CASE STUDY

SNAPATTACK

Breaking Free from MSSP: Empowering In-House Cybersecurity Excellence at a Fortune 500 Bank

with SnapAttack

Introduction

Picture this: You're heading up cybersecurity at a Fortune 500 banking institution. You've already made significant investments into improving your cybersecurity maturity, but now it's time to make a big leap: moving away from the outsourced SOC/MSSP model to bring your monitoring, detection, and threat-hunting capabilities in-house.

You have no doubt that moving away from the MSSP model is the right one for your organization. Like many rapidly growing businesses, you know that your needs have outgrown the capability that an MSSP can provide. Plus, your in-house team is now mature enough to monitor and respond just like your MSSP. That said, this is a major shift for your organization… **and a few questions remain top of mind for you:**

- How do we build strategic Threat Detection capabilities that take us beyond where we were with our MSSP?
- How do we actually execute that plan with limited time and personnel bandwidth?
- Can we develop robust detections using our existing security tooling, balancing alert sensitivity without creating excessive false positives?
- How do we demonstrate and communicate our growth to other business units?

This is where our customer began its journey toward proactive cybersecurity solution exploration with SnapAttack.

The Challenge

The goal was simple: This Fortune 500 financial institution wanted to fill the expertise gap, empower its existing team, and measurably mature its overall cyber defense capabilities. Unfortunately, the company faced several barriers to this goal:

They needed the team's expertise and efficiency to strategize and execute threat detection capabilities: While they had strategic threat intelligence personnel, they lacked the tactical rigor to execute the strategy effectively - especially now that they were moving away from the outsourced SOC / MSSP model. According to the bank's VP Senior Cybersecurity Manager, hiring more people wasn't necessarily the solution.

*"We needed to get smarter about how we do our detections and alerting because we have **more log sources, more cloud providers, more applications, more everything**. We couldn't just keep throwing bodies at the problem."*

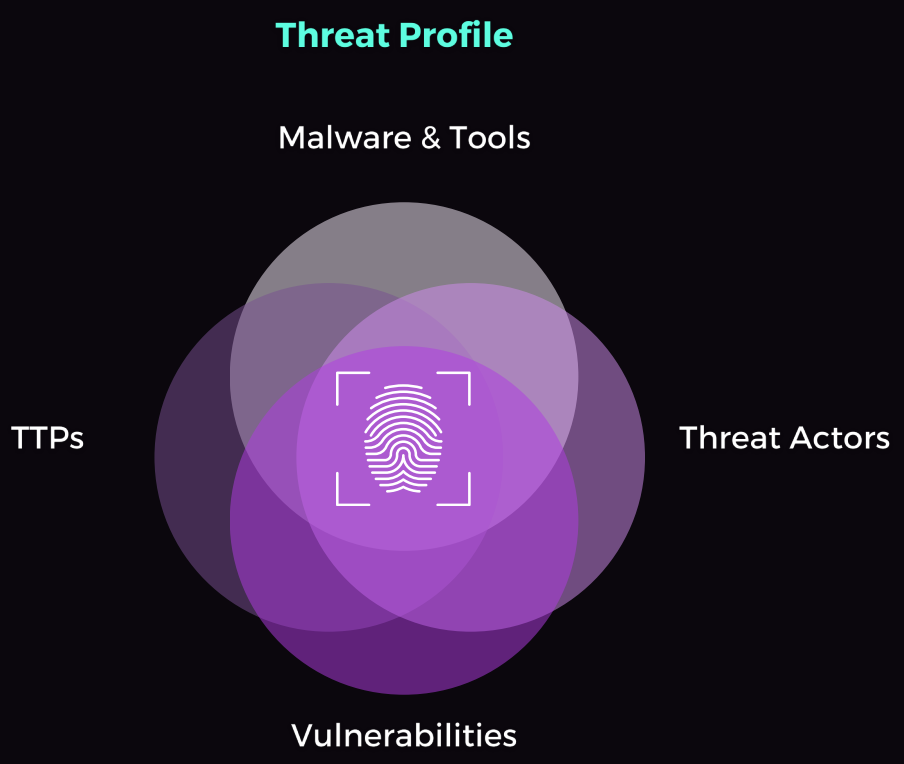
Their disparate tools made clarity and measurement a major challenge: Like many organizations, the bank's cybersecurity landscape was fragmented with disparate tools and a constantly evolving attack surface. This made it difficult to get a clear picture of their overall cybersecurity strategy.

