PENTERA

THE BUYER'S GUIDE TO SECURITY VALIDATION

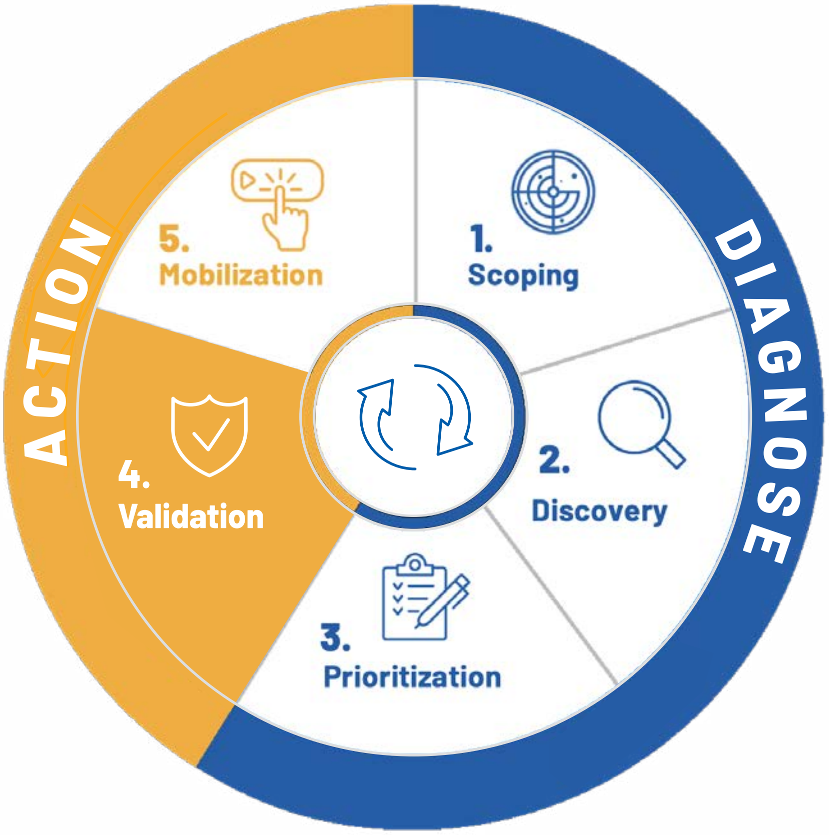
TABLE OF CONTENTS

Intro

The same old just isn't cutting it. You've probably even seen it yourself. A dynamic attack surface means risk to the business has skyrocketed and current security measures are struggling to keep pace. In fact, you're most likely reading this Buyer's Guide as you are looking for a new way to significantly reduce this risk.

> Gartner's insights reinforce this. They predict that:
>
> **By 2026 organizations that prioritize their security investments based on a continuous exposure management program will be three times less likely to suffer a breach.**
>
> *Gartner, "How to Manage Cybersecurity Threats, Not Episodes", August 21, 2023*

For those ready to embrace a new approach, Continuous Threat Exposure Management (CTEM) is a Gartner framework that changes the way security programs address vulnerabilities and improve security readiness. It's based on revealing the adversary's view of your IT environment and mapping exposures to guide remediation actions.



With CTEM, organizations assess and prioritize threats based on their business scope and importance and then validate to prove which ones most impact the organization. Rather than focusing on static vulnerabilities, teams look at full attack paths to provide context for remediation.

As a framework, CTEM already uses many existing technologies and processes. Vulnerability management, for example, is a practice common to nearly every security program. What makes CTEM unique is the validation piece. It’s no longer enough to assume security controls work the way that you intend them to, teams must know that they do - in short, they must validate them. This is why the key to getting started with a CTEM program is adding a security validation tool to your security stack.

This buyer's guide is designed to help you choose a security validation solution that fits your needs. We hope this guide can help shorten and simplify the process, so you can quickly identify the right solution for your organization.

Who needs a security validation (SecVal) solution?

Gone are the days when hackers only targeted large enterprises that could shell out millions of dollars in ransomware costs. Today, even the most modest mom-and-pop shops find themselves targeted by cyber adversaries. No one is immune from being at risk and having to manage it.

But not all businesses can afford to hire an on-site security team or dedicated Red Team. A SecVal solution can help by simplifying the complex task of identifying and prioritizing vulnerabilities and providing guidance on how to fix the relevant ones with a business impact. These capabilities allow any company to achieve a strong security posture.

Larger organizations with expansive security teams also stand to gain from integrating SecVal solutions into their workflow. These solutions ensure talent and time are reserved for exploitable risks that impact key business priorities. In addition, by taking over the routine security tasks, security teams have more time for innovation and elevating security measures.

SecVal solutions can also be beneficial for a wide range of practitioners:

CISOs
Provide comprehensive reporting to the CEO and board, showcasing real-time security postures and demonstrating progress and areas for improvement.
This can help illustrate the value of security investments.

Heads of IT
Identify true security issues that require fixing to better manage resources and reduce work on false positives. Facilitate security improvements by yourself, without relying on security experts to provide remediation guidance, and clearly communicate exposure trends to management.

