PORT::ZERO
CYBER SOLUTIONS
Protect Against Cyber Threats ®

PORT::ZERO Incident Response Command Suite

Technical White Paper | v1.0 PoC

rick@portzerocyber.com

877-317-4422

https://portzerocyber.com

The Cyber Resiliency Gap: A Market Opportunity

Transitioning from Static Planning to Dynamic Incident Readiness

The current cybersecurity landscape is saturated with "compliance-by-checklist" solutions that satisfy auditors but fail during active incidents. Organizations across both public and private sectors are burdened with static, non-integrated "shelfware" that provides a dangerous false sense of security.

PORT::ZERO Cyber Solutions disrupts this $10B+ market by replacing static planning with an automated, intelligence-driven Command Suite. By merging the rigor of NIST CSF 2.0 with the tactical depth of **MITRE ATT&CK®**, we have engineered a "Private-by-Design" SaaS platform that transforms incident response from a document into a dynamic, measurable capability.

Our mission is to bridge the gap between industry needs and technical execution, providing a scalable architecture that matures with the client through a unique, outcome-based financial model.

Section I: Introduction

1. The Crisis of Static Preparedness

Traditional Incident Response (IR) planning is broken. Organizations often pay for "shelfware", static documents that are outdated the moment they are printed. These templates frequently provide a false sense of security, pre-filling health scores and ignoring the specific asset complexities of hybrid-cloud environments.

2. The PORT::ZERO Solution: Private-by-Design

The **PORT::ZERO Incident Response Command Suite** is a SaaS-based Proof of Concept that replaces static templates with a linear, audit-ready "Command Flow." **The 0% Maturity Baseline:** We eliminate "security theater" by starting every engagement at a zero-percent readiness score, forcing a rigorous validation of people, assets, and strategy.

- **Architecture as a Feature:** Built on a "Private-by-Design" foundation, the suite utilizes AWS-native security, multi-tenant isolation, and encrypted persistence to ensure that sensitive organizational data remains sovereign and secure.

3. Key Differentiators

Feature	Traditional IR Consulting	PORT::ZERO Incident Response Command Suite
Data Integrity	Static Word/PDF files	Amazon Aurora (PostgreSQL) Persistence
Frameworks	Generic Checklists	**NIST CSF 2.0** Governance Alignment **MITRE ATT&CK®** Mapping
Output	Manual Templates	Automated, Immutable PDF Generation
Incentives	Flat Fee for "Completion"	**Maturity Rebates** based on hardening

4. Strategic ROI: The Maturity Rebate Model

Unlike traditional firms, PORT::ZERO Cyber Solutions introduces Outcome-Based Pricing. By leveraging the Suite's internal tracking, we offer financial incentives for organizations that demonstrably improve their security posture. This ensures that the platform isn't just a tool, but a driver for long-term organizational resilience.

Section II: Technical Architecture & Design Evolution

The transformation of the **PORT::ZERO Incident Response Command Suite** from a "paper concept" to a scalable SaaS platform represents a shift from static, reactive planning to a dynamic, intelligence-driven architecture. This section outlines the journey of bridging the gap between industry needs and technical execution.

1. Conceptual Genesis: From Paper to Logic

The architecture began by addressing a stark market reality: most organizations lack a functional Incident Response Plan (IRP). On paper, we moved away from "cookie-cutter" templates, choosing instead to anchor the suite in two world-class frameworks:

- **NIST CSF 2.0 Integration:** By aligning with the Govern, Identify, Protect, Detect, Respond, and Recover functions, the suite ensures that every plan is built on a foundation of recognized best practices.
- **The Maturity Model Approach:** Rather than a simple pass/fail, we implemented an Implementation Tier system (Partial to Adaptive). This allows businesses to measure their growth over time and justifies the "Maturity Rebate" business model.

2. Intelligent Mapping: MITRE ATT&CK® & OpenAI

To move beyond basic governance, the technical architecture integrates active threat intelligence and generative AI:

- **MITRE ATT&CK® Asset Mapping:** Users map their unique organizational assets and processes directly to threat actor Tactics, Techniques, and Procedures (TTPs). This transforms a generic plan into a targeted defense strategy, specifically identifying how to protect high-value assets against real-world behaviors.
- **AI-Augmented Synthesis:** We integrated the **OpenAI API** to act as a force multiplier. The suite autonomously generates high-fidelity Executive Summaries and Business Impact Analysis (BIA) reports. By analyzing organizational inputs, the AI provides strategic insights that would traditionally take a consultant dozens of hours to produce.

3. Engineering the Stack: VS Code, Streamlit, and Docker

The transition from conceptual logic to executable code involved a deliberate choice of tools optimized for both speed and security:

- **Frontend & Logic:** Developed in **VS Code** using **Python and Streamlit**. This stack allowed for rapid prototyping of the "Hacker-Crisp" UI and interactive data flows.
- **Containerization:** The entire environment was containerized using **Docker**. This ensures total parity between local development and the eventual AWS cloud environment, eliminating the "it works on my machine" barrier.

