SNAPATTACK

# Operational Purple Teaming in the Public Sector

Mobilizing a Threat-Informed Defense

# Table of Contents

**Cybersecurity in Government IN GOVERNMENT** ....3

- Threat Landscape ....3
- Agency Defenses ....4

**Security Opacity** ....4

- Traditional Network Defense ....5
  - BLUE TEAMING ....5
  - RED TEAMING ....5
- Resulting Challenges ....6
  - Reduced effectiveness ....6
  - Budget difficulties ....6
  - Closed offices ....6
  - Compliance issues ....6

**Solution: THREAT-INFORMED DEFENSE** ....8

- MITRE ATT&CK: The Foundation for Threat-Informed Defense ....8
- How the Military Has Done It ....9
  - One head, two hats ....9
  - Effect on the ground ....10
- Give Blue Teams Red Responsibility ....10
  - Preparatory self-evaluation ....11
  - Testing priorities ....11
  - Automation ....11
  - Focus on agency response ....11
  - How SnapAttack Enables Threat-Informed Defense ....12

**SnapAttack Can Help** ....13

- Objectives of SnapAttack ....13
  - Identify and quantify risks ....13
  - Validate threat remediation ....13
  - Reset capabilities ....14
  - Improve security investments ....14
  - Continuous testing ....15
- SnapAttack Overview ....16

**Conclusion** ....17

# Cybersecurity in Government >

**Defense deficit across federal agencies:**
Cybersecurity is a key concern for managers in the Public Sector. As the Cybersecurity & Infrastructure Security Agency (CISA) puts it: "In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission." Still, investment often lags behind industry.

## Threat Landscape

For much of 2020, the hottest topic in cybersecurity was the potential for foreign interference in U.S. elections. Back in October of that year, CISA and the FBI released joint advisories regarding Russian and Iranian actors pursuing advanced persistent threat (APT) activity designed to access election systems and undermine public confidence in the U.S. electoral process. While simultaneously Chinese actors continued their onslaught of Intellectual Property theft across government and commercial sectors.

It is now 2022, and the threat actors have largely remained the same. However, the targets have shifted, honing in on infrastructure disruption, ransomware for profit, and nation state IP Theft. Mirroring the 2020 elections, the 2022 midterms & 2024 general elections are looming, so we must be hyper vigilant to ensure that external meddling doesn't occur.

Other threats may have received less attention, but they are just as real. According to the Government Accountability Office (GAO), risks to federal government IT systems include "insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, steady advances in the sophistication of attack technology, and the emergence of new and more destructive attacks." Agencies throughout the U.S. government are at risk.

When COVID-19 drove many federal employees to work from home, attackers stepped up efforts to find vulnerabilities in agencies' remote-work environments. As Bryan Ware, Assistant Director for Cybersecurity at CISA, explained, "Bad actors are using these difficult times to exploit and take advantage of the public and business. ... We urge everyone to remain vigilant to these threats."

As the perimeter has collapsed, and the traditional work from brick-and-mortar office model has shifted to a blend of home office/traditional office, the SecOps defensive mindset is forever shifted to protect important critical assets.

## Agency Defenses

The threats are persistent and multifaceted, yet many federal agencies have let their defenses lag. Their resources are limited, so continuously evolving the security infrastructure to meet emerging threats may seem like a daunting challenge.

The primary obstacles to improving security controls and technologies are:

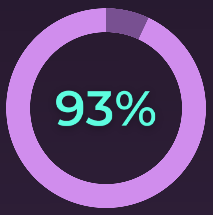
- **Perpetually tight IT budgets**: In a study of a dozen industries, the federal government was identified as the sector with the most "technical debt," meaning it faces the highest cost to bring legacy systems in line with current best practices. One GAO report found that some federal agencies are using IT systems with components that are more than 50 years old.
- **Staffing challenges:** Cybersecurity talent is hard to find and expensive for federal agencies, like many organizations. According to the Cyberspace Solarium Commission, about one in three cybersecurity jobs within the federal government are going unfilled.
- **Reactive spending**: Across the U.S. government, the typical agency spends 75%–80% of its IT budget on operations and maintenance. Decision-makers are focused on keeping the lights on, so to speak, with the processes and systems they already have in place, rather than understanding and mitigating the threats the agency is actually facing.