Red Teamers
Automate repetitive tasks to save valuable time and focus efforts on testing more complex internal applications, processes, identity, or system-wide scenarios. This makes Red Teams more effective, and can even contribute to employee retention.

Network and Security Analysts
Validate that detection alerts, rules, and policies are functioning as intended so that detection and response operations are effective and reliable.

What can I do with a security validation tool?

A security validation tool can support multiple organizational needs. The main use cases include:

CONTINUOUS ASSESSMENT

Indiscriminate attacks by threat actors means every business should be actively working to detect and respond. However, with continuous testing, security teams can take a proactive approach to reduce the time it takes to discover newly created gaps and allow teams to act on them before they are exploited. Using automation means teams can conduct routine tests at frequent intervals for a more accurate security picture.

> **We have continuous scanning in our highest risk environments so we're able to see the live results from the test and we can get that feedback immediately and then take action on it.**
>
> *Stephanie DeLarm, Associate Cybersecurity Engineer, Casey's*

PENETRATION TESTING

Penetration tests are usually done infrequently for compliance reasons by a third party, but they can be so much more. Run your own in-house tests on-demand across the entire IT environment at more frequent intervals to mitigate proven high-risk gaps.

MERGERS & ACQUISITIONS

Measuring cyber risk is part of due diligence and audit requirements before purchasing or selling a business. Assessing the security posture can help identify risks and guide integration strategies post acquisition.

CYBER INSURANCE

A strong security posture can assist in getting insurance approval and reducing premiums. Security validation provides evidence related to the cybersecurity posture level and validation practices.

RANSOMWARE ASSESSMENT

You may have an XDR solution, but are you ransomware ready? According to the 2023 Verizon Data Breach Incident Report, almost a quarter of all breaches include a ransomware step. Make sure that your controls are prepared to handle the latest and most common ransomware strains. By safely emulating ransomware attacks, teams can test their controls against the full attack chain and assess the potential blast radius across live environments.

> **Pentera provides better visibility into our risk exposure from ransomware.**
>
> *Paul Ernst, CISO & Managing Director, Sandler Capital Management*

VULNERABILITY PRIORITIZATION

Start fixing what actually matters. Prioritization should not be based on CVSS score alone, but on which security gaps are proven to have the highest risk impact in the live environment to the business so teams can determine which vulnerabilities, configuration issues, compromised credentials and more to fix first. Looking at the full attack path, and not only vulnerabilities empowers security teams to make this assessment.

RED TEAMING

Every security team should be running cyber attack scenarios to identify exploitable gaps. Those who have Red Teams can use SecVal as a force multiplier to significantly enhance their capabilities. For those without an internal Red Team, a SecVal solution can act as a Red Team in-a-box, letting the tool emulate real attack scenarios to uncover critical security gaps.

What are the must-haves in any security validation tool?

Security Operations is changing, and so is the market. A whole host of tools and solutions have surfaced, trying to help enterprises reduce their security exposure. For potential buyers, this means that they need to get into the details to make sure a technology actually delivers real security validation.

Many solutions claim to do this, but not all can. Below are the must-haves any SecVal tool should provide to conduct true security validation. We recommend that you read them through, but also test the waters for yourself. In addition to having all of the features below, it should also be easy for you to test the solution in your own environment (such as a 1-day POV).

Full automation

Automation of simulated attacks for continuous validation. This means allowing the system to operate independently and frequently for longer durations at any time of day or night, simulating attacks and validating defenses without constant human intervention. Automation optimizes resource utilization and efficiency, increases productivity, and reduces the chances of errors.

Testing in Production

Cybersecurity teams should aim to run as many comprehensive testing scenarios as possible. This can be done in the form of "Golden Image Testing", i.e in a controlled, sandbox environment, or by testing against live production environments or in development environments.

However, golden image testing is limited in scope because it doesn't take into account any changes in the production environment. Additionally, it can be difficult to replicate the same conditions as in a live production environment.

Finding the right security validation tool includes a proper approval mechanism and control to allow live-fire tests without compromising system integrity.

Full attack path mapping

Meticulously mapping the full attack pathway, often referred to as 'attack vectors', rather than simply pointing out individual vulnerabilities. This capability needs to include attack flows linking each step in the threat actor actions and providing actionable intelligence about security weaknesses as they are seen in the eyes of the attacker. Full attack path mapping allows security teams to understand, calculate and prioritize risks and remediation efforts, ensuring that remediation efforts address the root causes of vulnerabilities and are leveraged to cut off pathways and shut down attacks.

Use of real, safe attacks - not simulations

Safely using real attacks like an adversary provides the most accurate way to identify real areas of weakness across the attack surface. This can be done by mimicking real world TTPs using workflows such as Man-in-the-Middle (MITM) attacks, Pass the Hash, credentials cracking, network-based attacks, RCE exploits and LOLBAS payloads, among others.

