PORT CYBER DEFENSE

port-cyber-defense.com/ghostred

PUBLIC WHITEPAPER

GHOST RED

AUTONOMOUS AI ADVERSARY PLATFORM

DOCUMENT	Enterprise Whitepaper
VERSION	v2.5.0 — March 2026
CLASSIFICATION	Public — Enterprise Whitepaper
CERTIFIED TEAM	OSCP · OSWE · CPTS · CWEE

2	56%	13	<60s	13	8
HIGH Findings Detected	Attack Chain Probability	Web App Issues OWASP Top 10	Time to First Strike	Remediation Items Live	Compliance Frameworks

GHOST RED v2.5.0 · PORT CYBER DEFENSE · March 2026 · port-cyber-defense.com/ghost-red

SECTION 01 · EXECUTIVE SUMMARY

Executive Summary

Modern enterprises are under siege. Attackers are patient, AI-assisted, and increasingly indistinguishable from legitimate users. Traditional security postures — quarterly pen tests, reactive SIEM alerts, annual compliance audits — were designed for a threat landscape that no longer exists.

GHOST RED is Port Cyber Defense's proprietary autonomous AI adversary platform. Built by OSCP, OSWE, CPTS, and CWEE-certified engineers, it continuously simulates nation-state and APT attack patterns against your live environment — finding real exploitable paths before real attackers do.

Version 2.5.0 introduces significant platform advances: certificate transparency-based subdomain discovery via crt.sh, CISA KEV integration with 1,500+ actively exploited CVE signatures, a persistent false positive suppression engine, a fully integrated Analyst Verification workflow, Campaign Mode for multi-target operations, Quantum Readiness auditing, and a closed-loop Remediation Tracker. Every figure in this document is taken from live GHOST RED platform output.

2	56%	13	<60s	13	8
HIGH Findings Detected	Attack Chain Probability	Web App Issues OWASP Top 10	Time to First Strike	Remediation Items Live	Compliance Frameworks

> *"In a live engagement, GHOST RED identified 13 web application security issues with a 56% attack chain probability — meaning there is a 56% chance a real attacker could fully compromise the environment using the discovered vulnerability chain. No human operator required. — GHOST RED AI Engine, live engagement output"*

Why GHOST RED Exists

The gap between what security teams think they know and what attackers actually find has never been wider. Compliance frameworks tell you what controls to have. Penetration testers visit once a year. Vulnerability scanners produce lists that overwhelm remediation teams. None of these approaches answers the one question that matters: can a real attacker breach my environment today?

GHOST RED was built to answer that question — continuously, autonomously, and with the same tradecraft used by advanced threat actors. It does not simulate attacks in a sandboxed lab. It tests your real infrastructure, finds real exploitable paths, and delivers an AI-generated kill chain showing exactly how an attacker would move from initial access to crown jewel.

SECTION 02 · HOW GHOST RED WORKS

How GHOST RED Works

GHOST RED operates as a fully autonomous AI red team. From a single IP address, CIDR range, or domain name, the platform executes the complete cyber kill chain — automatically, continuously, and safely within defined scope boundaries. Configuration takes under two minutes. Results begin appearing within sixty seconds of launch.

Attack Modules

■ **Passive Recon** Certificate transparency via crt.sh discovers all subdomains that have ever had an SSL certificate — revealing the complete external footprint without touching the target. DNS verification, WHOIS, and OSINT enumeration run in parallel.

■ **Network Scan** Port scanning, service fingerprinting, OS detection, and banner grabbing across the entire discovered attack surface. CDN and WAF detection prevents false findings on edge infrastructure.

■ **Vuln Discovery** CVE correlation engine with 1,500+ vulnerability signatures including full CISA KEV integration — 1,546 actively exploited CVEs flagged in real time. Probe-based confirmation distinguishes real vulnerabilities from theoretical ones.

■ **AI Chain Engine** Autonomous attack path generation powered by Claude AI — chains vulnerabilities into complete breach scenarios with MITRE ATT&CK; mapping. Dual-engine architecture: rule-based for deterministic output, AI for adversarial reasoning.

■ **Web App Scan** Full OWASP Top 10 (2021) audit — 13 automated checks covering SQLi, SSTI, blind SQLi, host header injection, path traversal, subdomain takeover, security headers, SSRF, authentication failures, and software integrity.

■ **Quantum Audit** Post-quantum cryptography readiness — TLS version analysis, cipher suite assessment, RSA key size validation against NIST PQC standards. ECC key sizes correctly assessed: 256-bit ECC is not flagged (equivalent to ~3072-bit RSA). Only RSA keys below 2048 bits are flagged.

