

How Continuous Attack Resistance Helps Improve Security Maturity

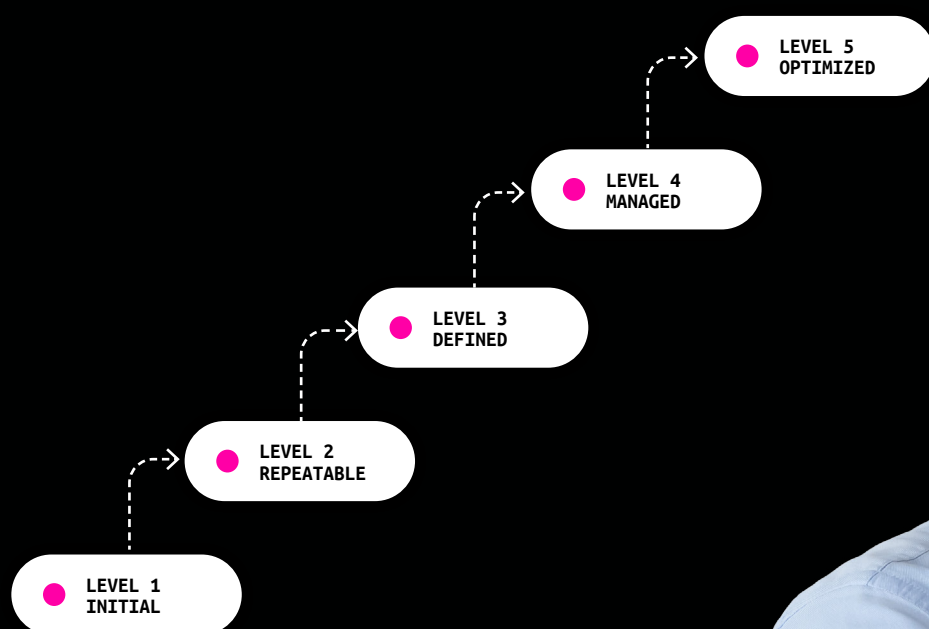


Table of Contents

Summary	3
Using the NIST Cybersecurity Framework and the Capability Maturity Model to Measure Maturity	4
What is the NIST CSFT?	
What is the CMM?	
Combining controls and maturity measurement	
What Is Continuous Attack Resistance?	6
Mapping Continuous Attack Resistance to the NIST CSF	7
Identify	
Protect	
Detect	
Respond	
Recover	
Continuous Attack Resistance Combined with NIST CSF and CMM	11
Assessing Security Maturity	12
Checklist to Assess Security Maturity	
Level 1: Initial	13
What does security look like at this level?	
What are the risks?	
Areas for growth	
How can continuous attack resistance help Level 1 organizations improve maturity?	
Level 2: Repeatable	14
What does security look like at this level?	
What are the risks?	
Areas for growth	
How can continuous attack resistance help Level 2 organizations improve maturity?	
Level 3: Defined	15
What does security look like at this level?	
What are the risks?	
Areas for growth	
How can continuous attack resistance help Level 3 organizations improve maturity?	
Level 4: Managed	16
What does security look like at this level?	
What are the risks?	
Areas for growth	
How can continuous attack resistance help Level 4 organizations improve maturity?	
Level 5: Optimizing	17
What does security look like at this level?	
What are the risks?	
Areas for growth	
How can continuous attack resistance help Level 5 organizations improve maturity?	
Take Your Security Maturity to the Next Level	18



Summary

Today's security leaders have limited resources while facing a nearly infinite number of systems, services, solutions, and threats. Determining where best to allocate resources is a complicated dilemma.

A security maturity model helps leaders identify and understand their organization's preparedness levels, identify security gaps, and make informed IT investment decisions. Too often, organizations aware of the latest security incidents and headlines react without a thoughtful game plan. A maturity model is proactive and provides best-practice guidance on the necessary capabilities for an organization's evolving security needs. A comprehensive security maturity strategy can also garner stakeholder support and facilitate discussions about achieving security goals.

One way to advance your organization's security maturity is to increase your attack resistance with preemptive testing from security experts. This community of security experts can assess your attack surface from an adversarial point of view to find the flaws that cybercriminals are most likely to target. With this approach security leaders gain a tangible way to minimize threat exposure and fortify security maturity.

This paper will show how preemptive, continuous security testing helps organizations fortify their attack resistance and improve security maturity as measured by key common frameworks: the [National Institute of Standards and Technology \(NIST\) Cybersecurity Framework \(CSF\)](#) and the [Capability Maturity Model \(CMM\)](#). Without advanced security maturity, organizations are vulnerable to cyberattacks against their people, products, processes, and technology.

Using the NIST Cybersecurity Framework and the Capability Maturity Model

First, we need to understand the fundamentals of security maturity measurement. There are two commonly used frameworks in the security profession, the NIST CSF and the CMM. Since continuous attack resistance is a relatively new practice within information security, employing two widely used frameworks will help ground what may be an unfamiliar concept.






Function	Category
Identify 	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect 	Identity Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Process and Procedures
	Maintenance
	Protective Technology
Detect 	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond 	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover 	Recovery Planning
	Improvements
	Communications

Table 1: The NIST CSF outlines necessary security team tasks organized by Functions and then by Categories within each Function.

