

Continuous Enterprise Risk Measurement

Business Risk Intelligence through Automated Testing

Executive Summary

In environments where data and inputs change frequently, one-time monitoring is not effective. Consider a GPS navigation system with traffic monitoring that updated only once a day. During rush hour times, many drivers would be met with outdated information about the current status of the roadways. Or imagine a diabetic that only tested their blood sugar once per week. Blood sugar levels fluctuate throughout the day and frequent testing of these levels enables people to respond quickly with more, or less, insulin as needed.

Point-in-time IT security posture assessment is like that navigation system without traffic updates or a diabetic who only tests their blood sugar weekly: ineffective for understanding real risks in an ongoing way. Many traditional IT security assessment practices like manual penetration testing and compliance audits are expensive and time consuming, and thus can be poorly aligned with the dynamic and volatile nature of the IT environment: because they are performed infrequently – sometimes yearly, sometimes quarterly – this makes them incapable of monitoring and reporting on the changing IT security dynamics and risk landscape of enterprise IT systems in an ongoing manner. This can lead to potentially costly risk exposure between test cycles.

Another concern with traditional IT security assessment tools is that findings are often disconnected from business risk. Simply knowing that there is vulnerability within a system does not tell an organization whether or not it is a true business risk, what the value of the exposed data is, or even if the problem is exploitable.

Continuous automated testing of a system is more effective at assessing IT security risks because it monitors the environment constantly. Automation enables tests to be conducted without increasing personnel overhead and provides metrics and trending information for use in high-level quantitative risk analysis. Organizations can leverage this data to provide enterprise risk awareness metrics that tie back to business by directly mapping technical vulnerabilities to the actual business data or systems that are impacted, and showing real-world, verifiable samples of data accessibility and system exploits.

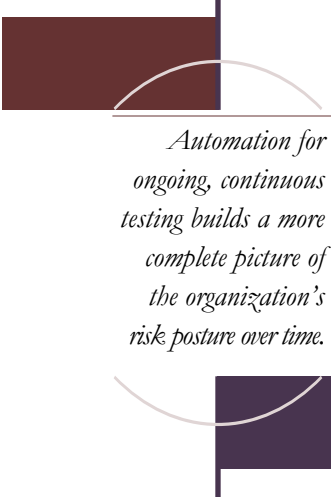
Contents

Executive Summary	1
Real-World Security Assessment	2
Intelligent Attack Path Analysis	2
Turning Data into Business Insight	3
Core Security Technologies and CORE INSIGHT Enterprise	3
Summary	4

SecurityCurve

Stay ahead
of the curve

Real-World Security Assessment



Automation for ongoing, continuous testing builds a more complete picture of the organization's risk posture over time.

Traditional IT security assessment tools do a solid job of providing a snapshot of where the organization is at a given point in time and they also comprise a robust mechanism for investigating what happened after the fact. But they do not provide continuous “before-the-fact” risk assessment. Security Risk Management models are good for what-if scenarios, but are often theoretical in nature, not taking into account the actual risk associated with whether or not a flaw is exploitable in practice. Log aggregation and security event information management (SEIM) tools are excellent for continuous monitoring, but require significant time investment in writing rules for accurate correlation. Moreover, by their very nature, they are dependent on an event already having occurred in order to be able to report it. If an event hasn't occurred yet, it won't be in the log. IT governance risk and compliance (IT-GRC) solutions provide configuration validation and mapping between compliance mandates but often fall down when an organization needs to assess true business risk to data in production.

Exploit-based security testing provides proactive and accurate insight into an organization's real-world risk posture because test probes and exploits are launched in advance of a breach occurring. This approach enables a company to validate whether or not theoretical exposures can be exploited on the production network. Rather than simply reporting on whether or not a system is

patched or vulnerable to a specific exploit like SQL-injection, exploit-based testing proves if it is possible for an attacker to “capture the flag” of sensitive data, such as a social security or credit card number on a backend database. It does this by actually extracting the data during testing. While exploit-based security testing is a powerful process, it has traditionally been labor intensive making it expensive and time consuming. To get the full value of exploit-based testing, human penetration testers must also invest additional effort to map a laundry list of exploits and exposures to the overall business risk impact. Few companies have the time or resources to invest in manual exploit-based testing on an ongoing basis.

Though there's no complete replacement for human penetration testers, there are many activities within the process that can be automated effectively, freeing up the human testers to perform more complex tasks that don't lend themselves well to automation. Increasing the automation component also allows for ongoing, continuous testing, which builds a more complete picture of the organization's overall risk posture over time.

Intelligent Attack Path Analysis

Basic scans of system patch levels and configuration settings are only part of the risk exposure picture. An unpatched system may not be vulnerable to business risk exposure for other reasons. For example, there may be no interesting data on a system; the system may be fully zoned from sensitive devices; the system may contain sensitive data but is being protected through other means such as a host-based intrusion prevention system; or strong access controls may successfully prevent unauthorized access to the data.

