SNAPATTACK

Making Threat Detection an Inside Job

A Practical Guide on Why and How to Build and Scale In-House Threat Detection

Table of Contents

Introduction

CISOs and security leaders are increasingly under pressure to “align security with the business.”

But what does that really mean in practice?

With the escalating scale and mounting sophistication of cyberattacks, the new reality in front of us is quite simple: defending against every threat out there is just not possible. To survive and thrive in today’s threat landscape, security operations teams must shift their focus toward building prevention, detection, and response capabilities that are actually tailored to the systems, risks, threats, users, and even behaviors that are unique to their organization. This tailored approach is fundamental to aligning security to the business.

According to ESG’s 2024 SOC Market Trends Report:

36% **Threat Intelligence -** 36% of organizations have a goal to operationalize Threat Intelligence better.

34% **Threat Detection -** 34% want to better detect threats by combining and/or enriching (utilizing) the data they already have about security incidents.

34% **Investigation/Triage -** 34% see a need to drive more effective engagement of security incidents based on critical business data and assets.

The challenge is precisely that every organization is different; there is no prescriptive, one-size-fits-all solution that easily enables strategic, focused, and effective security operations.

While the severe shortage of talent in cybersecurity continues to trend upward, it’s no surprise that MDRs and MSSPs that provide ‘Managed Detection’ and/or ‘SOC-As-A-Service’ continue to gain popularity. To be clear, this kind of service is extremely valuable for many organizations that don’t have a pressing need for more tailored capabilities aligned to their business. However, the MDR/MSSP business model only makes sense for providers when they can build an offering once and deliver it repeatedly, with minimal customization and tailoring, to many customers.

In other words, while some vendors might promise the world in terms of business alignment, the reality is that incentives simply don't align.

For those organizations that have needs that go beyond checking a compliance box, it often makes more sense to bring Detection Engineering, Threat Hunting, and Triage in-house instead of relying on an MSSP/MDR.

Of course, bringing Threat Detection in-house is no easy feat.

However, if any of these sentiments about your MSSP/MDR hit home, it might be time to consider a transition:

"Sometimes, alerts are incorrectly dismissed as "False Positives" by our provider because they don't know enough about the systems, assets, and entities being described in the alert."

"It takes too long for alerts to get investigated and escalated."

"My provider says they do Threat Hunting in my environment, but I never see or hear anything useful from them about it."

"We get far too many "False Positive" alerts that eat up my team's time."

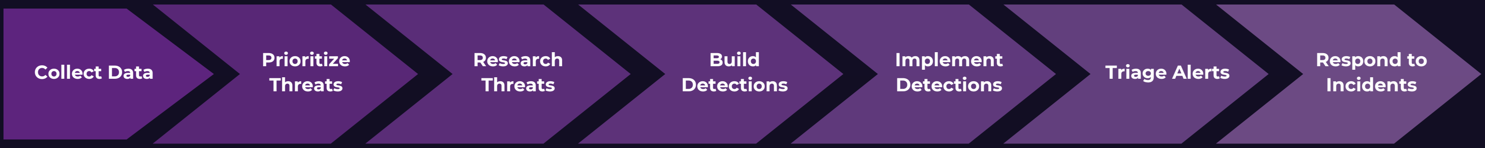
"The detections that our provider leverages are far too generic and they aren't building anything that's specific to our needs."

"They just can't keep up with the number of requests we have and they don't seem to understand what we need."

"We get too many alerts for extremely low-severity nothing-burger activities".

The Case for In-House Detection and Threat Hunting

Put simply, effective Threat Detection is a single motion that spans multiple distinct but highly related and interdependent teams and functions. If the outputs from one phase act as direct inputs for the next phase, then it should logically follow that unifying strategy and execution across all phases, under one roof, and with a common goal, will lead to better outcomes.



Introducing an MDR/MSSP into this equation invites agenda, information, and operations discontinuity. Because surprisingly, what's best for your business isn't necessarily what's best for an MDR/MSSP. Put another way, helping your organization detect the threats that matter most, detect more threats, and detect threats earlier is not always correlated with helping the MDR/MSSP increase revenue and profits.

Bringing more of these functions in-house—especially the functions that exist further to the left of this lifecycle enables you to:

- Eliminate competing interests that don't benefit your business.
- Set strategic objectives that better align with your organizational needs.
- Pave the way for more effective detection development, hunting, investigation, and response through information availability.
- Promote more tailored operations.

