
SNAPATTACK
Are we protected?
Mobilizing threat-informed defense
through continuous purple teaming

SNAPATTACK

Are you protected?

Despite all the tools out there—from spreadsheets and data to security automation, Artificial Intelligence, and machine learning—security leaders still can't answer the question:

Are we protected?

The problem

Threats and vulnerabilities are complex and rapidly changing. But the explosion of new tools and data feeds, the rise of remote work, and the prevalence of the cloud have created a perfect storm for companies and governments alike.

Why there's a problem

Where threat actors collaborate with each other, organizations have become increasingly siloed. Where attackers have removed barriers to scale, security leaders have adopted an endless array of point solutions and quick fixes—adding layer upon layer of inefficiency within the SOC. Where they're looking at the big picture, organizations seem to suffer from tunnel vision.

The solution: threat-informed defense

Threat-informed defense is about understanding your own defensive posture and the vulnerabilities in your attack surface (everyone has them) alongside the outside threats who seek to prey on them (everyone has these, too).

The best approach to threat-informed defense is to drive collaboration between red team operators and blue team defenders, detect techniques earlier in the kill chain, and move toward a proactive cybersecurity posture.

Threat-informed defense

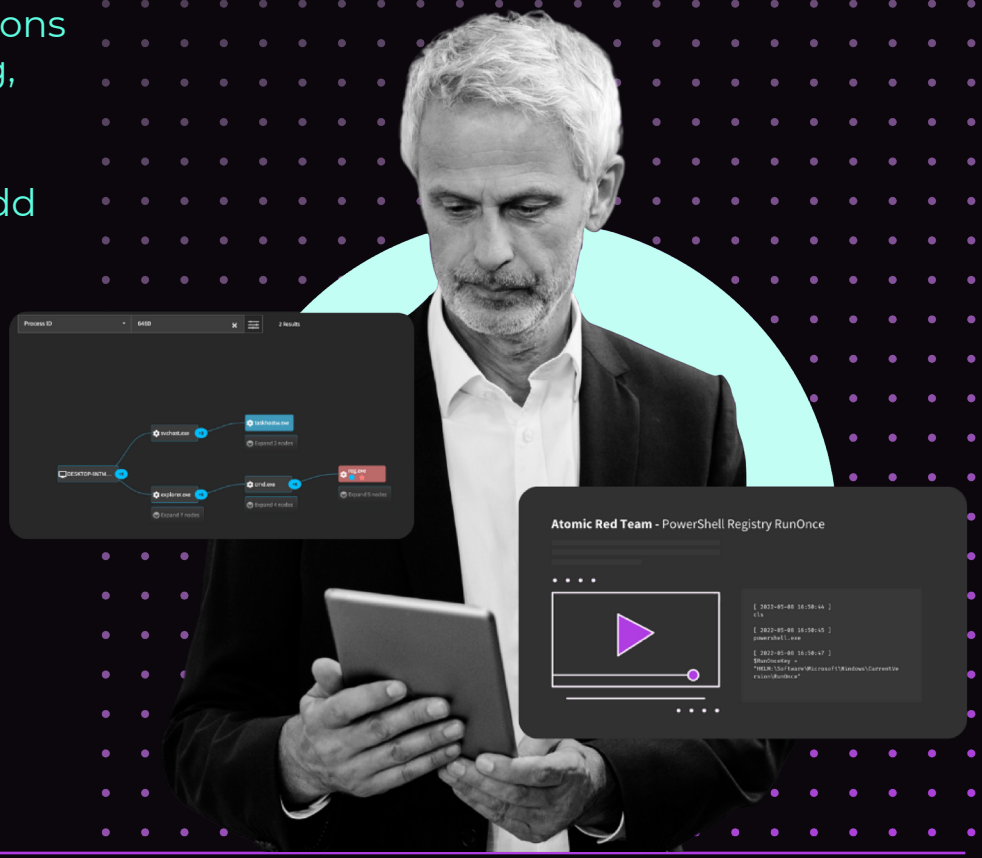
How we got here and where we're going

Previous solutions

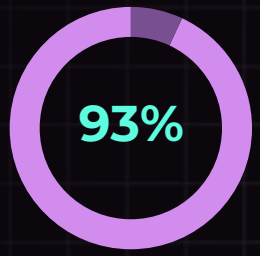
Where there's a need, there's a product— even if that product solves a narrow problem. As cybersecurity threats multiply at a dizzying rate, so too do the point solutions to counter each threat. CISOs are still left wondering, Are we protected?

