

Website Risk Management – a four-phase solution

Asset Identification

Vulnerability Management

Reporting/Communication

Protection

Organizations Must Develop a Strategy for Website Risk Management

Website security is more than a tally of the latest vulnerabilities that may threaten a company’s websites. It’s about managing risk. Website security data is not solely the domain of the security team: It’s utilized by auditors, compliance, product management, and developer organizations within a company, as well.

And, because there is no pre-existing infrastructure of independent software vendors pushing out standard patches for commercial products, applying the rules of traditional software is insufficient, inadequate, and simply doesn’t work. With rare exceptions, each and every website is unique custom code. And, even more unique to websites is they are – by design – open and available to the public; and, to hackers.

It is in the post-deployment, or operational, phase of the application lifecycle that a website risk management program delivers the most value to an organization. It is by far the most important and generally of the longest duration of any phase of an application’s life. As the most prevalent attack target, production websites are where the majority of an organization’s security resources should be applied.

Building a Website Risk Management Program for Production Website Security

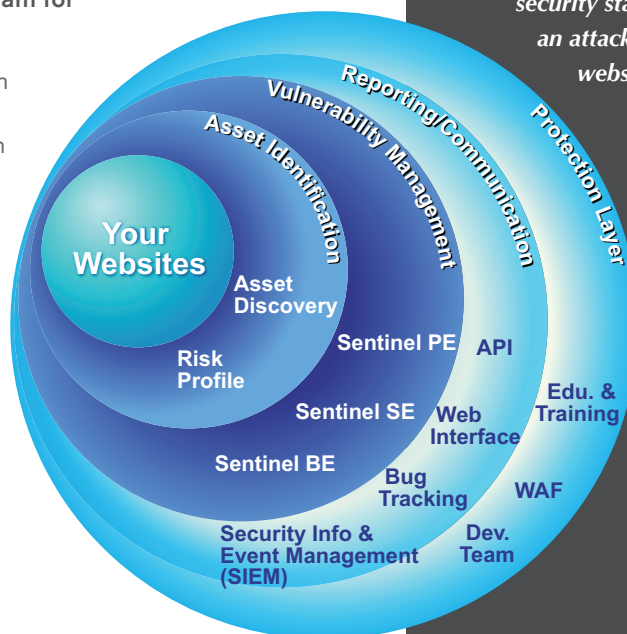
Even highly trained security professionals flinch when tasked with building a website security program from scratch. The question most often asked is: Where do I begin? The second is: What does an effective website risk management program look like?

WhiteHat has crafted a four-phase Website Risk Management approach built around securing and protecting your production – as well as QA – websites. The process for determining and managing the risk of your websites and the data they store and retrieve is a multifaceted one:

1. Asset Identification
2. Vulnerability Management
3. Reporting / Communication
4. Protection

Websites have emerged as the number one attack target of choice. Attacks have moved from the well defended network layer to the more accessible Web application layer that people use everyday to manage their lives to shop, bank, manage their healthcare, pay insurance, book travel and apply to college.

The ramifications for companies who do not adequately protect and secure their websites are clear: Loss of data, malware infection, loss of consumer confidence and failure to meet regulatory requirements. No company can afford the black mark of a website hack. With many states mandating full disclosure, the payment card industry and the federal government close behind with their own efforts at establishing security standards, the luxury of hoping an attacker will target someone else’s websites has passed.



1

Asset Identification and Profiling – gaining visibility

2

Vulnerability Assessment – flexibility in choice of offering

Asset Identification

You must identify all the website assets within your organization. This is not necessarily an easy task, particularly within a large organization. Business units may create new websites without involving the security organization. Company acquisitions and mergers can quickly add large numbers to your website roster. And over time, URLs are used that are completely unrelated to the company's brand, so you cannot necessarily identify all the relevant websites through hostnames alone.

Asset Prioritization – Risk Profiling

Once all your websites are identified, the next step is to categorize those sites in terms of business criticality, based on several factors:

1. Does it generate revenue?
2. Does it store and retrieve regulated data?
3. Does it contain any company-specific confidential data?