Advantage 1 → Unified Agenda and Strategy

It’s significantly easier to set an overarching strategy and establish objectives when you don’t have to de-conflict these agendas with the often opposing needs of your MDR/MSSP.

On the other hand, an in-house Detection Engineering and/or Threat Hunting team is far more incentivized to:

1. Consume threat intelligence to become more proactive in understanding which threats are most relevant to the organization.
2. Consult with security leadership to understand goals and set the correct objectives.
3. Collaborate with other security teams to identify gaps and recommend improvements.

These activities serve as the foundation for effective Threat Detection. Without them, the effectiveness of Threat Detection becomes unclear, difficult to measure, and impossible to manage.

SnapAttack’s Approach to Training

- **Types of Training:**
  - Detection Engineering
  - Threat Hunting
  - Threat Research
- **For each training type, you’ll need to focus on:**
  - Strategy Approach - Tying all activities back to a central strategy.
  - Processes
    - What’s the general response when you receive an alert?
    - When you get an alert, what next?
  - Procedures
    - If a specific alert appears, follow steps A-B-C.
    - If a different alert appears, follow steps X-Y-Z.

Advantage 2 → Information Availability

No external person or team can know your business, your technology, your assets, your employees, and your systems as well as you can. “Context is king” and a lack of context drives down effectiveness between phases of the Threat Detection lifecycle.

Here are just a handful of examples:

- **Detection Development –** Operators depend on strong data collection and threat prioritization to know which detections can and should be built.

- **Threat Hunting –** Hunters require an in-depth understanding of what to hunt for, how to hunt for it, and where to hunt for it. However, the answers to all of these questions will vary depending on the organization’s business, its technology stack, its current detection coverage, etc.

- **Triage –** Analysts need a complete understanding of the security use cases that detections are designed for so that they know how to think about investigating an alert. They might also need to know what role or function an asset, system, or even user serves within an organization to understand whether or not the activity they are observing is a threat.

- **Response –** Similarly, response times are impacted when operators are forced to spend time re-assessing the security use case, understanding potential impact, and figuring out the next steps.

```
3       .
53      ..
15      bin -> usr/bin
9:31    boot
15:50   dev
p 09:32 etc
ep 15:52 home
Sep 2015 lib -> usr/lib
Sep 2015 lib64 -> usr/lib
3. Jul 10:01 lost+found
1. Aug 22:45 mnt
30. Sep 2015 opt
21. Sep 15:52 private -> /h
1. Sep 08:15
```

Bringing Threat Detection in-house puts key context about your organization at the fingertips or within reach of operators.

- A Detection Engineer who is unsure what data might be available for a particular threat can reach out to a Security Engineer responsible for managing an appliance to figure out what should be getting logged, what isn’t logged, and how to enable logging.
- A Threat Hunter can leverage information from the Threat Intelligence team and consult with Detection Engineers to decide to conduct a hunting exercise for a specific new and emerging threat that is most relevant to the organization and isn’t already covered by existing detection rules.
- A SOC Analyst who doesn’t understand what to do with an alert can reach out to the Detection Engineer who created it to gain a clearer sense of the security use case, help that Detection Engineer flesh out tuning opportunities to reduce false positives, and even suggest new detection rules that would help automate some more manual investigation findings.
- An Incident Responder might be able to leverage their understanding of the organization to prioritize incidents based on the assets affected, the business lines that they impact, and even the users that are involved.

The unmatched knowledge that in-house teams have of your business and systems boosts Threat Detection more effectively than through external teams. This internal understanding enriches detection development, threat hunting, triage, and response by providing the necessary context to tailor strategies.

Advantage 3 → Tailored Operations

One size *absolutely* does not fit all when it comes to Threat Detection. Unfortunately, how an MDR/MSSP operates on a day-to-day or case-by-case basis is designed to solve challenges associated with servicing multiple clients. The key to scaling for these service-based businesses is to build processes and procedures once and modify them as little as possible across clients. These compromises force clients to give up granular control over processes and procedures that might help maximize their ability to detect the threats that matter most, detect more threats, and detect them faster.

However, with an in-house team, you are free to build and enforce more custom and effective processes and procedures for a variety of functions.