The wide array of tools on the market continue to add noise to the SOC workflow despite persistent gaps:

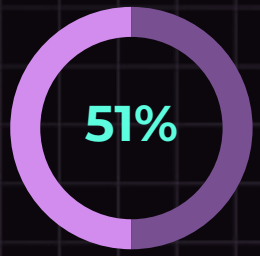
- SIEM tools moved things forward by aggregating events, but analysts are drowning in thousands of incoming alerts each day with little sense of the big picture. It costs money to capture log data, and to integrate tools—so organizations typically do a minimum to get by.
- EDR added an additional layer of defense by using data to identify threat patterns, but its benefits are confined to endpoints—and attackers have expanded their focus beyond endpoints and across the attack surface.
- XDR provided additional context by connecting data sources, but it still fails to translate attacker behaviors into operational defenses.



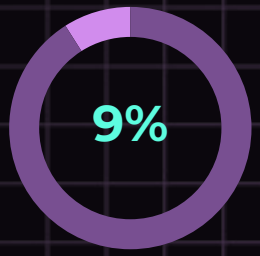
Threat-informed defense



of organizations receive more than 5,000 alerts every day



of these alerts are investigated due to lack of resources



of attacks generate an alert, which means thousands go undetected

Lingering problems

Today, CISOs continue to wrestle with the growing frequency of cyberattacks that pose significant risk to all aspects of their organizations, citing silos between teams, interoperability between tools, and inconsistent visibility as the greatest causes of anxiety.

The truth is, no matter how much you spend on technology or how many talented people you hire, there are holes. There will always be holes.

Every day, 93% of organizations receive more than 5,000 alerts, but security teams only have the resources to investigate about 51% of them (Cisco 2020 CISO Benchmark Report). And as overwhelming as that sounds, only 9% of attacks actually generate an alert—meaning thousands more threats are flying under your radar every day.

Toward a threat-informed defense

There are so many solutions on the market, yet none of them address the lingering anxieties and obstacles CISOs continue to bear. Many are either focused on signature-based detection, which is subject to change; or anomaly-based detections that simply don't work—or that can prove too noisy.

By starting at the source of these problems, aligning teams with succinct processes and equipping them with flexible tools, we can enable proactive action earlier in the kill chain. That's the goal of **purple teaming:** to bring teams together so they can understand attacker tradecraft, build robust defensive capabilities, and contextualize their coverage with confidence.

What is purple teaming?

pur·ple tea·ming

Verb
/ pUHR-puhl tEE-ming /

To put it simply, purple teaming is the convergence of blue and red teams into a single team, bringing together offensive and defensive efforts into one collaborative effort with the goal of elevating the overall cybersecurity strategy.

The process is often formalized as one-time or even quarterly events where security leaders identify goals, duration, and outcomes. Since the outcomes are defined, the goal is to identify any gaps associated with defending a particular attack vector and defenses that could be put in place to protect against that attack vector.

Purple teaming

Varying approaches

Purple teaming sounds great in theory, but what does it mean in practice? Depending on who you talk to, implementing a purple teaming operation varies greatly.

Breach and attack simulation (BAS) vendors have one approach, products that claim to facilitate purple teaming offer another, and then there's purple teaming products and service providers. Unfortunately, each falls short:

The BAS approach

What it is

Breach and attack simulation (BAS) vendors evaluate attacks and rank priorities for the defensive team.

Essentially, the security team will run tests and identify successful attacks in their environment to then give the blue team a clearer vision of where their priorities should lie.

Where it falls short

While BAS is a critical step in any company's SecOps workflow, it isn't comprehensive. To confidently and completely build out a defensive posture, the blue team needs to know more than just what was broken: they need the context of how it was broken and how it must be fixed.

