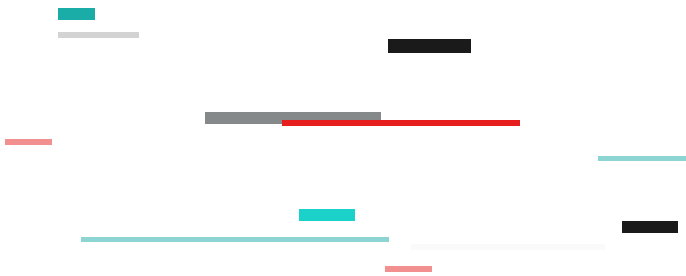


GUIDE



RANSOMWARE SECURITY

INTRODUCTION



While historical threat landscapes focused on technical perimeters and legacy strains like TrickBot, today's defensive environment faces a dynamic adversary. A fragmented Ransomware-as-a-Service (RaaS) market has driven total leak-site victims to a record-breaking 7,874 global exposures.

Crucially, this escalating volume has not triggered an increase in ransom payments. In a powerful headline reversal, ransom payment rates have plummeted for four straight years, hitting a record low of 23% by early 2026 (down from ~85% in 2019).

Because fewer victims are paying, threat actors are aggressively adapting. Instead of relying solely on standard network encryption, operators have pivoted heavily to data-theft extortion, which now factors into 73% of all attacks as of early 2026. This leaves target organizations to navigate complex operational downtime, critical relationship damage, and a grueling regulatory minefield during a crisis.

This environment is further complicated by the weaponization of artificial intelligence. Attackers aggressively leverage AI as an initial-access enabler to scale hyper-convincing phishing, real-time voice or video deepfakes, and lightning-fast lure generation. Rather than changing the core objectives of an attack, AI has industrialized the speed and precision with which adversaries exploit human and identity-layer vulnerabilities.

Most experts agree that prevention is the best approach to combating ransomware, but technology can only take us so far. Modern exploits routinely bypass traditional controls by using authorized credentials and injecting malicious code into legitimate processes.

While vulnerability exploitation remains a major risk, the human element is the primary catalyst for compromise, factoring into 62% of security breaches via social-engineering traps, identity-verification fraud, and help-desk takeovers. Despite advancements in prevention technologies like next-generation antivirus (NGAV), application control, detection and response (EDR/XDR/SOAR), and frameworks like MITRE ATT&CK, ransomware attacks continue to outpace static defenses.

The inconvenient truth is that preparing for high-stakes ransomware threats requires a whole-company approach. To succeed, organizations must implement the right plan, assemble the right stakeholders, and establish the right metrics to measure and communicate operational progress.

We'll provide a roadmap to get your extended team aligned on ransomware readiness, by aiming to answer the following questions.

01

ATTACK SURFACE AREA

How do you know how and where you're vulnerable to a ransomware attack?

02

THREAT DISCOVERY

Which discovery methods can you employ to determine your greatest areas of exposure?

03

OFFENSIVE SECURITY

When it comes to options—penetration testing, red teaming, purple teaming, or tabletop exercises—which will work best for you?

04

RISK REDUCTION

What can you expect to learn from these programs? How do you leverage lessons learned to enhance security on a continual basis?

05

OPEN-SOURCE COMMUNITY

Which open-source tools can you use to start a program on your own? How do they function and what are their use cases?

PROFILING THE RANSOMWARE ATTACKER

PRO-TIP

When trying to unpack how a ransomware attack happens, don't restrict your analysis to atomic artifacts like indicators of compromise (IOCs), file hashes, binaries, process trees, and other technical detritus. Remember, there are actual people behind these attacks. Increasing your knowledge of their motives and operations enhances your technical understanding and helps prepare your defenses.

TO BETTER PREPARE FOR A RANSOMWARE ATTACK, UNDERSTAND THE FOLLOWING ABOUT YOUR ADVERSARY:

MOTIVE

What drives them to target their victims and launch attacks?

MODE

How can their behavior be characterized? What does it tell you?

METHODS

What tools do they use, and how do they use them?

MOVES

Once they're in, what's next?

MOTIVE: PROFIT

The Attacker's Goal: If It's Valuable to You, Then It's Valuable to Them.

Back in the day, attackers targeted assets or data with intrinsic value: credit card numbers, credentials, and personally identifiable information (PII) that could be sold on black markets. One of the major innovations of ransomware groups is the monetization of the compromise itself.