Validates the entire enterprise

Testing standard "table-stakes" security controls found within any large-scale organization as a default. These include, but aren't limited to: Email Control Testing, NDR/NTA Alert Testing, ACL and Segmentation Testing, IPS/IDS Testing, Endpoint Control Testing, External Perimeter Controls (WAF/Firewall), Cloud Security and Policy Controls, and Credential and Password Controls. By conducting these tests regularly, security teams can ensure that security controls are in place and are functioning properly.

Validation coverage of all attack surfaces

Validation of every inch of the organization, including traditional IT infrastructure, cloud services, endpoints and even emerging technologies that may be incorporated into the business environment. According to the Verizon DBIR 2023, the use of stolen credentials is the top tactic used by threat actors to affect assets, and most breaches involve affected servers. Attackers are using personal credentials, public cloud credentials and others to infiltrate your core, internal network. By reflecting a 360-degree view of potential vulnerabilities, security teams can ensure that no aspect of the network is overlooked, from cloud to on-premises environments.

Up-to-date threat emulation capabilities

Vendor patching and updates testing capabilities that are aligned with recognized frameworks like MITRE ATT&CK and others. This ensures the solution is able to detect and respond to the latest threats and allows the team to correlate information with the existing security controls, so they can review and update them.

Agentless deployment

The tests should mimic an attacker's actions in your network. As such the deployment shouldn't be reliant on agents that provide a foothold in the organization. Look for a platform with minimum impact on performance on workloads. Adding a SecVal solution should be a seamless integration into your existing security operations workflows.

Reporting and mitigation steps

Real-time, clear and adaptable reporting that is accompanied by actionable mitigation steps and can be integrated to build workflows and existing tools for detailed technical analysis, or as an executive summary. This enables immediate action against any potential issues and ensures that all levels of the organization are informed and equipped to act. Reports also serve to improve communication with functional teams and executive stakeholders.

Company credibility

A provider with a proven track record, regular software updates, a robust customer base in production, referenceable customers within the same or similar business vertical and an untainted security history provides peace of mind and fosters a sense of trust. This is as important a factor as the capabilities of the tool itself.

Accompanying professional services

This is a plus, offering the flexibility to tailor solutions to specific organizational needs, supporting unique custom workflows and deployment scenarios and enhancing the overall value of the solution.

EVALUATION SCOPE

When discussing a SecVal solution with potential vendors, it's important to ensure that the solution provides meaningful and measurable value and aligns with operational goals. Here's a breakdown of what to consider and to ask them:

	SCOPE	DETAILS
A	**Impact of Leaked Credentials**	Ask to see the impact of leaked credentials against your environment. By verifying the solution's effectiveness in a live production setting, you will be able to understand its real-world implications for your business.
B	**Live Production Testing**	Ensure their testing focuses on live production systems over laboratory or sandbox environments. This will yield the most accurate representation of security posture and response capabilities. The focus on real systems ensures that the results are applicable and actionable.
C	**POV Duration**	A well-designed POV (Proof of Value) should aim to not extend for longer than a few days. This is indicative of the tool's efficiency and the vendor's confidence in its product. An extended POV period may suggest complexity or inefficiency that could translate to longer deployment times in actual use.
D	**Comprehensive Reporting**	Post-POV reporting is required, as well as a thorough briefing with all key stakeholders, including operators, beneficiaries, and leadership, to discuss findings and next steps.
E	**IP Scope**	Clearly define 2-4 IP ranges, covering multiple networks, to understand the potential impact across different segments of the organization's network.
F	**Multiple Attack Surfaces**	A robust security validation tool must be able to test across various attack surfaces, including but not limited to internal networks, cloud environments, and external perimeters, to ensure comprehensive coverage.
G	**Diverse Asset Testing**	The tool should demonstrate its effectiveness across a range of enterprise assets, such as workstations, servers, Active Directory, and public cloud assets.
H	**Diverse Scenario Testing**	Different testing scenarios like Black Box, Grey Box, and ransomware emulation should be defined to challenge the tool's versatility.
I	**High-Privilege User Testing**	Ensure the POV includes testing of high-privilege user scenarios in the POV is critical to understand the risk and impact of potential insider threats or credential escalation exploits.

SUCCESS CRITERIA

1. Does the engagement address key business objectives like net risk reduction or enhanced operational efficiency?

2. Does the platform teach users naturally and is it easy to use?

3. Do the results clearly guide teams toward logical actions like remediation and policy adjustment?

4. Is the process to begin testing, deployment, and engagement with the technology actually going to reduce the need for human interaction or will it increase it?

5. Do we see alert and control behavior correctly acting against actions taken where expected?

6. Is it clear after a Proof of Value that the platform is safe to use and that actions won't cause business critical disruption?

About Pentera

PENTERA

Pentera is the category leader for Automated Security Validation, allowing every organization to test with ease the integrity of all cybersecurity layers, unfolding true, current security exposures at any moment, at any scale. Thousands of security professionals and service providers around the world use Pentera to guide remediation and close security gaps before they are exploited.

For more info, visit: pentera.io

REQUEST A DEMO

PENTERA

THE BUYER'S GUIDE TO SECURITY VALIDATION

www.Pentera.io