

CORE INSIGHT ENTERPRISE: CSO USE CASES FOR ENTERPRISE SECURITY TESTING AND MEASUREMENT

How advancements in automated security testing software empower organizations to continuously measure information security standing and isolate trends in security performance throughout the enterprise in a previously unavailable manner – to better understand their exposure to real-world threats and more effectively manage IT risks.

About this Paper

Enterprise security testing and measurement solutions leverage entirely new methods of automated, exploit-based assessment to enable organizations to make more intelligent decisions in managing their overall IT-based risks.

This paper will outline a series of CSO-vetted use cases for the CORE INSIGHT Enterprise security testing and measurement solution and illustrate how the solution allows organizations to:

- Proactively gauge enterprise-wide security posture.
- Verify actual business risks introduced by IT exposures.
- Validate defensive solutions and mandated security controls.
- Isolate trends to measure security program efficiency over time.
- Chart return on existing IT security investments and defend budget.
- Inform executive-level decision making in managing IT-based business risk.

I - Empowering Executive Leadership with Better Decision-Making Metrics

Despite dedicating many years and large amounts of their IT budgets to the adoption of practices and solutions aimed at protecting their electronic infrastructure and critical data from potential loss and theft – while meeting related government and industry regulations – today’s organizations still struggle to isolate, aggregate and analyze all of the data necessary to confidently answer the questions: “Are we more or less secure today than we were X years/months/days/hours ago?” or “If we make X changes to our current IT infrastructure or defensive controls, what affect would that have on our overall security standing?”

Most organizations have implemented a complex ecosystem of layered defensive solutions and other controls to insulate against today’s onslaught of advanced cyber-attacks, and more specifically to prevent electronic data breaches. At the same time, many security executives have deployed different information-centric solutions for managing these defenses and monitoring threat activity in a centralized manner. However, while providing some level of protection and program oversight, each of these classes of solutions also has inherent shortcomings that hamper their ability to connect the security-relevant data they are collecting with actual threats to their critical business assets, for instance:

- Security Information and Event Management (SIEM) solutions promise continuous monitoring for emerging threats but rely upon historic log and alert data to draw conclusions, versus scoping exposures before potential incidents can occur.

- Governance Risk and Compliance (GRC) solutions aggregate and validate configuration and compliance data but fail to produce results that enable organizations to tie risk directly to specific business assets.
- Security Risk Management (SRM) solutions offer to map all potential routes of attack in an IT environment to gauge risks but use theoretical modeling, versus real-world exploit testing, to estimate exposures.
- Vulnerability Assessment (VA) scanning technologies provide organizations with reams of information about all of their potential points of risk but typically produce many false positives and don't illustrate how any reported vulnerabilities may be exploited.

By contrast, enterprise security testing and measurement solutions arm IT security leadership with precisely the right information they need to determine and prioritize risks by:

- Allowing them to continuously perform tests across a broad swath of their IT infrastructure to proactively identify available security vulnerabilities and paths to backend data before attacks can occur.
- Giving testers the ability to pre-define specific business systems and data that they seek to protect, and run comprehensive assessments that actively seek to assess any exposures affecting those assets.
- Utilizing highly automated, self-learning, GPS-like testing capabilities that closely replicate the specific activities of advanced malware programs and hackers to determine critical real-world risks.
- Actively exploiting vulnerabilities and any subsequent paths of exposure to prioritize risks and understand how attackers may leverage multiple weaknesses to advance privileges and access protected data.

II - Mapping IT / Technical Exposures to Actual Affects on Business

While existing IT security, risk and vulnerability management solutions, along with some compliance automation tools, have proven variably effective at helping organizations gain an understanding of their existing weaknesses and historic performance in protecting electronic assets, these tools haven't been capable of providing organizations with the timely, actionable information needed to proactively address potential vulnerabilities before attacks or data breaches can occur – or to tie identified risk points to specific business systems and data.

This reality frequently leaves organizations holding reams of reports and results regarding many of their potential security exposures, but these products lack any tangible ability to empower organizations to plan and enact assessments by first identifying the specific business assets and data (e.g., credit card numbers, customer account records, health records) that they deem most important, or to then seek out all of the various manners by which those certain assets could be breached.