Without a continued focus on cyber capabilities that are more preventative and proactive which can also be a force multiplier to existing staff and resources, organizations will still fall behind the ever-improving tactics of cyber adversaries.

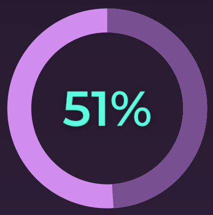
# Security Opacity >

### Why agencies fail to see gaps in protections:

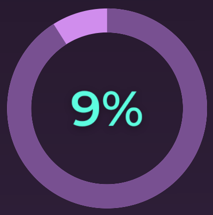
Federal agencies are increasingly being asked to do more with less. Unfortunately, that often means they stick with the same ineffective processes and technologies that they have used for years – or decades.



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

## Traditional Network Defense

Public and Private Sector organizations have traditionally separated security control testing into:

### > Blue teaming

Historically, blue teams work to achieve cybersecurity baselines to ensure cyber defenses work properly. **They focus on:**

- Correcting misconfigurations that create security vulnerabilities;
- Administering patches and updates to the organization's various applications and tools; and
- Deploying commercial products designed to secure specific parts of the network.

Much of blue team efforts are put forth towards reactive elements of shoring up defenses based on assessments and cyber hygiene improvements that come from vulnerability management programs and other compliance activities. Federal agencies typically dedicate most of their security testing resources to this area of activity and have struggled to move beyond the traditional defenses into more threat-informed capabilities.

### > Red teaming

Red teaming, the practice of attempting to breach cyber defenses to identify any gaps that may exist, usually receives less attention. Some agencies that do perform red team simulations do so only through limited, periodic testing by internal staff who have a wide range of other responsibilities. Other agencies outsource their red team testing.

Offensive capabilities have begun to be codified in different ways to help inform defensive teams, but this needs to continue to improve across the board to have situational awareness and understanding of gaps in the attack surface and where attackers may be probing. The following capabilities are starting to form in some organizations and will continue to mature as products and people take on a threat-informed approach.

- **THREAT EMULATION:** Threat emulation is a powerful way to emulate an attacker's behavior and capture the telemetry and behaviors behind attack tactics. Emulating an attack allows the red team to codify their attack techniques and provides a working template for blue teams to analyze that activity and create custom detections based on the emulated attack behaviors.
- **THREAT SIMULATION:** Simulating threats in your development or production environments can be powerful in understanding gaps in your attack surface. Breach and attack simulation tools let you run specific attack activity in your environment to test your defenses and examine your detection capabilities. Threat emulation and simulation coupled with integrated red and blue team activities allows for a full-service view of offensive tradecraft with relevant defensive detections.

Unless done continuously or integrated into the day-to-day workflow of Security Operations, red teaming is rarely frequent or robust enough to quickly identify security control failures created by changing internal or external conditions, or to enable the agency to fully understand its security strengths and weaknesses. Working to bring threat informed capabilities into the defensive workflow and continuously integrating attacker tradecraft into your defensive posture can help mature a cyber program to compete in the cyber battlefield of today's adversaries.

## Resulting Challenges

### > Reduced effectiveness

Absent regular testing, agency security leaders have a difficult time determining whether their cyber defenses are working. They have minimal insight into knowing whether crucial aspects of a security solution are working properly, which means some attacks may slip through failing defenses.

Similarly, absent effective testing, poor performance of security processes and staff may linger. Managers may misunderstand the threat landscape and fail to make good decisions about security priorities. Hiring managers could even add staff with skillsets inappropriate to the work required. Sporadic red team testing cannot reveal team failures, and ineffective processes can continue for months or even years, leaving agency data open to adversaries.

### > Budget difficulties

A misunderstanding of which threats are most pressing—in other words, which are most likely to occur, and to have the worst consequences for the agency—can result in waste within the portfolio of security solutions and staff resources. The pandemic and economic challenges have required many agencies to reallocate funds, leading to even tighter security budgets and increasing the pressure to optimize investments.