This information is key in determining the overall risk to the organization associated with each website. This, in turn, determines the amount and timing of the resources that must be allocated toward its security. Other factors may also be considered in terms of determining the overall risk to the organization – for example, when was the website developed and on what platform? If a site was developed many years ago, then this site was probably not developed with methodologies in place to prevent current attacks. In recent years programming platforms have been developed to automatically prevent many common website vulnerabilities. If a site was not developed on one of these platforms, then there is a greater likelihood that the site may contain more of these common types of vulnerabilities.

Within the year, WhiteHat will further assist customers with this process of risk assessment and asset prioritization, by providing our own risk profile recommendations. Of course, this profile can be managed and adjusted by the customer to adhere to its own internal risk management preferences.

With a complete picture of your inventory of websites, each site appropriately rated according to its risk profile, the process to select an appropriate vulnerability assessment/management solution becomes dramatically streamlined.

Built on a SaaS (Software-as-a-Service) – or Cloud-based technology platform, the WhiteHat Sentinel family all combine advanced proprietary scanning technology with expert website security analysis, to enable customers to identify, prioritize, manage and remediate vulnerabilities as they occur.

Unique to WhiteHat Security, every vulnerability discovered by any WhiteHat Sentinel Service is verified and prioritized, virtually eliminating false positives and radically simplifying remediation.

WhiteHat Security offers WhiteHat Sentinel Service at three service levels:

Sentinel Premium Edition (PE)

PE is ideal for larger, more complex, mission critical publicly-facing websites that are potential high-risk attack targets. These websites normally require frequent code updates, increasing the likelihood of introducing new vulnerabilities. PE includes configured assessment delivery and custom testing by the WhiteHat Security Operations Team to manually identify business logic flaws. PE comes standard with verified vulnerability reporting. Satisfies PCI 6.6.

Sentinel Standard Edition (SE)

SE is designed for medium risk websites that have complex functionality requiring extensive configuration. SE is an appropriate solution for companies that have best practice or PCI 6.6 compliance requirements. Sentinel SE includes configured assessment delivery and comes standard with verified vulnerability reporting.

Sentinel Baseline Edition (BE)

BE is an automated solution for smaller, less complex, lower-risk attack target websites. Sentinel BE detects vulnerabilities that lead to the most prevalent and dangerous types of attacks, such as SQL Injection and Cross-site scripting, ensuring websites are safe from the most serious threats in a cost effective manner. Satisfies PCI 6.6.

“ We take security and compliance challenges very seriously as we’ve seen more issues erupt in the public arena surrounding serious breaches with sensitive data housed online. Caremark is eager to engage with WhiteHat ... to demonstrate the measures we are taking to assure site visitors of the level of security we maintain across our websites.

– Shamoun Siddiqui, Manager, Information Security, CVS Caremark

3

Communication / Reporting – an open XML API gives you more control

Most large and growing organizations have multiple constituents and programs that need to be kept up-to-date with the current state of their website risk posture. WhiteHat's highly accurate vulnerability information combined with an open XML API makes WhiteHat Sentinel the only website risk management solution to provide reliable and precise website vulnerability data that can be shared and practically employed within an organization's existing communications and reporting infrastructure.

WhiteHat Sentinel's integration capabilities deliver crystal clear visibility to different business stakeholders, including risk management and compliance, product management and software development teams. Organizations have greater insight into their risk posture and can take corrective action, while communicating that action across the different compliance and reporting components within their infrastructure.

WhiteHat Sentinel integrates with industry leading bug tracking, security information and event management (SIEM) and Web application firewall (WAF) products, allowing website security data to be shared across departments. For the first time, website security can be integrated into an organization's operations, delivering new levels of visibility throughout that organization and greater levels of control to security professionals.

WhiteHat offers a RESTful (Representational State Transfer) XML API. The API currently supports vulnerability data, website configurations, and policy information. The WhiteHat open API can be accessed with either a specially generated API Key, or an authenticated session ID token.

The following companies have successfully integrated with WhiteHat Sentinel via its open XML API:

Archer Technologies – to manage enterprise risk by proactively identifying, tracking and managing the remediation of critical vulnerabilities in websites.

Jira bugtracking system – to give developers easy access to the information necessary to fix problems in custom website code.

Breach Security's ModSecurity, F5 Networks ASM and Imperva SecureSphere Web application firewalls – to enable real-time mitigation of website attacks.



