Cymulate

Extended Security Posture Management

The Ultimate Guide to Extended Security Posture Management (XSPM)

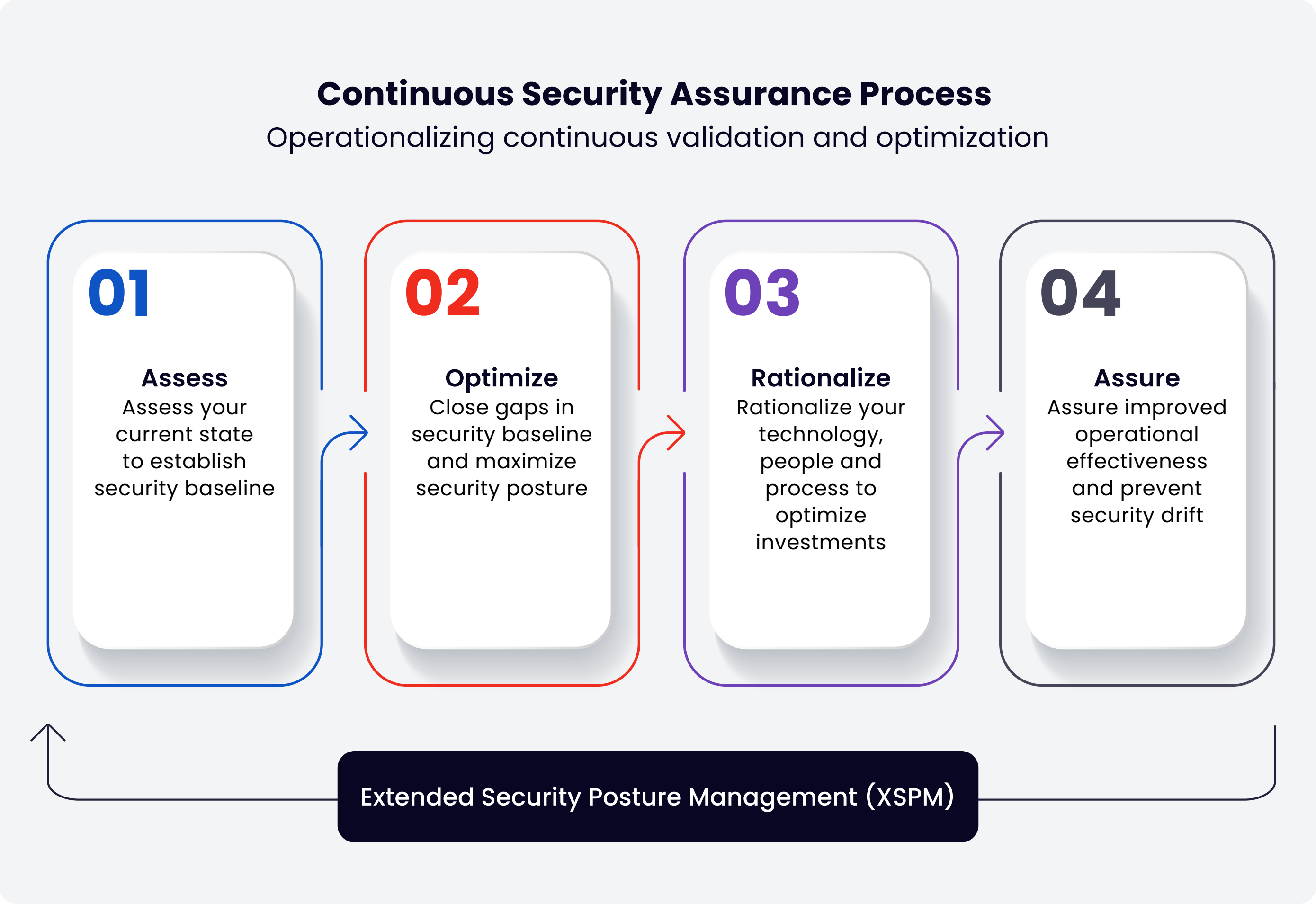
Roll out cyber-security optimization plan based on facts, data and an end-to-end baseline

Table of Content

01 Purpose of This Guide

To leave hypotheses and heuristics in the past and move forward to a fact-based, empirical discussion on cybersecurity. This guide will help you draw a baseline so you can know for sure how effective the cyber security program of your organization is.