If you're an architecture firm, you're not sitting on a mountain of sensitive consumer payment data. This simple fact used to shield specific industries from attack since they didn't own anything of value to attackers. Your typical cybercriminal doesn't care about the in-progress blueprints to a new building, after all.

But soon, attackers realized that if it has value to you, that value can be extracted. By locking up your systems or threatening to leak internal files, money could be made from almost any business. While the introduction of cryptocurrency provided an easy way to transfer that value anonymously over the internet, target organizations are pushing back.

The historic low in ransomware payment rates is forcing attackers to change their execution strategies, with identifying lateral movement as the dominant tactic in 79% of early 2026 cases. Because attackers abuse legitimate administrative paths to blend in, failing to intercept this east-west movement allows them to systematically wipe out backups, map out crown-jewel data, and escalate a single compromised machine into a catastrophic, company-wide outage.

MODE: OPPORTUNISTIC

The Attacker's Mantra: Get the Goods and Move On.

Ransomware attackers look for the path of least resistance to a goal that will make them money. This means they're far more likely to exploit known vulnerabilities or use compromised credentials than spend weeks probing a custom application for an entirely novel zero-day exploit. It's not that they're not capable, but they could have exploited another organization in that same time. Making sure there's no low-hanging fruit in your environment goes a long way in deterring this kind of threat.

This stands in stark contrast to politically motivated attackers or hacktivists. These hackers are interested in a specific target and will systematically evade detection to breach it. While any attacker prefers easy targets and will actively seek them, politically motivated adversaries are more likely to spend time and resources finding the hard way in if necessary.

METHODS: OPERATIONALIZED

Ransomware Is Big Business: A Fragmented and Volatile Ecosystem.

The ransomware market has shifted from a consolidated corporate structure to a highly volatile, atomized ecosystem with no single dominant brand. Major international law enforcement operations, such as Operation Cronos against LockBit and the subsequent ALPHV/BlackCat exit scam, did not kill the threat; instead, they served as the catalyst for widespread market fragmentation.

The market now counts over 124 active groups. As of early 2026, Qilin leads the volume of attacks, followed closely by newer entrants like The Gentlemen and veteran groups such as CIOp. Despite massive affiliate churn and the continuous collapse and reshuffling of these groups, such as the rapid rise and April 2025 collapse of RansomHub, the "enterprise-level" sophistication of these operations remains unchanged. They utilize advanced customer-service lines to walk victims through payment variables, proving that the criminal org chart will seamlessly reshuffle to keep profits flowing.

MOVES: BRAZEN

Extortion Has Changed: The Rise of Encryptionless Attacks.

The readiness question for a modern enterprise has fundamentally changed. Historically, organizations asked whether they could restore from backup. Today, threat actors have modified their playbooks to prioritize exfiltration-only, encryptionless extortion, rendering traditional recovery defenses insufficient on their own.

Because backups do not stop public blackmail or regulatory exposure, security teams must move past simple vulnerability discovery. The focus must shift to detection and response testing. The core strategic questions you must answer are clear: Can we detect and contain an adversary before data leaves the perimeter, and do we have an active playbook for a data leak we cannot undo?

Thanks to ransomware-as-a-service (RaaS), sophisticated attacks are available to a mass market backed by enterprise-level support operations and infrastructure. This commercialized ecosystem remains highly lucrative, with the total on-chain ransomware payments reaching \$820 million in 2025. Instead of relying on a single dominant strain, today's fractured criminal market utilizes highly specialized internal divisions. Modern extortion syndicates employ dedicated departments for payroll, customer service, product management, and human resources, alongside aggressive recruiting practices to acquire access brokers and exploit developers.

THE SAD AND UGLY TRUTH:

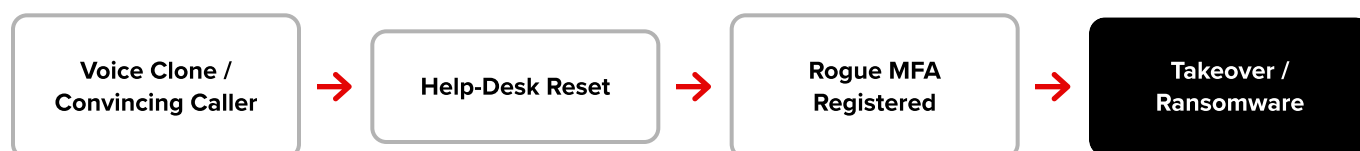
It's Not Rocket Science.

