Channel Partner Guide to a Successful POC

Executing a Successful Komodo Systems POC

This guide outlines the standard operating procedure for conducting a successful Proof of Concept (POC). Following these steps ensures a seamless installation and provides the customer with clear metrics for a successful evaluation.

Phase 1: Defining the Scope & Success Criteria

Before software is installed, the channel partner and customer must align on the POC's success criteria.

- **Device Inventory:** Define the specific number and types of devices to be monitored.
- **Network Mapping:** Identify the specific network segments involved.
- **Timeline:** The standard evaluation period is 30 to 45 days.
- **Success Metrics:** Identify the customer's "pain points." Use these to establish 3 to 5 objective success criteria (e.g., "Successful identification of X-type vulnerabilities within 48 hours").
- **Pre-Flight Check:** Complete the **Pre-POC Questionnaire** to ensure no technical surprises.

Phase 2: Environment & Hardware Readiness

The partner is responsible for ensuring the customer's environment meets Komodo's technical standards.

- **Infrastructure:** Determine the physical server location (e.g., on-premises data center) or VM environment.
- **Technical Compliance:** Review the Server Requirements to ensure hardware compatibility.
- **Access Provisioning:** Secure the necessary server rights (IDs and Passwords) and submit them to Komodo Systems.

Phase 3: Deployment & Configuration

To ensure the software is optimized for the specific environment, Komodo Systems will install and configure the software.

- **Remote Access:** Provide Komodo Systems with VPN access for remote configuration.
- **Installation:** Komodo engineers will install and configure the software based on the parameters established in Phase 1.

Phase 4: Active Evaluation & Partner Engagement

Once the software is live, the evaluation period officially begins. The channel partner plays a critical role as the primary point of contact.

- **Customer Hands-on:** The customer begins to evaluate the predefined features.
- **Semi-Weekly Check-ins:** Partners should conduct twice-weekly follow-ups with the customer to address questions, ensure engagement, and troubleshoot minor roadblocks.

Phase 5: Final Review & Transition

At the end of the 30 to 45-day window, the channel partner conducts a formal review with the customer.

- **Performance Audit:** Meet with Komodo Systems and the customer to review the initial success criteria.
- **Outcome Documentation:** Document how the solution addressed the customer's pain points to facilitate a smooth transition to a full production license.

Tips for Partners
Keep the focus on the Pre-POC Questionnaire. Most deployment delays are caused by missing server credentials or firewall restrictions that weren't identified during the initial scoping call.

Success Criteria Example

To align your POC success criteria with **NIST CSF 2.0,** move beyond "Does the software work?" to "How does this reduce institutional risk?" Since you are managing an on-premises product, these criteria focus on visibility and control within the customer's own infrastructure. **Tip**

By using NIST-aligned criteria, you help the customer's **CISO (Chief Information Security Officer)** justify the budget. It transforms the POC from a "tool test" into a "compliance solution."

POC Success Criteria & NIST Alignment

Please work with the customer to identify at least **three** specific objectives from the list below. A successful POC is defined by the software's ability to meet these benchmarks within the 30 to 45-day window.

1. Asset Management & Visibility (NIST ID.AM)

Goal: Establish a comprehensive inventory of all devices on the designated network segments.

- **Success Criterion:** The system must automatically discover and categorize 100% of active assets (Servers, workstations, IoT) within the scoped segments.
- **Validation:** Comparison of the Komodo inventory export against the customer's existing (manual) asset list.

2. Vulnerability & Risk Assessment (NIST ID.RA)

Goal: Identify and prioritize technical vulnerabilities based on risk.

- **Success Criterion:** Identification of at least one critical or high-severity vulnerability that was previously unknown to the customer.
- **Validation:** Generation of a Risk Assessment Report detailing the vulnerability, its location, and the potential impact.

3. Policy & Governance (NIST GV.PO)

Goal: Ensure the software supports the customer's internal security policies.

- **Success Criterion:** Successful configuration of customized alerting thresholds that align with the customer's specific "Acceptable Risk" levels.
- **Validation:** Verification that the system triggers notifications only for events that violate defined policy parameters.

4. Protective Technology (NIST PR.PT)

Goal: Verify that the solution provides the necessary technical logs and audit trails.

- **Success Criterion:** The system must maintain a tamper-evident audit log of all administrative actions taken during the POC.
- **Validation:** Review of the Audit Log export at the 30-day mark.

Partner Instructions for Success Mapping

To make the "Success Criteria" legally and commercially binding for the sale, use the table below in the Pre-POC document:

NIST Category	Customer Pain Point	Success Metric	Status
Identify (ID.AM)	"We don't know what's on Segment B."	Discovery of all IP-connected devices.	Pass or fail
Protect (PR.PT)	"We need better audit trails for compliance."	Generation of weekly automated compliance reports.	Pass or fail
Govern (GV.SC)	"We struggle to manage 3rd party risk."	Identification of unauthorized external connections.	Pass or fail