4. Data Evolution: Moving to PostgreSQL RDS

A critical pivot in our architecture, facilitated by Kiro.dev, was moving away from a restricted dictionary-based data structure to a robust Database Architecture:

- **Scaling Persistence:** By migrating to **Amazon RDS (PostgreSQL)**, we transitioned from local session-state storage to a persistent, relational structure.
- **Library Management:** This allows for easy retrieval and updating of current threat libraries, asset inventories, and historical IR plans.
- **Multi-Tenancy & Security:** PostgreSQL provides the granular isolation necessary for a multi-tenant SaaS, ensuring that client data is logically separated and ready for **AWS Cloud** scalability.

Strategic Trajectory: The Path to AWS

The final stage of this PoC architecture is the migration to a full **AWS environment**. Utilizing services like **AWS Control Tower** and **IAM Policy Autopilot**, we are moving toward an infrastructure that scales vertically with client growth and horizontally across diverse industries in South Carolina and beyond.

Section III: Strategic Roadmap & AWS Evolution

The Strategic Roadmap for the **PORT::ZERO Incident Response Command Suite** focuses on transitioning from a functional Proof of Concept to a high-availability, enterprise-ready SaaS. Scalability, Governance, and Automated Resilience characterize this phase.

Phase 1: Infrastructure as Code (IaC) & AWS Migration

To move from local Docker containers to a globally accessible platform, we are implementing a "Cloud-Native" migration strategy:

- **AWS Control Tower & Landing Zones:** Establishing a multi-account environment to ensure strict separation between development, testing, and production data.
- **Elastic Container Service (ECS) on Fargate:** Migrating the Dockerized Streamlit app to a serverless container environment. This removes the overhead of managing EC2 instances while allowing the suite to scale automatically during peak usage or active incident surges.

Phase 2: Enhanced Multi-Tenant Isolation

Building on the **PostgreSQL RDS** foundation, we are refining our "Zero Leakage" data policy:

- **Row-Level Security (RLS):** Implementing granular database policies to ensure that even within a shared database, a client's session can only ever "see" its own data.
- **Tailscale/Private Access:** For high-compliance clients, we are exploring private-access gateways to ensure the Command Suite isn't just "on the web," but acts as a private extension of their own secure network.

Phase 3: Advanced Intelligence Integration

Once the AWS environment is stable, the roadmap introduces deeper automation:

- **MITRE ATT&CK® Dynamic Sync:** Automating the retrieval of the latest TTPs from the MITRE database so that client mapping is always informed by real-time threat intelligence.
- **Automated Audit Trails:** Every action taken within the "Command Flow" is logged to an immutable **AWS CloudWatch** or **CloudTrail** archive, providing an ironclad audit trail for regulatory bodies.

Phase 4: Market Expansion & Maturity Rebates

The final phase of the roadmap moves the Suite from a product to a partnership:

- **The Maturity Rebate Rollout:** Full implementation of the outcome-based pricing model. This uses the suite's internal "Maturity Score" (derived from NIST 2.0 implementation) to trigger financial incentives for clients.
- **Strategic Advisory Scaling:** Using the automation of the Command Suite to allow PORT::ZERO Cyber Solutions to advise hundreds of organizations simultaneously without losing the "boutique" quality of high-level cybersecurity consulting.

Strategic Summary: The Vision for PORT::ZERO Cyber Solutions

The goal is not just to provide a tool, but to build a Security Ecosystem. By combining the rigor of NIST 2.0, the intelligence of **MITRE ATT&CK®**, and the scalability of **AWS**, PORT::ZERO Cyber Solutions is creating a platform that matures with the client.

Conclusion: The New Standard for Incident Readiness

The development of the **PORT::ZERO Incident Response Command Suite** marks a departure from the "compliance-by-checklist" era. By moving from a paper concept to a containerized, AI-augmented SaaS architecture, we have proven that enterprise-grade security planning can be both accessible and rigorous.

Our journey, from identifying the critical lack of functional plans to engineering a "Private-by-Design" AWS environment, was driven by a single mission: **to ensure that when a crisis hits, the plan is ready, the assets are mapped, and the path to recovery is clear**.

The PORT::ZERO Cyber Solutions Advantage:

- **Intelligence-Driven:** Beyond static text, we integrate the **MITRE ATT&CK®** framework to map defenses against real-world adversary behavior.
- **Framework-Aligned:** Every module is built to satisfy the governance requirements of NIST CSF 2.0.
- **Scalable & Secure:** Leveraging **AWS RDS** and **Docker**, we provide a multi-tenant environment that ensures data sovereignty for every client.
- **Incentivized Maturity:** We don't just find gaps; we partner with our clients to close them through our unique **Maturity Rebate** model.

A Call to Action for Resilient Leaders

Cyber resilience is no longer an optional IT requirement; it is a core business function. Whether you are a state agency managing public trust or a private enterprise protecting intellectual property, the **PORT::ZERO Incident Response Command Suite** provides the roadmap to move from a 0% baseline to an "Adaptive" security posture.

The architecture is built. The methodology is proven. It is time to move your incident response plan off the shelf and into the Command Suite.