What is the NIST CSFT?

The NIST CSF provides cybersecurity guidance on how organizations can identify, prevent, detect, and respond to cyberattacks. This framework, published by NIST, standardizes how security professionals describe security coverage. The two primary components of the framework are Functions and Categories. The Functions are Identify, Protect, Detect, Respond, and Recover. These represent the most basic tasks for any security organization. Inside of each Function are several Categories, which are more detailed tasks. For example, inside of Identify is Asset Management—identifying the assets in an organization. See Table 1 for a brief overview of the NIST CSF.

NIST does not intend the CSF to be a maturity model. Instead, the CSF is a set of controls for an organization to implement and manage how it classifies security. In this paper, we will combine the controls of the CSF with the maturity levels outlined in the CMM to show a comprehensive solution.

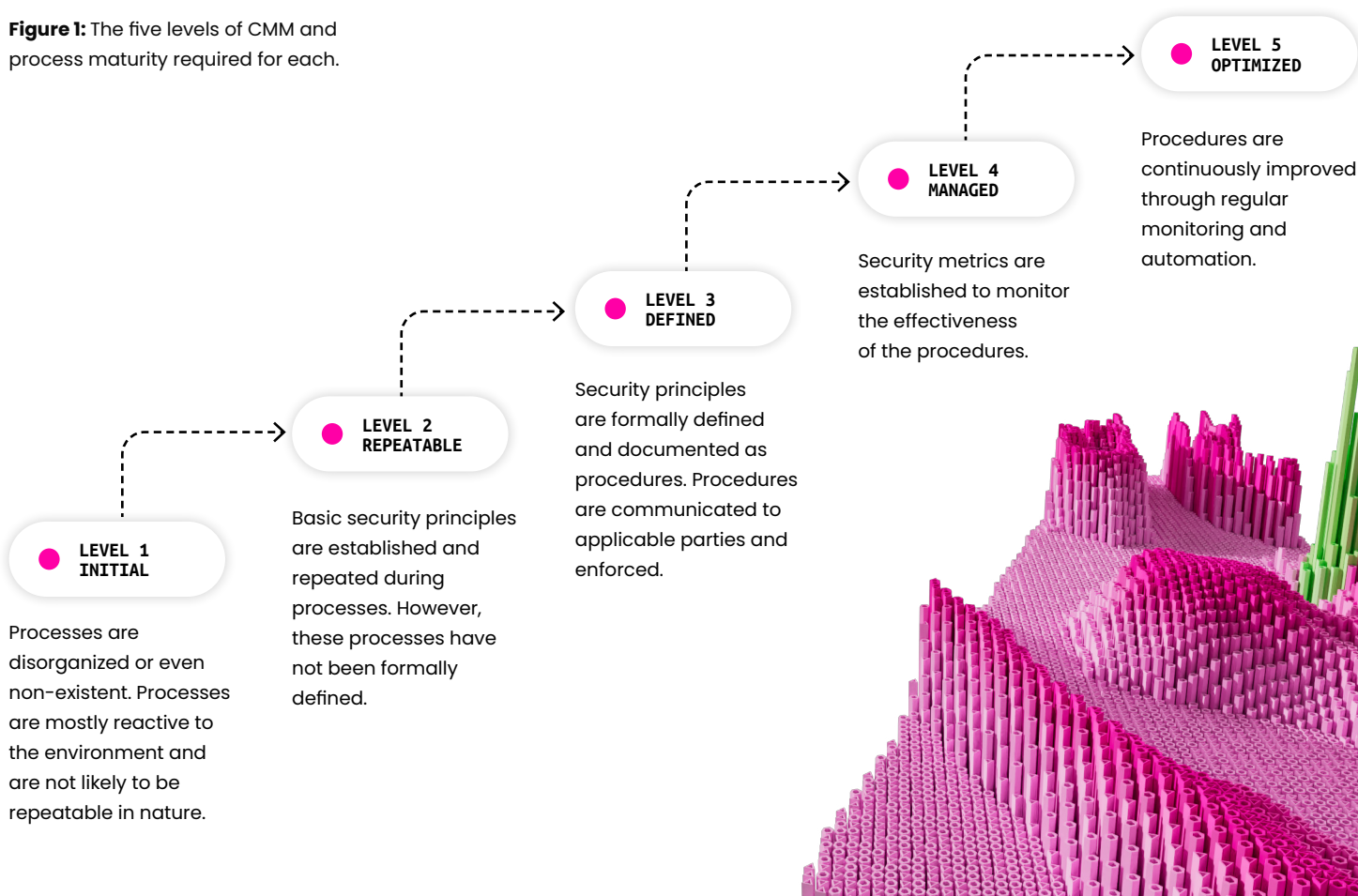
What is the CMM?

The CMM is a methodology used to develop and refine an organization's security processes and procedures. The [Software Engineering Institute \(SEI\)](#), a research and development center sponsored by the U.S. Department of Defense (DOD), initially designed the CMM for software development. Today, the CMM is widely used to assess maturity in information technology.

The CMM has five levels of maturity: Initial, Repeatable, Defined, Managed, and Optimized. Figure 1 shows the levels and the required process and procedure maturity required for each.

As an organization improves its people, processes, procedures, and technologies, it advances in maturity. In the context of cybersecurity, a more mature organization should have less risk exposure.

