Applying the IMPACTO Model: A Hypothetical Use Case for Deploying Airlock and CrowdStrike Falcon in a Port Environment

**Disclaimer**

This use case is entirely hypothetical and is provided solely as an example to illustrate the IMPACTO Model. It does not represent actual events or actions taken by the Port of Valencia—or any other port authority.

By Kyle Villano

Version 0.1

© 2025 Kyle Villano – This document is part of the IMPACTO Model project and is licensed under the Creative Commons Attribution‑ShareAlike 4.0 International License (CC BY‑SA 4.0). To view a copy of this license, visit <https://creativecommons.org/licenses/by-sa/4.0/>

**Introduction**

A large Mediterranean port (comparable to the Port of Valencia, handling five million TEUs annually) recognizes the critical importance of protecting its operations from cyber-physical attacks. The port authority has historically faced challenges integrating new security tools—especially across both **IT** and **OT** networks. Two major purchases have recently been approved to address endpoint security concerns:

1. **CrowdStrike Falcon** for real-time endpoint detection and response (EDR).
2. **Airlock** for a “deny by default” application-control model (allowlisting) to block unauthorized executables and scripts.

Rather than simply installing these tools and assuming security has improved, the port authority opts to adopt the **IMPACTO Model**. By rigorously following the model’s emphasis on Maturity Classification (MCF), Capability Classification (CCF), and continuous risk/capability measurement (PCP–ACP, PRP–ARP), the port ensures real, measurable improvements over time.

**2. Context and Motivation**

**2.1 Drivers for Change**

* **Emerging Threats:** Prior penetration tests at maritime facilities worldwide show how endpoint or OT compromises can disrupt crane automation, cargo handling, or vessel traffic management.
* **Regulatory Pressure:** New cybersecurity mandates for critical infrastructure require robust endpoint protection and documented proof of risk mitigation.
* **Strategic Investment Rationale:** Board members estimate a single day of port disruption can cost millions of euros, presenting a clear business case for robust endpoint security.

**2.2 Desired Outcome**

The IMPACTO Model ensures:

* **Maturity (MCF)**: The port develops disciplined processes and skilled teams to manage, operate, and continuously improve the new solutions.
* **Capabilities (CCF)**: The advanced features of CrowdStrike Falcon and Airlock (e.g., real-time threat intelligence, script allowlisting) are enabled and used—not just purchased and left idle.
* **Value Realization**: Risk metrics (PRP–ARP) show genuine progress toward safer endpoints, fewer security events, and faster incident handling.

**3. Defining POC–AOC and Key Profiles**

Before diving into IMPACTO Stages, the port clarifies its **Projected Operating Context (POC)**—what they envisioned pre-purchase—and then tracks the **Actual Operating Context (AOC)** over time.

**3.1 Projected Operating Context (POC)**

* **Enterprise/Organization:** Coverage initially for all administrative endpoints, with planned expansion to OT segments controlling cranes and logistics.
* **Function:** Strengthen endpoint defense and reduce malware intrusions, unauthorized software usage, and living-off-the-land techniques.
* **Architecture:** Hybrid environment (on-prem Windows servers, some Linux-based port control systems), with moderate-scale Active Directory for staff authentication.

**3.2 Actual Operating Context (AOC)**

Six months into deployment, the port discovered:

* **Broader Scope:** Many unaccounted-for OT endpoints running older OS versions, requiring special integration steps.
* **Contractor Systems:** ~20% more endpoints than projected—many in third-party contractor facilities.
* **New Cloud Services:** A cloud-based container-tracking platform introduces new compliance requirements.

These real-world changes demonstrate the importance of regularly updating the **AOC** so that neither endpoints nor user groups remain hidden or unmanaged.

**3.3 Profiles: PCP–ACP and PRP–ARP**

1. **Purchased Capability Profile (PCP):**
   * Deny by default on all endpoints via Airlock.
   * Real-time threat detection by CrowdStrike Falcon (with threat intelligence feed).
   * Integration between the two tools for quicker blocklisting of known malicious executables.
   * 100% coverage of administrative endpoints + 70% coverage of critical OT endpoints within six months.
2. **Actual Capability Profile (ACP):**
   * Discovered shortfalls—only 80% of admin endpoints and 50% of OT endpoints were covered by Airlock at first.
   * Macro allowlisting was not fully enabled due to staff training delays.
   * Automated correlation between CrowdStrike and Airlock was partially successful but needed better runbooks.
3. **Purchased Risk Profile (PRP):**
   * Anticipated 40% drop in commodity malware infiltration.
   * Mean Time to Detect (MTTD) to shrink from ~days to ~hours.
   * Large-scale disruptions (impacting crane operations) to be extremely unlikely.
4. **Actual Risk Profile (ARP):**
   * A measured ~35% reduction in infiltration attempts.
   * Some “unknown file” alerts linger >24 hours before action, creating delays.
   * OT coverage gaps remain, but no major incidents so far.