They didn't have the necessary context to maximize the value they could get from their existing SIEM and EDR tools: Like many security teams, the bank's teams struggled to get enough value out of their SIEM/EDR because they didn't have the time to build their own high-quality detections AND put out ongoing fires at the same time. For example, while this organization leveraged Splunk's risk-based alerting feature, detection teams often found themselves assigning arbitrary scores as a starting point, adjusting as they got more and better data. With SnapAttack, they now have a data-driven risk score to start, which can be adjusted as needed, providing a better starting point.

*"Before SnapAttack, we didn't have a data-driven methodology to use as a starting point for our RBA risk scores, which made it **more challenging to find the sweet spot between eliminating risk and generating unnecessary alerts.**"*

The Solution

As they explored solutions, the bank discovered SnapAttack, a product designed to optimize Detection Engineering and Threat Hunting. **SnapAttack filled the gaps the bank was facing by offering unique features that met the bank's specific challenges head-on:**

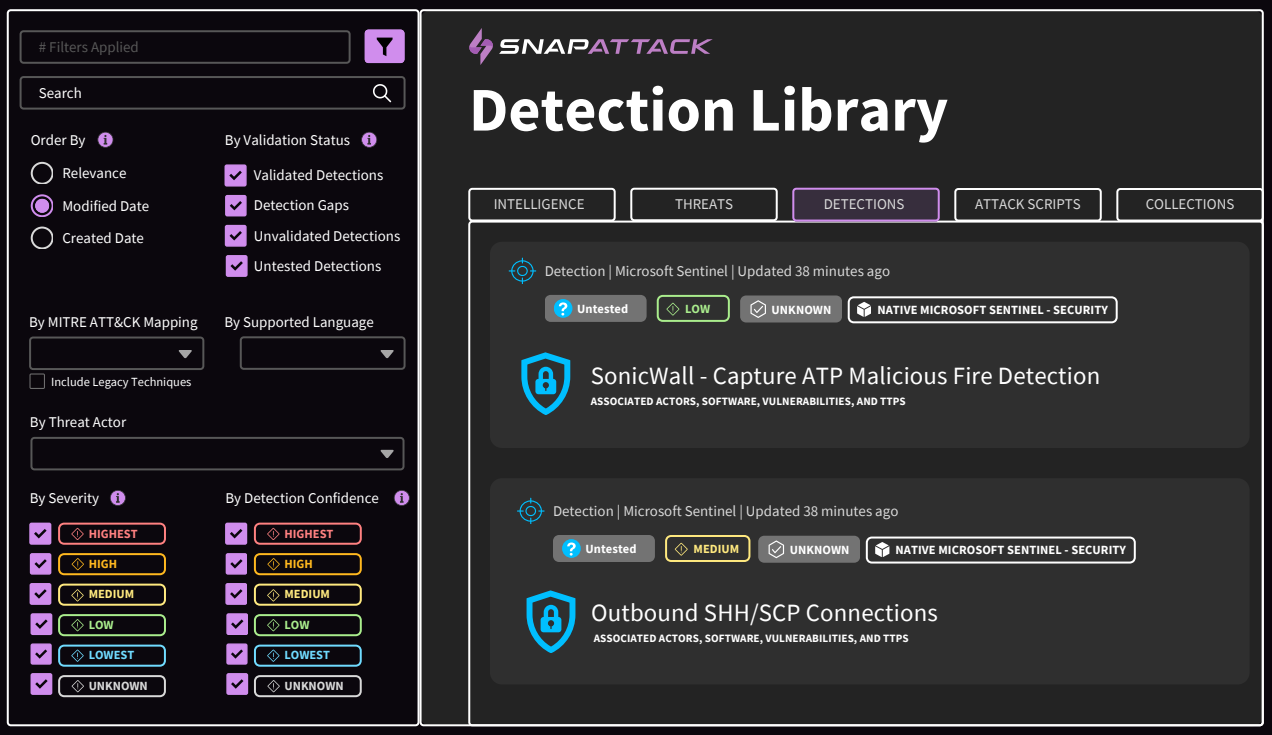


1

SnapAttack's Threat Profiles and MITRE Mapping features provided context, confidence, and directionality, which enabled the bank to develop more strategic threat detection capabilities.