■ **False Positive Engine** Persistent suppression rules eliminate known false positive patterns across all scans: CDN/WAF targets, ECC key misidentification, generic CVE matches. Rules accumulate over time — accuracy improves with every engagement.

Compliance Framework Mapping

Every finding is automatically mapped to relevant control requirements across all selected frameworks, generating evidence-ready output for auditors.

Framework	Scope	GHOST RED Coverage
DORA	Financial entities — EU resilience regulation	ICT risk, incident reporting, third-party risk, TLPT simulation
NIS2	Critical infrastructure operators — EU	Network security, incident handling, supply chain, cryptography
ISO 27001	Global information security standard	Asset management, access control, vulnerability management
PCI DSS	Payment card data environments	Network scanning, pen testing, web app security, encryption
HIPAA	US healthcare data protection	PHI access controls, audit logging, transmission security

NIST CSF	US federal and enterprise framework	Identify, Protect, Detect, Respond, Recover — full lifecycle
SOC 2	Service organisation controls	Security, availability, confidentiality trust service criteria
SWIFT CSP	Banking messaging infrastructure	Mandatory security controls for SWIFT network participants

SECTION 03 · AI ATTACK CHAIN ENGINE

AI Attack Chain Engine

The most powerful capability in GHOST RED is its AI Attack Chain Engine. Where traditional vulnerability scanners deliver a list of issues ranked by CVSS score, GHOST RED delivers a story — the exact sequence of steps an attacker would take from initial foothold to crown jewel, with probabilities, timing estimates, and MITRE ATT&CK; technique IDs at every stage.

> *"Exploitable vulnerabilities identified. Entry point: missing HSTS on port 443. Chain probability: 56%. Crown jewel: Active Directory, intellectual property, customer database. — GHOST RED AI Engine — live engagement output"*

Dual-Engine Architecture

GHOST RED runs two chain engines in parallel. The Rule-Based Engine fires immediately after scan completion, producing a deterministic kill chain from discovered findings using MITRE ATT&CK; mappings and sector-specific threat modelling. The AI Engine (powered by Claude) then generates a second, deeper analysis — reasoning about the same findings as an elite threat actor would.

If no API key is configured, the rule-based engine runs autonomously. Both engines produce the same output format: a complete kill chain with step-by-step breakdown, probability score, estimated time to compromise, and immediate mitigation actions.

Kill Chain — Step by Step

MITRE ID	Phase	What GHOST RED Maps
T1595	Reconnaissance	Certificate transparency + DNS enumeration maps all subdomains. Entry vectors ranked by confidence and CVSS.
T1190	Initial Access	Exploit of public-facing application. CVE-confirmed vulnerabilities flagged as immediate-action items.
T1136	Persistence	Backdoor account created or SSH key injected to maintain access independent of the initial exploit.
T1548	Privilege Escalation	Local privilege escalation via misconfigured sudo rules or kernel exploit to achieve root/SYSTEM.
T1550	Lateral Movement	Credential material (NTLM hashes or Kerberos tickets) extracted and used to authenticate to additional systems.
T1486	Impact	Ransomware deployed across domain-joined systems. Crown jewel data exfiltrated prior to encryption.

SECTION 04 · FINDINGS & WEB APPLICATION AUDIT

Findings & Web Application Audit

Every vulnerability discovered by GHOST RED is classified, scored, and presented in a findings dashboard. Probe-based confirmation distinguishes real vulnerabilities from theoretical ones. The persistent false positive suppression engine eliminates known noise patterns — ensuring findings represent real risk, not scanner artefacts.

Probe-Based Confirmation

Confidence	Meaning	Action Required
CONFIRMED	Active probe succeeded — vulnerability is exploitable on this target	Patch immediately. Treat as actively exploited.
PROBABLE	Strong evidence — version or banner confirms vulnerability window	Prioritise in current sprint. High exploitability risk.
POSSIBLE	Signature match — active probe was inconclusive	Investigate and verify manually. Do not dismiss.

False Positive Suppression Engine

GHOST RED v2.5.0 introduces a persistent false positive suppression system — a rules engine that eliminates known noise patterns before they reach the report. Rules are applied after every finding is generated and accumulate over time as new patterns are identified.