Figure 1: The five levels of CMM and process maturity required for each.



Combining controls and maturity measurement

Why does this paper combine the NIST CSF framework and the CMM methodology to measure security maturity? Because to measure security maturity, organizations need insight into what needs to be done and how to do it. While the NIST CSF defines what a team does by classifying tasks as Functions and grouping them into Categories, the CMM covers how by ensuring processes and their documentation, measurement, and improvement.

Before we combine the frameworks, we'll demonstrate how ethical hackers can add to a security program. We will then apply specific continuous attack resistance examples and their implementation to improve maturity in each area of control.

What Is Continuous Attack Resistance?

Continuous attack resistance combines automation with preemptive adversarial testing techniques to find unknown security vulnerabilities and reduce cyber risk on a continual basis. This continuous security feedback loop helps organizations advance their security maturity by providing these primary benefits:

1. Gain access to valuable skills and expertise that aren't otherwise available or may be cost-prohibitive.
2. Keep up with the rapid pace of new application changes and releases.
3. Allocate limited resources more effectively to ensure tangible risk reduction.
4. Feed vulnerability findings into existing software development processes for faster remediation.

The global community of ethical hackers has a wide range of skills and experience. Many hackers are full-time security professionals, others are developers or IT experts, and some are full-time hackers. The diversity of the community is an advantage when tackling the cybersecurity skills gap.

Continuous attack resistance can improve your organization's attack resistance through three distinct types of engagements:

- **Bug bounty and vulnerability disclosure programs** help to **test and fortify critical assets** with preemptive testing methods led by ethical hackers. With VDPs, businesses set guidelines for hackers and security researchers to submit vulnerabilities found in defined assets and systems. This approach helps to complement your existing security team with a community that has the skills and expertise to find exploitable vulnerabilities around the clock.
- On-demand **Penetration Testing as a Service (PTaaS)** provides more focused, methodology-driven testing to **demonstrate compliance and even validate coverage of other security controls**. Unlike traditional penetration testing that come with long lead times and high overhead costs, PTaaS offers a more cost-effective, on-demand delivery model that businesses can leverage for deeper analysis of their digital assets.
- Lastly, to understand how your attack surface evolves over time, **automated attack surface management** allows your business to inventory your digital asset landscape as new applications are deployed, and prioritize risk based on where you are most vulnerable. With this data you can **expand your adversarial testing scope** to maximize your business's attack resistance.

Vulnerability disclosure programs (VDPs) set guidelines for hackers and security researchers to submit vulnerabilities found in defined assets and systems. Many hackers appreciate the challenge, and VDPs harness that ingenuity to provide a continuous source of new vulnerabilities.



Mapping Continuous Attack Resistance to the NIST CSF

Continuous attack resistance doesn't satisfy every category within the CSF—no security technology or service does. However, applying adversarial testing to your program addresses many security concerns. Outlined below are the relevant CSF Categories within each of the five Functions and how continuous attack resistance fits.

Identify

The Identify Function assists in identifying and managing cybersecurity risk processes to systems, people, assets, data, and business processes. The categories most relevant to continuous attack resistance are Asset Management, Risk Assessment, and Supply Chain Risk Management.

Asset Management—The Asset Management Category inventories, manages, and classifies all enterprise assets. HackerOne Assets combines continuous asset discovery and monitoring workflows with human-led adversarial testing to reduce risk. Digital assets including web applications, IP addresses, web properties, and other related organizationally owned or operated assets are ranked based on exposure to risk, helping security and operations teams to prioritize remediation.

Risk Assessment—The Risk Assessment Category identifies and documents enterprise threats while assessing potential cybersecurity risk and relative organizational impact. The HackerOne Attack Resistance Platform allows hackers to flag these vulnerabilities and score them using the [Common Vulnerability Scoring System \(CVSS\)](#) or categorize them using [Common Weakness Enumeration \(CWE\)](#).

Supply Chain Risk Management—The Supply Chain Risk Management Category establishes and uses an organization's priorities, constraints, risk tolerances, and assumptions to drive supply-chain risk decisions. This category also helps the organization develop and implement processes to identify, assess, and manage these risks. With continuous attack resistance, ethical hackers may discover unknown third-party software vulnerabilities or other assets susceptible to certain types of attacks.



Identify



ASSET MANAGEMENT



RISK ASSESSMENT



SUPPLY CHAIN
RISK MANAGEMENT

Protect

The Protect Function outlines appropriate safeguards to ensure critical infrastructure service delivery and defense against threats to business processes, digital assets, data, and information. The CSF Categories most relevant to continuous attack resistance are Awareness and Training, Data Security, and Information Protection Processes and Procedures.

Awareness and Training—This category ensures an organization’s personnel and partners provide cybersecurity awareness education and training for cybersecurity-related duties. Hacker-discovered vulnerabilities raise awareness to security staff and are training examples for developers. The HackerOne Attack Resistance Platform offers a centralized view of an organization’s vulnerability exposure and routes reports to appropriate organizational teams. Integrations with third-party developer education platforms utilize the vulnerabilities to improve developer training.

Data Security—This category protects the confidentiality, integrity, and availability of data as per the organization’s risk management strategy. Hackers identify data leaks where sensitive data—such as customer databases and system credentials—have been posted online or on the dark web. HackerOne allows an organization to retain hackers and penetration testers to search for leaked information.

