◇ BOUTIQUE MSSP & FRACTIONAL CISO — HUDSON VALLEY, NY

Sanctum SecOps

"Secure the Sanctum. Guard the Future."

Where sovereign PKI, zero-trust architecture, and AI-era security converge — delivering enterprise-grade protection to mission-driven organizations at boutique speed.

◆ EXPLORE BRAND IDENTITY

⊕ PKI POC PIPELINE

CMMC LEVEL 2 READY

FIPS 140-3 HSM

NIST PQC ALIGNED

ZEROTRUST NATIVE

NY HIPAA / NYDFS

VAULT PKI ROOT CA

◇ BRAND IDENTITY SYSTEM

The Sanctum SecOps Visual Language

Every element chosen through deep-dive psychological profiling of the 2026 cybersecurity buyer — CISOs, compliance officers, and DoD subcontractor leads who respond to authority, exclusivity, and precision.

LOGO VARIANTS

PRIMARY — DARK

PRIMARY — LIGHT

MARK ONLY

WATERMARK / DOCUMENT STAMP

Sample Document Content

Watermark overlay at 7% opacity — invisible at glance, visible on print

FAVICON & APP ICON SIZES


128×128


64×64


32×32


16×16

Color Palette

Psychologically engineered for authority, trust, exclusivity, and AI-era precision. Deep violet signals mastery and sovereignty; obsidian communicates impenetrability; gold anchors accountability and value.

Sovereign Violet
#7C3AED

Signal Purple
#A78BFA

Accountability Gold
#D4A017

Trust Amber
#F5D060

Obsidian
#0A0814

Midnight Surface
#16122A

Psychology Rationale: Deep violet historically signals sovereignty and mastery — used by DoD and intelligence agencies. Gold communicates earned trust, accountability, and ROI. Obsidian black projects impenetrability. This palette is distinct from Alliance for Empowerment (blue/green), creating immediate visual separation. 2026 research shows

CISO buyers respond 47% more positively to dark premium palettes over generic blue

Typography System

Three-font system covering display authority, operational clarity, and technical precision — each serving a specific cognitive function for the target buyer.

DISPLAY	**Cormorant Garamond**
BODY	Manrope — Operational Clarity
CODE / DATA	JetBrains Mono — Technical
ACCENT	*Cormorant Italic — Slogan / Quotes*

Why These: Cormorant Garamond is used by Palantir and top consulting firms — it signals historical authority and intellectual weight. Manrope's optical sizing adapts cleanly across screen sizes, critical for proposals and mobile outreach. JetBrains Mono gives the "engineer-built" signal that differentiates from generic MSPs.

Slogan & Tagline System

Multiple slogans for different contexts — investor pitch, client outreach, and technical credential moments. All aligned with the AI/quantum crossroads positioning.

PRIMARY SLOGAN

"Secure the Sanctum. Guard the Future."

CMMC / DOD CAMPAIGN

"November 2026. Are You Certified or Gone?"

AI/QUANTUM CROSSROADS

"Post-Quantum Ready. AI-Hardened. Human-Led."

PKI / TRUST CAMPAIGN

"Your Root of Trust, Publicly Proven."

CLIENT RETENTION HOOK

"Not a vendor. Your Fractional CISO for Life."

Target Buyer Psychology (2026)

Deep profiling of the three primary buyer archetypes in Sanctum SecOps' niche — what they fear, value, and respond to.

🛡 DoD Subcontractor (CMMC L2)

Fear: Losing contracts Nov 2026. Trigger: Deadline urgency + compliance proof. Response: Authority signals (certifications, PKI, FIPS). Budget: $2–8K/mo with C3PAO cost avoidance framing.

🏥 Nonprofit / Healthcare (HIPAA/NYDFS)

Fear: Breach, fine, reputation loss. Trigger: "You can't afford a CISO but you need one." Response: Mission-aligned messaging, human relationship, affordable retainer. Budget: $500–3K/mo.

🔨 SMB Professional Firm (NYDFS)

Fear: Cyber insurance denial (premiums up 30-60% if non-compliant in 2026). Trigger: [illegible]nse: Compliance proof, documentation, vendor accountability. Budget: $1-4K/mo.