By comparison, automated security testing and measurement solutions enable organizations to continuously assess and monitor IT infrastructure using real world attack techniques. Using self-learning, GPS-like automated attack planning algorithms, combined with proven exploit-based vulnerability testing engine technology, this new breed of solution can be set to identify existing, verified paths of exposure to specific sets of business assets and information defined as mission-critical by the business.

By taking this approach, IT security leaders including Chief (Information) Security Officers (CSOs/CISOs) can garner the truly actionable data they need to best inform strategic security decisions based on underlying business goals. As a result, security teams can more efficiently address available weak points, respond to any important changes in their overall standing, constantly manage IT-driven risks, validate mandated security controls, and measure their performance over time.

III – Continuously Validating Security Controls

The rapidly changing nature of IT environments, and even of security infrastructure itself, makes it such that organizations must continually test their security and compliance controls to ensure that they remain both protected and within the scope of required guidelines. This is driven not only by increasing IT-based complexity and risk, but also by the growing number of regulations that require incremental testing.

Despite the fact that most enterprise security organizations currently conduct greater numbers of proactive security assessments, many security leaders recognize that these assessments of IT resiliency represent a point-in-time snapshot. Unfortunately, these snapshots certify only that security and compliance controls were able to function effectively at the specific moment that they were tested.

The continued evolution of advanced cyber-attacks, combined with the litany of industry and government regulations aimed at hardening defenses and preventing breaches, have pushed organizations into a position where they must constantly assess the effectiveness of their controls to prevent significant capital risks.

Via the adoption of continuous, proactive security testing and measurement, organizations can:

- Frequently and consistently validate the effectiveness of their controls.
- Keep security systems and processes up to date with the current state of their overall IT infrastructure.
- Address the specific requirements laid out for them in individual regulations.
- More efficiently and cost-effectively prepare for audits.

Perhaps even more importantly, by providing a constant stream of actionable data based on real-world security assessments, testing and measurement solutions enable security professionals to confidently speak to the day-to-day state of IT security throughout the enterprise.

IV – Managing Data from Disparate Security Technologies to Chart Exposures

For well over a decade, organizations have worked diligently to address the evolving scope of IT security through the deployment and integration of many layers of IT security defensive controls. From traditional signature-based anti-virus (AV) systems to highly pervasive data leakage prevention (DLP) solutions, today's mature security implementations represent an extremely complex ecosystem of layered defenses and security controls. This presents organizations with acute challenges within the context of integrating disparate technologies and correlating information to drive management-level decision making.

Many large and security-mature organizations have moved to address this specific challenge by implementing security management, risk management, and compliance automation solutions that filter performance, event and log data to offer a high-level viewpoint into their ongoing ability to ward off attacks and assess the efficacy of security controls. However, despite aggregating security data and attempting to rationalize that information to chart exposures, these solutions have not allowed IT security management to effectively understand risk on a broad scale within the context of real-world exploitability, or tie security findings to the protection of specific business assets.

In contrast, IT security management can feed the data provided by all of the defensive controls and management systems into enterprise security testing and measurement solutions to continuously analyze their security infrastructure against real-world threat models.

Using a set of purpose-built systems connectors, enterprise security testing and measurement solutions can directly integrate with and continuously validate data from systems including:

- Vulnerability scanners (network and web apps): to identify and prioritize exploitable weaknesses and scope out available paths of attack to protected data across multiple vectors and vulnerabilities.
- Network management systems: to import specific network topographies, define assessment surfaces and verify that security processes and mandated controls are performing properly.
- Data loss prevention solutions: to determine if protected data is accessible to attackers and can be extracted in clear or encrypted form, circumventing existing DLP policies.
- Patch management solutions: to enable immediate remediation by deploying patching agents to identified penetration points and automate testing of installed patches to validate their efficacy.

V – Providing Expanded Testing Services to Development and Other IT Groups

Traditional models of security testing – from red team pen testing to secure development initiatives – have almost always been conducted in a narrow fashion, helping to inform certain groups of specialized workers regarding specific types of vulnerabilities and exposures resident on set groups of systems.