Information Protection Processes and Procedures—This category ensures security policies, processes, and procedures are maintained and used to manage the protection of information systems and assets. HackerOne Penetest, HackerOne’s PTaaS solution, allows an organization to test its security processes and procedures correctly. With these protocols in place, organizations see improved workflows and greater efficiencies. Other benefits include speed to certification, reduced overall costs, and the flexibility to run multiple tests simultaneously. Standard tests include [SOC2](#), [FISMA](#), [ISO 27001](#), [PCI-DSS](#), and others.

Detect

The Detect Function enables the timely discovery of cybersecurity events and threats. Continuous attack resistance aligns directly with the Security Continuous Monitoring category.

Security Continuous Monitoring—This category includes monitoring the organization’s network, endpoints, and connections to detect threats and vulnerabilities. The HackerOne Attack Resistance Platform combines the ingenuity of human security experts with real-time attack surface insight to provide continuous security testing of your digital landscape. Ethical hackers test an organization’s applications from an adversarial point of view to rapidly find highly exploitable vulnerabilities across the attack surface.



Protect

● AWARENESS AND TRAINING

● DATA SECURITY

● INFORMATION PROCESSES AND PROCEDURES



Detect

● SECURITY CONTINUOUS MONITORING

Respond

The Respond Function includes activities to react appropriately to a detected cybersecurity incident. The categories most relevant to continuous attack resistance are Analysis and Improvements.

Analysis—The Analysis Category objectives include the ability to triage and investigate detection system alerts effectively. Continuous attack resistance from ethical hackers coupled with a dedicated security analyst team helps to triage and assess the severity of reports submitted by ethical hackers. HackerOne's Triage Services allow your team to prioritize vulnerabilities, accelerate code fixes, and minimize the opportunity for malicious attacks.

Improvements—The Improvements Category objectives ensure organizational response activities are improved by incorporating lessons learned from current and previous detection and response activities. Specific hacker-submitted vulnerabilities are helpful to educate security staff and development teams. To avoid these vulnerabilities in the future, organizations can leverage findings to improve how they respond to similar future vulnerabilities. Partnering with a dedicated Security Advisory Services team can help ensure that vulnerability data is efficiently fed back to development teams to expedite remediation. In fact, incorporating vulnerabilities submitted by ethical hackers into existing development workflows can reduce recurring vulnerabilities by up to 98%.



Respond

ANALYSIS

IMPROVEMENTS



Incorporating vulnerabilities submitted by ethical hackers into existing development workflows can reduce recurring vulnerabilities by up to 98%.

Recover

The Recover Function includes the activities necessary to maintain resiliency plans and restore capabilities or services impaired due to a cybersecurity incident.

Improvements—The Improvements Category objectives ensure organizational recovery activities are improved by incorporating lessons learned from current and previous detection or response activities. Organizations can expand their continuous testing scope to cover applications with the potential for similar vulnerabilities. Using continuous attack resistance can also flag gaps within existing security controls during pre-production, which, in turn, can help curate developer training programs to foster better secure coding habits.

See Table 2 for an overview of where continuous attack resistance and HackerOne products and services map to the NIST CSF.



Recover



IMPROVEMENTS

Function	Category	Continuous Attack Resistance Activity	HackerOne Product(s)
Identify 	Asset Management	Attack-surface mapping, reconnaissance	HackerOne Assets
	Business Environment		
	Governance		
	Risk Assessment	Vulnerability intelligence	HackerOne Attack Resistance Platform
	Risk Management Strategy		
	Supply Chain Risk Management	Vulnerability disclosure program, bug bounties, PTaaS	HackerOne Response, HackerOne Bounty, HackerOne Pentest, HackerOne Challenge
Protect 	Identity Management and Access Control		
	Awareness and Training	Critical vulnerability training	Training tool integrations via HackerOne API
	Data Security	Leaked data detection	HackerOne Response, HackerOne Bounty, HackerOne Pentest, HackerOne Challenge
	Information Protection Process and Procedures	Pentesting	HackerOne Pentest
	Maintenance		
	Protective Technology		
Detect 	Anomalies and Events		
	Security Continuous Monitoring	Vulnerability disclosure programs, bug bounties, PTaaS, ASM	HackerOne Attack Resistance Platform
	Detection Processes		
Respond 	Response Planning		
	Communications		
	Analysis	Triaging	HackerOne Triage Services
	Mitigation		
	Improvements	Vulnerability intelligence	HackerOne Security Advisory Services; SDLC integrations via the HackerOne API
Recover 	Recovery Planning		
	Improvements	Vulnerability intelligence, critical vulnerability training	In-platform reporting and tracking via the HackerOne Attack Resistance Platform; training tool integrations via the HackerOne API
	Communications		

Table 2: Continuous attack resistance security mapped to NIST CSF Categories

Continuous Attack Resistance Combined with the NIST CSF and CMM

With continuous attack resistance defined, the CMM understood, and the NIST CSF detailed, it's time to put them all together. Table 3 shows NIST CSF Functions on the left side and CMM maturity levels across the top. Relative maturity is shown for each function at each maturity level. Within the description are specifics for each category where continuous attack resistance is applicable.

