White Paper: Unified Security Scores Between Security Rating Vendors

By: Cygienic Pte Ltd

Abstract

In the dynamic landscape of cybersecurity, businesses and organizations are increasingly reliant on cybersecurity rating vendors to evaluate their security posture. These vendors provide a comprehensive assessment of a company's security practices, allowing stakeholders to make informed decisions. This white paper explores the commonalities in how various cybersecurity rating vendors assess organizations, focusing on shared cybersecurity checkpoints and scores. It argues that the diverse cybersecurity checkpoints these vendors use can be grouped into three overarching categories: Systems Compromised, System Vulnerability, and System Configuration. Additionally, this paper discusses the slight variations in how vendors give weight to these categories, but ultimately, the final security rating for a company is largely consistent across all the rating companies.

We looked at the following vendors to compare and contrast checkpoints and security ratings for our clients: **Cygienic.com, Bit-Sight, Security-Score-Card, Up-Guard, and Black-Kite**

Introduction

In a world where cyber threats continue to evolve, understanding the security posture of a business or organization has never been more critical. Cybersecurity rating vendors have emerged as key players in the assessment and analysis of an entity's cybersecurity practices. These vendors play a pivotal role in helping businesses manage and mitigate cybersecurity risks. Their evaluations are integral in assisting organizations to make informed decisions concerning their security measures, identify areas of improvement, and instill trust among stakeholders.

This paper examines how cybersecurity rating vendors approach their assessments and identifies a common set of cybersecurity checkpoints. It further categorizes these checkpoints into three main groups: Systems Compromised, System Vulnerability, and System Configuration. It also discusses how vendors may slightly differ in the weighting of these categories but converge to provide a consistent final security rating.

Common Cybersecurity Checkpoints

A notable observation in the cybersecurity rating industry is the shared set of cybersecurity checkpoints that vendors consider when assessing an organization. These checkpoints serve as key indicators for evaluating the strength of an entity's cybersecurity posture. The following list comprises some of the common cybersecurity checkpoints found in assessments from the vendors:

Systems Compromised

- Compromised systems: Identifying any systems that have been compromised or breached to one of the following services:
- Spam distribution
- Proxy services
- Phishing emails
- Malware host
- Botnet network

System Vulnerability

- CVE vulnerabilities: Identifying and managing Common Vulnerabilities and Exposures.
- SSL renegotiation: Assessing the security of SSL renegotiation.
- TLS fallback: Identifying vulnerabilities related to TLS fallback.
- TLS ticketbleed: Evaluating protections against the TLS Ticketbleed vulnerability.
- Open ports: Assessing the security of open network ports.

System Configuration

- DKIM (DomainKeys Identified Mail): Evaluating the implementation of email authentication.
- STARTTLS: Ensuring the availability and correct configuration of STARTTLS for email security.
- Outdated web browser: Checking for the usage of outdated and insecure web browsers.
- Certificate without revocation control: Identifying SSL certificates without proper revocation control.
- X-Frame-Options: Evaluating the implementation of X-Frame-Options.
- CSP (Content Security Policy): Ensuring a robust Content Security Policy.
- Cookie HttpOnly: Checking for the HttpOnly attribute on cookies.
- Cookie-Secure: Assessing the security of cookies through the Secure attribute.
- Cookie-Samesite: Evaluating SameSite attribute implementation.
- Listable directory found: Identifying exposed listable directories.
- Domain registration management: Evaluating the management of domain registrations.
- Cookie notification: Assessing the entity's notification of cookie usage.
- Privacy notification: Analyzing the entity's privacy notification practices.
- DMARC policy management: Analyzing the implementation of DMARC policies.
- SPF policy: Ensuring Sender Policy Framework (SPF) is correctly configured.
- SPF management: Assessing the management of SPF records.
- DNSSEC: Evaluating the implementation of Domain Name System Security Extensions.
- HSTS header: Assessing the presence and configuration of the HTTP Strict Transport Security header.
- Specific ASP.net version exposed via header: Analyzing the exposure of ASP.net version information.
- X-Content-Type-Options: Evaluating the use of the X-Content-Type-Options header.
- HTTPS redirect support: Ensuring proper support for HTTPS redirection.
- Insecure SSL/TLS version: Identifying outdated or insecure SSL/TLS versions.
- SSL certificate missing from server response: Checking the presence of SSL certificates.
- SSL certificates expiring soon: Monitoring SSL certificate expiration dates.
- Secure cookies not used: Ensuring the secure use of cookies.
- Weak SSL algorithms: Identifying the usage of vulnerable SSL algorithms.
- Server information header exposed: Assessing the exposure of server information.
- X-Powered-By header exposed: Analyzing the exposure of the X-Powered-By header.

- Open relay: Identifying open relays that may allow unauthorized access.
- XSS protection: Ensuring adequate protection against Cross-Site Scripting attacks.
- MIME type X-content: Evaluating the handling of MIME types for content.
- Referrer policy: Analyzing how the entity's referrer policy affects security.
- Cache control: Evaluating the control mechanisms for caching sensitive data.
- Expect-CT TLS: Examining adherence to Certificate Transparency in TLS
- Cookie consent: Evaluating the handling of cookie consent.
- Domain configuration: Analyzing the overall domain configuration.

Weighting of Categories

Cybersecurity rating vendors may differ slightly in how they weight the three main categories: Systems Compromised, System Vulnerability, and System Configuration. Some vendors may place more emphasis on the identification of compromised systems, while others may prioritize system vulnerability assessment. System configuration is often viewed as a crucial factor in assessing an organization's security posture, but the specific emphasis may vary among vendors.

Conclusion

In the world of cybersecurity, standardization and consistency are essential. Cybersecurity rating vendors have developed a common set of cybersecurity checkpoints that help organizations and stakeholders gauge the effectiveness of security measures. These checkpoints can be grouped into three overarching categories: Systems Compromised, System Vulnerability, and System Configuration. While different vendors may slightly adjust the weight they give to these categories, they generally converge to provide a similar final security rating.

This white paper highlights the importance of understanding the shared cybersecurity checkpoints, their categorization, and the varying priorities of different vendors. Ultimately, this standardized approach benefits organizations by providing clear, reliable, and actionable insights into their cybersecurity practices, enabling them to make informed decisions, strengthen their security posture, and build trust with stakeholders. As cybersecurity continues to evolve, the collaboration between organizations and cybersecurity rating vendors will be vital in maintaining the integrity of the digital landscape.