It applies to both executives and security practitioners so they can work together to optimize the organizations' cybersecurity investments, solutions, and processes.



Continuous Security Assurance Process

Operationalizing continuous validation and optimization

01 Assess
Assess your current state to establish security baseline

02 Optimize
Close gaps in security baseline and maximize security posture

03 Rationalize
Rationalize your technology, people and process to optimize investments

04 Assure
Assure improved operational effectiveness and prevent security drift

Extended Security Posture Management (XSPM)

02 | Challenges of Legacy Validation Methods

In the past, most testing was done manually by contractors, once or twice a year, leaving security staff with a to-do list that in today's dynamic environments become utterly irrelevant by the time they get to work on it. The penetration testers and security consultants were happy to come back for another round and redeem their coupon.

The need for automation was there for many years and naturally led to the emergence of automated testing technologies. Automation had great value in making testing continuous. However, end-to-end security posture validation requires a holistic approach that early testing methods such as **Attack Surface Management, Automated Red Teaming or Breach and Attack Simulation** failed to provide individually. Each method was focusing on one part of the process and, therefore, unable to deliver clear - cut visibility to organizations. They were disparate, disjointed tools – each only covering a portion of a larger set of desired capabilities.
These solutions and approaches failed at drawing an end-to-end baseline of the security posture.

From a business stakeholder perspective, executives felt frustrated at these testing solutions' inability to optimize existing security posture or to clearly prove the value of cybersecurity spend.
They found these legacy solutions' inability to clearly visualize and rationalize risk and investments to their board disheartening. They couldn't even tell whether they were or weren't protected against the attack in yesterday's news.

For technical and operational staff, these legacy methods were complex, arduous to run, and resource-intensive, requiring months and vendor/third party consulting services to set up and run. Most required highly skilled staff to run with coding and advanced cybersecurity skill sets.
Most were incomplete, missing critical portions of the cyber security kill chain, and concerns over downtime and safety led many of these solutions to only be run in an extremely limited fashion, or worse, mainly in lab environments far from the real production environment.
The overall manual nature of these solutions made it impossible to run them continuously, yielding only mere snapshots at a time, in an era where the enterprise landscape and its attackers change daily.
As new threats emerged, these solutions lacked the capability of turning newly found TTPS (THREATS, TACTICS AND PROCEDURES) and IOC'S (INDICATORS OF COMPROMISE) into actionable, testable routines.

03 Common Business Challenges and Use Cases

Breach Feasibility

By far, the most critical capability is taking away assumptions and knowing exactly how susceptible you are by enabling end-to-end security posture validation. Beyond just a set of existing testable series of tactics, techniques, and procedures (TTPs) and indicators of compromise (IoCs), the solution must be automatically updated daily with new attack testing as they materialize in the wild.

Security Controls Efficacy

The solution should provide ways to shore up any gaps and misconfigurations, optimizing your first- and third-party security controls. By doing such, the enterprise reduces risk and prevents security drift. It should also effectively show if such optimization can protect against the latest exploits and vulnerabilities and reduce patching frequency and costs.

Employee Phishing Awareness Campaigns

Having a way to test and, more importantly, educate your employees, vendors and partners is a must. Running full phishing campaigns enables you to see where additional education is needed. Running these campaigns can be used to gamify the educational process, which increases its efficacy.

End-to-End Baselining and Trending

The solution should provide clear-cut visibility and detailed end-to-end baselining of an enterprise's security posture, and a continuous methodology to track and trend over time.
Doing so protects from security drift and evolving threats. Like ATT&CK Mapping, it becomes a common language and data set for all to use and understand.

External Digital Security Footprint

Through reconnaissance and active testing of an enterprise's external footprint, the solution should help prevent attacks by showing where the enterprise is exposed in data and resources facing the world.