BAS is a necessary step in any purple teaming platform—it's absolutely built into ours—but it's only a starting point that ultimately leaves the red and blue teams siloed.

Varying approaches

Conventional purple team products

What it is

The aim is to simplify and centralize the reporting process between red and blue teams. Both teams use integrated, automated systems to document their process and results in one location so that over time, the tool generates reports showing the progression of both teams' efforts.

Where it falls short

While reporting is critical for the tracking and management of purple teaming activities, the teams are still not working in tandem as a truly purple team. Simply observing each others' activities and combining them into one report or platform is not enough to break down the wall between the two and orchestrate inclusive exercises.

Purple teaming services

What it is

Purple teaming services facilitate cybersecurity exercises, often involving outsourced red teams, in an effort to bridge the gap between defense and offense.

Where it falls short

While this fills the gap left by purple team products, it is still missing the critical "continuous" element. Event-based exercises fail to holistically bridge the disconnect between red and blue teams: in the end, the two are still separate, operating in different realities with misaligned objectives.

How purple teaming can go wrong

Most solutions on the market aim to solve individual problems—but they view purple teaming as a point solution rather than a comprehensive, continuous activity.

Why?

Barrier 1

They treat it like a point-in-time operation

Without continuous action and implementation, the findings from purple teaming reports are left undiscussed and ignored until the next planned exercise—which could be a full year away.

Building a full purple teaming suite requires an array of commercial and open-source tools, and organizations rarely have the capacity or workflow to use these tools to their full potential.

Barrier 2

Misaligned incentives

When red and blue teams have opposing goals and competing processes, they're looking out for their own team rather than the shared organization—so when the real thing comes along, they're not trained to think any differently.

Barrier 3

Lack of resources and operational maturity

Many organizations never reach the level of operational maturity needed across people, processes, and technology to enable meaningful collaboration.

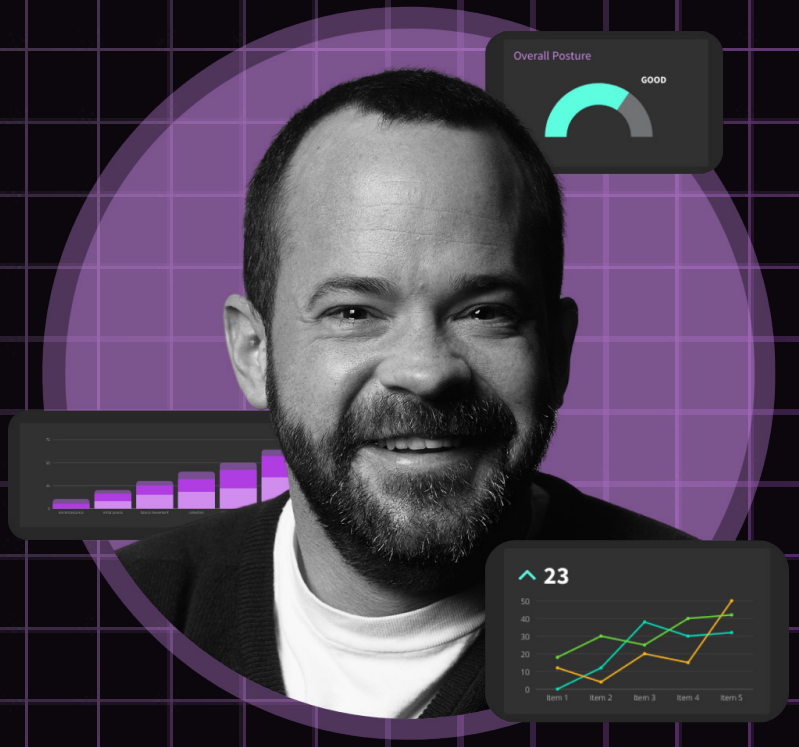
- **PEOPLE:** Offensive red teamers are expensive, hard to find, and even harder to keep. If the program lacks maturity or if defensive controls are too basic, the investment in offensive red team talent will be wasted on revealing obvious holes that should have already been addressed.
- **PROCESS:** In any SOC, processes are largely reactive. The most valued team members constantly get pulled into operational processes such as triaging priority alerts, incident response, security architecture, and anything else that comes up.
- **TECHNOLOGY:** Building a full suite of purple teaming tools requires assembling countless commercial and open-source tools, which often have different query languages, spotty interoperability, and a disjointed workflow. It takes someone with a high degree of technical maturity to configure the tools to their full potential. The highly technical person involved in this complex configuration is often the only one who knows how to use or tune the system effectively. When that person gets poached by another employer, this creates even more problems for the SOC.