Comparing **PCP vs. ACP** and **PRP vs. ARP** offers the port a clear view of how effectively purchased features have turned into real-world capabilities—and how well that has reduced actual risk.

**4. MCF and CCF: Tracking Maturity & Capabilities**

**4.1 Maturity Classification Framework (MCF)**

The port adapts references from **SOC-CMM** and aspects of **C2M2** to define how People and Process maturity evolve. The MCF focuses on four domains within IMPACTO:

* **Business** domain: Budget alignment, ROI analysis, strategic goals.
* **People** domain: Staff roles, training, and runbook coverage.
* **Process** domain: SOPs, incident response steps, cross-team collaboration.
* **Technology** domain: Implementation depth, coverage, advanced analytics usage.

By **Stage 3** or beyond, the port expects well-defined runbooks for software approvals, incident handling, staff training, and integrated OT coverage.

**4.2 Capability Classification Framework (CCF)**

The port’s CCF references **MITRE ATT&CK** to map potential adversarial techniques to CrowdStrike and Airlock’s features:

* **Deny-by-Default Execution Control (Airlock)**: Blocking unapproved binaries, macros, scripts.
* **Real-Time EDR (CrowdStrike)**: Detecting suspicious processes, “living off the land” patterns, lateral movement.
* **Integration & Automation**: Automatic ingestion of threat intel (hashes, IOCs) from CrowdStrike to instantly update Airlock blocklists.
* **Reporting & Analytics**: Dashboards that show block events, near-miss attempts, and coverage of TTPs.

As the port climbs from the initial usage (Stage 1–2) to more advanced usage (Stage 4–5), it employs more thorough analytics, better integration, and more robust coverage of advanced adversary TTPs.

**5. Applying the IMPACTO Stages (0–5)**

Below is how the port’s adoption of Airlock and CrowdStrike Falcon evolves through each IMPACTO Stage. **Note**: Different domains (Business, People, Process, Technology) may move at different speeds; the overall stage typically reflects the slowest domain, unless there is a strong plan to close gaps.

**5.1 Stage 0 – Purchased**

* **Business:** The board just approved funds, but there is no formal business case or risk measure.
* **People:** No staff assigned; no training. The tools risk becoming “shelfware.”
* **Process:** Minimal or no runbooks.
* **Technology:** Airlock, CrowdStrike licenses acquired; minimal or no real deployment.
* **Risk Reduction:** Negligible. Tools are not configured, so the purchased risk improvements remain theoretical.

**Key Action**: Assign a Security Champion, define ownership, and outline the initial use case scope (admin endpoints + partial OT coverage).

**5.2 Stage 1 – Ad Hoc Deployment**

* **Business:** Rationale is “we need EDR for compliance” but lacking deeper ROI.
* **People:** A single IT generalist checks CrowdStrike alerts occasionally; no formal training.
* **Process:** Incident handling is reactive; no standardized runbooks for allowlisting.
* **Technology:** Airlock enabled on a small subset of endpoints; CrowdStrike is running in default mode.
* **Risk Reduction:** Some basic blocking of known malware. Inconsistent coverage across endpoints.

**Key Action**: Begin basic training, define short runbooks (e.g., software approval workflow), and gather logs/metrics to assess potential ROI.

**5.3 Stage 2 – Managed Deployment**

* **Business:** Multi-year operating costs for CrowdStrike and Airlock appear in the budget. Basic risk metrics are introduced (e.g., blocked malware attempts).
* **People:** Formal roles: “Airlock Administrator,” “EDR Analyst.” A few staff attend vendor trainings.
* **Process:** Standard runbooks for typical incidents. Basic post-incident reviews to adjust blocklists.
* **Technology:** Key features turned on (e.g., script blocklisting, real-time EDR alerting). Possibly partial automation for known malicious hashes.
* **Risk Reduction:** Measurable drop in commodity threats and improved incident triage.

**Key Action**: Document coverage levels, finalize runbooks for software-approval requests and incident response, schedule more advanced training.

**5.4 Stage 3 – Formalized Integration**

* **Business:** Metrics on risk reduction (e.g., mean-time-to-detect or block) guide budget decisions. Leadership sees security as supporting reliable port operations.
* **People:** Competency frameworks align staff roles; cross-functional collaboration with crane/OT teams.
* **Process:** Comprehensive runbooks are regularly maintained; monthly reviews or cross-team incident debriefs.
* **Technology:** Deeper coverage of advanced features (macro allowlisting, real-time correlation with CrowdStrike). OT endpoints integrated where feasible.
* **Risk Reduction:** The difference between PRP and ARP shrinks as coverage expands. Fewer unknown or unmanaged endpoints remain.