Pattern	Rule	Reason
256-bit ECC key	Suppressed	256-bit ECC = ~3072-bit RSA equivalent — strong, not weak
CVE POSSIBLE on CDN	Suppressed	Origin server not testable through CDN edge node
XSS POSSIBLE on CDN	Suppressed	Cannot confirm injection without direct server access
SQLi POSSIBLE on CDN	Suppressed	Cannot confirm injection without direct server access

Web Application Security Audit — OWASP Top 10

GHOST RED includes a dedicated web application scanner covering the full OWASP Top 10 (2021) with 13 automated checks. The scanner tests all ten categories and produces a coverage matrix. In a live engagement, GHOST RED identified the following verified findings:

Severity	CVSS	Finding	OWASP	Impact
HIGH	7.5	Missing HSTS Header	A05:2021	Downgrade attacks and credential interception on untrusted networks
MEDIUM	6.1	Missing X-Frame-Options	A05:2021	Clickjacking attack surface on all authenticated pages
MEDIUM	6.5	Missing Content Security Policy	A05:2021	XSS escalation risk — no script source restrictions
MEDIUM	6.5	Server Version Disclosure	A05:2021	Version fingerprinting enables targeted CVE exploitation
MEDIUM	6.5	Overly Permissive CORS Policy	A01:2021	Wildcard CORS allows any origin to make credentialed requests

LOW	4.0	Missing Referrer-Policy	A05:2021	Referrer header leaks sensitive URL fragments

SECTION 05 · CISA KEV INTEGRATION

CISA KEV Integration

GHOST RED v2.5.0 integrates with the CISA Known Exploited Vulnerabilities (KEV) catalogue in real time. The KEV catalogue is maintained by the US Cybersecurity and Infrastructure Security Agency and represents the definitive list of vulnerabilities known to be actively exploited in the wild by threat actors.

Every finding in GHOST RED is cross-referenced against the full KEV catalogue. KEV-confirmed findings are automatically upgraded in severity and prominently marked in both the platform UI and PDF reports. Ransomware-linked CVEs receive additional highlighting.

KEV Metric	Current Value
Total actively exploited CVEs	1,546
Ransomware-linked CVEs	313
Sync frequency	Every 24 hours (automatic)
Source	CISA official feed + GitHub mirror fallback
Severity upgrade	Automatic for KEV-confirmed findings

> *"A vulnerability that is 'merely' medium severity by CVSS score may be CRITICAL in practice if it appears on the CISA KEV list — meaning real threat actors are actively exploiting it right now. GHOST RED surfaces this distinction automatically. — GHOST RED KEV Integration Module"*

SECTION 06 · QUANTUM READINESS AUDIT

Quantum Readiness Audit

Quantum computing threatens to render today's public-key cryptography obsolete. RSA, ECC, and Diffie-Hellman key exchange — the foundations of TLS, SSH, and VPN security — are vulnerable to Shor's algorithm on a sufficiently powerful quantum computer. NIST has already finalised its first post-quantum cryptography (PQC) standards. Organisations that do not begin migration now face a retroactive decryption risk on data intercepted today.

GHOST RED v2.5.0 includes a dedicated Quantum Readiness Audit module that assesses TLS and cryptographic posture against current NIST PQC guidance. The audit runs automatically after every scan where HTTPS services are discovered.

What the Quantum Audit Checks

■ **TLS Version** Identifies TLS 1.0/1.1 (deprecated), TLS 1.2 (acceptable), TLS 1.3 (recommended). TLS 1.3 with X25519 provides the best currently-available quantum resistance.

■ **Cipher Suites** Flags RSA key exchange (vulnerable to Shor's algorithm), 3DES and RC4 (classically weak), and AES-128 (recommended upgrade to AES-256 per NIST PQC guidance).

■ **Key Sizes** Validates RSA keys at 2048-bit minimum. Important: 256-bit ECC keys are correctly identified as strong (equivalent to ~3072-bit RSA) and are NOT flagged. Only RSA keys below 2048 bits are flagged as weak.

■ **PQC Readiness** Assigns a 0-100 readiness score and binary PQC-ready flag. Recommendations generated for each gap identified.

■ **Certificate Info** Extracts TLS certificate subject, issuer, validity period, and algorithm — providing the full cryptographic fingerprint of each HTTPS service.

Score	Status	Recommended Action
85–100	PQC Ready	Maintain posture. Monitor NIST PQC standard updates for migration timeline.
60–84	Transitional	Upgrade to TLS 1.3. Migrate RSA key exchange to ECDHE/X25519 within 12 months.
30–59	At Risk	Immediate TLS upgrade required. Deprecated ciphers and key sizes present.
0–29	Critical	Critical cryptographic failures. Vulnerable to current and future quantum threats.