### > Closed offices

More and more people are coming into the office these days, but COVID-driven office closures or a blended work model can still further complicate threat detection at government scale as red teams and penetration testers cannot go onsite to perform their work. This may limit their effectiveness in uncovering issues with on-premises solutions that they cannot physically access.

### > Compliance issues

A federal agency that does not have visibility into the performance of its cyber defenses likely also faces challenges around regulatory and compliance assessments. A once-a-year testing regime cannot prove that the organization is adequately detecting and preventing the known and emerging threats it faces throughout the year.

# 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.

# Solution: Threat-Informed Defense >

**Integration and automation improve testing efficacy:**
Public and Private sector personnel have long understood that to secure an organization, its protectors need to think like the enemy. Understanding where and how an adversary will attack helps them optimize their defenses and mitigate any impacts of that attack. This is what SnapAttack calls a "threat-informed defense" strategy.

A Threat-informed defense focuses on identifying the adversary's tactics, techniques, and procedures (TTPs); identifying the organization's valuable data and defense capabilities; and building tight bonds between red and blue teams to prepare the organization for known threats and to test its defenses.

Focusing all security teams on the threats that matter most improves the effectiveness of the agency's overall security posture. And by routinely testing defenses against known threats, organizations can ensure that their defenses will perform if and when they come under attack.

## MITRE ATT&CK: The Foundation for Threat-Informed Defense

The foundation of a threat-informed defense strategy is the MITRE ATT&CK framework. Launched in 2015, it is a framework of known adversary tactics, techniques, and common knowledge (A. T. T. C. K.), a kind of periodic table that lists and organizes malicious-actor behavior in an accessible, user-friendly format. It looks like this; you can examine specific behaviors by clicking on an adversary tactic within the MITRE Corporation's "Navigator" tool.

However, MITRE ATT&CK is not just a framework to understand adversary behavior—it is a tool for improving security effectiveness. How and why? For years in cybersecurity, defenders lacked a common vision of the threat landscape. In the private sector, cyberthreat intelligence was often based on after-the-fact forensic data and indicators of compromise (IOCs) such as known-malicious IP addresses or domains, and hash values of known malware.

With the birth of the MITRE ATT&CK framework in 2015, this era of strategic ambiguity came to an end. ATT&CK gives the cybersecurity community a single, easy to access repository of adversary behavior to set a baseline against which they can prepare their cyber defenses. It forms the basis of a threat-informed defense strategy, a transformational approach to security. With the knowledge ATT&CK provides, teams can shift from an ad hoc approach of meeting cybersecurity regulations to countering known, dangerous threats.

## How the Military Has Done It

Since the September 11 attacks, the U.S. military has been transitioning from a traditional approach to defense, which separates intelligence teams from military operators, into a more integrated strategy. As a result, a tight feedback loop has developed between groups that traditionally would have operated separately—for example, those responsible for analyzing drone feeds on the battleground in Afghanistan and the forces deployed downrange to defend the United States.

For the U.S. Cyber Command, the U.S. military's cyberspace operations command, this transition toward a tight intelligence-operations link looks like a shift in focus from securing the network perimeter to a mentality of threat-informed defense.

### > One head, two hats

Since its founding, USCYBERCOM has operated under the direction of a combatant commanding officer who is also the director of the U.S. National Security Agency (NSA).

General Paul Nakasone, Commander of USCYBERCOM, reported in March 2019 to a U.S. House subcommittee, "The tight links between USCYBERCOM and NSA created a mutually beneficial intelligence-operations cycle that let us rapidly find and follow leads, discover new information, and create opportunities to act in conjunction with partners."

With weeks until the 2022 midterm elections, the Dept. of Defense is fully engaged to defend the U.S. electoral system from foreign interference and foreign influence alongside interagency partners.

"This is an enduring, no-fail mission for U.S. Cyber Command and the National Security Agency, who bring unique insights and actions to the whole-of-government effort," said U.S. Army Gen. Paul M. Nakasone, Commander of USCYBERCOM and Director of NSA/Chief, Central Security Service. "Together, we bring speed and unity of effort against any foreign adversary who might seek to undermine our democratic institutions."

