RiskSense Solutions Qualifying Questions

Ransomware Assessment

Q. Do you understand your ransomware exposure? Is that question being asked by your leadership?

A. RiskSense Value: RiskSense has developed a global index of all known vulnerabilities that are being used by ransomware. Leveraging your existing scan data we can easily and clearly show your organization's specific exposure to ransomware. RiskSense can supplement your scan program with authenticated scans to more accurately show your ransomware exposure.

Q. Do you believe you have controls in place to detect and protect your organization against ransomware? When was the last time you validated these controls specifically for ransomware?

A. RiskSense Value: As part of the offering, our team actually identifies which assets are susceptible to ransomware and sees if they can bypass existing security controls. This identifies gaps and/or misconfigurations in your existing controls specific to ransomware detection and prevention.

Q. Are you prepared to handle a ransomware attack? Do you understand all the implications of an infection on the rest of the environment?

A. RiskSense Value: RiskSense assists you in protecting the critical data that is targeted by ransomware. Ransomware is constantly evolving and improving, so defenders also need to constantly evolve and improve. This includes reviewing your Ransomware exposure on a continual basis vs. a point in time review. This methodology ensures your organization is prepared to detect and prevent the latest ransomware tactics, techniques and procedures.

Q. How do you prioritize ransomware-specific vulnerabilities for remediation?

A. RiskSense Value: RiskSense focuses on the vulnerabilities that are being used by ransomware and prioritizes them based on their exploitability. We determine exploitability using Threat Intel, Asset Exposure, Asset Criticality, and several other indicators that a vulnerability is being actively used in the wild. We provide a clear fix for the identified vulnerabilities.

Full Spectrum Risk-Based Vulnerability Management (FS-RBVM) Platform

Q. Do you own vulnerability scanners and how often are you performing scans within your environment? Do your scans include internal network, external network, web applications, IoT devices, DevOps/SDLC, Cloud PaaS, Containers, and Penetration Tests?

A. RiskSense Value: The RiskSense solution gathers scan data from your existing scanning solutions out of the box including internal network, external network, web applications, IoT devices, DevOps/SDLC, Cloud PaaS, Containers, Penetration Tests, etc.

Q. How many consoles or reports does it take to get visibility into vulnerabilities for internal network, external network, web applications, DevOps/SDLC, Cloud PaaS, Containers, Penetration Tests?

A. RiskSense Value: The RiskSense solution ingests all this disparate scan data into a single unified view of your vulnerability posture. With this single view, RiskSense takes a risk-based approach of the vulnerabilities focusing on exploitability to provide prioritized remediation.

Q. Do you have to manually consolidate reports from different tools to get complete visibility and to assign remediation to different users/teams?

A. RiskSense Value: Because the RiskSense solution has visibility into all the vulnerability information within the environment and the ability to create workflows for remediation, including integrating with 3rd party ticketing systems, it's easy to streamline and consolidate remediation efforts across different environments.

Q. How do you correlate threats to vulnerabilities within your organization?

A. RiskSense Value: RiskSense brings in numerous threat sources, correlates with vulnerability data, and calculates a Vulnerability Risk Rating (VRR) for each and every vulnerability in order to determine exploitability and permit accurate prioritization.

Q. Has your organization adopted a risk-based vulnerability management and prioritization program?

A. RiskSense Value: RiskSense uses several factors like its custom Vulnerability Risk Rating (VRR), asset business criticality, asset exposure, threat intelligence, and probability of a breach to calculate the risk score. The goal of risk-based prioritization is to determine the most exploitable vulnerabilities so that organizations can prioritize remediation based on risk to the business.

Q. How do you report your current vulnerability posture to the Executive Leadership Team and Board of Directors?

A. RiskSense Value: RiskSense provides different reporting metrics depending on the audience, from the Engineer responsible for patching all the way to the Board. Some key information RiskSense provides is the RiskSense Security Score (a measure of risk, modeled after a credit score with a low of 300 (poor) and a high of 850 (perfect)) across the entire organization, Risk-based funnels mapped to assets with Critical Risk Indicators, Vulnerability and Threat Distribution, Exploitable Hosts by Business Criticality, Asset coverage and insights, historical trending with context, and a Year over Year High Impact Vulnerabilities Cyber Hygiene View among other information. RiskSense allows you to create persona-based reports and dashboards to convey only the information needed by specific roles within the organization.

Q. What does your Application Security program look like today? Which vulnerability scanner types (SAST/DAST/OSS/Container) and brands are you using?

A. RiskSense Value: RiskSense RBVM analyzes all of your infrastructure and application vulnerability data, even across CVE- and CWE-based vulnerabilities. Correlating with threat data allows you to visualize and compare groups of assets, prioritizing vulnerabilities by specific application and code location to determine where your resources are best invested.

Q. Do you have a 3rd party helping you in this effort?

A. RiskSense Value: With RiskSense's Comprehensive Vulnerability Management, we can save you time, money, and produce a superior result.

Q. With what frequency do you scan your applications for vulnerabilities?

Q. What are you doing with the output from these tools?

Q. If you're dissatisfied with your current Threat and Vulnerability Management strategy, where does improving it live on your priority list?

Q. If you could dramatically improve your vulnerability management outcomes without a material increase in operating cost, would you?

Penetration Testing and Vulnerability Management

Q. Does your current security program include penetration testing?

A. RiskSense Value: RiskSense has been performing penetration testing on behalf of our clients for 14 years, focusing on web application, network, IoT, and mobile

applications. RiskSense demonstrates to our customers complex exploits and attack paths, while focusing on 100% coverage of the target network and applications. Utilizing our RiskSense platform, vulnerability and exploit data from the pen test is available in near real time, allowing same day reporting and discussion with our analysts. This service ultimately provides the visibility, prioritization, and actionable remediation recommendations needed to shrink your attack surface and reduce your overall cyber risk exposure.

Q. Does your current security program include regular vulnerability scanning?

A. RiskSense Value: The RiskSense Vulnerability Management Service provides comprehensive vulnerability management at monthly, quarterly, or custom-defined intervals to swiftly and accurately identify vulnerabilities and misconfigurations on your network. You're provided with a detailed analysis of the assessment results, offering recommendations to remediate identified security gaps. The service is delivered via the award-winning RiskSense RBVM solution, which allows for contextualization of the assessment findings with external threat data and RiskSense Proof of Concepts, providing a risk-based prioritization of the vulnerabilities.

Q. Do you believe you have security controls in place to protect your organization against a targeted cyber attack?

A. RiskSense Value: As part of the RiskSense offering, our team identifies which assets are susceptible to exploitation. Penetration testing identifies gaps and/or misconfigurations in your existing security controls.

Q. How do currently prioritize new vulnerabilities and track remediation of previously identified vulnerabilities?

A. RiskSense Value: No organization has the resources necessary to remediate every discovered vulnerability. The rapid rate of new vulnerabilities discovered means that IT and InfoSec departments are flooded with 10s of thousands of new findings every year. We determine exploitability using Threat Intel, Asset Exposure, Asset Criticality, and indicators that a vulnerability is being actively used in the wild. RiskSense provides a built-in workflow and ticketing system or can integrate with your existing IT ticketing system. We provide a clear fix for the identified vulnerabilities.

For more information, please visit www.risksense.com.