> *"Organisations that defer post-quantum cryptography migration are not just facing a future risk — they face a present one. Adversaries are collecting encrypted traffic today to decrypt when quantum computers become available. The time to act is now. — GHOST RED Quantum Audit Module"*

SECTION 07 · CAMPAIGN MODE — MULTI-TARGET OPERATIONS

Campaign Mode

Enterprise security teams do not protect a single target — they protect an entire estate. GHOST RED Campaign Mode enables security teams to manage multiple simultaneous scan targets under a single named engagement, with unified reporting across all targets.

A campaign might cover an organisation's full external attack surface: primary web application, staging environment, API gateway, administrative portal, and subsidiary domains — all running concurrently, all feeding into a single consolidated view.

Campaign Capabilities

- **Multi-Target Launch** Add unlimited targets to a campaign. Each target runs a full independent GHOST RED scan with its own findings, chain, and compliance mapping.
- **Unified Dashboard** All campaign targets visible in a single view with aggregate finding counts, scan status, and completion tracking across the estate.
- **Consolidated PDF** Single-click campaign PDF report aggregates findings across all targets — critical findings first, per-target breakdowns, unified compliance mapping.
- **Sector Profiles** Pre-configured sector launch profiles (Banking, Healthcare, Government, Enterprise) apply the right compliance frameworks and threat modelling instantly.
- **Campaign History** All campaigns persist in the GHOST RED database. Re-run campaigns to track security posture improvement over time.

SECTION 08 · REMEDIATION TRACKING & CLOSED-LOOP SECURITY

Remediation Tracking

Discovery without remediation is theatre. GHOST RED closes the loop between finding a vulnerability and proving it is fixed. Every finding automatically creates a remediation ticket in the live Remediation Tracker — connecting your security team, development team, and auditors.

Status	Definition
OPEN	Finding confirmed, no remediation action taken. Requires immediate attention.
ASSIGNED	Assigned to a team member with a due date. Fix in progress.
IN PROGRESS	Active remediation work underway. Ticket owner has acknowledged the finding.
REMEDIATED	Fix deployed. Awaiting verification re-test by GHOST RED.
VERIFIED FIXED	GHOST RED re-scan confirmed the vulnerability is no longer exploitable.
ACCEPTED RISK	Risk accepted by authorised party. Documented for audit trail. Not ignored — recorded.

Compliance Evidence Generation

Every action in the Remediation Tracker is timestamped and attributed. The full audit trail — who was assigned, when the fix was deployed, when GHOST RED verified it — is exportable as compliance evidence. This transforms GHOST RED from a security tool into a compliance documentation engine, dramatically reducing manual effort for ISO 27001, SOC 2, DORA, and NIS2 audit cycles.

SECTION 09 · REPORTING — AI REPORT & PDF EXPORT

Reporting

GHOST RED generates professional reports on demand from every scan and campaign view. Reports are produced in seconds — written at the level of detail that CISOs, auditors, and technical teams actually need.

AI Report

The AI Report is generated by Claude AI against raw scan data. It produces a narrative security assessment covering: executive summary with business impact framing, attack surface analysis, critical finding explanations in plain English, compliance gap analysis, and a prioritised remediation roadmap. Designed to be handed directly to a CISO or board — no interpretation required.

PDF Report

The PDF Report is a professionally branded document including every finding with full technical detail: cover page with engagement statistics, executive summary, findings index, full per-finding detail with evidence, attack chain visualisation, port map, OWASP audit results, compliance mapping, and immediate action plan.

Campaign PDF

Campaign Mode adds a unified multi-target PDF aggregating findings across the entire estate. Critical findings from all targets appear first in a consolidated index, followed by per-target breakdowns and a cross-target compliance summary.

> *"You are not just getting a report. You are getting proof — photographic, technical, and AI-analysed evidence that your environment has been tested by the most advanced autonomous adversary platform available. — Port Cyber Defense"*

SECTION 10 · PLATFORM ARCHITECTURE & SECURITY

Platform Architecture & Security

GHOST RED is deployed as a self-contained platform — on-premise, air-gapped, or private cloud. There is no third-party data sharing. Scan results, findings, and evidence never leave your environment. The platform is designed to the same security standards it audits.

Deployment Options

■ **On-Premise** Full platform deployed within your network. All data stays on your infrastructure. Suitable for classified environments and strict data residency requirements.

■ **Private Cloud** Deployed in your AWS, Azure, or GCP tenancy. You control the infrastructure, data, and access controls.

■ **Air-Gapped** For environments with no internet connectivity. GHOST RED operates fully offline with the rule-based chain engine. AI engine available with local LLM integration on request.

■ **Sovereign (Hosted)** Port Cyber Defense-hosted deployment at ghostred.port-cyber-defense.com — fully managed, Cloudflare-protected, SSL/TLS enforced. Clients access via browser — no installation required.