For example, within Protect, the categories most relevant to continuous adversarial testing are Awareness and Training, Data Security, and Information Protection Processes and Procedures. Moving from left to right in Protect, you will see processes move from non-existent or ad hoc to defined, managed, and automated.






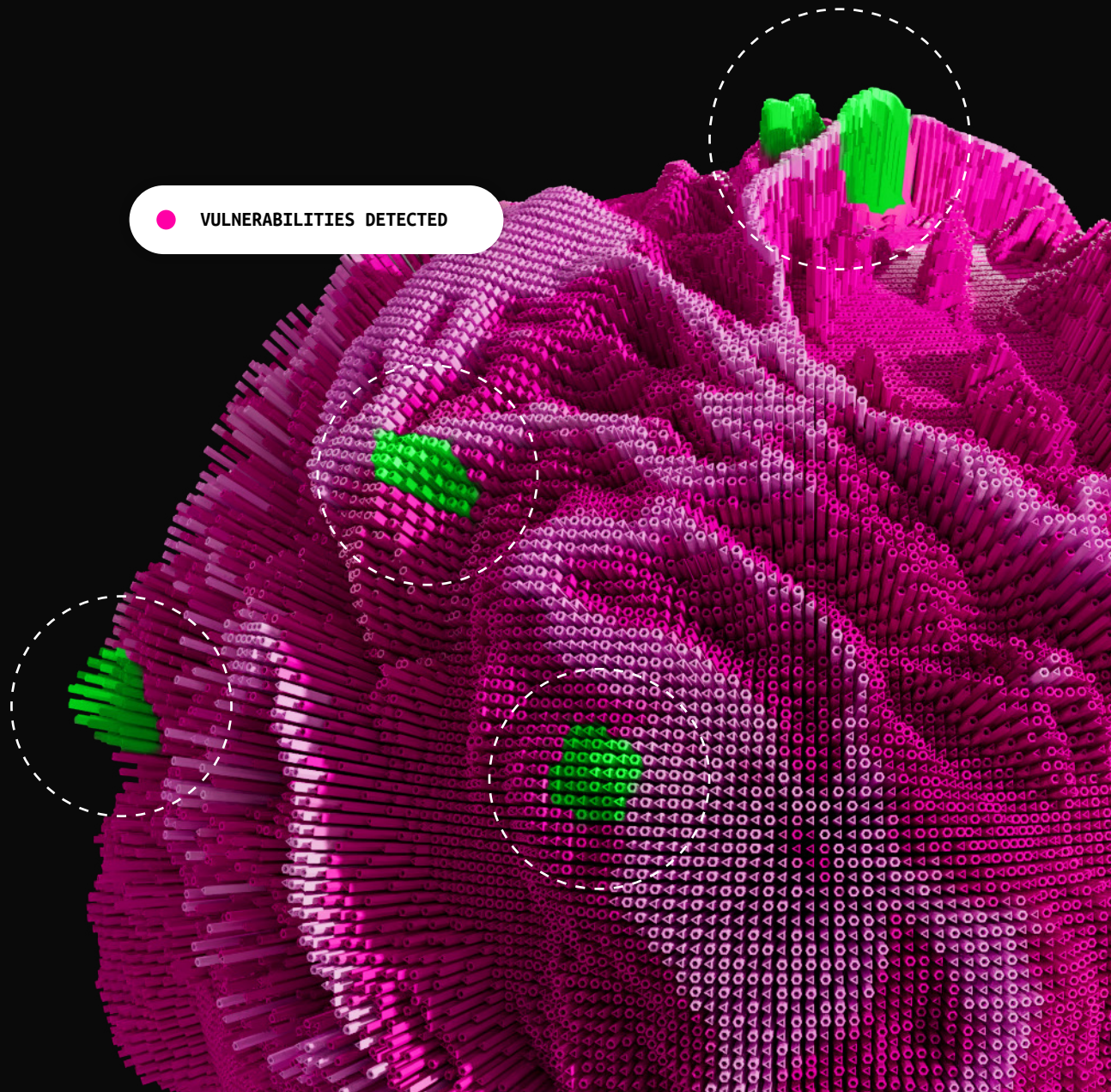
	Initial	Repeatable	Defined	Managed	Optimizing
Identify 	No asset management. Little to no cybersecurity risk identification. No supply chain risk identification. Incomplete or outdated governance.	Basic asset management. Immature process for organizational risk identification. No supply chain risk identification.	Attack-surface mapping process defined. Standard management of asset risks. Supply chain understood and risk defined.	Continuously monitor business risks. Implement a continuous attack-surface mapping process. Develop a process to identify supply chain risk.	Continuously monitor risks and incorporate them into business decisions. Risk information flows to and from the supply chain.
Protect 	Information security training is limited and ad hoc. There is no overall data protection. Penetration tests are few and done annually.	Annual information security training available. Need to implement environment-wide data protection mechanisms. Penetration tests multiple times per year for deployed applications and infrastructure.	Information security training required for all staff. Data types are formally defined and protected according to classification. Penetration testing extended to the development environment.	Information security training scored, and staff managed to a minimum. Proactively managed data protection. Penetration testing is done across development and deployment. User knowledge testing available continuously.	Information security training is customized to employee type. Automated data protection and penetration testing are on demand across all environments.
Detect 	Limited monitoring of internal and external assets.	Expanded monitoring of internal and external assets. Inclusion of external signals.	Monitoring of all assets based on risk level. Proactive efforts to understand the exposure of highest-value assets and their business criticality.	Monitoring of all assets automated and by risk level. Consider criticality. Continuous efforts to look for changes in the environment. Information sharing with some supply chain partners.	Monitoring of assets is continuously adjusted based on risk understanding. Monitor and prevent risk with the supply chain in place.
Respond 	No practice of event triage. Little to no investigative or forensic skills. No feedback loop.	Basic triage capabilities in place for highest-risk assets. Some investigative skills in an organization. Ad hoc feedback on some events.	Defined triage levels and response times for all asset classes. Dedicated resource for investigations/forensics. Digital Forensics and Incident Response (DFIR). Best-effort feedback loop.	Triage process automated and based on risk scoring against assets. Formal investigation process in place. Formal process for (manual) feedback defined. Postmortems look both at incident handling process improvements and root cause analysis for other incidents needing mitigation or remediation.	Triage is automated and measured against desired response times. Investigation escalation and SLAs in place. An automated feedback process is in place.
Recover 	The process for recovering from incidents is reactive or non-existent.	Incident response resources are applied consistently to incidents.	A continuity and disaster recovery plan is in place. The business continuity plan covers continuity of business processes and is typically owned by business units and is separate from a disaster recovery plan which is owned by an asset owner, usually IT (could be shadow IT).	Recovery times and impacts of incidents are monitored and minimized.	Regularly tests and updates to capabilities of all IT personnel, processes, and technologies.