4

Protection – control over your website security

The Protection phase recognizes three different ways to manage website vulnerabilities: developer-driven remediation, improved security education and training, virtual patching via WAFs.

Developer Remediation

By providing developers with accurate and actionable website vulnerability reports and education, developers become more willing teammates in the website risk management challenge. WhiteHat Sentinel's Web-based reporting provides granular customized reports, with:

- Detailed vulnerability descriptions
- "Retest now" functionality to immediately confirm effective vulnerability remediation
- Trend reporting across enterprise/websites
- Web services API for data export to bug-tracking systems or SIEMs

Security Education and Training

WhiteHat Education Services provides the up-to-date knowledge and skills required to understand and deliver meaningful security measures.

Because WhiteHat Sentinel is continuously assessing hundreds of production Web applications on a weekly basis - finding and analyzing vulnerabilities within such a broad and deep collection of real-world websites – our understanding of website risk management is unmatched. As a result, our courses for developers, security professionals, and IT management incorporate the enormous wealth of experience from WhiteHat's core business.

WAF Integration – Virtual Patching

Integration of a WAF with WhiteHat Sentinel detects and defends website vulnerabilities much more efficiently, and resolves the disconnect between compliance intentions and actual security. With virtual patching, the entire industry is brought to a new level of website protection, with extreme accuracy and efficiency – delivering rapid identification and immediate repair of vulnerabilities.

“ Our high security standards and partnerships with WhiteHat and Imperva ensure the security of our customers' sensitive data, and really are helping to set the standards for the industry as a whole. Our security is leaps and bounds ahead of on-premise solutions, and it's making the decision to migrate over to cloud solutions even easier for large enterprises.”

– Joe White, information security architect, SuccessFactors

Conclusion

Attacks are on the rise and will continue to grow. By applying WhiteHat's recommendation to operationalize website risk management, you can best protect critical data, ensure compliance and narrow the window of risk. WhiteHat Sentinel, the company's flagship product family, is the most accurate, complete and cost-effective website vulnerability management solution available. It delivers the visibility, flexibility, and control that organizations need to prevent Web attacks.

About the WhiteHat Sentinel Service

Website risk management is not a one size fits all issue. WhiteHat's goal is to ensure that businesses have options available that suit their specific needs and budgets based on their unique risk exposure. Our family of services addresses the diverse and ever-changing website security needs of the enterprise and allows customers to choose their service level based upon their risk profile.

WhiteHat Sentinel is currently available in three service levels Baseline Edition (BE), the Standard Edition (SE) and the Premium Edition (PE) for an annual subscription fee. All WhiteHat Sentinel service levels deliver high-quality, accurate, and verified results, and include the WhiteHat Sentinel open XML API that enables integration with existing bug-tracking, SIEM systems and Web application firewalls (WAF). This information sharing results in improved development practices; more accurate risk assessment; and more effective mitigation strategies. Only WhiteHat Sentinel provides assessment results that are reliable enough to be shared directly with other applications and provide a solid foundation for an effective website risk management program.

"The ability to leverage software vulnerability information from WhiteHat Sentinel integrated with Archer, enables DTCC to recognize the economic benefit of the completion of remediation tasks with assigned accountability. WhiteHat Sentinel provides excellent software vulnerability information by levels of risk that is aligned with an accountability model within Archer to manage risk and track key performance indicators to measure the health of the vulnerability management process."

*– Jim Routh, CISO
Depository Trust & Clearing Corporation*

About WhiteHat Security

WhiteHat Security is the leading provider of website security solutions that protect critical data, ensure compliance and narrow the window of risk. WhiteHat Sentinel, the company's flagship product family, is the most accurate, complete and cost-effective website vulnerability management solution available. It delivers the flexibility, simplicity and manageability that organizations need to take control of website security and prevent Web attacks. Furthermore, WhiteHat Sentinel enables automated mitigation of website vulnerabilities via integration with Web application firewalls.



WhiteHat Security, Inc. | More information is available at www.whitehatsec.com
408.343.8300 | 3003 Bunker Hill Lane, Santa Clara, CA 95054

Product names or brands used in this publication are for identification purposes only and may be trademarks of their respective companies.
Copyright © 2009 WhiteHat Security, Inc. 071009