Compliance

All recent compliance regulations include continuous security validation in their requirements. Thus the solution must be able to provide proof that the enterprise is doing such.

ATT&CK Mapping

From cybersecurity novices to and, people working in adjacent IT roles, switching to utilizing ATT&CK Mapping, references, and explanations will lead to the entire team speaking a common language and work more effectively.

M&A

As part of due diligence and exposure to potential risk investigation and evaluations performed prior to a merger or an acquisition, extended security posture management tools provide good visibility to possible liabilities or alternatively, boost the process if the results are good.

SIEM/SOC Validation & Optimization

A solution should help you test and validate that your SOC is adequately alerted to all activity. It should also provide prescriptive remediation capabilities. Finally, in the process of doing so, the team is further educated, tested and ready for when real attacks occur, reducing dwell time and mean time to remediation.

04 The Four Fundamental Pillars of Extended Security Posture Management

01 Attack Surface Management (ASM)

Emulating an attacker during the reconnaissance phase as they perform a comprehensive analysis on their target organization. ASM tools scan the domains, sub-domains, IPs, ports, etc., for internet-facing vulnerabilities. It is also looking for Open-Source Intelligence (OSINT) that can later be used in a social engineering attack or a phishing campaign.
This tool helps organizations understand how hackers might get an initial foothold.

02 Continuous Automated Red Teaming (CART)

CART tools go beyond just the reconnaissance page to answer the question "how can an adversary breach my defenses?" These tools attempt to penetrate the organization by analyzing the exploiting exposed vulnerabilities and autonomously deploying attack techniques that penetrate into the network.
For example, they can trigger the attack with a well-crafted phishing email. After gaining the initial foothold, the attack subsequently propagates within the network in search of critical information or assets.

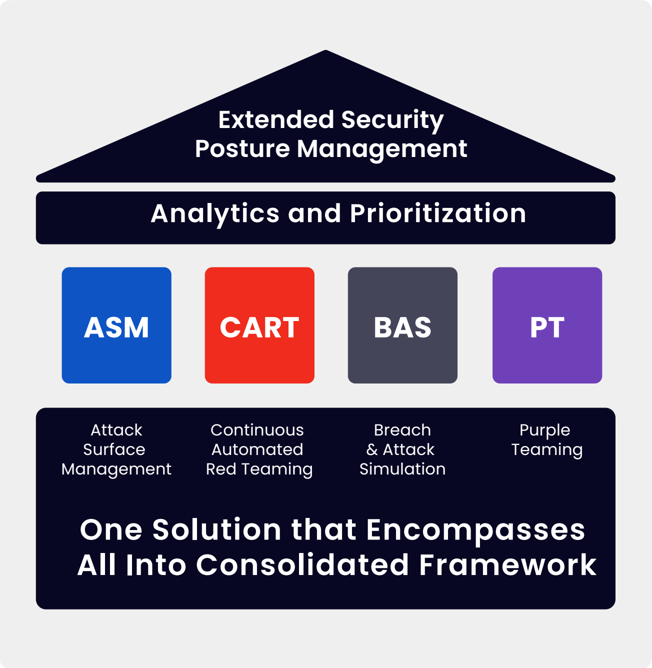
03 Breach Attack Simulation (BAS)

Breach and Attack Simulation tools answer the question "how well are my security controls and processes performing?" It launches simulated attack scenarios out of the box, and correlates findings to security controls (email and web gateways, WAF, Endpoint etc.) to provide mitigation guidance. These are primarily used by the blue team to perform for security control optimization.

04 Advanced Purple Teaming

Purple teams expand BAS into the creation and automation of custom advanced attack scenarios. These tools usually leverage the MITRE ATT&CK® framework extensively, enabling security teams to create complex scenarios from predefined resources and custom binaries and executions. Customed scenarios can be used to exercise incident response playbooks, pro-active threat hunting and to automate security assurance procedures and health checks. Altogether you get an end-to-end baseline of the security posture, rather than a partial picture.

