EMA Vendor to Watch: Verodin

Corporate Information

Headquartered in Reston, Virginia and founded in 2014 by veteran security entrepreneurs Christopher Key (CEO) and Ben Cianciaruso (COO), Verodin was founded after two years of development on their technology solution. Verodin's mission is to empower customers with previously unseen instrumentation that provides the foundation for verifying and measurably maturing their security controls in a programmatic way against evolving threats and their consequences.

Value Proposition

Verodin identified that although the concepts of "Defense-in-depth" and "Layered-Security" are sound, a core problem is that each solution acts in a relative silo with respect to the entire program or strategy and is therefore unable to provide a means to understand the cumulative effectiveness of the tools as a comprehensive system.

Verodin achieves this through creating a comprehensive, dynamic, and automated solution to assess and provide insights on the organization's true security posture via its people processes and security tools. *The solution is capable of testing the effectiveness of deployed processes and technology controls across the environment on a continuous basis without affecting the operational environments integrity, stability, or performance.* Verodin then provides details on whether the processes and controls in place will prevent, detect, or allow an attack vector. This creates an entirely new level of visibility into the controls and how operations personnel respond to incidents.

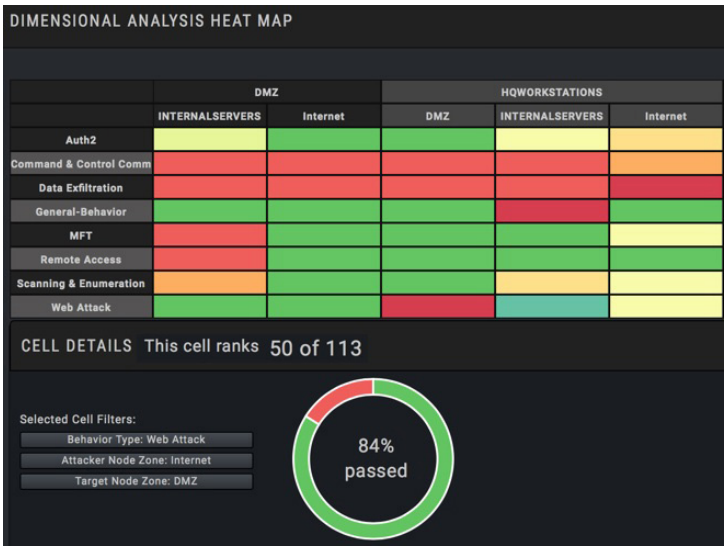

Figure 1: Verodin Identifies Controls Weaknesses

Verodin's attack simulations are indistinguishable from a real attack. The simulations are designed to fool defenses into responding as if an attack is taking place without actually attacking the real systems. The solution is comprised of two primary components: Verodin Actors which participate in executing the simulated attack and the Director which provides the front end GUI and manages the Verodin Actors. There are three types of Actors: Network, Endpoint and Cloud. Network Actors are deployed within the enterprise's Security Zones (i.e. DMZ, Remote Users, HQ Desktops, etc.). The pre-installed, self-contained Linux VM's enables quick installation in any part of the environment. Network Actors assume the roles of attacker and target, acting out the simulation across the network. Network Actors do not actually attack each other; they create simulated traffic to generate the appearance of the attack with traffic and logs. Network Actors can emulate/simulate any form of network-based attacks to fool the network monitors. Endpoint Actors are deployed on specific systems to test endpoint defenses. Cloud Actors are deployed externally to simulate external attackers. Verodin will continuously validate the prevention, detection, and response controls put in place remain effective and working. No clients or agents are required, no span ports are needed, and best of all, no production systems are placed in jeopardy.

EMA Perspective

Companies worldwide are waging a war on cyber-threats. Whether accidental or malicious, data or systems focused, or internally or externally originated, each must be dealt with. Each year organizations spend hundreds of thousands of dollars individually and billions collectively to protect themselves from any and all threats that may come their way. Unfortunately, these attempts often fall short of success, as is evidenced by the plethora of breach notifications and the billions of compromised records. These failures demonstrate a core problem that exists at all organizations in all industry verticals, from government to retail, across manufacturing and financial services, throughout retail and food services to energy. No industry is immune to compromise. Given the level of investment in threat detection, prevention, response, and remediation technologies, how can breaches continue? Can it be that none of these technologies are actually effective at performing their functions? Is this a pervasive incompetence on the part of the leadership and/or operational personnel? Though either or both of these premises can be true on an individual-case basis, neither is true across the board.

The problem most organizations face is not a lack of (or poorly chosen) technology or personnel that are incompetent, it is their ability to understand the scope of controls and therefore the gaps in controls across their environments as a whole. Though it is true that each of the chosen technologies can produce reports to show how it is working in its own control area, the problem is that each technology only delivers information regarding its specific area of control. The cybersecurity technology market is by far the most fragmented of any IT solutions area. Due to the nature of threats, vendors choose a coverage area like endpoint, perimeter, mobile/BYOD, data loss, threat intelligence, access control, etc. with each solution area protecting only a relatively small area of the organizations' attack surface. Tools like log aggregation and SIEM can put the alerts together for a singular dashboard of incidents and issues, but they are reactive and only identify when logs indicate a control is under attack or has failed. They cannot tell operations and management if the controls they have in place are working together or have any gaps in coverage between them, and whether as a whole they effectively enforce the organizations' security policies.

Though each control and process may appear to be working correctly independently of one another, layered security requires that they operate cohesively for proper effect. Until this point, organizations could only test controls at a point in time via vulnerability and penetration testing. Though useful, these approaches suffer from several weaknesses. First, point-in-time checking is only accurate at that point-in-time. Once changes are made, systems must be retested. Second, retesting can be time-consuming and costly. Third, penetration testing often has the effect of negatively impacting production systems causing performance impacts or even outages.

Verodin's continuous testing capabilities using attack simulations allow organizations to understand the context and relevance of an attack or malicious behavior within the environment, moving security from a reactive mode into a proactive position of readiness without jeopardizing production assets.