### > Effect on the ground

**USCYBERCOM successes demonstrate:**

- Operational teams are more effective when they understand their adversaries. The tight bonds that the military's cyberspace operations group has deliberatively forged with the intelligence community gives USCYBERCOM personnel the world's best-informed adversary mindset. For example, when Russian government hackers broke into Pentagon networks, Cyber Protection Teams on the National Mission Force understood their tactics and were well-positioned to remove the threat.
- When defense planning incorporates intelligence data, decision-makers understand which cyberspace operations should be prioritized. Investments of human resources and IT spend are based on the best possible understanding of the threats facing the nation (or the federal agency).
- The joint USCYBERCOM-NSA Election Security Group, stood up again in early 2022, aligns both organizations' efforts to disrupt, deter, and degrade foreign adversaries' ability to interfere with and influence how U.S. citizens vote and how those votes are counted.

Civilian agencies that similarly merge intelligence and operations—i.e., red team and blue team activities—for their cybersecurity function can achieve similar benefits in the purple team's understanding of adversaries and strategic planning.

## Give Blue Teams Red Responsibility

Operationally, purple teaming puts a threat-informed defense into practice. A blue team becomes "purple" when it emulates and simulates the adversary as a means of evaluating its own effectiveness. Purple teams focus on the overarching threat landscape, working to understand both the TTPs they can expect from adversaries and the performance of their defenses against those threats.

Purple teams' purpose is to ensure the organization is continuously optimizing its cybersecurity readiness. Integrating red and blue responsibilities enables those tasked with protecting networked assets to routinely validate that their perspective encompasses all aspects of that landscape. The operational construct of the purple team brings the concept of threat-informed defense to life.

**Purple Team – threat-informed approach:**

1. Preparatory self-evaluation
2. Focus on agency response
3. Automation
4. Testing priorities

## > Preparatory self-evaluation

**In planning such a threat-informed approach to security, federal agencies' security teams should consider:**

- To what degree do we understand which threats are most likely to impact our operations, and which would have the greatest impact?
- Are we confident that we have identified the vulnerabilities that pose the greatest risk to our organizational mission?
- How much visibility do we have into our security-control architecture and the effectiveness of our security teams?

## > Focus on agency response

**Unlike a blue team evaluation of the settings in specific technology solutions, purple team assessments gauge the speed and efficacy of the agency's overall response to a threat. When that overall response is inadequate or slow, a purple team platform can parse out what went wrong.**

Perhaps:

- Sensors within the security infrastructure failed to detect the simulated attack;
- Connectivity issues between solutions meant that data on the detected behaviors failed to reach the security information and event management (SIEM) system;
- The SIEM detection content failed to generate the correct alerts for security staff; or
- Staff responded too slowly or inappropriately.

## > Automation

**Manual testing is not scalable. The testing priorities of a threat-informed defense strategy require continuous simulations of adversary behavior, which is not feasible for the staff of any organization, much less a resource-constrained federal agency. A less resource-intensive approach is to automate simulations of real-world attack scenarios.**

Purple teams can leverage a technology platform with a pre-existing library of adversary emulations to validate the effectiveness of specific security controls on an ongoing basis. The efficiency of an automated approach makes testing scalable and persistent. It also frees up the human purple team to focus on solving any problems that the simulations and emulations reveal across the security infrastructure.

