAttack includes threat hunting and training capabilities that don't just streamline threat hunts for your advanced team members – they make it quick and easy for your most junior analysts to level up their skillset to the caliber of a threat hunter.

SNAPATTACK