The most effective way to protect against a ransomware attack remains an open secret, and the fundamentals are remarkably straightforward. Organizations must consistently patch applications and operating systems, enforce the principle of least privilege globally, disable unnecessary ports, segment internal networks, and employ robust encryption.

The primary difference in the current threat landscape is that cyber hygiene can no longer be limited to technical infrastructure. With adversaries leveraging AI tools to optimize social engineering, baseline hygiene must expand to include rigid service-desk identity verification and robust authentication controls. Traditional safeguards and regular backup programs are still vital, but they must be paired with proactive verification to match the speed of modern initial-access tactics.

THE HUMAN LAYER: SOCIAL ENGINEERING AS INITIAL ACCESS

While defensive strategies historically treated initial access as a technical problem solved by patch management, the dominant modern ransomware entry point is the human layer. Adversaries systematically exploit classic persuasion principles, such as urgency, authority, and isolation, to bypass critical thinking. In this context, AI serves strictly as an offense enabler; it does not invent new vulnerabilities, but it has industrialized the scale and localization of the threat.



This sequence is a highly repeatable adversary pattern. The Scattered Spider retail and manufacturing wave illustrated this danger when attackers bypassed technical perimeters entirely by talking IT help desks into executing unauthorized credential and MFA resets. The resulting operational disruptions hit major enterprises like Marks & Spencer, Co-op, Harrods, and Jaguar Land Rover (JLR), halting JLR's production for weeks and costing the UK economy an estimated £1.9B to £2.5B.

Per Mandiant M-Trends data, while AI optimizes attacker workflows, intrusions still succeed because of basic process gaps: weak identity verification, over-permissioned accounts, and inconsistent MFA. Defeating this threat requires process-driven controls that reduce cognitive load at the moment of decision so the safe choice is the easy choice:

- **Out-of-Band Callbacks:** Mandate verification of high-risk requests by terminating the inbound interaction and initiating a new path using an organization-supplied, known-good number.
- **Dual-Authorization Workflows:** Enforce a strict manager or PIN-approval chain for all help-desk account resets, administrative modifications, and capital movements.
- **Blameless Process Culture:** Build an environment where employees point to a rigid standard process rather than owning the personal friction of saying “no” to an urgent request.

To delve more into this topic, make sure to check out these Bishop Fox webinars:

- [Attacking and Defending Deepfakes: A Red Teamer's Perspective](#)
- [Tactics of Deception: Protecting Trust and Purpose](#)

HOW TO PREPARE WITH OFFENSIVE SECURITY PROGRAMS

The most mature security programs are those that maintain a healthy balance of defensive and offensive security tactics. Despite the tired “cloak-and-dagger” stereotype offensive security seems unable to shed, these practices can truly shine light into darkness.

By using the insights gained from an offensive security program, you’ll hone your defenses using realistic adversary emulation. An offensive security program will identify where your organization is vulnerable to a ransomware attack, demonstrate exactly how an attacker would move laterally to secure leverage, and make actionable recommendations on how to address any technical gaps.

PRO-TIP

Start at the End. It sounds like a riddle, doesn’t it? What we mean is to start your ransomware readiness assessment by determining your operational objectives. Consider which of the following take priority, keeping in mind that these requirements may evolve as you uncover blind spots in your environment:

1

Vulnerability Discovery

Are you focused on uncovering hidden entry points, unpatched assets, or compromised identity credentials before attackers can exploit them?

2

Asset Management

Do you need greater visibility into the assets on your network, specifically mapping out how crown-jewel data flows across the environment to prevent unauthorized exfiltration?

3

Detection and Response Improvement

Do you want to evaluate how effectively your internal security operations can detect, contain, and neutralize an active, hands-on-keyboard adversary before they achieve lateral movement?

4

Team Cohesion

Do you want to ensure your cross-functional teams are ready to manage a high-stakes extortion event, from detection to response to public disclosure?

Knowing your desired outcomes and planning how you will respond are essential. Ensure that all stakeholders are involved in decision-making, planning, and execution.

The following table includes five ways to assess and improve your ransomware readiness. Use your targeted outcomes as guideposts to map your organizational needs against the approaches outlined in the table below.