Even in those organizations where proactive security testing and vulnerability management practices have been closely embraced on management levels, there has not been the ability for security testing capabilities to be distributed broadly across an enterprise without the overhead expense of hiring or contracting experienced staff. Yet, at the same time as threats and IT risks along with regulatory compliance demands, have proliferated, the need for broader application of testing methodologies has advanced across the entire enterprise.

For instance, web applications development teams require the ability to test the security of new applications before they are ever brought into production. In a less targeted example, most departmental IT staff needs to test both new systems and those that are already deployed in their offices to ensure they are properly protected or do not harbor security exposures.

Using enterprise security testing and measurement solutions, organizations gain the unique ability to delegate automated proactive security testing and measurement capabilities throughout their business units and departments, essentially providing automated security testing capabilities as a service across their operations and staff.

About CORE INSIGHT Enterprise

CORE INSIGHT™ Enterprise is an automated security testing and measurement solution that allows you to continuously and proactively assess the security of your organization's most critical information assets. By traversing exploitable web application, network and client-side weaknesses throughout your enterprise, INSIGHT reveals paths of exposure to specific assets – providing clear, definitive metrics for efficiently validating your security controls and addressing data breach threats.

The solution employs groundbreaking technology that proactively replicates the steps attackers would take to breach valuable information assets. Unlike other solutions, CORE INSIGHT Enterprise starts with customers identifying which systems and data they want most to protect. INSIGHT then automatically calculates paths of attack and begins to exploit multiple layers of defense until the security of critical assets is either confirmed or breached. Assessment results are delivered via a dashboard and reports that present metrics regarding the efficacy of security controls in terms relevant to the business.

By providing management with the ability to filter through the mountains of systems, security and compliance data they aggregate on a constant basis to continuously validate that their security processes and controls are working, CORE INSIGHT Enterprise empowers IT, security and business leadership to finally offer a confident answer to the question: “Are we more secure today than we were yesterday?”

Core Security Technologies – Building on Established Capabilities

Core Security Technologies, makers of the most advanced, commercial-grade automated penetration testing solution on the market today, CORE IMPACT Pro, is the only company with precisely the right combination of strategic vision, technological underpinnings and human assets to develop and sustain the market's first true enterprise security testing and measurement solution, CORE INSIGHT Enterprise.

While INSIGHT Enterprise represents an entirely new product – built from the ground up using previously unavailable technological means to automate the process of testing broad swaths of IT infrastructure in a highly intelligent manner – the concept of proving exploitable vulnerabilities and illustrating available paths to protected data using proactive assessment lives at the heart of all of Core's efforts – from its products and services to the work of its CoreLabs vulnerability research team – all of which are consistently recognized as global leaders in their individual fields.

In building CORE INSIGHT Enterprise, Core tapped into over a decade of internal research and development around vulnerability exploitability and automated attack planning, the latter of which represents a specific technological process for which the company is currently seeking a patent, to go with its existing array of patented automated security testing technologies.

With its vast expertise in defining the leading causes of today's most prevailing threats, in addition to creating and maintaining the industry's most respected library of security testing exploit code – one that many organizations use today to safely test their exposure to real-world malware attacks and hacking techniques – Core is ideally and uniquely positioned to create this entire new class of solutions that leverage the inarguable validity of proactive testing to better understand, benchmark and manage IT-driven risks.

Core's overall culture revolves around the aggressive pursuit of any means through which today's organizations can rapidly improve their overall security standing by assessing the ability of attackers to utilize available vulnerabilities to infiltrate or compromise their IT systems. Bringing to market the world's first true IT security testing and measurement solution – CORE INSIGHT Enterprise – is in every way representative of the company's continued and focused commitment to that same goal.

For additional information on the CORE INSIGHT Enterprise security testing and measurement solution, please contact us at 617-399-6980 or via email at info@coresecurity.com. You can also visit our web site at www.coresecurity.com.



WWW.CORESECURITY.COM

COPYRIGHT © 2010 | Core Security Technologies