This comprehensive framework provides a comprehensive understanding of current levels of risk, exposure, drift, and even potential savings – all are is essential and strategic to an organization who usually make cyber-security related decisions based on hypotheses – regardless of the level of cybersecurity maturity, skills, and resources they own.


Extended Security Posture Management
Analytics and Prioritization
ASM
CART
BAS
PT
Attack Surface Management
Continuous Automated Red Teaming
Breach & Attack Simulation
Purple Teaming
One Solution that Encompasses All Into Consolidated Framework

Altogether, you get an end-to-end baseline of the security posture rather than a partial picture.
This comprehensive framework provides a comprehensive understanding of current levels of risk, exposure, drift, and even potential savings – all these are essential and strategic to an organization that makes cyber-security related decisions based on hypotheses – regardless of the level of cybersecurity maturity, skills, and resources they own.

05 The Additional Power of Vulnerability Prioritization Technology

Once the baseline is set, the cybersecurity discussion becomes data-driven and fact-based. From then on, there's no more room for assumptions.
Everyone – Executives, CISO, SOC, blue and red teams – get a clear picture of the current security posture. The efficacy of the security controls, penetration paths, drift as well as overlap. It is only imperative that the next step would be optimization, but wouldn't it be easier if the tool you're using could integrate with standard vulnerability management solutions to provide some guidance on where to begin? Which vulnerabilities are more exposed, which are more exploited, which aren't at all accessible?

The following illustration shows how organizations can evaluate the trade-off between duration of patching and cost of minimizing risk to eventually make educated decisions:

80%

Patch **80%** of all endpoints and **100%** of business critical endpoints within two weeks **$3M/Yr**

OR

75%

Patch **75%** of all endpoints and **95%** of business critical endpoints within 4 weeks **$1M/Yr**

06 Benefits for Executives

Continuous Security Optimization Framework

CIOs and CISOs need to constantly re-evaluate which elements of their cybersecurity solution stack they should keep, replace, or eliminate. To do so, they need accurately and evaluate their levels of risk, create a baseline and trend it over time.
In doing such, they will reach and remain in the Goldilocks' zone between security requirements and operational efficacy. They need to ensure they maintain adequate visibility, that security controls are well-tuned, misconfigurations and gaps are found and removed, that incidents are being detected and not flying under the radar. They need to evaluate the security posture of critical assets and infrastructure, employees' level of cyber awareness, incident response plans and, most importantly, they need to validate their security controls.

Security Posture Validation

When done right, as a CISO you know:

- Assess your current state to establish a security baseline for visibility and control.
- Rationalize your technology, people and process to eliminate overlap.
- Assure improved operational effectiveness and prevent security drift.
- Continuous automated validation - neither additional workforce nor costs required.
- Maximize security posture and close gaps in security baseline.

Precise data enables optimizing their security solution stack by eliminating overlapping solution features and reallocate funds to cover exposed areas.

Investment Rationalization and Optimization

Allocating funds in direct proportion to the company's priorities also applies to cybersecurity.
This adjustment requires a quantified estimate of the effectiveness of the existing stack of cybersecurity solutions for each business unit, based on extensive and broad-range security validation and with in-depth analysis, including a clear picture of which solutions are instrumental in protecting which business unit. With these data in allocating for security purposes to reflect the company's priorities becomes much more manageable and effective.

The example below shows how to reallocate funds based on priorities for a company that deems their R&D is a more critical business unit than Customer Success or Marketing. As the security validation testing indicates that, in contradiction to their defined priorities, their security spend in Sales & Marketing and Customer Success (CS) is higher than in R&D, they can redistribute funds and realign business units' security effectiveness score with their defined priorities.

