invicti
AppSec with Zero Noise

EBOOK

Good Habits of Bad Actors

Life hacks for your security strategy

Give someone a fish and they'll eat for a day. Teach someone how to phish and they'll clear out your bank account.

Malicious hackers do a lot of damage annually, both financially and to brand reputation. They're good at what they do, thoroughly studying the weakest points of access and investigating the entire environment before making their move. And, they operate on minimal exposure, leaving as little forensic footprint as they can by using the latest tools, such as bending generative AI to help make phishing attacks more convincing. From phishing to ransomware and brute-force attacks, the bad guys are efficient and unabating.

Hacking by the numbers

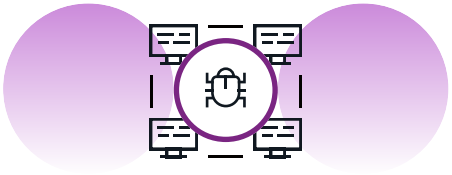
- By 2025, malicious hackers will run up about $10.5 trillion in global costs every year[1]
- It's estimated that only about 1% of cybercriminals are caught and punished[2]
- It takes 207 days to identify a breach and 70 days to contain it, on average[3]
- 83% of breaches are financially motivated within organized crime groups[4]

[1] Cybersecurity Ventures
[2] Cyber Experts
[3] IBM Cost of a Data Breach Report 2023
[4] Verizon Data Breach Investigations Report 2023

In 1986, famed hacker The Mentor published an essay, 'The Conscience of a Hacker,' which became known as "The Hacker's Manifesto." In the essay he wrote: "Yes, I am a criminal. My crime is that of curiosity. My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike."

More than 35 years later, it's hard not to think that all too many people have taken the words "I am a criminal" far too literally. When scrutinizing the current state of cybersecurity, it is clear that criminal hackers are indeed curious, they are many, and they know how to work together relentlessly. But we can learn from them. Many of the hackers, ethical or not, who followed this manifesto through the late 1980s and 1990s are embedded into IT today, helping us shape processes and procedures with the years of knowledge and wisdom they've accumulated from being part of that collective. If you pay attention to these learned habits and best practices, then you can stay off the phishing hook, too.

Next page
Good habits of bad actors that will give you an advantage



Hacker habit: Monitor and understand your environment, including who has access to what.

Hackers are very aware of their target environment. They monitor and absorb everything they can, including publicly available information about their targets and the security tools they use. Such an observational eye allows them to piggyback off of other flaws and bugs and go even deeper into physical and virtual systems. One example is an attacker looking for the network signatures of out-of-date software that has known exploits.

Your AppSec hacks

#01 Map your entire threat landscape.

That includes your digital attack surface where software is connected to your organization's network, your physical attack surface where endpoint devices live, and your human attack surfaces targeted through social engineering and phishing attacks.

- Use a dynamic application security testing (DAST) tool to probe your web attack surface for weaknesses like an attacker would.
- Establish and manage a web asset inventory to understand every potential attack point.
- Implement a software bill of materials (SBOM) to keep track of third-party components.

#02 Get a handle on access control.

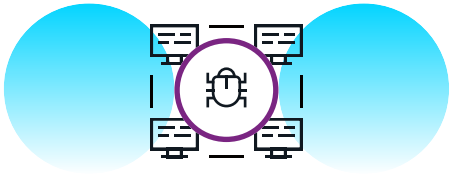
Authentication and authorization are used to prove identity and permissions, and are typically verified together. If either one or both are compromised, attackers can gain access to systems and APIs yielding sensitive data that might enable further attacks.

- Maintain fine-grained access control logic at the application level, not just the server level.
- Include authorization and authentication in all planning and design, and closely manage third-party infrastructure that might break auth flows.
- Check access control during regular code audits to ensure it is already included at code level.
- Implement specialized libraries that are already battle-tested for security.
- Practice the Principle of Least Privilege by ensuring that apps and people have the minimal level of access to get the job done. And no more.

Don’t forget your APIs!

Every modern enterprise utilizes an array of web services and APIs, but many organizations don’t include API security in their overall strategy. Invicti enables you to import API definition data through multiple industry-standard formats, and it will automatically add new API definition files that are found during crawling.

Learn more about covering your APIs and securing your hidden web attack surface →



Hacker habit: Share knowledge and tools with peers to help them work smarter, not harder.

Threat actors are extremely efficient at knowledge-sharing (ever been down a Reddit rabbit hole? We have.) They know how to work together in groups, collaborating on tools and workflows to make their lives – and their crimes – easier. Plus, readily available learning materials on the Internet mean that, with practice, hackers can fairly easily become experts in specific areas of security and development.

Your AppSec hacks

#01 Improve DevSecOps processes.

Too often, developers and security professionals work in silos and suffer from friction. They don't use the same tools and workflows, and they don't share information with each other. By improving collaboration, everyone is on the same page and can reduce risk easier.