Here are some examples:

- **Detection Development –** How a detection is developed and tested before moving to production can impact the volume and quality of alerts that the SOC is then responsible for triaging. Introducing additional requirements and measures enables teams to address these challenges at a level that works best for your organization. For example, if you have a severe alert fatigue issue, you might require that a new detection rule be tested in silent mode for two weeks before being enabled. Conversely, if you want to prioritize speed and don't have an alert fatigue problem, you might be able to waive certain testing requirements that an MDR/MSSP would have to follow as part of their processes.

- **Threat Hunting –** A business could maximize the ROI of Threat Hunting exercises by building processes that encourage Threat Hunters to enumerate and disseminate information from findings that go beyond whether or not they found a security incident. For instance, standard output from a threat-hunting exercise could identify gaps in data collection, improperly configured controls, or even problematic trends in user/employee behavior.

- **Triage –** An organization might be able to speed up MTTR by enabling a SOC Analyst to prioritize or process certain alerts differently, depending on the nature of the security use case, the entities alerted on, or the potential impact associated with it. A team could even improve overall alert quality and reduce the need for more resources by requiring that analysts document false positives and share them with Detection Engineers in weekly review sessions.

This customization is key to tailored detection development, insightful threat hunting, and refined triage practices. Ultimately, building internal capabilities empowers organizations to enhance their overall threat detection and response, achieving a more robust security posture.

In-House Challenges to Detection Engineering and Threat Hunting

Building a successful in-house threat detection team doesn't come without some hurdles, such as finding the right talent, building good processes, and using the right technology. If it were easy, people wouldn't need MDRs and MSSPs.

People Problems

According to Enterprise Strategy Group's 2024 SOC Market Trends Report, nearly 9 in 10 organizations are feeling the impact of the cybersecurity skills shortage in today's labor market. But let's be honest, this is nothing new.

We can't create more qualified candidates for you, however, we can tell you what key attributes you should be looking for, even when experience and hard-technical skills are in short supply:

1. **Methodology and Data Literacy**
   Candidates should exhibit a scientific approach to problem-solving and possess the capability to analyze and interpret data. In other words, the ability to continuously ask new and interesting questions, figure out how to find answers using data, and use those answers to ask better questions (or drive outcomes for the organization).

2. **Curiosity and Learning Ability**
   The rapidly evolving threat detection landscape demands professionals who are innately curious and driven to learn autonomously. Those with a genuine interest in exploring new ideas and acquiring knowledge independently can quickly fill gaps and update their skills. This intrinsic motivation ensures they adapt effectively to the field's ever-expanding challenges.

3. **Communication and Collaboration**
   Effective threat detection requires strong communication skills to engage security teams and secure support. Candidates must convey the value and urgency of initiatives clearly, fostering collaboration across stakeholders.

It’s impossible to know it all and have experience in “all of the things,” but you CAN focus on hiring people who have the right blend of soft skills, as well as the mindset to become effective quickly.

SnapAttack’s Augmentation Capabilities

SnapAttack offers its product alongside a few professional services such as Detection Engineering-as-a-service and Threat Hunting-as-a-service. This allows us to help our customers directly address time and skill deficits through a blend of productized expertise and managed services.

Process Challenges

Establishing robust processes is critical for building an efficient and effective in-house threat detection team. However, establishing these processes presents its own set of challenges due to the dynamic nature of cybersecurity threats and the evolving needs of the organization.

- **Version Control –** Unlike standardized MDR and MSSP solutions, in-house teams must create processes tailored to their unique environment, risk profile, and goals. This requires ongoing customization and iterative improvements—challenging, but worthwhile.

- **Documentation –** Reliable, repeatable processes require clear documentation to ensure team members understand their roles and execute consistently. Standardizing procedures simplifies onboarding, reduces errors, and improves accountability. Striking the right balance between thorough documentation and agility is key to enabling swift threat responses.

- **Integration with the Broader Business –** Threat detection requires collaboration with departments like IT, legal, and compliance for comprehensive risk management. Effective processes need clear communication, defined escalation paths, and cross-functional workflows. Building these connections ensures a holistic security posture despite the challenges.

Technology Challenges

While the right technology can significantly enhance an in-house threat detection team's effectiveness, the wrong ones can absolutely break it.

