

OVERVIEW

MAX Partner Services Delivery Overview

Partner Requirements, Responsibilities, and Delivery Model

Partner Personnel Needs & Requirements

These are the required personnel that a partner must have in place in order to begin implementing MAX services for SSC.

- **Vendor Risk Consultant (Senior):** This role is the main point of contact with customers. The VRC must be able to think strategically about a customer's needs and use their knowledge of SSC data to deliver for the customer. Key skills include being a Certified MAX delivery practitioner, having hands-on cybersecurity and/or Third-Party Risk Management expertise, and being an outstanding communicator.
- **Administrative Support/Vendor Risk Consultant (Junior):** This person acts as a backup to the senior consultant. They take the lead on Vendor Escalation Calls, guiding vendors through the Likelihood Assessment and Remediation Plan. They also handle vendor and customer emails and questions, escalating issues to SSC MAX Partner Support as needed.
- **Project Manager:** This role is responsible for tracking the overall progress of MAX delivery for all customers. For new customers, they support the configuration process and ensure a smooth hand-off from sales to delivery.
- **Risk Operations Center - MAX Analyst:** The focus of this role is to analyze, manipulate, and consolidate SSC data for the customer and vendor engagement teams. This includes analyzing findings, removing false positives, and identifying patterns and trends to report on. They also assist customers with assessments and analyze questionnaire responses.

Delivery Model Responsibilities Overview

This model outlines three rolling phases for services delivery:

1. **Phase 1 (Immediately):** SSC provides analysis and email notifications, while the Partner handles direct customer and vendor engagement.
2. **Phase 2 (Q4 2025 – Q1 2026):** SSC sends email notifications, and the Partner performs the analysis of findings and incidents, in addition to direct customer and vendor engagement.
3. **Phase 3 (Q2 2026 – Q3 2026):** SSC provides Tier 2 and Tier 3 support, and the Partner is fully responsible for completing all MAX tasks and delivering all outputs.

MAX Vendor Engagement: SSC vs. Partner Responsibilities (Phase 1)

	Output	SSC Responsibilities	Partner Responsibilities
Reactive Reporting: Daily Notifications	High or Critical Indicator Detected Zero-Day as a Service (ZDaaS) Finding	Share findings and suggested remediation with the Vendor	Update customer on status at weekly meeting
Proactive Reporting: Issued on a monthly basis	Monthly Indicator Summary Report	Share indicators and suggested remediation with the Vendor	Update customer on status at weekly meeting
Vendor Escalation: Quarterly Basis (in the event that the vendor's score continues to decrease or the vendor experiences repeated incidents)	Partners can deliver MAX services within weeks using SecurityScorecard's certification	Share findings and suggested remediation with the Vendor, setup call	Meet with the vendor Agree the course of action that the Vendor will pursue Assess the degree of vendor engagement

MAX Technical Requirements

These are the technical requirements needed by the Partner in order to successfully deliver MAX to customers:

- **MAX Workstation (Tasks and Workflows) and SSC Platform:** Used to perform key tasks like reviewing daily findings, removing false positives, generating Likelihood Assessments, and uploading/downloading documents.
- **Customer and vendor email solution:** Must be able to send at least 100 emails per 1,000 vendors per day and retain email logs for up to one year & generate tickets to track correspondence and maintain 99% uptime.
- **Customer and vendor contact management system:** Used to track contact details and log changes.
- **Meeting scheduling platform:** Assists in scheduling meetings and is integrated with the email and contact management systems.
- **Teleconferencing solution:** Allows for meetings with up to 15 participants and screen sharing.
- **Document management system:** Used to save and edit files from various sources, including the MAX workstation and email.
- **Open-Source Breach Investigation and Analysis:** Requires the ability to investigate dark web sites and validate data breach reports.
- **Python IDE or similar:** Necessary for calling SSC data via API.