Correctly patched and configured systems can pose business risks if a compromised user has authorized access to them, and a patched system may be vulnerable to compromise if it has connectivity to or from a vulnerable system. A scan could easily miss this exposure because the vulnerable system, for example a database, is behind a patched system, such as a web server. The web application on the server has a flaw but it does not lead directly to backend database access. However, it does enable an attacker to place code on the web server itself, which in turn, can be used to launch an attack on the backend database. As a consequence, the test process needs to infiltrate the web server before attack paths behind it can be discovered and explored.

To get the real vulnerability and exposure picture requires continuous testing though the myriad and frequently changing paths in a complex network ecosystem. Manual, path-based testing replicates real-world attacks but is complicated and time-consuming. Automation increases the accuracy of the results because it can reduce human error and more rapidly parse through the multiple backend attack path possibilities. With learning capabilities, an automated tool can incorporate results from previous test runs and use the data to determine priorities and paths for which exploits to attempt next, increasing accuracy and speed over time. This is like the GPS navigation system mentioned earlier – faster routes can be learned and blocked routes detoured to allow the driver to most efficiently navigate based on changing situations.

Another benefit of using attack path analysis is translating the results from IT risk to business risk. Rather than looking only for unpatched systems, organizations can use automated exploit-based testing tools to launch business-oriented discovery operations. For example, a company knows there is a breach point into the network, but not what business data is accessible from the breach point. Rather than run a series of unrelated tests, the business can hone in on the information it has defined as most sensitive – in this case social security numbers (SSNs) – and launch a focused data test-run to look for every attack path to any social security numbers within the network.

Turning Data into Business Insight

Knowing there are verifiably exploitable attack paths shows organizations exactly where the IT risks and associated business risks are in the network – and where fixes are required. The next step is to turn this data into real business insight by measuring overall security performance and effectiveness over time. Attack path information can also be used to validate whether or not the controls in place to satisfy compliance to regulations and mandates are working as expected. It can also be leveraged by comparing security and attack path findings to metrics gathered from other parts of the enterprise, and against anonymized data from other enterprises and peers.

Growing the maturity of an IT risk management practice requires the ability to measure performance and the effectiveness of controls. Exploit-based, attack path testing provides a basis for real-world controls testing. In theory and when modeled, a series of processes and technical controls may be perceived as effective; but it is not until they are tested in production that the efficacy can be truly validated. The TSA (Transportation Security Administration) has procedures and technical controls to prevent banned objects from being brought on a plane, but test subjects are sent through the lines with banned objects to test effectiveness. Going back to the example of the business test that searched for available SSNs, and verified a database where SSNs reside was accessible to attackers, the organization could then use the test tool to validate additional pieces of information that would be useful in the remediation prioritization process. Specifically, the tool determines if the system where the data resides is vulnerable because it is unpatched, if the actual data can be extracted, and whether or not an alert was generated when the data was accessed.

Moving to the next level of maturity, the organization uses the test information to determine where within the attack path the process or control failed. A remediation plan is implemented and then the control is tested again. If the attack path has been blocked, the control can be deemed effective, while if a new path can be exploited, remediation work continues until the exposure has been closed. This enables the organization to create a more effective, business-sensitive remediation program using automated path-based test results.

Automated exploit-based, attack path testing complements other IT security assessment tools like vulnerability scanners because the successful exploit points in the path show the company where remediation activities will return the best results. In this way, the often large and confusing list of vulnerabilities produced by scanning is turned into usable business intelligence that pinpoints not only where the fixes are required to close the most impactful business exposures, but also whether or not the fixes worked. The organization can prioritize the remediation activities based on this insight for intelligent defense against attackers and attack patterns, rather than taking a poorly organized approach in an attempt to patch or remediate everything at once.

Business insight into the remediation process shows the organization which servers, platforms and applications should be patched or fixed first and also helps sift through the various remediation options by illustrating the earliest point in the path where a control or fix can be implemented. If that fix works, other remediation steps may not be required. By learning where controls and fixes are most effective, the organization can build metrics on risk impacts to assess mitigation alternatives based on effectiveness vs. cost.

Core Security Technologies and CORE INSIGHT Enterprise

Core Security Technologies was founded in 1996 to help companies improve their penetration testing activities through automation. Core Security currently has 180 employees on three continents. Core Security's flagship product, CORE IMPACT® Pro assists white hat penetration testers by automating repetitive tasks. The product has evolved over the years and is currently deployed at over 1000 customers.

The company's new CORE INSIGHT Enterprise™ builds on over 10 years of research, deployment expertise, and customer experience feedback. INSIGHT Enterprise was developed to complement penetration testing and the IMPACT Pro product by increasing automated security testing functionality and incorporating newly developed capabilities that emulate complex cyber-criminal behavior for ongoing enterprise risk assessment – and to translate these findings into business intelligence that can be used by a number of constituencies in the organization.

