VERODIN
NOW PART OF FIREEYE

PEOPLE & PROCESS CONDITIONING

Incident Response Teams

Supercharge first responder capabilities with controls validation, real-world experience training, and automated configuration assurance.

PEOPLE ARE YOUR STRONGEST ASSET

In cybersecurity, technology is often regarded as the primary variable for incident mitigation. But, organizations should never overlook their most valuable asset: people. Technology is simply a tool to augment human intuition. The industry-wide talent gap makes it challenging to attract and retain top cybersecurity talent -- analysts often operate understaffed and overwhelmed. To harden skills and increase efficiencies, organizations sponsor resource-intensive tabletop exercises, red team assessments, and quarterly penetration tests. Unfortunately, these legacy approaches are limited to a point-in-time and cannot impact lasting progress.

BRIDGE THE GAP BETWEEN OFFENSE & DEFENSE

Effective incident response conditioning requires an ongoing feedback loop between offense and defense. Instead of simply "poking holes", red team success must be measured by its ability to communicate gaps, validate modifications, and improve blue team response capabilities. The Verodin Security Instrumentation Platform (SIP) empowers red and blue teams to continuously stress-test the people, processes, and technologies safeguarding mission-critical assets -- resulting in faster, safer, and automated insights that directly translate into business value. After optimizing layered defenses across network, endpoint, email, and cloud controls, Verodin SIP monitors configurations and proactively alerts if unintended changes in the environment impact effectiveness -- this way the SOC analysts always receive accurate and properly formatted data to respond to.

FIGHT LIKE YOU TRAIN

Virtual environments and labs cannot substitute the real-world. Verodin SIP facilitates non-theoretical and scalable experience-training to support core objectives; programs can safely demonstrate their ability to defend against real exploits rather than simulated targets.By observing malicious behaviors within the context of their production environment, analysts empirically understand how their layered defenses are responding to threats across the entire lifecycle of an attack -- from initial infection to lateral movement, persistence, and data exfiltration -- and determine how to take the best course of remediation action based on their unique tool sets and configurations. For further validation, Verodin SIP can perform "stealth" test exercises to verify that gaps have been hardened, analysts are well-practiced, and correct response procedures and processes are being followed. This unique ability to see into the future and change the outcome significantly reduces the financial and operational impact of an incident.

OPERATIONALIZE THREAT INTELLIGENCE

Verodin SIP is a force-multiplier for offensive teams -- what used to take weeks, like reverse engineering and weaponizing a PCAP, is now accomplished in minutes. Verodin SIP's Open Content Library is extremely robust, driven by community research and completely customizable. Verodin's Behavior Research Team (BRT) focuses on weaponizing intelligence and research from the community. Tests are mapped to industry standard models and frameworks, like NIST and MITRE ATT&CK. Analysts can easily create their own tests and, if they choose, share them with the broader community. This results in unparalleled test coverage, giving users visibility into how their controls are configured and if business goals are being met.

VERODIN
NOW PART OF FIREEYE

PEOPLE & PROCESS CONDITIONING

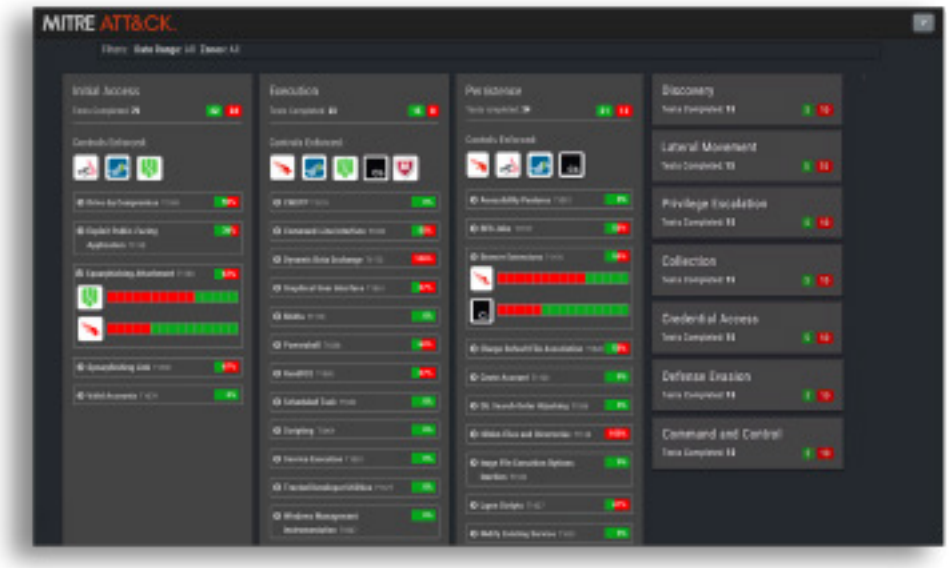
end-to-end cybersecurity validation

VERODIN SECURITY INSTRUMENTATIONN PLATFORM (SIP)

Verodin's Security Instrumentation Platform (SIP) provides evidence of the effectiveness of customers' cybersecurity controls, enabling them to validate the protection of their business-critical assets. Verodin instruments cybersecurity initiatives by deploying its SIP software into an organization's IT environments to test the effectiveness of endpoint, email, cloud, and network controls. SIP continuously executes tests and analyzes the results to proactively alert on drift from a known-good baseline, validate and optimize control configurations, and provide evidence demonstrating if the controls purchased and deployed are delivering the desired business outcomes. This capability enables enterprises to quantifiably validate if their controls are actually protecting assets, providing resiliency and keeping them safe.

BENEFITS

1. Transform your war-gaming strategy from a theoretical exercise to a scalable, evidence-based methodology
2. Real-world talent evaluations and experience training
3. Purple Team: bridge the gap between offense and defense
4. Demonstrate cybersecurity readiness to leadership
5. Improve incident prevention and detection configurations
6. Calibrate integrations with case management and alerting mechanisms
7. Rationalize and prioritize resource allocation
8. Operationalize the MITRE ATT&CK™ matrix and other industry-standard frameworks



MITRE ATT&CK DASHBOARD WITHIN VERODIN SIP

Screenshot displays a randomly generated sample data set.