Barrier 4

Report driven outcome

When purple teaming is viewed as an outcome rather than a continuous activity, reports are often the final output. And when threats are constantly changing and evolving, a one-time report loses its long-term value almost immediately, leaving security leaders right back where they started.

“When threats are constantly changing and evolving, a one-time report loses its long-term value almost immediately...”



Continuous purple teaming as a threat-informed defense

Imagine a world where a security team operated more like a multidisciplinary software development team.

The roster might include a front end engineer, a back end engineer, a quality assurance engineer, a product manager, and a designer—all working together, focused on building a new feature they have real confidence in.

If we apply this analogy to purple teaming, the cross-disciplinary team is working toward a common goal: enhanced security in the form of detections that can be used for detection rules, hunt packages, and so on.

In other words, offense informs defense in a continuous loop. The team would include:

Cyber threat intelligence analysts

to inform about the latest threat actors and malware

Red teamers

to replicate an attack

Blue teamers

to develop behavioral analytics

A platform

that could validate those analytics against the attacks as a testing mechanism

Such a holistic approach to threat-informed defense helps your security operations team drive a more proactive cybersecurity stance with confidence and clarity.

What are the other benefits of a continuous threat-informed approach?

This integrated process also results in a pool of resources that can accomplish the end-to-end workflow, from strategic prioritization, to the separation of duties for designing and coding the feature, to testing the individual pieces of code, to integrating the code, and finally, to validating whether or not the feature actually accomplishes the initial goal.

Let's take a closer look at what makes this approach possible—and successful:

Elements of continuous purple teaming

Collaboration

Continuous purple teaming begins with realigning teams' mindsets–once everyone is marching in the same direction, they see themselves as one unified team rather than natural enemies.

- Portable and flexible across security tools + data models
  - Universal detection translator
  - No-code detection builder
- Help red teams collaborate with blue teams by creating and sharing their own threats
  - Attack capture lab on demand
  - CapAttack portable sandbox
- Help blue teams collaborate with red teams by building detections directly off captured threat data

Robustness

Transform high-quality threat intelligence on adversary tradecraft with a repeatable workflow using adversary emulation for creating confident detection.

- Thousands of ready-to-use, validated detections
  - Detection repo
- Validate your detections in our attack capture lab before deploying into your environment
- Dozens of direct integrations with the most popular EDR, SIEM, NDR, and cloud telemetry tooling
  - CrowdStrike®, Mandiant®, Splunk, Securonix, and more
- Improve awareness of existing threat coverage by verifying it against the MITRE ATT&CK matrix

Elements of continuous purple teaming

Context

By understanding your security posture and adversary tradecraft, you gain critical context on your ability to prevent and contain.

- No-code detection builder—helps you tune detections to eliminate false positives
- Watch your security posture score improve as you fill gaps in the MITRE ATT&CK coverage matrix with high-confidence detections
- Identify gaps in coverage for any given attack using the MITRE ATT&CK coverage matrix
- Universal Analytic Translator with built-in validation and error checking

“By understanding your security posture and adversary tradecraft, you gain critical context on your ability to prevent and contain.”

How SnapAttack enables threat-informed defense

How SnapAttack enables threat-informed defense

Accelerates scale

» By demonstrating an attacker's behavior down to the keystroke, SnapAttack enables even junior analysts to understand and defend against countless variations of each incoming threat.

We bring our behavioral detections to your environment so regardless of tools, query language, and team maturity, you have everything you need to research, write, validate, and deploy high-confidence behavioral detections across your entire technology estate.