Platform Security Controls — 23/23 Hardening Checks

Control	Implementation
Authentication	bcrypt password hashing (12 rounds). Session expiry: 8h absolute + 30min idle.
CSRF Protection	Per-request CSRF tokens on all state-changing operations.
Rate Limiting	API: 300 req/60s. Login: 5 attempts/15min. Scan launch: 5/60s.
Input Validation	All targets, usernames, ports, and parameters validated server-side.
Audit Logging	Structured audit log for all security-relevant actions with timestamps.
Path Blocking	Sensitive paths blocked at nginx and application level: .git, .env, /version.
DDoS Protection	Cloudflare WAF + Bot Fight Mode + rate limiting at edge.
Multi-user Isolation	Scan ownership enforced — analysts access only their own scans.
Network Security	Internal services isolated. Only standard HTTP/HTTPS ports exposed externally.
SSL/TLS	End-to-end encryption enforced. Certificates automatically managed and renewed.

SECTION 11 · COMMERCIAL OVERVIEW & INVESTMENT CASE

Commercial Overview

Port Cyber Defense is a specialist cybersecurity company founded by practitioners with OSCP, OSWE, CPTS, and CWEE certifications — the gold standard in offensive security. GHOST RED represents three years of platform development, distilling nation-state attack tradecraft into an autonomous AI product that any security team can operate.

The Market Opportunity

The global penetration testing market is valued at over $1.9 billion and growing at 13% annually. The adjacent vulnerability management market exceeds $15 billion. GHOST RED competes in both — replacing manual penetration tests with continuous autonomous simulation, and replacing passive vulnerability scanners with active exploitation confirmation.

The regulatory driver is accelerating adoption. DORA (effective January 2025) mandates Threat-Led Penetration Testing for EU financial entities. NIS2 requires continuous security monitoring for critical infrastructure operators. ISO 27001:2022 requires ongoing vulnerability management. GHOST RED satisfies all three simultaneously.

Competitive Differentiation

Capability	Traditional Scanner	Annual Pen Test	GHOST RED
Continuous operation	✗	✗	✓
Active exploit confirmation	✗	✓	✓
AI kill chain generation	✗	✗	✓
CISA KEV integration	✗	✗	✓
False positive suppression	✗	✗	✓
OWASP Top 10 web audit	Partial	✓	✓
Quantum readiness audit	✗	Rarely	✓
Compliance auto-mapping	Partial	✗	✓
Closed-loop remediation	✗	✗	✓
Results in under 60 seconds	✗	✗	✓
crt.sh subdomain discovery	✗	✗	✓

Licensing Tiers

Tier	Target	Scans/Month	Targets	Users	Price
Recon	SME security teams	25	10	3	€990/month
Assess	Mid-market enterprises	100	500 hosts	10	€2,500/month
Defend	Enterprise security operations	Unlimited	Unlimited	Unlimited	€8,000/month
Sovereign	MSSP / government / air-gapped	Unlimited	Unlimited	Unlimited	Custom / from €150,000/yr

SECTION 12 · GET STARTED — REQUEST YOUR FREE DEMO

Get Started

Port Cyber Defense engineers will run a live GHOST RED simulation against your environment — or a sandboxed replica — at no cost. You will see real findings within 48 hours. The same results shown in this whitepaper, against your infrastructure.

2	56%	13	<60s	13	8
HIGH Findings Detected	Attack Chain Probability	Web App Issues OWASP Top 10	Time to First Strike	Remediation Items Live	Compliance Frameworks

Free Demo Includes

- ✓ Full attack surface mapping including crt.sh subdomain discovery
- ✓ Live kill chain simulation with AI-generated attack narrative
- ✓ OWASP Top 10 web application audit (13 automated checks)
- ✓ CISA KEV cross-reference — actively exploited CVEs flagged
- ✓ Quantum cryptography readiness assessment
- ✓ Compliance gap analysis — DORA, NIS2, ISO 27001, PCI DSS
- ✓ Analyst verification workflow demonstration
- ✓ Executive PDF report — delivered same day

Contact Port Cyber Defense
info@port-cyber-defense.com · port-cyber-defense.com/ghost-red
OSCP · OSWE · OSED · CPTS · CWEE · CWPE · CAPE

"You are not just getting a report. You are getting proof — the same proof shown in this document — that your environment has been tested by the most advanced autonomous adversary platform available. Book your demo today."

GHOST RED v2.5.0 · Port Cyber Defense · port-cyber-defense.com/ghost-red · March 2026