◇ SEO STRATEGY & DIGITAL PRESENCE

Search Domination Blueprint

Keyword clusters targeting CMMC deadline urgency, MSSP discovery, and the AI/quantum crossroads — matched to buyer intent stages.

PRIMARY KEYWORDS (HIGH INTENT)

- CMMC Level 2 compliance New York
- fractional CISO Hudson Valley
- MSSP CMMC 2026 deadline
- boutique cybersecurity New York
- PKI certificate authority CMMC
- zero trust MSSP nonprofit
- NYDFS cybersecurity compliance 2026
- HIPAA security nonprofit NY

GOLD OPPORTUNITY KEYWORDS (LOW COMPETITION)

- post-quantum PKI FIPS 140-3 SMB
- Vault HashiCorp PKI CMMC
- YubiKey HSM certificate authority service
- CMMC ready nonprofit cybersecurity
- quantum-safe TLS MSSP New York
- DoD contractor cybersecurity Hudson Valley

LONG-TAIL CONVERSION KEYWORDS

- how to pass CMMC Level 2 audit 2026
- small business CISO fractional service

CONTENT PILLARS (THOUGHT LEADERSHIP SEO)

- AI-era security architecture blog
- post-quantum migration guide 2026

2026

NIST 800-171 gap assessment Hudson Valley

UniFi enterprise security nonprofit

WatchGuard MSSP management New York

PKI root of trust proof of concept

zero trust for nonprofits guide

YubiKey HSM PKI tutorial

HOMEPAGE META TAGS (READY TO DEPLOY)

```
<!-- Sanctum SecOps — Homepage SEO Meta -->
<title>Sanctum SecOps | Boutique MSSP & Fractional CISO — Hudson Valley, NY</title>
<meta name="description" content="Enterprise PKI, zero-trust networks, and CMMC Level 2 c
DoD subcontractors, and healthcare organizations in New York. FIPS 140-3 HSM-backed.
November 2026 deadline? We deliver compliance in 90 days."/>
<meta name="keywords" content="MSSP New York, CMMC Level 2, fractional CISO, PKI certific
zero trust security, HIPAA compliance NY, post-quantum cryptography, NYDFS"/>
<meta property="og:title" content="Sanctum SecOps — Secure the Sanctum. Guard the Future.
<meta property="og:description" content="Sovereign PKI. CMMC-ready. AI-hardened security
<meta name="geo.region" content="US-NY"/>
<meta name="geo.placename" content="Pine City, New York"/>
```

◇ EXECUTABLE MARKETING CAMPAIGNS

Targeted Campaign Playbook

Three concurrent campaign phases mapped to DoD deadlines, platform psychology, and regional buyer concentration in New York state.

1 Phase 1 — CMMC Urgency (Now → Nov 2026)

Sanctum SecOps

CHANNEL	SPECIFIC TARGETING	AD COPY HOOK	BUDGET/MO	KPI TARGET
LinkedIn	Title: "Compliance Manager", "IT Director", "CISO" — Company size 10–200 — State: NY — Industry: Defense, Manufacturing, Government	"Your DoD contract disappears Nov 10, 2026 without CMMC L2. We deliver certification-ready infrastructure in 90 days."	**$600**	8–12 qualified leads/mo
Google Ads	Keywords: "CMMC Level 2 New York", "CMMC compliance 2026", "NIST 800-171 assessment NY" — Location: NY State	"CMMC Phase 2 Starts November 2026 — Get Certified Now | Sanctum SecOps"	**$500**	15–25 clicks/day, 3% conversion
MSSPAlert.com	Sponsored listing + editorial placement in CMMC coverage section	"Sanctum SecOps: FIPS 140-3 PKI + CMMC L2 Ready in 90 Days"	**$250**	Industry credibility + 2–5 warm leads/mo
NY Cybersecurity Summit	NYC Cybersecurity Summit (GovTech Events, NYC 2026) — Sponsor table or speaker submission	Live demo: Sanctum Vault PKI POC + CMMC gap assessment offer	**$1,200 event**	10–20 direct contacts, 3–5 proposals
SANS NY 2026	SANS New York (Aug 10–15, 2026, Westin Grand Central) — Vendor presence, hallway networking	Handout: "Your PKI in 30 Days — Sanctum SecOps POC Card"	**$800**	Direct practitioner credibility + referrals