1 **Capabilities - Not all analytics tools are built equal, but the best ones will excel in most of these areas.**

- Data Storage – Easy to extract, ship, and store data.
- Data Normalization – It is possible and minimally painful to structure and format data in ways that make it easier for consumers.
- Search - Easy to use, fast, and come with more complex functions if necessary.
- Enrichment Engine – It is possible and painless to add context to events and/or alerts from other sources.
- Rules Engine – Relatively easy to use, there are no limits to the amount of rules that you can run, and the rules are highly customizable with additional functions.

2 **Cost**

While the investment may seem significant, it's important to recognize that it's an expected part of finding a solution that truly supports your team's growth. Opting for a lower-cost, simpler solution might save money upfront, but it often comes with limitations that can hinder long-term success. Consider the time, effort, and potential disruption of migrating to a new solution down the line—sometimes paying more now avoids greater costs later.

3 **Ease of Use**

Analytics tools are just that: tools. To extract value from them, experts need to wield these tools. However, more complex is not always better. You can't get value out of a solution that isn't easy enough for your team to leverage. In other words, solutions designed to solve traditional big data problems, which address a different problem set than security challenges, or those requiring significant ongoing maintenance by actual engineers, are not ideal.

Buy-In

The answer to the meaning of life is 42.

All joking aside, the key to finding buy-in probably has something to do with taking a long hard look at what your MSSP/MDR is actually costing you, beyond the face value of the service, now and in the future.

What exactly is the cost of…

- …a missed incident?
- …high MTTD and MTTR?
- …all the time and energy spent making up for the deficiencies in your current service?

Is your MSSP/MDR actually saving you more money than it is costing you? It might be—and that's great! But as your business grows, the challenges you face will grow too, and the costs may start to outweigh the benefits. The longer you wait to address these challenges, the harder and more expensive it becomes to solve them on a larger scale. **Here's why:**

1. **Risk**
   Security risks will grow alongside your business, making them harder and costlier to manage later.

2. **Scalability**
   Your needs will eventually outpace what an MSSP/MDR can provide, as we've outlined earlier.

3. **Transition**
   Moving away from an MDR/MSSP requires acceptance of risk because bringing things in-house is not an instantaneous or seamless process.

It is more cost-effective to accept fewer risks now, while the business is still growing than it is to accept them later, when the impact could be magnitudes greater.

The Roadmap to Building a Threat-Hunting and Detection Engineering Team

Securing Buy-In

One of the most essential skills for a cybersecurity leader is translating technical concepts into terms that non-technical stakeholders understand, especially when those stakeholders may be wary of additional cybersecurity spending. **Here are some key tips for making a compelling case:**

First, you have to make the case for WHY.

- The priority is to educate leadership about why an in-house approach is necessary. This might involve explaining how the traditional MSSP/MDR model wasn’t designed to address today’s evolving threat landscape. You will have to show them why a tailored approach is critical for aligning cybersecurity with the business and for reducing operational risk. This will be even more effective if you can quantify the business risk in terms of things like the hard dollar cost of operational downtime.

- Once you make the case for why the outsourced model is fundamentally flawed, then you have to position in-house detection engineering and threat-hunting teams as a strategic advantage, underscoring the benefits mentioned in the above section with clear examples of what those advantages look like in practice.

Then, you have to alleviate concerns around the HOW – Unfortunately, showing leadership why they need to make a change does not actually get you to the finish line. To get there, you have to address potential concerns by anticipating common questions, such as:

- **"How will we manage and transition with minimal business disruption?"** Outline clear, actionable steps to manage a smooth transition, emphasizing that the shift will not be done overnight and can be conducted with minimal disruption to daily operations. Be sure to emphasize the long-term viability and additional that in-house operations offer.

- **"Do we have adequate internal skill sets?"** Leaders may worry about whether the organization has the necessary in-house expertise needed to make this shift. It's important to acknowledge potential roadblocks honestly. However, by highlighting solutions like SnapAttack, which streamline detection development and provide a clear process, you can address concerns and put doubts to rest.

- **"Will we remain compliant?"** Many executives trust MSSPs due to their compliance certifications and structured processes. Reassure leadership that the in-house model can meet or even exceed these compliance standards.

- **"How will we measure success?"** It might be helpful to start your answer to this question by being honest about how hard it is to measure the success (or lack thereof) of an MSSP/MDR provider. Then, you have to articulate specific OKRS (objectives and key results), showing what you plan to track and how each individual KPI will offer more clarity of where your cyber resilience stands in the short term and more ROI over the long term.