Table 3: Security maturity shown for areas of NIST CSF helped by continuous adversarial security testing.

Assessing Security Maturity

At this point, with an understanding of the maturity model and how continuous attack resistance can help, the next step is to understand how it can apply to your organization. This next section outlines common traits of organizations at each maturity level and steps to progress to the next stage of maturity using continuous attack resistance methods.

At each level, the description provides an overview according to CMM, an outline of security risks, areas for growth overall in security maturity, and specific recommendations on where to apply continuous attack resistance.



● LEVEL 1:

Initial

What does security look like at this level?

- Processes are disorganized or non-existent.
- Processes are primarily reactive to the environment and are not likely to be repeatable.

What are the risks?

- There is a high risk of security breaches and the potential loss of sensitive data.
- It is impossible to detect or prevent cyber threats reliably.
- Security personnel are overwhelmed and unable to be effective.

Areas for growth

At Level 1, organizations must strike a balance between conserving resources and reducing risk. It is essential to cover the basics and implement solid, dependable systems and processes.

For example:

- Assess the current state of security to prioritize resource needs.
- Scope the attack surface and identify business impact or critically sensitive assets.
- Identify the most likely threats using a model such as the [OWASP](#) Top 10.
- Determine regulatory compliance requirements; e.g., [PCI](#), [HIPAA](#), [CMMC](#).
- Develop a basic vulnerability management program for valuable, business-critical assets.
- Implement basic security testing for internally developed applications and systems.

How can continuous attack resistance help Level 1 organizations improve maturity?

- Inventory your internet-facing applications and benchmark your risk profile with attack surface management (ASM). HackerOne Assets can accomplish this. (Identify)
- Execute pentests for all regulatory compliance requirements. HackerOne Pentest can accomplish this. (Protect)
- Implement a vulnerability disclosure program (VDP) or bug bounty program to allow concerned third parties to submit issues. HackerOne Response and Bounty can accomplish this. (Detect)



Identify

Inventory your internet-facing applications and benchmark your risk profile with attack surface management (ASM). HackerOne Assets can accomplish this.



Protect

Execute pentests for all regulatory compliance requirements. HackerOne Pentest can accomplish this.



Detect

Implement a vulnerability disclosure program (VDP) or bug bounty program to allow concerned third parties to submit issues. HackerOne Response and Bounty can accomplish this.

● LEVEL 2:

Repeatable

What does security look like at this level?

- Basic security principles are established and repeated during processes.
- Processes are not formally defined.

What are the risks?

Organizations at maturity Level 2 are typically growing rapidly. Security lags behind other aspects of the business. The organization may now face more targeted threats but is ill-equipped to deal with them.

- The presence of perimeter security causes a false sense of security.
- Security spending does not align with cyber risk.
- Risk of unplanned work or security incidents can cause operational delays.
- Lack of security resources forces the organization to accept a higher level of risk.

Areas for growth

- Ensure full documentation of all security processes and policies.
- Break down the “security silo” and build it into other IT functions, including development.
- Increase focus on risk management and invest resources to fill gaps and minimize cyber risk.
- Develop a security communications strategy that involves key business stakeholders.
- Provide ongoing security feedback to other functions, particularly engineering and development.
- Take a proactive approach to vulnerability management; e.g., through external assessments.

How can continuous attack resistance help Level 2 organizations improve maturity?