**Key Action**: Expand advanced macro control, ensure OT segments have Airlock coverage, refine metrics on infiltration rates and response times.

**5.5 Stage 4 – Data-Driven Solution**

* **Business:** Advanced risk quantification (e.g., ALE-like models) informs expansions. Security is recognized as essential to the port’s brand.
* **People:** Specialized roles or strong external partnerships handle advanced threat hunting and data analytics.
* **Process:** KPI/KRI-driven improvements. If macro-based threats spike, new block rules are deployed quickly.
* **Technology:** Integration with SIEM or SOAR for near real-time correlation. Proactive detection of anomalies.
* **Risk Reduction:** Real-time visibility and near real-time response. Substantial drop in infiltration attempts, minimal false positives.

**Key Action**: Automate inbound threat intel to update Airlock blocklists; track MTTD/MTTR in near real-time dashboards; refine compliance reporting.

**5.6 Stage 5 – Optimizing Solution**

* **Business:** Security is a recognized differentiator—shared with shipping lines, insurers, and customers to illustrate operational resilience.
* **People:** Ongoing staff rotations and upskilling maintain fresh perspectives; the security culture is embedded across all teams (IT, OT, contractors).
* **Process:** Continuous improvement is ingrained; every incident leads to immediate runbook updates. Sharing threat intel extends to partner supply chains.
* **Technology:** Fully orchestrated EDR + allowlisting environment; advanced ML-based anomaly detection. Low false positives; near-zero dwell time for real attacks.
* **Risk Reduction:** Residual risk remains consistently within or below the target thresholds. Clear, measurable ROI.

**Key Action**: Sustain a real-time adaptation mindset; pilot new vendor features, share success stories, measure improvements in multiple frameworks (e.g., MITRE ATT&CK coverage).

**6. Operational Intelligence (OI)**

Throughout the process, the port uses **Operational Intelligence (OI)** to improve both the MCF and CCF dimensions:

* **Threat Intel Feeds**: CrowdStrike automatically flags emerging “living off the land” binaries; Airlock updates blocklists.
* **Red Team Exercises**: Validate newly introduced macro rules or older OS coverage. Gaps are patched quickly, feeding knowledge back into runbooks.
* **Incident Post-Mortems**: Each real or near-miss event is carefully dissected to refine roles, processes, or coverage for next time.

**7. Outcomes and Value Realization**

**7.1 Closing the Gap Between Purchased & Actual**

By systematically moving from **Stage 0** (idle purchase) to **Stage 5** (fully optimized), the port authority ensures:

* **PCP → ACP**: Over 90% coverage of critical endpoints in both IT and OT.
* **PRP → ARP**: Documented reductions in malware infiltration and faster incident handling than initially predicted.

**7.2 Tangible Business Benefits**

* **Reduced Downtime:** Crane operations and cargo flows stay largely uninterrupted—even amidst active malware campaigns.
* **Stronger Compliance & Insurance Position:** Demonstrable maturity (Stage 3+ in MCF) can lower insurance premiums and ease audits.
* **Proactive Risk Management:** Early threat detection, improved staff training, and integrated reporting align with the port’s broader strategic goals.

**7.3 Evolving the Culture**

At **Stage 5**, cybersecurity is no longer an afterthought or “cost center”; it becomes a hallmark of the port’s reliability and resilience. This cultural shift drives ongoing investment and fosters collaborative relationships with shipping lines, logistics providers, and insurers, all of whom benefit from a safer maritime ecosystem.

**8. Conclusion**

This revised hypothetical example shows how **IMPACTO Model (v0.1)** helps ensure that newly purchased cybersecurity solutions—like **CrowdStrike Falcon** and **Airlock**—become fully embedded, measurable contributors to an organization’s security posture. By tracking:

* **Maturity** (via MCF for People and Process)
* **Capabilities** (via CCF to realize purchased features)
* **Risk Profiles** (purchased vs. actual)
* **Operating Context** (projected vs. actual)
* **Operational Intelligence** (continuous feedback)

…the port authority navigates each IMPACTO Stage (0–5). In doing so, they optimize both the technical efficacy and the organizational readiness needed to achieve **true risk reduction** and **clear business value**.

© 2025 Kyle Villano – This document is part of the IMPACTO Model project and is licensed under the Creative Commons Attribution‑ShareAlike 4.0 International License (CC BY‑SA 4.0). To view a copy of this license, visit <https://creativecommons.org/licenses/by-sa/4.0/>