RANSOMWARE READINESS PROGRAMS			
SIMULATION PROGRAM & GOALS	WHAT TO EXPECT	WHO PARTICIPATES	PRO-TIP
External Penetration Testing Identify exploitable vulnerabilities and weaknesses in the perimeter.	A report of vulnerabilities to patch, systems to decommission, network diagrams, and open ports to disable (e.g., RDP).	Penetration testing service provider with no organization involvement (or some, and negotiated in advance).	Prepare your team for the test by notifying all stakeholders (to avoid setting off any unnecessary alarms).
Internal Penetration Testing Discover the most likely vulnerabilities, attack paths, and exploit chains that an internal threat actor could leverage to gain access to your sensitive data and critical functionality.	A report with guidance on how to properly segment your network, implement stronger authentication, and mitigate their discovered vulnerabilities.	Penetration testing service provider with minimal organization involvement (negotiated in advance).	Prepare your team for the test by notifying all stakeholders (to avoid setting off any unnecessary alarms).
Red Teams Measure the efficacy of people, processes, and technology in real-world scenarios.	Detailed attack graphs and architecture diagrams. An assessment report with technical findings, timelines, and remediation recommendations.	Offensive security service provider actively planning and collaborating with the organization.	Base scenarios on specific outcomes; an ‘assumed breach’ approach to a Red Team engagement will often save time and money with identical outcomes.
Purple Teams Test and improve people, processes, and technology with Red Teams and Blue Teams working together.	A Purple Team is very similar to a Red Team but simply conducted with full knowledge of both the attackers and defenders, making it a great learning opportunity.	Offensive security service provider actively planning and collaborating with the organization.	If you’ve never conducted a Red Team engagement, a Purple Team can be a great first step and offers a lighter introduction to adversary simulation.
Tabletop Exercises Anticipate, assess, and respond to operational and strategic security risks in a facilitated group setting.	A paper-based (i.e., tabletop) exercise with key stakeholders and an after-action report detailing key takeaways.	Security services provider facilitates with cross-functional team participation.	Establish the strategic goals with clarity and include as much cross-department representation as possible. After all, a ransomware attack will touch the entire organization.

TOP FIVE RANSOMWARE SIMULATION DO'S & DON'TS

THE DO'S

1 Get Clarity on Your Goals.

Before engaging an outside firm, first gather your team to discuss the following critical questions. Document your answers once you reach consensus.

- Why are we doing a ransomware simulation program right now?
- What are we most concerned about in our environment?
- What are the worst-case scenarios regarding operational downtime?
- How do we plan on using the results of these programs?
- Do we have the capacity to implement the changes needed to address any gaps we find? If not, where will we find the resources and what are the next steps?

2 Determine if You'll Pay the Ransom (Before an Attack Happens).

This is the most important question business leadership, in consultation with counsel, must confront. While law enforcement and security experts universally advise against paying, organizations must face reality before an attack happens.

However, paying a ransom is no longer a simple cost-benefit call. The landscape demands navigating severe modern complexities:

- **Tightened Cyber-Insurance Scrutiny:** Insurance is not a guaranteed safety net. Underwriting requirements have tightened significantly, and getting a payout requires proving rigorous, proactive security controls were already in place.
- **Legal and Sanctions Exposure:** Paying a ransom carries heavy compliance risks. OFAC sanctions mean payments to certain threat groups are a live legal liability; legally, you may not be allowed to pay.
- **Falling Success Rates:** Payment rates are declining globally because paying doesn't guarantee data recovery. Decryption tools regularly fail, and data is often left unrecoverable.

Ultimately, you should use your simulations to route these operational and regulatory specifics through legal counsel ahead of time. Establish your protocols now, because figuring out insurance technicalities and compliance boundaries while your network is dark is a losing strategy.

3 Establish the Rules of Engagement Up Front.

There should be clear-cut rules of engagement—whether it’s a penetration test or a Red Team engagement—on when, how, and if live environments get involved. Know what your goals are internally and then clarify these goals and negotiate the plan with your penetration testing team before the simulation begins.

For example, assume you decide to separate your production environment from a test environment (or, better yet, already have this setup in place). Running the simulation against your test environment will avoid any downtime risk. That said, what you gain in risk avoidance, you lose in visibility into the real-world risks facing your business operations.