- Extend penetration testing to the development organization. Use HackerOne Pentest and Challenge to test applications for vulnerabilities once code is deployed, using common frameworks like OWASP Top 10. (Protect)
- Establish a bug bounty program for the highest-risk assets. HackerOne Bounty can be implemented and scoped to focus on these assets. (Detect)
- Push vulnerabilities to security management and code repository systems for expanded visibility across other functions. The HackerOne Attack Resistance Platform integrates with GitHub, GitLab, Jira, ServiceNow, and other systems. (Respond)
- Set up a triage process for vulnerabilities submitted by hackers via the bug bounty program. HackerOne provides triage services. (Respond)



Protect

Use HackerOne Pentest and HackerOne Challenge to test applications for vulnerabilities once deployed, using common frameworks like OWASP Top 10.



Detect

HackerOne Bounty can be implemented and scoped to focus on the highest-risk assets.



Respond

The HackerOne Attack Resistance Platform integrates with GitHub, GitLab, Jira, ServiceNow, and other systems.

Set up a triage process for vulnerabilities submitted by hackers via the bug bounty program. HackerOne provides triage services.

● LEVEL 3:

Defined

What does security look like at this level?

- Security principles are formally defined and documented in procedures.
- Procedures are communicated to relevant parties, enforced, and monitored.

What are the risks?

- Security can slow down the organization, impeding business and technology objectives.
- Security teams can become overloaded due to the number of systems, tools, and alerts in place.
- Security teams struggle to determine ROI from existing processes and tools.
- Security leaders struggle to allocate security resources to critical issues, and risk management is still challenging.
- Shadow IT is still not accounted for and represents risk from unknown vulnerabilities, compliance issues, security gaps, and data loss.

Areas for growth

- Measure and track security maturity against an established framework; e.g., NIST CSF.
- Define security metrics that the team will use to measure effectiveness; e.g., MTTR reporting.
- Begin implementation of continuous testing to secure operational infrastructure.
- Use contextual cybersecurity analysis and peer benchmarking to assess cyber risk accurately.
- Develop a customized security strategy that scales to support business objectives.
- Use tailored, proactive security measures to identify and remediate weaknesses.

How can continuous attack resistance help Level 3 organizations improve maturity?

- HackerOne Assets monitors your organization's external perimeter to expose unmanaged application risks. (Identify)
- Use hacker-discovered vulnerabilities to educate security staff and developers. The HackerOne Attack Resistance Platform has integrations with developer education systems to focus training. (Protect)
- Refine bug bounty program to focus on highest-risk assets and adjust rewards to incentivize desired hacker behavior. Customers can define HackerOne Bounty scope. HackerOne Security Advisory Services can also assist with program design. (Detect)



Identify

HackerOne Assets monitors your organization's external perimeter to expose unmanaged application risks.



Protect

The HackerOne Attack Resistance Platform has integrations with developer education systems to focus training.



Detect

Customers can define HackerOne Bounty scope. HackerOne Security Advisory Services can also assist with program design.

● LEVEL 4:

Managed

What does security look like at this level?

- Established security metrics monitor the effectiveness of procedures, processes, and consistency of delivery and operations.
- Processes, projects, and measurability are clearly defined and effectively controlled.
- Requirements are an experienced infosec team, adequate resources, executive support, a sufficient budget, and strong leadership.

What are the risks?

- Complacency or organizational personnel changes that cannot sustain this level of intensity.
- Relaxing of controls or mission focus, perhaps due to competing priorities.
- Shadow IT risk is unknown if the scope does not cover the entire organization.
- The organization must continue to invest in maintaining and sustaining this maturity level. This applies to every new tool, employee, process, and project.

Areas for growth

- Integrate security findings into workflows for other areas of the business; e.g., engineering.
- Evolve metrics and use them to drive organizational change.

How can continuous attack resistance help Level 4 organizations improve maturity?

- Benchmark vulnerability management against other organizations in the same industry or using the same technology stack. The HackerOne Attack Resistance Platform aggregates vulnerabilities found across all customers and allows for benchmarking so organizations can understand their performance. (Identify)
- Extend data protection to look for leaks posted on internet repositories and the dark web. Adversarial testing methods such as ethical hackers or penetration testing can detect shared secrets by looking for leaked customer information and credentials. (Protect/Detect)
- Administer response times and service-level agreements (SLAs) to acknowledge and respond to hacker-reported vulnerabilities. The HackerOne Attack Resistance Platform provides a program overview to track these metrics. (Respond)
- Response to vulnerabilities can be automated using the Common Vulnerability Scoring System (CVSS). Integrate hacker-discovered findings into your vulnerability management workflow via the integrations available from the HackerOne Attack Resistance Platform, with higher-priority vulnerabilities being priority routed. (Respond)



Identify

The HackerOne Attack Resistance Platform aggregates vulnerabilities found across all customers and allows for benchmarking so organizations can understand their performance.



Protect/Detect

Adversarial testing methods such as those from ethical hackers or penetration testers can flag shared secrets and look for leaked customer information and credentials.



Respond

The HackerOne Attack Resistance Platform provides a program overview to track hacker-reported vulnerabilities.

Integrate hacker-discovered findings into your vulnerability management workflow via the integrations available from the HackerOne Attack Resistance Platform, with higher-priority vulnerabilities being priority routed.

● LEVEL 5:

Optimizing

What does security look like at this level?

- Procedures are continuously improved through constant monitoring and automation.
- Security controls are comprehensively implemented, automated, and continuously monitored and improved.
- Security skills, technologies, and processes are regularly monitored and improved.

What are the risks?