Drives collaboration

» Cyber threat intelligence (CTI), red teams, and blue teams are enabled to collaborate in one single platform, streamlining the purple teaming process and empowering all teams. CTI can provide context that can be immediately actioned by red teams and blue teams alike.

Red teams can capture and memorialize attacks as data. Blue teams can define detections-as-code and manage translation and versioning effectively. And both teams' efforts can be immediately validated against each other to determine an organization's coverage.

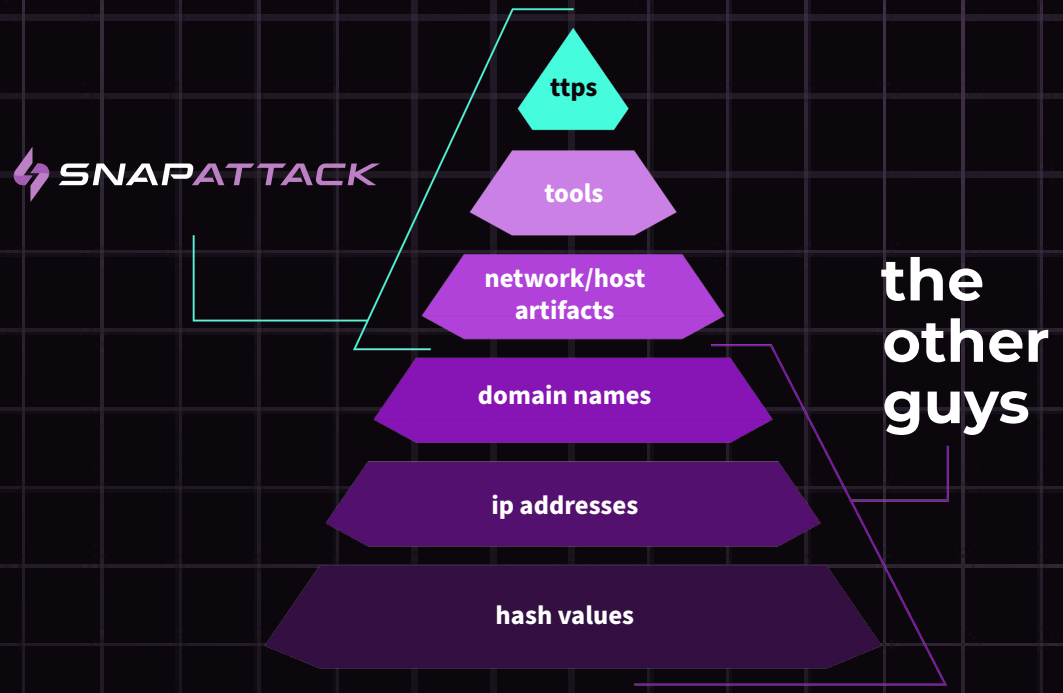
» SnapAttack is the only comprehensive solution in the market that rolls detection engineering, adversary emulation, purple teaming, and threat hunting into a single product that enables security leaders and teams to use existing technology more effectively and streamline collaboration across SecOps teams.

How SnapAttack enables threat-informed defense

Enhances confidence

- Turning intelligence into threat-informed defense means opening the aperture beyond Indicators of Compromise (IOCs) and into the world of adversary tradecraft, emulation, and detection engineering designed to thwart even sophisticated actors.
- SnapAttack operates at the peak of the **Pyramid of Pain**, giving CISOs and security leaders the foresight and end-to-end perspective of the entire threat hunting process.
- By using the MITRE ATT&CK framework, it's much easier to standardize and measure organizational coverage, manage detection backlogs, and gain quantifiable evidence of program effectiveness.