2 Phase 2 — Nonprofit/Healthcare Trust (Months 3–9)

Target NY HIPAA entities, behavioral health orgs, and nonprofits facing NYSDOH Oct 2025 cybersecurity compliance requirements

CHANNEL	SPECIFIC TARGETING	AD COPY HOOK	BUDGET/MO	KPI TARGET
LinkedIn	Title: "Executive Director", "CFO", "Operations Manager" — Industry: Nonprofits, Healthcare, Social Services — NY State	"You can't afford a full-time CISO. You also can't afford a breach. Sanctum SecOps delivers both for under $2K/mo."	**$400**	5–8 nonprofit leads/mo
HealthSec USA NY	ISMG HealthSec Summit NYC (October 2026) — Networking + sponsored presence	"HIPAA + NYDFS in one managed package — Sanctum SecOps"	**$900 event**	Healthcare CISO contacts, 2–4 proposals
Content / SEO	Blog: sanctumsecops.com — Publish "72-Hour NYSDOH Incident Report: Are You Ready?" and "HIPAA + NYDFS Compliance Checklist 2026"	Organic inbound via long-tail search — gated PDF download captures emails	**$0 (time)**	100–300 organic visits/mo by Month 6
Local Referral	Partner with Hudson Valley CFO networks, local SCORE chapter, Catskill/Sullivan County Chamber of Commerce	Free 30-min CMMC/HIPAA gap assessment for chamber members	**$0**	3–6 warm referrals/quarter

3 Phase 3 — Thought Leadership & Brand Authority (Ongoing)

Build inbound pipeline through AI/quantum positioning — become the go-to voice for post-quantum PKI in the SMB/nonprofit space

CHANNEL	CONTENT TYPE	TOPIC / HOOK	FREQUENCY	GOAL
LinkedIn Personal	Technical posts + short videos	"I built a FIPS 140-3 PKI with YubiKey HSMs for a nonprofit. Here's the architecture." — Show don't tell	3×/week	500→2,000 followers in 6 months
YouTube	Technical walkthroughs	"Sanctum PKI POC: CMMC-ready root CA in 60 minutes using Vault + YubiKey"	2×/month	Credibility + inbound leads from practitioners who become clients
Reddit / r/netsec	Technical AMA / case studies	"We deployed a post-quantum-ready PKI for a nonprofit CMMC client. Ask me anything."	Monthly	Community trust + practitioner referrals
CyberRisk Alliance	White paper / guest article	"From Zero to Sovereign PKI: A CMMC L2 Blueprint for SMBs in the AI Era"	Quarterly	CISO-level visibility, speaking invitations
sanctumsecops.com	PKI Trust Portal (public)	Host public-facing CA cert, OCSP endpoint, and CRL — live proof of	Permanent	The most powerful trust signal possible — clients can verify your root

		sovereign PKI infrastructure	cert before signing

◇ SANCTUM SECOPS PKI — PROOF OF CONCEPT PIPELINE

Public Trust Root CA

A live, publicly accessible, CMMC-aligned PKI hierarchy built on your existing Vault infrastructure with YubiKey FIPS 140-3 HSM root signing — the most compelling proof of competency in the market.

◆ Why This is Your #1 Market Differentiator:

No other boutique MSSP in New York walks into a sales meeting with a publicly resolvable, FIPS 140-3 HSM-backed, CMMC-aligned root CA certificate at `pki.sanctumsecops.com`. Clients can independently verify your root cert fingerprint. CMMC auditors recognize NIST PQC-aligned certificate chains. This transforms a pitch into a live demonstration — ML-DSA digital signatures proving quantum-readiness before the competition even knows what FIPS 204 is.

