SaaS Application Security (SAS) Assessment

OVERVIEW

SaaS Applications are typically accessed by users via both corporate and personal devices; SaaS applications provide productivity and collaboration benefits for organizations.

However, these applications and the often sensitive data stored in the public cloud present unique security challenges and risks, such as accidental data exposure by users. To prevent this exposure and ensure threats do not propagate through these SaaS applications, you need granular visibility control of SaaS applications with security policies applied to all data and users.

The OnX security team can help by providing visibility of SaaS application activity, and deliver a detailed analysis of usage by user and device to easily determine if there are any data risks or compliance-related policy violations.

Also, we can scan your cloud application environment with cloud-based malware prevention to identify known and unknown malware and prevent a SaaS application from becoming an insertion point for advanced threats into an organization's computing environment.

Allow OnX to scan your SaaS App environment and hunt for:

- Malicious Outsiders
- Malicious Insiders
- Accidental Data Exposure
- Security Risk
- Compliance Issues: PII, PHI, etc.

ASSESSMENT FOCUS AREAS

With our SaaS Application Assessment tools, we review customer's data residing within enterprise-enabled SaaS applications that is not visible to an organization's network perimeter. OnX can connect directly to sanction SaaS applications to provide data classification, sharing/permission visibility, and threat detection within the application.

This yields unparalleled visibility, allowing your organization to understand the level of data risk violations and control access to shared data via a contextual policy.

ONX APPROACH

1. Review Documentation and Artifacts
2. Interview Key Personnel
3. Sensor Deployment
4. Analysis
5. Verify Findings and Re-interview

Phase 1: Review Documentation and Artifacts

> The team will collect and review documentation regarding the organization's corporate SaaS application policies and other relevant information that is in scope for the assessment.

Phase 2: Interview Key Personnel

> Interviews of key personnel will be conducted to help determine the best scan testing plan deployment.

Phase 3: Sensor Deployment

> Scanning using industry best practices and the experience/judgment of the security assessment team.

Phase 4: Analysis

> Analyze the behavior of SaaS applications in scope for the assessment.

Phase 5: Verify Findings and Re-interview

> The team will investigate specific issues in the scope of the assessment to add more details to report if necessary.

> Identify and evaluate the gaps in security.

> Second interviews of key personnel will be conducted verify issues with artifacts.

Once Assessment is Complete:

> The team will conduct analysis and report creation.

> A detailed presentation of findings and recommendation is provided.

RELATED SERVICES

> OnX Improve Your Security Posture (OIYSP) Assessment
> Firewall Rule Review (FRR)
> Security Governance Consulting
> Information Security Consulting

PROJECT MANAGEMENT

OnX includes a project manager as part of all projects to manage the overall project team, create and maintain the project plan, communicate status on a recurring basis and facilitate escalations as needed. This will minimize risks and ensure timely and successful service delivery.

Additionally, OnX maintains a knowledge base of "lessons learned" comprised of feedback from all service deliveries to help prevent unforeseen delays and other impacts on the project.

WHY ONX?

OnX's full-lifecycle support services encompass design, installation, integration, implementation, and project management. Our core competencies have scaled to include Software Development Security improvements, Security Operations Services, and Information System Security Management.

> Our security consultants are members of AIIM, AITP, CSA, ISSA, IEEE, HIMSS, CSI-SD and many other organizations. Our team members hold certifications including CEH, CHCIO, CISSP, CHFI, ECSA, DAWIA Level III, CCSK, CDIA, and ECMp.
> Our experienced Information Systems Security Professionals (ISSPs) work with our other IT subject matter experts (e.g., OpenStack, Hadoop, VMware, Cloud, etc.) to design and integrate custom enterprise security solutions, giving our clients access to skills and expertise beyond their in-house IT teams and traditional resellers.
> We have 30+ years as a Solution Provider with Data Center and Managed Services heritage and expertise.