Taking the First Step

So, you’ve decided to bring detection engineering and threat hunting in-house, and you’ve overcome the initial hurdles. But now it’s game time—how does the real work actually begin?

First, it’s essential to remember: Rome wasn’t built in a day. Building a mature in-house capability takes time.

Milestone 1 → Go Hybrid

The first milestone to reach is where you have some form of hybrid model, one where you either outsource Detection Engineering or T1 SOC. This enables you to dip your toes into the world of in-house Threat Detection without necessarily leaving massive capability gaps behind and necessitating a massive hiring event.

- **Choosing to Outsource T1 SOC and Opt for In-House Detection Engineering**
    - This means that your organization will be responsible for owning and maintaining the SIEM(s) and EDR(s) and building and maintaining detection rules while the outsourced team triages the alerts. This approach, while less common, gives your team the ability to drive outcomes more effectively and directly without being burdened by running the SOC on a day-to-day basis.

- **Choosing to Outsource Detection Engineering and Opt for In-House T1 SOC**
    - This means that your team will be primarily responsible for engaging, investigating, and escalating alerts generated by the 3rd party that manages an SIEM & EDR for you, regardless of whether you or they technically own it. This approach can allow your team to dabble with Detection Engineering and Threat Hunting and build additional skills without having to take complete ownership of them.

Importantly, either model enables you to break the link between managing detection rules and managing alerts, which most service providers want tight control over because it has a direct impact on their overhead.

Milestone 2 → Build a Flat Threat Detection Team

The second milestone likely involves building a non-traditional, “flat” Threat Detection Team that is responsible for Detection Engineering, T1 SOC, T2+ SOC, and IR. Sharing these responsibilities will give your team a clear sense of how the overall Threat Detection ecosystem operates, how proficiency in the earlier phases of the lifecycle can drive better outcomes in later phases, and allow them to learn new skills in all areas.

You’ll also want to start building some repeatable processes and procedures that answer questions, like:

- How should alerts be investigated?
- What kind of documentation do we need to build before we release a new detection rule?
- How do we prioritize things?

However, don’t forget that at this point, you don’t have to be great, you just have to be good enough. As a leader, don’t get caught up in trying to optimize for the first point-problems you identify just yet. Instead, use this time to explore what’s working well, analyze the foundational challenges that are holding your team back, such as skills or technology, gather information, identify some basic KPIs, and start planning for long-term growth.

Milestone 3 → Begin Specializing, Measuring, and Reporting

Milestone 3 is where your in-house capabilities rise from being a sideshow to becoming the main event.

Specialization

Reaching such levels of prestige requires specialization, as not everyone is cut out to do all of the jobs in Threat Detection (and let’s be honest, it’s impossible to do all of them at an expert level).

It is at this phase of growth that you should consider assigning leads for Triage and IR while building a dedicated function for Detection Engineering. Don’t jump right to Threat Hunting! There are some essential skills and habits in Detection Engineering that you don’t want Threat Hunters to miss out on (specifically, the willingness and ability to automate hunts as rules). Instead, start with Detection Engineering and eventually spin the threat-hunting capability out.

Measurement

“You can’t manage what you can’t measure”, so this is also the time to flesh out more specialized KPIs for each function and, importantly, enumerate the relationships between KPIs across functions. Remember, each phase of Threat Detection is linked to the ones that came before it. Don’t try to fix a downstream problem without figuring out what root causes are driving it.

Reporting

Finally, make sure that you are actively capturing the value that your teams are delivering, communicating this value to leadership, and soliciting feedback. You need more funding and increased headcount to achieve your goals, right?

Milestone 4 → Go for Perfect

Milestone 4 is for when everything else is humming along smoothly. It's reached when you know where you are today, have a clear sense of where you need to be, and know how you'll get there.

This is where you'll need a crack team of expert Threat Hunters. No, not folks who can search for IoCs. We're talking about people who can do their own in-depth research into new and emerging threats, know exactly where the gaps in your defenses are, and have the skills and time to explore those gaps to flesh out incidents and identify opportunities to improve.

Ready to ditch your MDR or MSSP? Here's How SnapAttack Can Help!

SnapAttack was designed to support organizations looking to transition away from the MSSP/MDR model. **It addresses the core challenges faced by teams aiming to bring cybersecurity in-house:**

It solves technology problems → SnapAttack integrates seamlessly with your SIEM and EDR platforms, even if you're juggling multiple systems, giving you comprehensive visibility and control.