## > Testing priorities

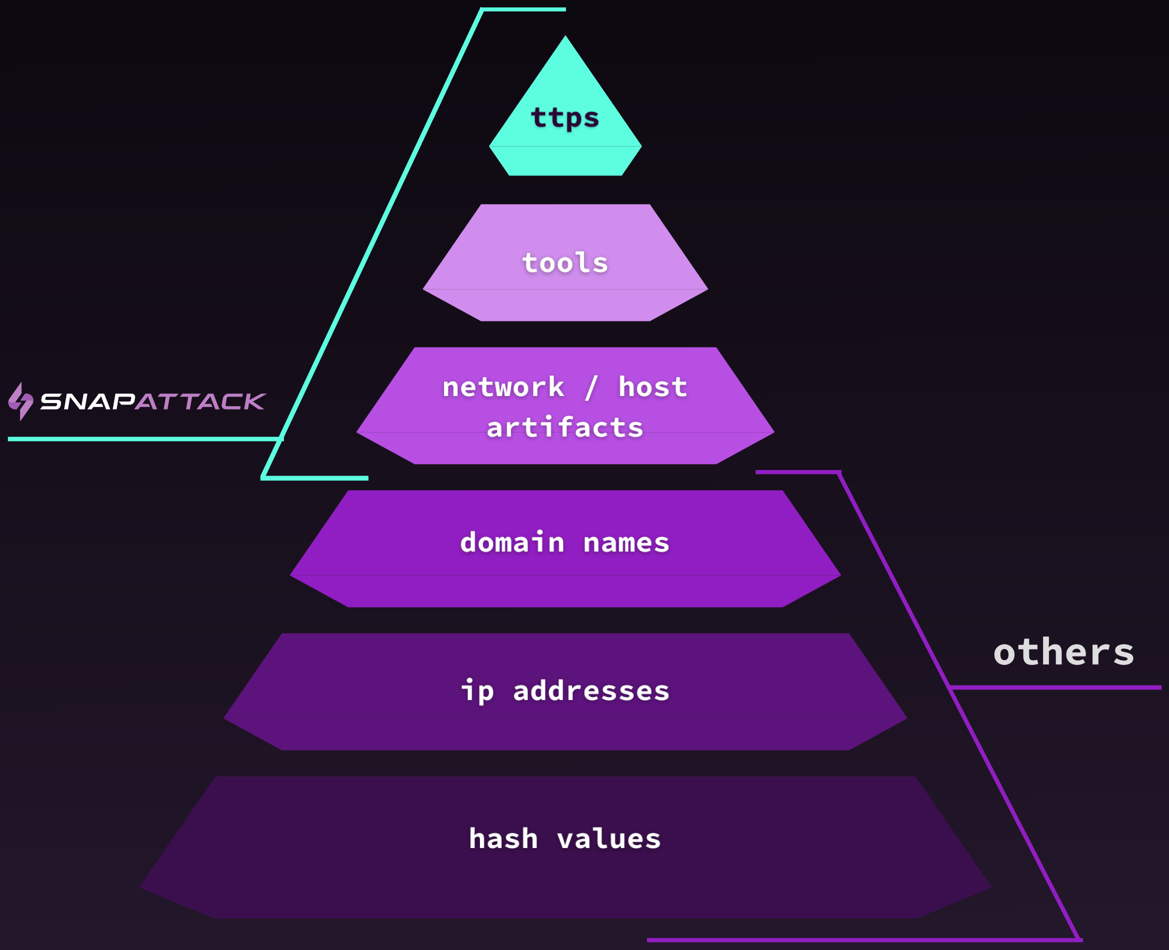
**To fully gauge the performance of an agency's security apparatus, its purple team program should focus on:**

- Deeply understanding the organization's risk profile and threat model to highlight likely adversarial approaches at achieving their attack objectives
- Protecting the agency's "crown jewel" applications and data;
- Evaluating the effectiveness of people, processes, and technologies;
- Validating defenses against the specific TTPs that the adversary will deploy; and
- Establishing a mechanism to continuously assess the infrastructure's performance against known threats, and to adjust threat models to incorporate testing against new threats as they emerge.

## How SnapAttack Enables Threat-Informed Defense

**By enhancing 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.



adapted from David J. Bianco's "pyramid of pain"

# How SnapAttack Can Help >

**Embedding purple teaming into security operations:**
The SnapAttack Threat Informed Defense Platform streamlines the creation of emulated attack scenarios and the execution of simulated breaches against an agency's IT resources. By integrating scenario-based emulation and simulation into the security operations process, SnapAttack enables blue teams to gauge their own performance—and that of every other element in the agency's threat detection and response apparatus.

## Objectives of SnapAttack

### > Identify and quantify risks

The Threat Informed Defense Platform enables agencies to collect accurate data on the performance of their security infrastructure against actual threats. If the threat emulations are planned carefully to mimic attacker behavior and the attack simulations calibrated to reflect the agency's most pressing cybersecurity concerns, then they will validate how well every aspect of their security controls (people, processes, and technologies) performs.