- Use tools that work with popular issue trackers and CI/CD platforms like Jira and Jenkins.
- Establish a process for clear, consistent communication about security posture.
- Improve compliance and accuracy with tools that offer built-in checks and reports.
- Put security into the CI/CD pipeline and fail builds if critical flaws are discovered.

#02 Make security everyone's job.

For any organization that takes security seriously, it's imperative that everyone who works there understands it's also their responsibility to follow best practices and ensure they're reducing risk with every action they take.

- Establish a security champions program to leverage security advocates and share knowledge.
- Implement a set of best practices with consistent training programs for security.
- Clearly communicate security processes, policies, and goals from leadership down.

Are you making the most of integrations?

Building security automation right into your existing workflows helps developers keep pace with the rapid speed of software development without skipping any critical security steps. Invicti integrates out-of-the-box with many popular developer tools like issue trackers, collaboration platforms, and vulnerability management solutions – and almost any other system via its full-featured REST API.

Learn more about building security into your SDLC with Invicti's 50+ integrations →

Hacker habit: Question and verify everything to ensure you have the most useful information.

In his manifesto, The Mentor says that his crime was outsmarting his victims – and he wasn't wrong. Many hackers take every opportunity to question and verify so that they know they're operating with the most valuable information possible. If we want to keep pace, we need to relentlessly question and verify everything, just like they do before an attack.

Your AppSec hacks

#01 Prioritize accuracy in your tech stack.

Accuracy is a key component of cybersecurity, especially web application security where a misstep in your strategy can cause a domino effect of problems or add to security debt. Accurate tools enable you to find real vulnerabilities before they become really big problems, saving your team time.

- Combine dynamic and interactive (DAST+IAST) scans to check every corner of an application.
- Select an automated tool to save time, reduce manual workloads, and improve accuracy.
- Look for an application security solution with zero noise to lower false positive rates.

#02 Reduce the attack surface.

When you've mapped your entire threat landscape and have an asset inventory in place, it's time to start reducing your attack surface with the guidance of accurate, verifiable security scan results. It's critical that you uncover any weaknesses you can and remediate them promptly, including lost, hidden, and forgotten assets.

- Embed continuous scanning throughout the software development lifecycle (SDLC).
- Constantly assess risks and understand how to maximize opportunities.
- Implement, maintain, and share a web asset discovery and management system.
- If you're overwhelmed, start with easy win items (like attackers would).

Proof-based scanning improves accuracy.

Most security scanners are plagued by noisy false positives, sending teams on the hunt for threats that aren't even real. Proof-based scanning from Invicti cuts down on the noise and verifies 94% of major exploitable vulnerabilities with 99.98% accuracy. That way, your DevSecOps team knows when a security threat is real – if a scanner can exploit it, so can a hacker.

Learn more about proof-based scanning with Invicti →

Conclusion

The bad guys are all about ROI at the end of the day. At the same time, no target is too small, especially if it'll end up lending more data that will enable a larger attack. Keeping up with them might seem daunting, but with a combination of good habits and accurate tools, there's no reason for any organization to struggle with deploying secure software quickly and efficiently.

As an industry, we must take hacker best practices and apply them to our tried-and-tested security strategies. When approaching best practices, break out your strategy into four key pillars: Coverage, Efficiency, Accuracy, and Continuity. When effectively embedded into modern application environments, the ideas and processes behind these four pillars help ensure that organizations are covering all their bases for security.

#01 Coverage

Find everything and test everything, following in the footsteps of bad actors who are relentless about discovering gaps in your security coverage.

#02 Efficiency

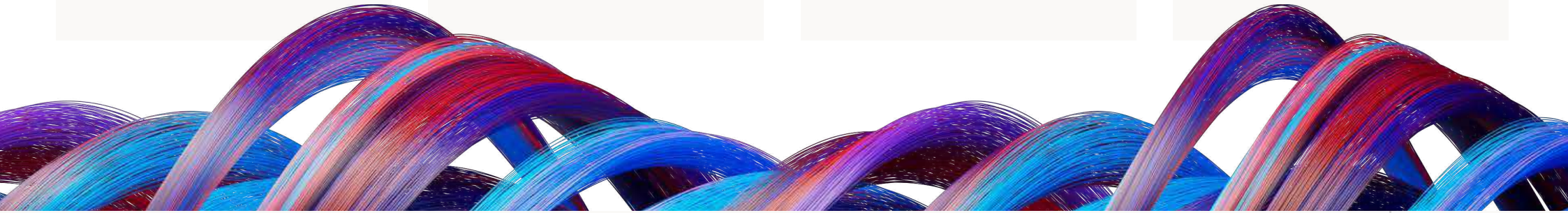
Embed security into the SDLC to test and remediate at the speed of development so that teams large and small can deploy new functionality faster and more securely.

#03 Accuracy

Have confidence in your data by selecting security tools with features like proof-based scanning and automated remediation guidance delivered right to your developers.