It solves people and process problems → SnapAttack bridges skills gaps, supports on-the-job learning and facilitates a structured process that fosters greater collaboration across teams. Because the platform is horizontally oriented, it guides your teams through a workflow that enables them to build and hone their skill sets by asking the right questions:

- What are the threats?
- Which ones matter most?
- What is our coverage for those threats?
- How do we mitigate risk?
- How can we measure improvement over time?

It solves buy-in problems → With robust reporting and dashboards, SnapAttack makes it easier to demonstrate value and secure stakeholder support no matter which milestone you're at within your journey.

With SnapAttack, you're not just adopting a tool, you're beginning a journey from external reliance to full in-house capability. **Here's how we guide teams through each step of that transformation:**

1 Augmentation - SnapAttack Platform + Services

You get the platform, along with our expertise to operate it on your behalf—combining products and services for maximum impact. This automatically reduces your reliance on external MDRs or MSSPs.

2 Get Tools and Customized Training to Start Doing It Yourself

This step aligns with Milestone #2 by addressing skill gaps within your team and introducing structure, measurable goals, and alignment with a threat-informed strategy specifically tailored to your business needs.

- **First, we expand your team's capabilities with targeted training in the three essential skill areas →**
    - Detection Engineering
    - Threat Hunting
    - Threat Research

- **Next, we build a strong foundation of understanding, alignment, and process discipline within each skill area →**
    - Strategic Alignment – Ensuring actions align with a central strategy.
    - Processes – Developing general incident-handling steps, like determining the next steps upon receiving an alert.
    - Procedures – Creating specific actions based on alert type.

3

- **Finally, we support your team with platform tools that provide context and streamline workflow →** SnapAttack's platform enhances threat intelligence actionability by tying research and sandbox reports directly to attack scripts and detections. Beyond that, pre-written, validated detection content helps you move from understanding the threat to defending against it up to **98% faster.**

3 Streamline and Aim for Continuous Improvement

This step aligns with milestones #3-4—focusing on continuous improvement. While SnapAttack's platform offers a wealth of pre-written content, as your in-house detection engineering and threat-hunting functions mature, you may want to leverage SnapAttack's features as we do, building fresh content from scratch. **SnapAttack offers a wealth of resources and built-in features to help you:**

Unify Your Strategy →

- Threat Profile – Guides the strategy by unifying detection engineer and threat hunt teams, prioritizing threat actors, malware, and TTPs based on your industry, geographic region, and more.
- Threat Collections – Translates threat-specific objectives into actionable items, with all context, intel, reports, detections, and tests accessible in one place.

Streamline Execution → With your threat profile in hand, your teams are equipped to align their execution with your broader strategy, focusing on the threats that matter most to your organization.

- Sandbox – Perform in-depth threat research and quickly translate findings into usable detection capabilities.
- Detection Builder – Build and manage portable detections efficiently, without the need for in-depth coding knowledge.
- Attack Script Execution Framework – Develop, manage, and run tests from one centralized location.

Features to Measure and Articulate Value → Dashboards and reporting tools help you communicate progress and demonstrate value by showing measurable outcomes and supporting continuous improvement efforts.

- MITRE ATT&CK Priority + Coverage – Measure and improve detection coverage by Technique & Sub-Technique priority, deploying quickly to close high-priority gaps.
- Threat Profile Priority + Coverage – Track detection coverage across prioritized threats and deploy to address critical gaps.
- Detection Health – Easily identify, track, and action detections that have updates, deployment errors, and performance issues.
- NIST 800-53 – Track and assess compliance with NIST 800-53 security and privacy controls.

Conclusion

3

Bringing threat detection and threat hunting in-house isn’t just a shift in operational responsibility—it’s a strategic leap toward a more secure, agile, and business-aligned security posture. While the journey may seem daunting, the rewards far outweigh the challenges. By owning and optimizing detection capabilities, your organization gains unmatched insight, control, and resilience, allowing you to detect threats earlier, respond faster, and drive measurable business outcomes.

SnapAttack is here to help you navigate this transformation. Whether you’re augmenting your current capabilities, building from the ground up, or refining a mature program, SnapAttack provides the tools, training, and expertise to empower your team every step of the way.

It’s time to rethink the status quo, prioritize what matters most, and make threat detection an inside job. Let SnapAttack help you turn your vision of in-house threat detection into a reality.

About SnapAttack

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.