品項名稱:

FireEye Verodin 安全儀表平台

產品介紹:

安全團隊保護他們組織關鍵的資產，在當今不斷變化的威脅環境中，具有挑戰性的憲章，困難重重。 這些團隊在安全技術上進行了重大投資，以保衛自己的組織，在許多方面都這樣做沒有授權的案件有效地展示或驗證這些功能以兌現其諾言，以防止對手妥協他們的系統和網路。

商品特色:

1.評估當前的安全性的工具功效

2.發現您未發現的差距安全和基礎設施

3.衡量團隊的時間檢測和響應

4.找出最大的設備優化機會

5.改善配置設定和消除具體弱點

6.確定哪些控件最有價值，最無價值的設備

7.量化改進隨著時間的改善防禦

8.增強團隊自動化連續監測

9.合理化投資價值證明給高階主管

OVERVIEW

Get Started with Verodin Security Instrumentation Platform.

The global leader in continuous security validation.

CISOs ARE MEASURED ON THEIR EFFECTIVENESS

Security teams protect critical assets for their organizations, a challenging charter with difficult odds in today's dynamic threat environment. These teams make major investments in security technologies to defend their organizations, doing so in many cases without being empowered to effectively demonstrate or validate these capabilities to deliver on their promises to prevent adversaries from compromising their systems and networks.

Some teams try to close this gap by relying on limited tests from overstretched staff or outsourced red teams with significant time constraints. Others count on limited technologies like vulnerability scanners and automated penetration tests that don't fully and accurately represent the real threat environment.

The future success of security teams calls for a new paradigm - a way to verify and continuously test the promises of others. That new approach is the Verodin Security Instrumentation Platform, (SIP) a cybersecurity risk assessment and management platform that enables teams to ensure their critical assets are always protected.

IMPROVED EFFICACY, DELIVERED IMMEDIATELY

With the Verodin platform, you can rapidly quantify and prove your ability to defend your organization from the expanding threat landscape of sophisticated adversaries around the world and their latest attacks, whether your architecture is wholly on-premise, hybrid, or in the cloud.

Start by safely assessing and capturing discrete, quantified evidence of the effectiveness of your overall security architecture against real adversary attacks. The results highlight specific individual attacks and even entire areas in the extended kill chain that defeat or bypass your security technologies. You can leverage these insights to optimize your controls, working with specific performance data and vendors as needed, and ultimately transform your entire program.

Quantifying your efficacy improvements makes it easier to demonstrate results and rationalize your investments within a business framework to your executives.

All this is continuous, automated, and repeatable, allowing you to focus on defending your business more strategically while the Verodin platform vigilantly underpins your overall security effectiveness.

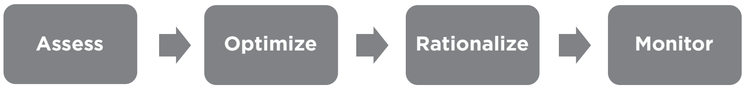
OVERVIEW

KEY BENEFITS

- Assess current security tools efficacy against real adversary attacks
- Discover previously undetected gaps in your security and infrastructure
- Measure your team's time to detect and respond
- Identify the greatest opportunities for optimization
- Improve configurations to target and eliminate specific weaknesses
- Determine which controls are most and least valuable
- Quantify improvement to defenses over time
- Augment team with automated, continuous efficacy monitoring
- Rationalize value of investments to executives with proof

BE CONFIDENT IN YOUR SECURITY POSTURE

Quickly configure the platform, connecting actors, an alert source, and any specific controls for additional depth. Graphically add your high-level infrastructure. Select discrete tests or preconfigured sequences of tests from the vast library of real attacks from adversary techniques and malware. Safely run these tests immediately and continuously to validate specific controls are working properly. Dashboards populate in real-time with detection, alert, miss, and prevention rates as tests run. The platform also validates that events are properly timestamped, correctly parsed, and if the correlation rules and threat models defined generated appropriate alerts. Reports are available to view and export outlining your overall security effectiveness over time. Through continuous ongoing validation, you build proof for you, your executives, and your board to achieve and maintain confidence in your program.



Assess → Optimize → Rationalize → Monitor

Foundational steps for a continuous security validation program.

KEY COMPONENTS

Director – the central controller and manager of continuous validation across your dynamic production environment, available as a deployable or cloud-based/ SaaS platform or on-premises as a virtual appliance and installable software .

Actors – safely perform tests in production environments to validate the effectiveness of network, Windows, Mac, and Linux endpoint, email and cloud security controls and ensure your infrastructure is configured correctly.

Integrations – seamlessly and directly integrate with defensive technologies and infrastructure to extensively validate how effective controls are and identify improvements to implement where they are misconfigured.

Attack library – thousands of attacks in every stage of the adversary lifecycle, including the extended kill chain; the platform is open, customizable, and extensible, and updated frequently by our expert Behavior Research Team.

Frameworks – attacks are aligned to MITRE ATT&CK and NIST frameworks to easily tie effectiveness into your security assessment programs

Dashboards & Reports – live graphical display with results of tests run in your environment, and reports of efficacy improvements over time containing real, quantitative data that can be used to inform your executives.

request demo

verodin.com   571.418.8684