4 Consider the Escalation Path — Where It Begins and Ends.

Modern ransomware attacks move fast. Adversaries are heavily weaponizing AI to scale hyper-convincing phishing and lightning-fast lure generation, meaning an initial foothold can escalate to domain-wide compromise at machine speed.

Ransomware simulation programs are designed to escalate and will likely branch off into unexpected domains and directions. To prepare for this, decide how far you’ll let the exercise escalate. What are the triggers? Your assessment team can also guide you on the best escalation procedures for your organization’s size, geography, and industry.

5 Establish Clear and Documented Communication Lines — Before, During, and After the Exercise.

When an attack hits, communication is usually the first thing to break down. Because modern attacks cause intense relationship damage, critical operational downtime, and grueling regulatory scrutiny, your internal communication must be on point.

Before the simulation begins, establish out-of-band communication channels for the exercise’s stakeholders. Document exactly who inside the organization knows the test is happening (to avoid burning your SOC team’s trust) and define how indicators of compromise (IoCs) will be de-conflicted in real time. Testing your communication lines under simulated stress ensures that if a real crisis hits, you’ll be ready.

THE DON'TS

1 **It's Not a 'One and Done.'**

Readiness isn't a trophy you 'achieve;' it's a continuous, iterative process. The proliferation of Ransomware-as-a-Service (RaaS) is causing the threat landscape to shift too fast for annual check-the-box exercises.

What a simulation offers is a point-in-time diagnostic of where your security controls, detection rules, and response policies fail. Use these insights to constantly tune your defenses, because static security policies are a green light for dynamic adversaries.

2 **Don't Limit Yourself by Treating This as a Purely Technical Endeavor.**

Ransomware attacks are existential crisis moments for any company, not isolated IT headaches. A cyber attacker doesn't limit themselves to only probing technical vulnerabilities, particularly when hunting for large game. As such, treat it by addressing risk via a 'whole company' point-of-view. Allow the assessment to test your business processes as much as your technical ones.

3 **Don't Forget the Question of IP Allow-Listing (or Disabling a WAF).**

IP allow-listing is the practice of adding the IP address of the pen tester to an allow-list to avoid auto-blocking or setting off unnecessary alerts (disabling a WAF may also be required). For a standard penetration test, scoped allow-listing is highly practical and can lead to faster discovery of more higher-priority risks. Rather than waste time on the time-consuming "easy stuff," a penetration tester can spend more time on probing higher-value, at-risk assets—the ones your attacker targets.

At the same time, using an allow-list for a Red Team exercise would not be recommended. It's ultimately your decision, but what we've found is that without allow-listing for a pen test, the assessment will test your pen testers' abilities, rather than expose your organization's biggest risks.

4 **Don't Overthink Red Team Tactics.**

During a Red Team exercise, uncertainty rules the day. Embrace it and make sure you approach each new situation or discovery with multiple strategies. A primary goal of a Red Team is to build muscle memory into your organization's response procedures, because a loss of control will increase the chance of failure.

To avoid getting stuck, follow the PACE principle of planning: make sure to have Primary, Alternative, Contingency, and Emergency plans. Like Mike Tyson says, "Everyone has a plan until they get punched in the face."

5 Don't Neglect to Train Your Employees.

While vulnerability exploitation is a major corporate risk, the human element remains the primary catalyst for compromise through social engineering, identity fraud, and help-desk takeovers. Because threat actors heavily target the identity layer using AI-driven tactics, your workforce is the front line.

Security training must evolve beyond compliance videos. Relying on gut checks fails because human deepfake detection is poor; studies show correct identification of high-quality video deepfakes falls below 25%. "Seeing is believing" has become a liability.

Train employees on strict out-of-band verification and build a culture of trust. If an employee is too terrified to report a clicked phishing link or an approved MFA prompt, their silence gives attackers the time they need to escalate a foothold into full domain encryption. An empowered workforce is your fastest early-warning system.

RANSOMWARE READINESS SELF-ASSESSMENT

At the start of this guide, we suggested that starting with the end goal in mind is the best recommendation for deciding which offensive security program will work best for your organization. It is also a good idea for gauging your organization's level of ransomware readiness.

To surface your goals, we posed pointed questions across the following key goal categories: vulnerability discovery, asset management, detection and response improvement, and team cohesion. We'll use these same goal categories in the checklist below.