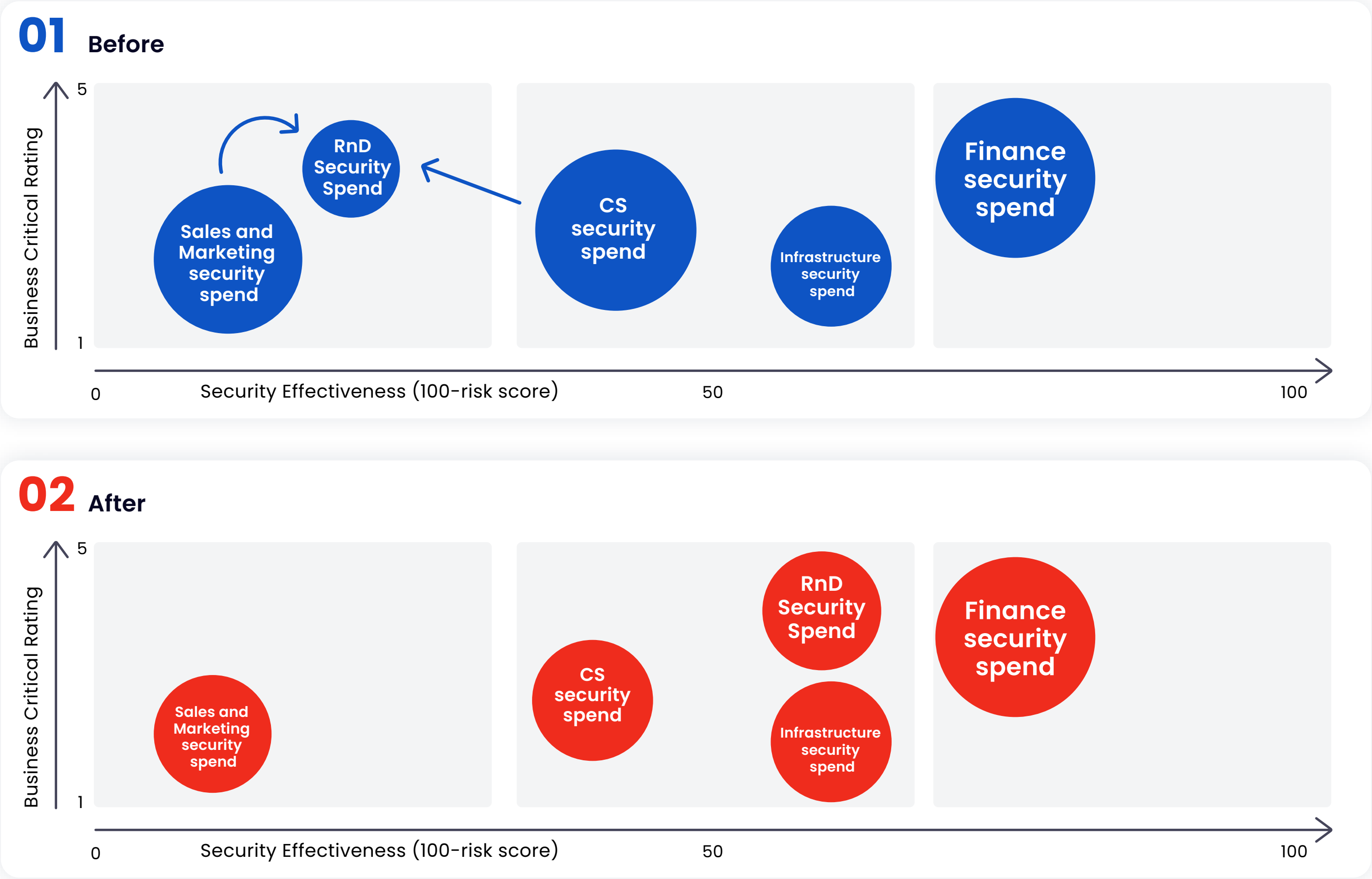


Figure Name: Reallocate security spend based on operational effectiveness and business criticality

Compliance

CISO and CIO tasked with evaluating their company's infrastructure degree of compliance need to be in a position to identify and remediate compliance gaps with the ever-growing list of rules and regulations applying to cybersecurity resilience, from major ones like GDPR, HIPAA, or PCI-DSS, to lesser-known or less encompassing ones such as AICPA SOC2, SOX, GLBA, FISMA, FedRAMP and others.

All these standards require continuous validation of policy enforcement, best achieved through the automation of security assurance processes enabling a detailed identification and quantification of cyber risks.