- Level 5 organizations are in high-risk industries that demand advanced levels of cyber readiness.
- Security teams must move quickly to mitigate new threats, so processes must be impenetrable.
- A complex security stack and the use of third-party tools introduce additional risk.
- Maintaining complete visibility of all assets and vendor relationships is a significant challenge.
- Competing internal priorities force the security team to accept the additional risk or spontaneously adjust.
- Shadow IT increases the risk of data loss, vulnerabilities, compliance issues, and security gaps.

Areas for growth

- Build and maintain situational awareness of the evolving attack surface and threat landscape.
- Engage with a deep bench of on-demand security talent to address specific needs and concerns.
- Develop analytics to demonstrate security posture to business leaders, benchmark performance against industry peers, gain insight into vulnerability trends, and inform secure coding practices.
- Use innovative security initiatives to identify and address unknown security risks proactively.

How can continuous attack resistance help Level 5 organizations improve maturity?

- Use hacker-gathered vulnerability intelligence to identify areas of potential weakness. The HackerOne Attack Resistance Platform gives security teams information on where they may want to investigate or threat-hunt proactively. (Identify)
- Identify and discover software supply chain or connections; e.g., hunt for exposed credentials on the dark web. Identify new assets stood up by shadow IT; e.g., search the dark web for disclosed credentials or chatter around key supply-chain vendors. (Identify)
- Penetration testing can be done at any time, on demand, using hackers with the skills needed for the job. Use HackerOne Pentest select testers and perform tests quickly and integrate a HackerOne Challenge to conduct more curated adversarial testing for specialized goals. The HackerOne API allows for integration into an organization's DevOps and SOC processes. (Protect)
- Triage takes the burden of vulnerability validation off of your security teams, and bug-tracking integrations allow for the appropriate party to be notified and fix issues accordingly. HackerOne Triage Services and platform integrations allow for this. (Respond)
- Internal personnel are measured against hackers, giving management measurement of their people's skill level and effectiveness. The HackerOne Attack Resistance Platform can provide stats on vulnerabilities found and criticality per staff member, offering security and development management insights for staff training and work assignments. (Recover)

**Identify**

The HackerOne Attack Resistance Platform gives security teams information on where they may want to investigate or threat-hunt proactively.

**Protect**

The HackerOne Attack Resistance Platform offers a suite of adversarial testing methods that enable preemptive discovery of critical vulnerabilities.

**Respond**

HackerOne Triage Services ensure optimal vulnerability response times while developer bug tracking integrations ensure timely remediation.

**Recover**

The HackerOne Attack Resistance Platform can provide stats on vulnerabilities found and criticality per staff member.

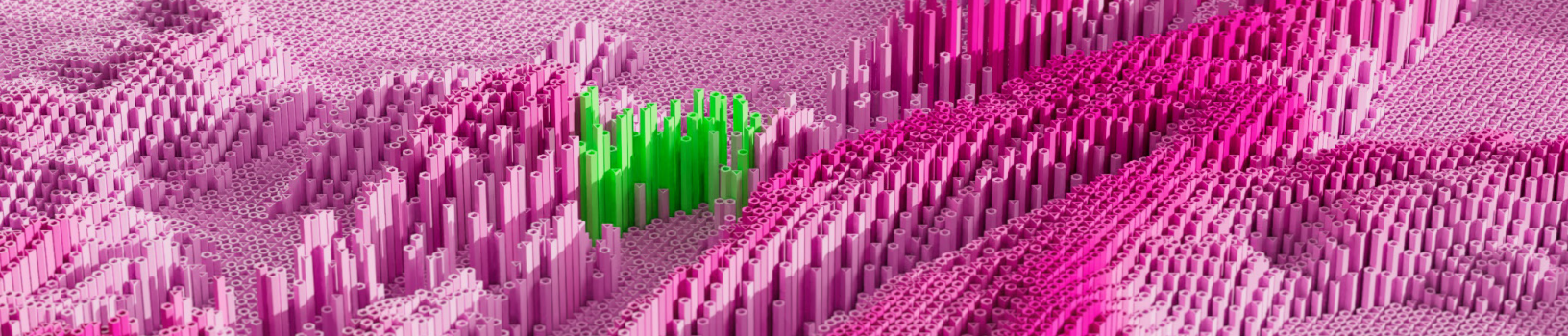
Take Your Security Maturity to the Next Level

Continuous adversarial security testing supports organizations on their journey to reduce cyber risk and improve their attack resistance. Tapping into the global hacking community provides on-demand access to diverse skills, experience, and ingenuity. Hackers can fill crucial gaps in modern security programs through a range of customizable engagements.

Any organization seeking to improve security maturity can utilize continuous adversarial security testing. But before embarking on any security improvement program, it is essential to understand where your organization stands. The maturity model in this guide provides a starting point for any organization wanting to assess maturity level. By combining the NIST CSF and CMM frameworks, your organization can understand current security maturity levels and set goals to move forward.

**Improve your
security maturity
with continuous
attack resistance.**

[Learn More](#)



HackerOne has vetted hackers for
organizations including:



Lufthansa



zoom



citrix

PayPal

Uber

HYATT®



Google



Adobe

A.S. Watson Group



yahoo!

priceline



slack

yelp



TOYOTA

hackerone

With over 2,000 customer programs,
more companies trust HackerOne
than any other vendor

Contact Us