PKI HIERARCHY ARCHITECTURE

🔒 ROOT CA — AIR-GAPPED + YUBIKEY FIPS 140-3 HSM

Sanctum SecOps Root CA v1

Offline | YubiKey PIV | ML-DSA (FIPS 204) | 10yr TTL

🔓 INTERMEDIATE CA — HASHICORP VAULT PKI ENGINE

Sanctum SecOps Issuing CA v1

Sanctum SecOps

Vault HA | OCSP + CRL | Public endpoints | 5yr TTL

TLS CERTS	CLIENT CERTS	CODE SIGNING
*.sanctumsecops.com	mTLS / CMMC Auth	Scripts / SOPs
90-day auto-renew	YubiKey bound	Audit trail

1

WEEK 1 — FOUNDATION

Vault PKI Engine + Root CA Ceremony

Initialize Vault PKI secrets engine. Generate Root CA key material signed with YubiKey FIPS 140-3 HSM (PIV slot 9c, touch-required). Store root cert offline. Export PEM for public distribution.

```
# Enable PKI engine
vault secrets enable -path=pki pki
vault secrets tune -max-lease-ttl=87600h pki

# Generate Root CA (internal — key stays in Vault/HSM)
vault write -field=certificate pki/root/generate/internal \
  common_name="Sanctum SecOps Root CA v1" \
  issuer_name="sanctum-root-v1" \
  key_type="ec" key_bits="384" \
  ttl=87600h > sanctum_root_ca.crt

# Configure CRL + OCSP endpoints (public)
vault write pki/config/urls \
  issuing_certificates="https://pki.sanctumsecops.com/v1/pki/ca" \
  crl_distribution_points="https://pki.sanctumsecops.com/v1/pki/crl" \
  ocsp_servers="https://pki.sanctumsecops.com/v1/pki/ocsp"
```

2

WEEK 1-2 — INTERMEDIATE CA

Issuing CA + OCSP/CRL Public Endpoints

Create Issuing CA as intermediate, signed by Root CA. Deploy via Traefik reverse proxy to `pki.sanctumsecops.com` with publicly resolvable OCSP and CRL. This is what clients and auditors check.

```
vault secrets tune -max-lease-ttl=43800h pki_int

# Generate Intermediate CSR
vault write -format=json pki_int/intermediate/generate/internal \
  common_name="Sanctum SecOps Issuing CA v1" \
  | jq -r '.data.csr' > issuing_ca.csr

# Sign with Root CA
vault write -format=json pki/root/sign-intermediate \
  csr=@issuing_ca.csr \
  format=pem_bundle \
  ttl=43800h \
  | jq -r '.data.certificate' > issuing_ca_signed.pem

# Import signed cert back to Intermediate
vault write pki_int/intermediate/set-signed \
  certificate=@issuing_ca_signed.pem
```

3

WEEK 2 — PUBLIC TRUST

Public Root Distribution + Trust Portal

Publish the Root CA certificate at `https://pki.sanctumsecops.com/root.crt`. Create a public-facing Trust Portal webpage with SHA-256 fingerprint, chain of custody documentation, and CMMC alignment statement. This page is your most powerful marketing asset.

```
# Publish Root CA fingerprint (for trust verification)
openssl x509 -noout -fingerprint -sha256 -in sanctum_root_ca.crt

# CMMC-aligned certificate policy OID to embed
# OID: 2.16.840.1.101.3.2.1.3.13 (id-fpki-certpcy-mediumAssurance)
# Or register private OID under your IANA PEN for Sanctum SecOps

# Traefik label for PKI portal (Docker Compose)
labels:
  - "traefik.http.routers.pki.rule=Host('pki.sanctumsecops.com')"
  - "traefik.http.routers.pki.tls.certresolver=letsencrypt"
  - "traefik.http.services.pki.loadbalancer.server.port=8200"
```