07 Benefits for Security Professionals

Whether the security leadership, analysts, SOC, blue or red teamers - confidence comes from knowing that innovative solutions:

- Comprehensively cover all stages of the kill chain (or MITRE ATT&CK framework)
- Can be easily implemented in less than an hour without professional services
- Leverage their existing staff effectively.

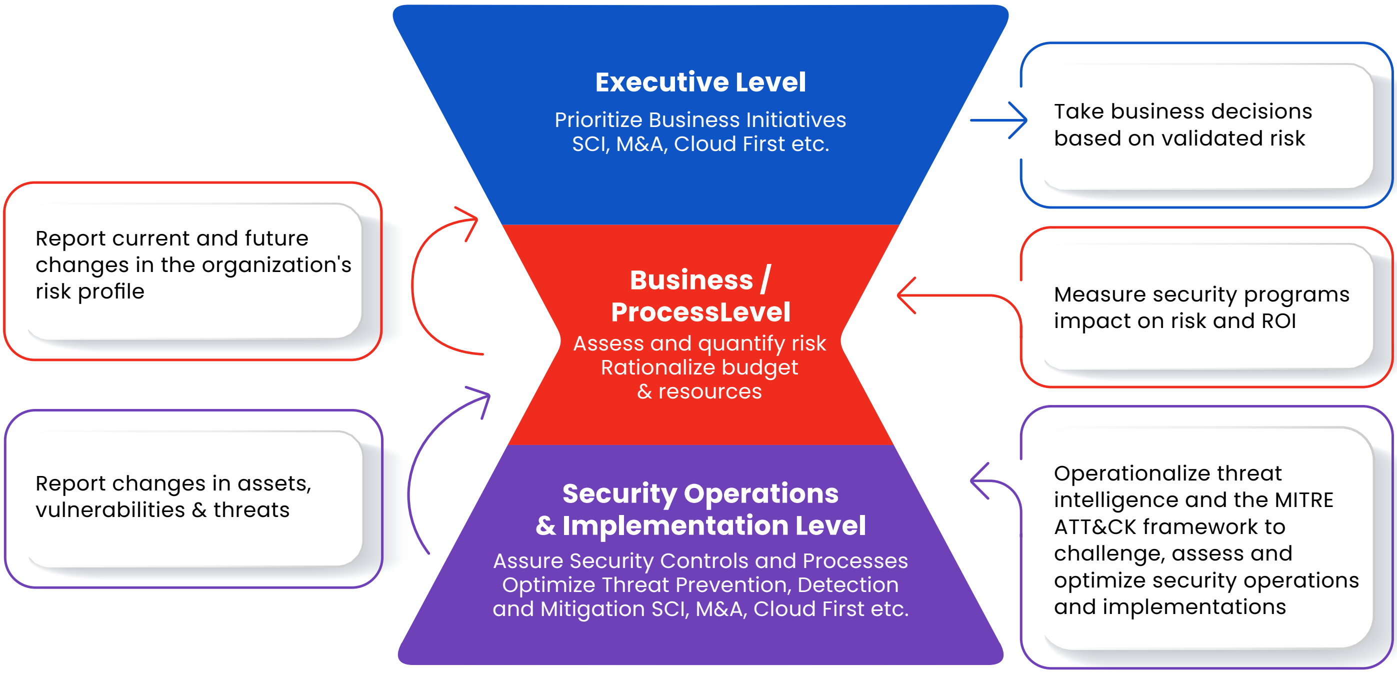
They need to check if the information brought to the SOC attention cover all penetration attempts, or, in other words, whether all relevant alerts are invoked. CI/CD practices created a need to continuously check whether policy rules are optimally configured and enforced across the board.

Those in charge of security to regularly test their SOAR, processes, and playbooks to measure and correct the security drift.
Comprehensive data is essential to boost confidence in the ability to find gaps, misconfigurations, and vulnerabilities, and enables effectively both shoring up and optimizing security posture.
Detailed information about the effect of emerging vulnerabilities on attack surfaces is what leads to effective patching prioritization. Similarly, a method to rapidly evaluate security resilience and potential exposure to emerging threats, as well as specific instructions to prioritize and process patching minimizes drift and, as a bonus, facilitates reporting to management at any time.