SnapAttack's threat profile and MITRE mapping features provided context amidst the chaos of information, offering a coherent strategy with which security leaders could guide their teams with confidence. **This allowed security leadership to answer critical questions, like:**

- Where do we stand today?
- Which threats matter most to us?
- Where do we need to focus first?



2

Greater Efficiency in Detection Engineering

SnapAttack was built to offer the most advanced detection engineering lab so businesses don't require the world's most advanced detection engineering teams. It streamlined the bank's detection development process through its high-quality detection library - filled with endless, high-quality, pre-built detection content.

3

Additional context that enabled the bank to get more value from its existing security tooling.

One unexpected benefit that SnapAttack delivered to this Fortune 500 bank was a better process for the bank's Splunk risk-based alert scoring. Because the detection content within SnapAttack was high quality, tested, and rich in context (tailoring recommendations with things like confidence rank and severity rank), Chris was able to assign a more scientific risk score for each detection.

4

Greater Visibility to Measure and Analyze Progress

And finally, SnapAttack's MITRE mapping capabilities provided a clear picture of their cybersecurity posture and progress over time.

The Results

According to Chris, the benefits of implementing SnapAttack are still in the process of being fully realized. **However, in just a few months, he's adamant that significant, tangible ROI has already been achieved:**

Better Detection at a Lower Cost

Because SnapAttack was able to help this bank identify which data actually mattered to them, the organization was able to optimize the storage of the log sources most relevant to their detection estate.

More Streamlined Detection Engineering Processes

What once was a process of ping-ponging through log data, searching through X and other internet sites to see if someone had already put something out for a given threat, SnapAttack came in and acted as a compass for detection development with its high-quality detection library.

So when a new threat emerged, the senior cybersecurity manager Chris could simply type it into SnapAttack's search bar to find pre-built detections or reach out to SnapAttack's best-in-class customer support team to request new ones, often getting the new detections developed and delivered within a day or two.

More ROI, More Efficiency, and Fewer Gaps

By extending the capabilities of the in-house security team and supplementing their existing skills with SnapAttack's content and detection-building features, the bank saved the budget that would have been spent on expanding the team or hiring expensive consultants.

*"We no longer have to build from scratch every single time. We're not going at it alone because **SnapAttack augments what we do and extends the team.**"*

Armed with SnapAttack, this Fortune 500 bank's security teams were finally able to work smarter, not harder. **As a result, the bank was able to realize its initial goals and enhance its cybersecurity defenses, all while optimizing its resources.**

Once Chris' teams learned how to use SnapAttack to streamline their workflows, it was off to the races. Month over month, more and more team members are leaning on SnapAttack to add directionality to threat hunts and detection engineering. **Today, team members across threat intelligence, hunting, and detection are all leveraging SnapAttack with a more unified focus on tackling the latest emerging threats.**

Are you making the move away from the outsourced SOC / MSSP model in the near future? SnapAttack's platform, alongside its superior customer support and implementation resources, can help. **Contact us to see how we can help your team navigate the transition with both clarity and confidence.**

SnapAttack is the enterprise-ready platform that helps security leaders answer their most pressing question: "Are we protected?"

By rolling intel, adversary emulation, detection engineering, threat hunting, and purple teaming into a single, easy-to-use product with a no-code interface, SnapAttack enables you to get more from your technologies, more from your teams, and makes staying ahead of the threat not only possible - but also achievable.

Whether you're an analyst or a CISO, a red teamer or a blue teamer, SnapAttack unlocks the potential of your security operations and enhances existing toolsets.