SnapAttack encourages agencies' security teams to structure their testing regime around the MITRE ATT&CK framework's library of known attacks. For emerging threats, the Threat Informed Defense Platform regularly draws on a variety of internal and external threat intelligence sources.

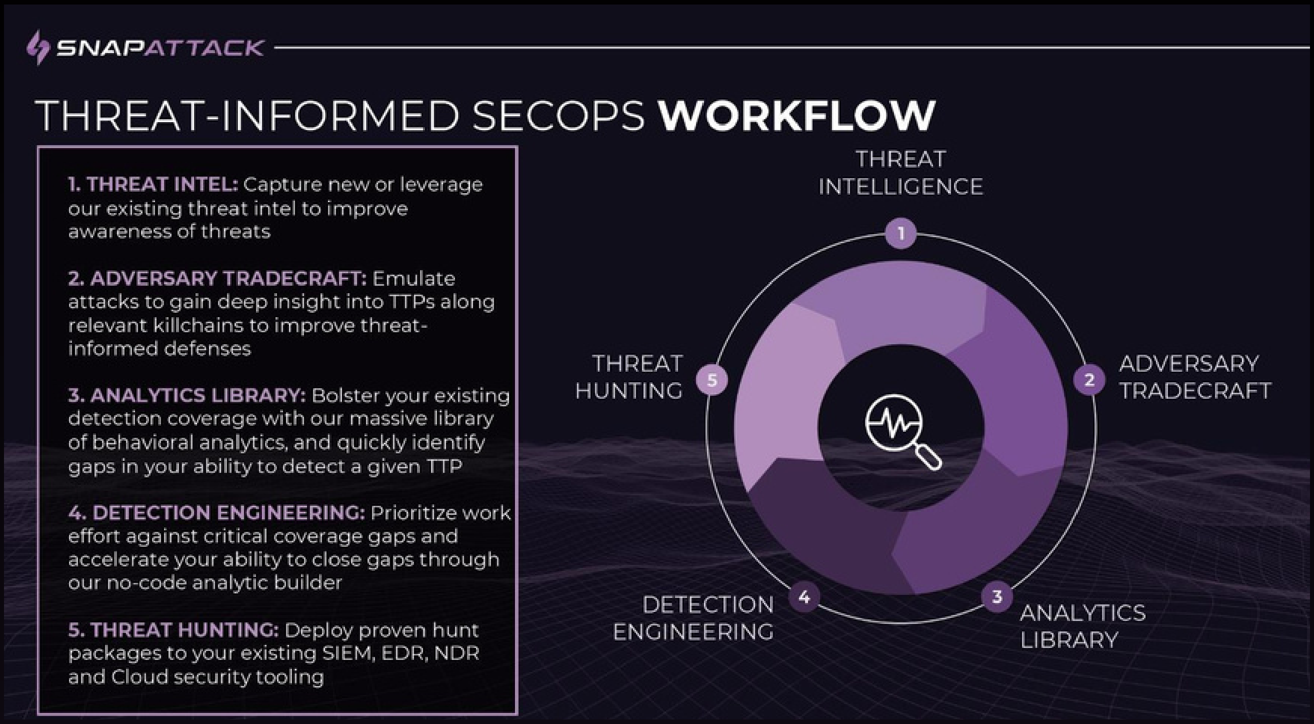
### > Validate threat remediation

Agencies need to root out control failures that leave their data and applications at risk by automating security control validation. They need a persistent and scalable solution that identifies threats in a timely manner in order to remediate the risk.

Purple teams supported by SnapAttack can determine:

- Which technology settings and security controls need adjustment;
- Areas where processes have room for improvement; and
- Staff training and/or skills gaps that hiring can close.

After an attempted remediation, the Threat Informed Defense Platform can re-run attack simulations to ensure that the correction eliminated the vulnerability.