Security Posture Management

When done right, as a cybersecurity practitioner you can:

- Leverage my existing team. No coding required.
- Test and secure comprehensively.
- Deploy quickly, with a light touch and no professional services required.
- Optimize my cybersecurity posture and reduce risk.
- Get immediate results.
- If attacked, you can recover gracefully.



Executive Level
Prioritize Business Initiatives
SCI, M&A, Cloud First etc.

Business / ProcessLevel
Assess and quantify risk
Rationalize budget
& resources

Security Operations & Implementation Level
Assure Security Controls and Processes
Optimize Threat Prevention, Detection and Mitigation SCI, M&A, Cloud First etc.

Take business decisions based on validated risk

Measure security programs impact on risk and ROI

Operationalize threat intelligence and the MITRE ATT&CK framework to challenge, assess and optimize security operations and implementations

Report current and future changes in the organization's risk profile

Report changes in assets, vulnerabilities & threats

08 Solution Consideration Check List

A single, comprehensive platform

A single solution incorporating ASM, CART, BAS and Purple Teaming to set an end-to-end baseline by testing all possible scenarios and penetration routes, including the latest threats.

Serviceable to all, regardless of cyber-maturity levels

The global cybersecurity professionals' shortage means your solution has to provide off-the-shelf offensive and defensive options that are both usable by all capable of lightening the workload of skilled cyber practitioners.

Off the shelf templates with flexible customization

An open framework for the creation and automation of custom attack scenarios leveraging MITRE ATT&CK framework, integrable in

- IR playbooks
- Pro-active threat hunting Security assurance procedures and
- Health-check procedures

Simple light touch deployment

A SaaS solution with easy implementation that enables automated, continuous testing shortly after deployment, without requiring additional resources.

Actionable Analytics

Automated executive and technical reports generation

- **Executive/Business reports** enabling decision-makers to evaluate security investment effectiveness, spot potential redundancies, and free the funds to plug holes in the security posture
- **Technical reports** providing SOC and IT team with exhaustive and clear remediation instructions

Essential Features

01 SaaS vs. On-Prem.

Protecting your environment begins by taking no disruptions risk with CPEs or agents unless necessary. It is safer to use SaaS services.

02 Provide immediate incorporation of emerging threats

The ever-evolving nature of the threat landscape demands a solution with continuous threat updates.

03 Exhaustive attack kill chain coverage

Stages - from analysis to pre-exploitation, exploitation, and post-exploitation, including:

- Internet and DarkNet scouring for signs of offensive intent
- Phishing module to test risk level across the workforce

Environments - from on-prem to cloud to clouds, bare metal to VMs to containers.

04 Support living-off-the-land and pivoting in testing

Opportunistic testing must mimic the skills and tactics of real-world attackers who find new paths when hitting a dead-end.

05 Support chaining of tests

Incorporate all vectors along the attack kill chain and support compound testing, chaining across multiple attacks kill chain vectors.

06 Supports safe testing in production environments of tests

Runs in your production environment across active workloads, not on environment emulations.

07 Support entire enterprise environment

On-premises, hybrid, native cloud environments - and covers a wide array of operating systems, bare metal, virtualized workloads, containers, and more.

Summary

When the requirements are well understood and realized, security posture management provides clear-cut business and technical benefits at strategic levels. Selecting a solution that works off a single platform, that is fast and simple to deploy, can be managed effectively and is beneficial to all security professionals no matter the maturity skill level is key. The platform needs to be comprehensive in coverage and provide prescriptive, simple-to-follow technical remediation tips as well as executive reports clearly explaining risk and how it can be managed and reduced. The vendor should also be committed to an open, vendor agnostic education program. By doing so, enterprises will see significant reductions in risk, optimization of security posture, their investments in cybersecurity maximized and simplified.

Start Your Free Trial

Contact us for a live demo, or get started with a free trial