#04 Continuity

Keep going no matter what hurdles you face and get into the habit of scanning frequently to test and retest application security at every stage of development.

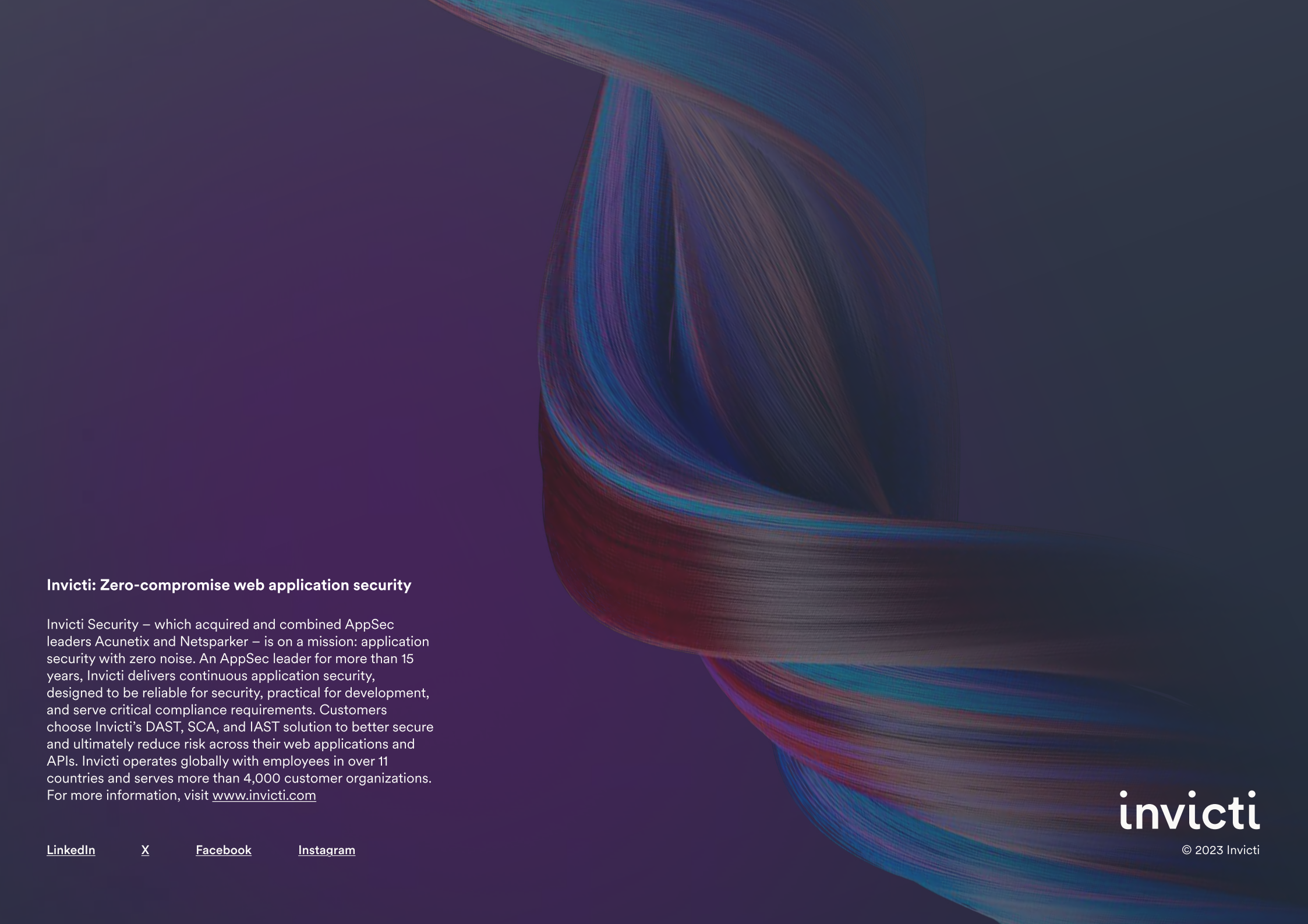


A combination of best practices, modern security tools, and reduced friction for DevSecOps will help you stay one step ahead of the bad guys to outsmart them before they outsmart you.

Interested in learning more about what Invicti and application security with zero noise can do for you?

Book a demo →

invicti



Invicti: Zero-compromise web application security

Invicti Security – which acquired and combined AppSec leaders Acunetix and Netsparker – is on a mission: application security with zero noise. An AppSec leader for more than 15 years, Invicti delivers continuous application security, designed to be reliable for security, practical for development, and serve critical compliance requirements. Customers choose Invicti's DAST, SCA, and IAST solution to better secure and ultimately reduce risk across their web applications and APIs. Invicti operates globally with employees in over 11 countries and serves more than 4,000 customer organizations. For more information, visit www.invicti.com

LinkedIn X Facebook Instagram

invicti