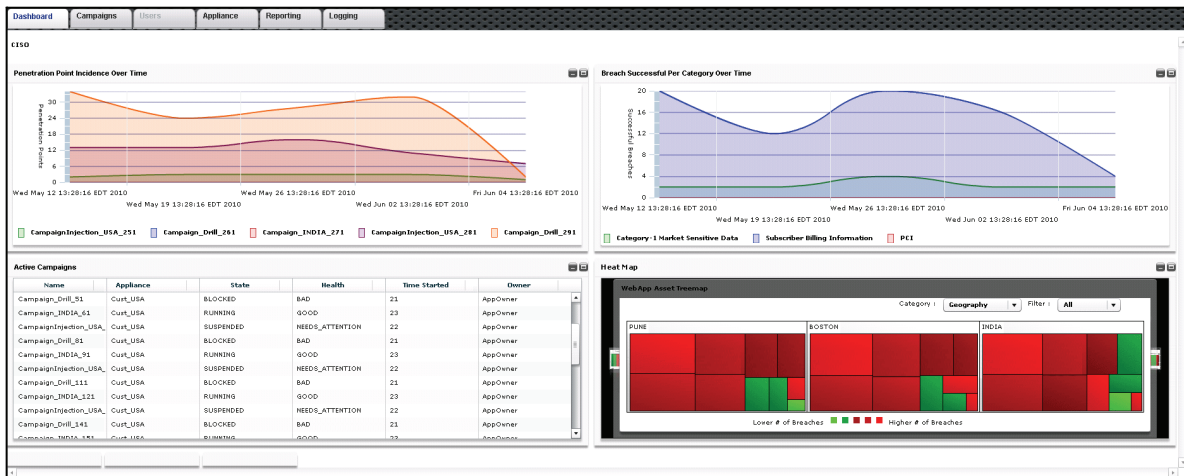
CORE INSIGHT Enterprise uses automated “campaign” based testing to increase risk awareness and measurement capabilities across the entire enterprise. Campaigns are business-focused test runs that identify where business data is exposed using patented, automated attack path algorithms. INSIGHT Enterprise can be used to proactively validate controls and evaluate exposure to real-world threats before attacks occur.

INSIGHT Enterprise was developed with the input of existing Core customers. It provides a CISO Dashboard which is a console-based view of enterprise risk that shows the specific paths where IT risks and breach points lead to exposure of sensitive business data and systems. INSIGHT Enterprise also allows companies to run “what-if” tests in the lab environment to see how proposed changes to IT systems will impact risk posture. It is an advanced evolution of the vulnerability management process that integrates business-aware requirements into the remediation framework.



*Build metrics on
risk impacts to
assess mitigation
alternatives based
on effectiveness
vs. cost.*





The CORE INSIGHT Enterprise CISO Dashboard

The CISO Dashboard also provides graphs and charts of security posture metrics like trending data, number and location of breach points, and paths of exposure for sensitive business data and systems. Organizations can use the metrics for measurement and improvement over time to see where IT risk increases or decreases are reported. The data can be organized in a number of different views depending on the constituents' areas of interest or responsibility. So the operations team can see where the patches or firewall rules require updates, the development team can see which web applications need re-writes or patches, internal audit can see compliance control validations, and the CISO can see the overall enterprise security trends.

Summary

Continuous, ongoing, exploit-based testing provides a more accurate picture of an enterprise's risk posture than quarterly scans or tests. To create a complete picture, enterprises also need a way to translate the real-world IT risks into quantifiable business risks to know where and what to fix first to get the greatest return on investment.

CORE INSIGHT Enterprise is a console-based view of the attack paths and exploits discovered across networks, systems and applications. The console brings enterprise risk into focus for executives and IT professionals by showing where breach points have led to successful retrieval of sensitive data or exploit of a specific business system. It translates IT data into business risk and shows trends and metrics so improvement, or need for improvement, can be tracked over time and remediation resources can be applied to the precise points where they will deliver the most benefit.

From an enterprise risk management view: quarterly security assessments are good, but ongoing IT security and risk measurement is a whole lot better.

SecurityCurve

Stay ahead
of the curve

All contents (except where otherwise noted)
© 2010 Diana Kelley and SecurityCurve

diana@securitycurve.com
www.securitycurve.com

Funding for the research and writing of this document was provided by Core Security Technologies.

www.coresecurity.com

Security Curve gives companies the market and technology insight they need to make agile business moves so they can stay ahead of the security curve. Our clients benefit from targeted intelligence, comprehensive research, and focused solutions to stay ahead of the competition in a rapidly changing market.

Diana Kelley, Partner

Diana Kelley has extensive experience delivering strategic, competitive knowledge to large corporations and security software vendors. She was Vice President and Service Director for the Security and Risk Management Strategies (SRMS) service at Burton Group, the Executive Security Advisor for CA's eTrust Business Unit, and a Manager in KPMG's Financial Services Consulting organization.