SNAPATTACK

THREAT-INFORMED SECOPS **WORKFLOW**

**1. THREAT INTEL:** Capture new or leverage our existing threat intel to improve awareness of threats

**2. ADVERSARY TRADECRAFT:** Emulate attacks to gain deep insight into TTPs along relevant killchains to improve threat-informed defenses

**3. ANALYTICS LIBRARY:** Bolster your existing detection coverage with our massive library of behavioral analytics, and quickly identify gaps in your ability to detect a given TTP

**4. DETECTION ENGINEERING:** Prioritize work effort against critical coverage gaps and accelerate your ability to close gaps through our no-code analytic builder

**5. THREAT HUNTING:** Deploy proven hunt packages to your existing SIEM, EDR, NDR and Cloud security tooling

The threat informed SecOps workflow

## > Reset capabilities

Using the Threat Informed Defense Platform to identify the strengths and gaps in security technologies and processes enables an agency to rationalize its current security controls and solutions. Verizon estimates that 82 percent of successful enterprise breaches should have been stopped by existing controls—but weren't. That's because security controls are complex systems that tend to fail silently. The only way to know whether they're working is to actively test them on a continuous basis.

Automating security control validation makes confirmation of controls' effectiveness a routine process within the security ecosystem. In addition to identifying gaps that require remediation, automated testing reveals overlaps in the security control stack. By consolidating and eliminating unnecessary controls, an agency can improve the efficiency and effectiveness of its overall security program (people, processes, and technology).

## > Improve security investments

Measuring, monitoring, and modifying prospective investments in security tools can ensure that the agency chooses the best option for each element of its solution stack. This can be accomplished by using security outcomes that results from offensive minded approaches to evaluating detection coverage across the environment. Testing defenses using emulation and simulation techniques creates specific, data-driven insights around threat detection capabilities which enable decision-makers to focus on those improvements and investments that matter most to the agency's security posture.

The net result of comprehensive Threat Informed Defense is that the agency's cybersecurity processes are effective and efficient. Security portfolio investments are rationalized, while weaknesses in controls are identified and fixed via new capabilities. Senior management and the board have confidence in the data-driven explanation of the agency's security effectiveness.

Moreover, if an external event such as COVID-19 requires rapid reallocation of investment dollars, the Threat Informed Defense Platform helps decision-makers rationalize their budgets based on the agency's threat-informed defense strategy. [CBW1] [CBW2] [CBW3]

## > Continuous testing

Security control testing cannot be a single-point-in-time event. SnapAttack turns threat-informed defense into a routine, standard part of organizational operations. Purple teaming capabilities run in the background, day in and day out, to ensure that they identify emerging threats or newly introduced vulnerabilities soon after they appear. The Threat Informed Defense Platform makes this possible.

Ultimately SnapAttack is the cloud and enterprise-ready platform that helps security leaders answer the most pressing question:

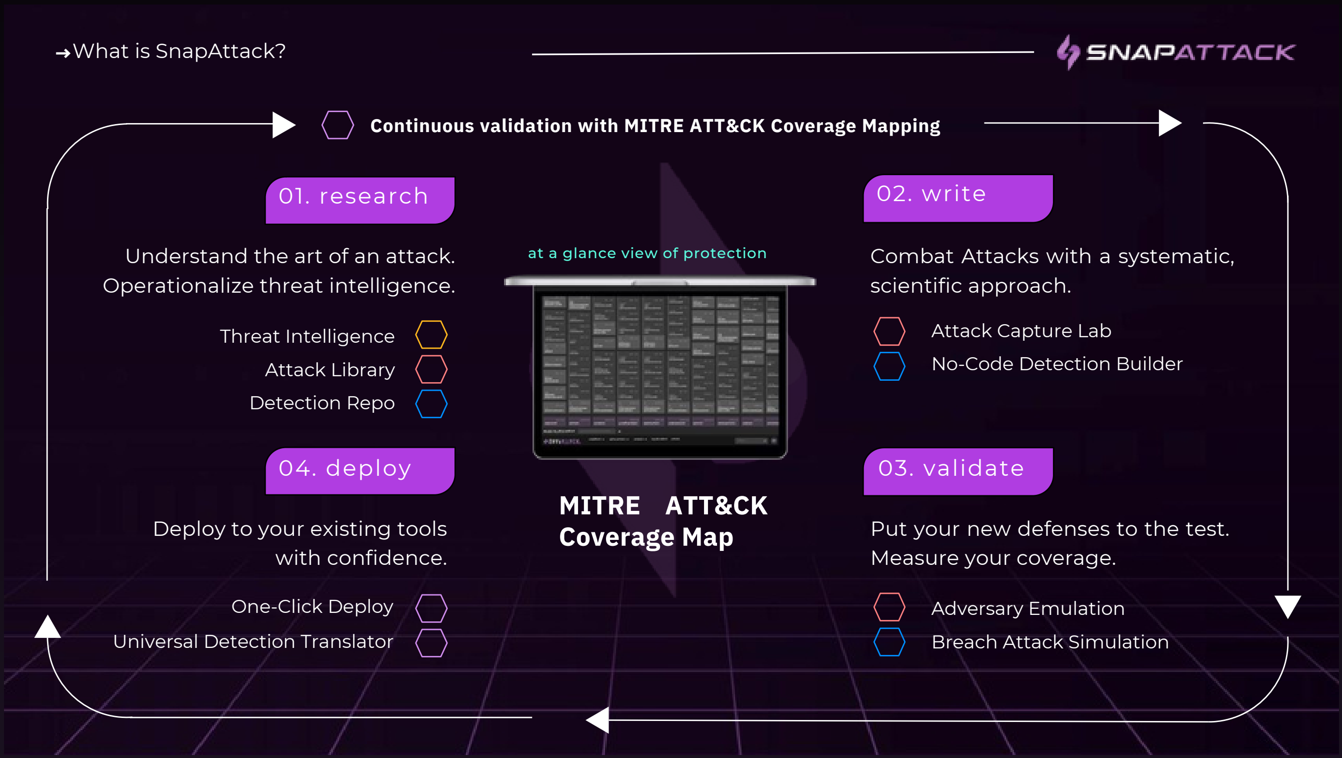
***"Are we protected?"***

By rolling intel, adversary emulation, attack simulation, detection engineering, threat hunting, and purple teaming into a single, easy-to-use solution 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.

## SnapAttack Overview

### Leverage a threat library that aggregates offensive tradecraft:

Utilize Adversary/Threat emulation, emulate adversary attacks in safe, sandboxed, environment — or safely run live threats. Implement Attack replay, view captured video, keystrokes, and event logs from attacker and victim machines and share knowledge between team members. Get involved earlier in the kill chain, observing detection hits and labeled attacks overlaid on the video timeline. Drive collaboration, enable red teams to asynchronously share knowledge with blue teams and collaborate on specific attack scenarios. These capabilities and more will enable you to answer the question "are we protected".



→What is SnapAttack?

SNAPATTACK

Continuous validation with MITRE ATT&CK Coverage Mapping

01. research

Understand the art of an attack. Operationalize threat intelligence.

- Threat Intelligence
- Attack Library
- Detection Repo

02. write

Combat Attacks with a systematic, scientific approach.

- Attack Capture Lab
- No-Code Detection Builder

at a glance view of protection

MITRE ATT&CK Coverage Map

04. deploy

Deploy to your existing tools with confidence.

- One-Click Deploy
- Universal Detection Translator

03. validate

Put your new defenses to the test. Measure your coverage.

- Adversary Emulation
- Breach Attack Simulation

SnapAttack Overview

# Conclusion >

### Federal agencies need SnapAttack:

Federal agencies may fall behind industry in some areas of IT, but they cannot let security lapse—the risks to data and applications are too great. As adversaries evolve, so too must agencies' cybersecurity infrastructure. Moving to a threat-informed defense is key. Agencies must integrate their security intelligence and operations activities, so that they are regularly testing their technologies, processes, and people against both known and emerging adversary TTPs.

The SnapAttack Threat Informed Defense Platform automates a threat-informed approach to both validating controls that are in place and prioritizing prospective improvements to the security infrastructure. Such an approach is imperative to ensure that an agency's cybersecurity controls are both efficient and effective.

**SnapAttack is the only comprehensive solution in the market that rolls detection engineering, adversary emulation, purple teaming, and threat hunting into a single, easy-to-use platform that enables you to use your existing technology more effectively and streamline collaboration across teams.**

**Please contact your sales advisor, or reseller partner for further information, or to schedule a demonstration of the platform. We look forward to working with you!**

**Would you like to learn more about SnapAttack? Please subscribe to our newsletter.**