VULNERABILITY DISCOVERY

When was the last time you ran a penetration test internally? How about externally?

WHY THIS IS IMPORTANT:

Having a baseline documented understanding of your technical exposures (internally and externally) provides a clear view of your current exposure, especially when tracking that progress over time.

HOW TO INTERPRET "READINESS" FROM THE ANSWER:

The more frequent your penetration testing program is, the more likely it will provide an accurate picture of your security posture. In other words, you're nowhere near 'ransomware ready' if you haven't run a single assessment against your environment.

What were the results from previous assessments? How many high-and critical-severity findings did you identify?

WHY THIS IS IMPORTANT:

Pay attention to the content of the results over time. While a single finding may be severe and require attention, it is important to determine whether it is indicative of a larger issue or if it is a one-off problem? Are the same sorts of issues found year after year?

HOW TO INTERPRET “READINESS” FROM THE ANSWER:

Make sure that you’re improving security over time. Make new mistakes. Individual security issues come and go, but as long as they don’t present persistent patterns of vulnerabilities, you’re on the right track.

How, when, and where have you implemented any recommended fixes?

WHY THIS IS IMPORTANT:

Basic cyber hygiene practices like implementing patches, removing unnecessary privileges, and reconfiguring insecure systems are the best ways to reduce ransomware risk.

HOW TO INTERPRET “READINESS” FROM THE ANSWER:

The more advanced your organization is at maintaining basic hygiene across your critical assets (and measuring it over time), the better.

ASSET MANAGEMENT

Which assets do you anticipate are the most at risk to a ransomware attack? Do you have visibility across the entirety of your attack surface?

WHY THIS IS IMPORTANT:

You can’t secure a server that you don’t know exists. Fighting back against shadow IT isn’t just good for your IT department’s sanity, it’s also good security.

HOW TO INTERPRET “READINESS” FROM THE ANSWER:

When your penetration testing team asks for the company’s external exposure, do you have an up-to-date, comprehensive answer?

DETECTION AND RESPONSE IMPROVEMENT

When was the last time you tested your ability to detect specific tactics, techniques, and procedures (TTPs)? What did you learn and what did you do about what you discovered?

WHY THIS IS IMPORTANT:

Having a baseline documented understanding of your detection capability (including speed of detection across varied samples) can provide a quick snapshot into areas that may need additional investment, fine-tuning alerts, or adjusting policy.

HOW TO INTERPRET “READINESS” FROM THE ANSWER:

Organizations that continually assess and improve their threat detection and response capabilities will be more ransomware ready with each iterative exercise.

What are the specific steps you’ll take once you detect ransomware in your environment? Is your goal to isolate and recover without paying ransom or do you have other goals in mind when/if an attack happens?

WHY THIS IS IMPORTANT:

A plan A and a plan B are both necessary ingredients for ransomware readiness (and in fact, for any cybersecurity crisis). Not everyone will agree, and that’s best to find out now, before the fan gets hit by you-know-what.

HOW TO INTERPRET “READINESS” FROM THE ANSWER:

This is a litmus test question. It’s a lofty goal but teams that achieve clarity, consensus, and communication on what to do, how to do it, and who does what and when are closer to readiness.

TEAM COHESION

How prepared are you to take time away from regular business to sit in a conference room and test your ransomware readiness?

WHY THIS IS IMPORTANT:

Tabletop exercises are one of the best ways to assess ransomware readiness and establish a go-forward plan to address weaknesses—on both the technical and business sides. Yet they require valuable time, attention, and input from department heads and some of their team members, so gauge interest and set expectations early on.

HOW TO INTERPRET “READINESS” FROM THE RESULTS:

The more interest you can gain the higher up in the organization hierarchy, the more likely you’re already high up on the ransomware ready scale (and ready for even more improvement).



ABOUT BISHOP FOX

Bishop Fox is the leading authority in offensive security, providing solutions that help organizations secure their most critical assets against sophisticated cyber threats. Since 2005, we've partnered with Fortune 100 enterprises and high-growth innovators to deliver high-impact security testing and advisory services. Our comprehensive service offerings include tech-enabled, human-driven Continuous Security Testing, red teaming, and penetration testing for applications, cloud, networks, IoT, and AI/LLM.

LEARN MORE AT [BISHOPFOX.COM](https://bishopfox.com)