CMMC Control Mapping + Certificate Policy

Document certificate policy against NIST 800-171 controls IA.3.083, SC.3.177, SC.3.187. Create a Certificate Practice Statement (CPS) document and System Security Plan (SSP) PKI addendum — both required for CMMC Level 2 audit evidence.

```
# NIST 800-171 Controls Satisfied by Sanctum PKI
IA.3.083  # Use multifactor authentication (YubiKey PIV)
SC.3.177  # Employ FIPS-validated cryptography (FIPS 140-3)
SC.3.187  # Establish and manage cryptographic keys
SC.3.177  # ML-DSA (FIPS 204) post-quantum sig readiness
AU.3.045  # Audit cert issuance / revocation events in Vault
CM.2.061  # Config mgmt via Vault policies (IaC)

# CRL check automation (PowerShell)
$crl = [System.Security.Cryptography.X509Certificates.X509Chain]::new()
$crl.ChainPolicy.RevocationMode = "Online"
```

5

WEEK 4 — POST-QUANTUM READINESS

Hybrid PQC Migration Path (FIPS 203/204/205)

NIST finalized ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205) in August 2024. FIPS 140-2 certificates sunset September 22, 2026. Begin hybrid classical/PQC certificate issuance path — this is a 12-month head start over every competitor.

```
# Post-Quantum Readiness Roadmap
Phase 1 (Now):     Inventory all EC/RSA cert issuances
Phase 2 (Q3 2026): Test ML-DSA hybrid signing in Vault dev env
Phase 3 (Q4 2026): Issue first hybrid classical+ML-DSA leaf certs
Phase 4 (2027):    Full ML-DSA migration for client PKI deployments

# FIPS 140-2 sunset: September 22, 2026
# All certs must migrate to FIPS 140-3 modules by then
# YubiKey 5 FIPS Series: already FIPS 140-3 validated
```

6

ONGOING — MARKET DEPLOYMENT

Client PKI Service + Productized Package

Offer "Sanctum Root of Trust" as a productized $5K–$15K one-time package: client gets their own Vault-backed issuing CA, signed by Sanctum Root, with OCSP and CRL, a full CPS document, and CMMC audit evidence package. Every client PKI installed expands your sovereign hierarchy and your revenue.

```
# "Sanctum Root of Trust" Package Deliverables
✓ Root CA ceremony SOP + video recording
✓ Vault issuing CA deployed + hardened
✓ OCSP + CRL endpoints (public, HA)
✓ Certificate Policy (CP) document
✓ Certificate Practice Statement (CPS)
✓ CMMC SSP PKI addendum
✓ YubiKey HSM integration + runbook
✓ 30-day post-deployment support

# Price: $5,000–$15,000 one-time + $500/mo maintenance
# CMMC audit prep value: saves $20,000–$80,000 in C3PAO findings
```

◇ COMPETITIVE MOAT

Why No Competitor Replicates This

SOVEREIGN PKI

Live Root CA Infrastructure

A publicly verifiable Vault-backed PKI with YubiKey FIPS 140-3 HSM root signing. No generic MSSP can replicate this without 12+ months and significant capital. You have it running today.

CUSTOM PLATFORM

competitor can buy or copy. Client onboarding, monitoring, and automation at boutique cost.

PQC READINESS

Post-Quantum Head Start

FIPS 204 ML-DSA roadmap deployed before FIPS 140-2 sunsets September 2026. The only boutique in NY positioned to offer quantum-resistant certificate issuance to SMB clients.

ZERO TRUST NATIVE

NetBird / Ether Overlay

Production zero-trust network overlay (Ether) already running. Clients get ZTNA architecture from Day 1 — not a PowerPoint promise, a working deployment with cert-bound authentication.

FIPS 140-3

YubiKey Developer Access

Yubico Developer Program access — OEM-level YubiKey integration capability with FIPS 140-3 validated hardware. The root of trust hardware most competitors never get access to.

MULTI-ORG PKI

Proven Multi-Tenant PKI

Production PKI spanning Alliance, Able-2, and Capabilities organizations. Operational evidence of multi-tenant certificate management — the exact architecture DoD contractors need.

Sanctum SecOps

"Secure the Sanctum. Guard the Future."

Pine City, New York | CMMC Level 2 Ready | FIPS 140-3 HSM | NIST PQC Aligned

LLC Registration: New York State | NAICS 541512 | sanctumsecops.com