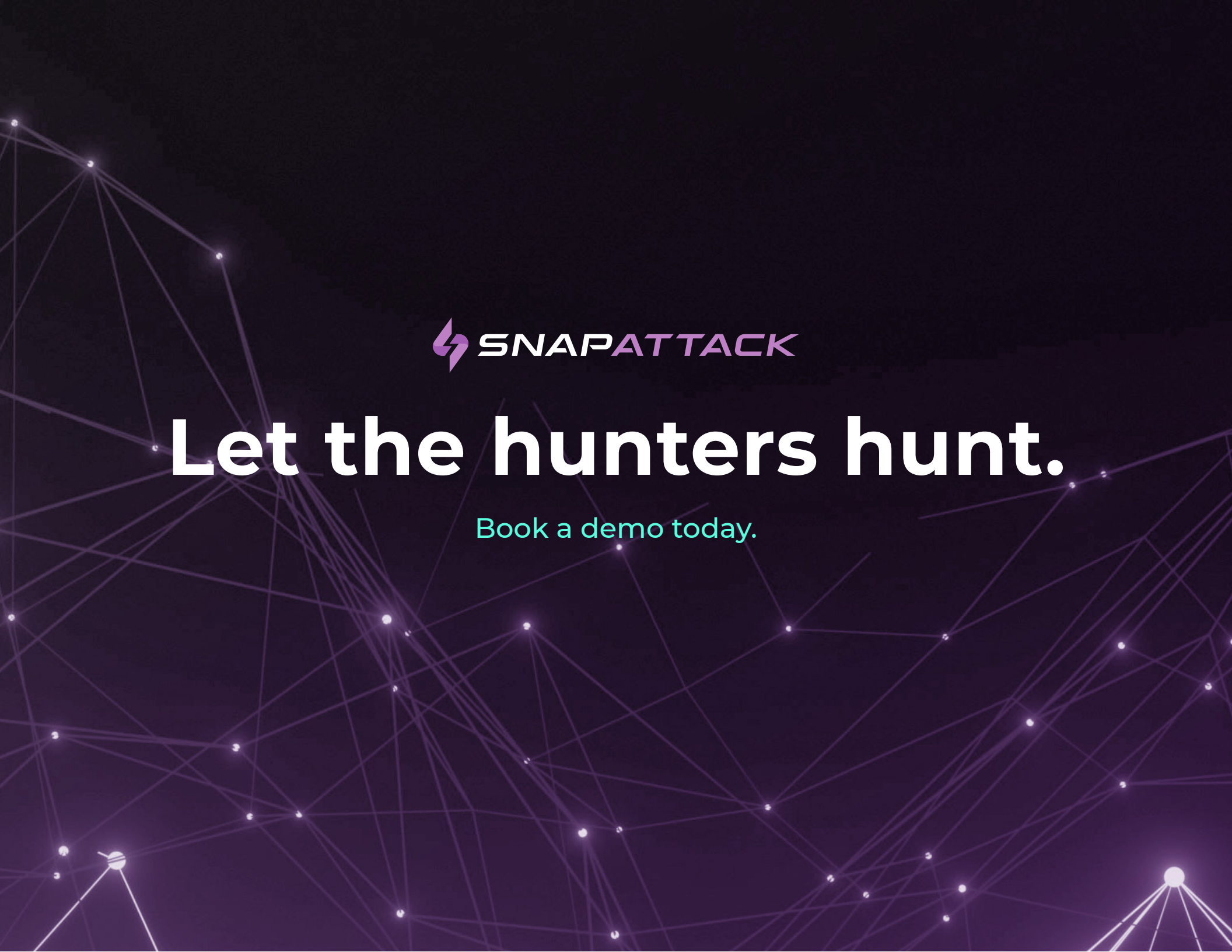
We accelerate the journey from understanding to deploying a given detection so that you can enhance your coverage and your confidence.



SNAPATTACK

Key takeaways

- The market has tried and failed to substitute point solutions and tool after tool to properly prepare teams and organizations.
- Real protection starts with continuous purple teaming—done the right way.
- Knowing what to expect from an adversary begins with knowing what to expect from your own teams. With an integrated, holistic view of your SecOps and heightened collaboration, you gain clarity and visibility into where each team has gaps.
- Breaking down organizational barriers allows teams to share robust intelligence, offensive tradecraft, and detection analytics, taking your organization from reactive to proactive and upleveling skill sets across team members.


SNAPATTACK
Let the hunters hunt.
Book a demo today.