KMSEC (PTY) LTD

OMG PRIVATE PRACTICE BUSINESS WEEKEND 2026

Security Optics for Eye Doctors & Medical Professionals

War stories, embedded device hacks, and practical operational security for modern clinical practice



Who Am I?

Keith Makan

MSc, PhD Candidate, and offensive security researcher specializing in binary analysis, secure architecture, and deep technical risk discovery.

Global Experience

Internationally published author and speaker bringing elite vulnerability discovery experience from engagements across the US, Europe, and China.

About KMSEC (PTY) LTD Consultancy

Established 2021

Cape Town boutique firm focusing on highly technical offensive security and architecture assurance.

Research-Driven

Bespoke binary analysis and vulnerability frameworks uncovering edge-case risks generic scanners miss.

Regulatory Alignment

Bridging strict medical and financial mandates (POPIA, HIPAA, FSCA) with secure clinical delivery.

Comprehensive Agenda

PART I

Threat Evolution & History

Macro breach trends and systemic failures: Change Healthcare, Vastaamo, Düsseldorf, and Eye Care Leaders.

PART II

Root Failures & Analysis

Anatomy of a private practice from a hacker's map, why MedSec is hard, POPIA pressure, and root failures.

PART III

Emerging Challenges

AI-adaptive zero-days, 2027 post-quantum mandates, and IoMT device lifecycle blindspots.

PART IV

Pragmatic Practice Defense

Mapping clinical attack surfaces, enforcing baselines, and continuous threat assurance.

PART I

THREAT EVOLUTION & HISTORY

Global Medical Breaches: The Foundation (2009–2019)

A decade of accelerating hacking incidents and massive record exposures set the stage for modern clinical extortion

CHART 01: INCIDENT VELOCITY (2009–2019)

Hacking Overtakes Insider Disclosure (510+ Breaches/Yr)

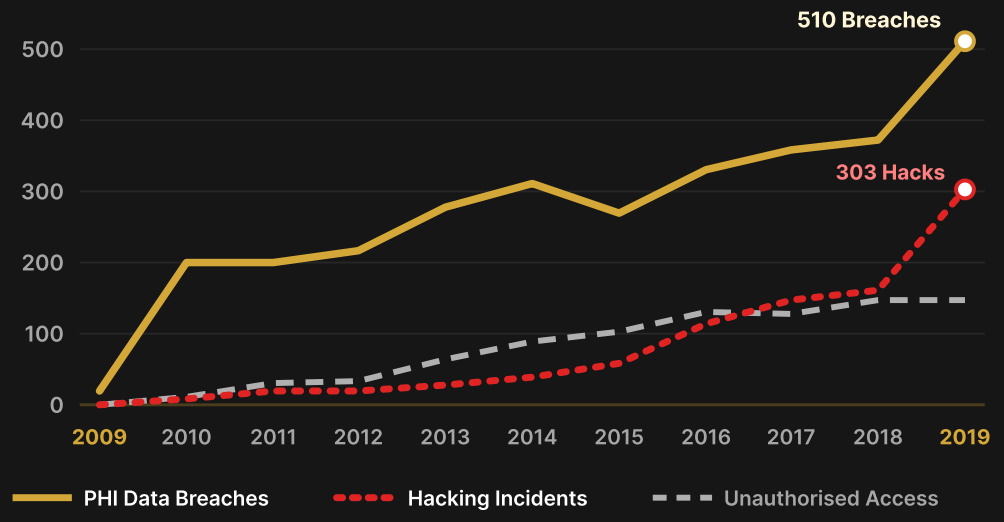
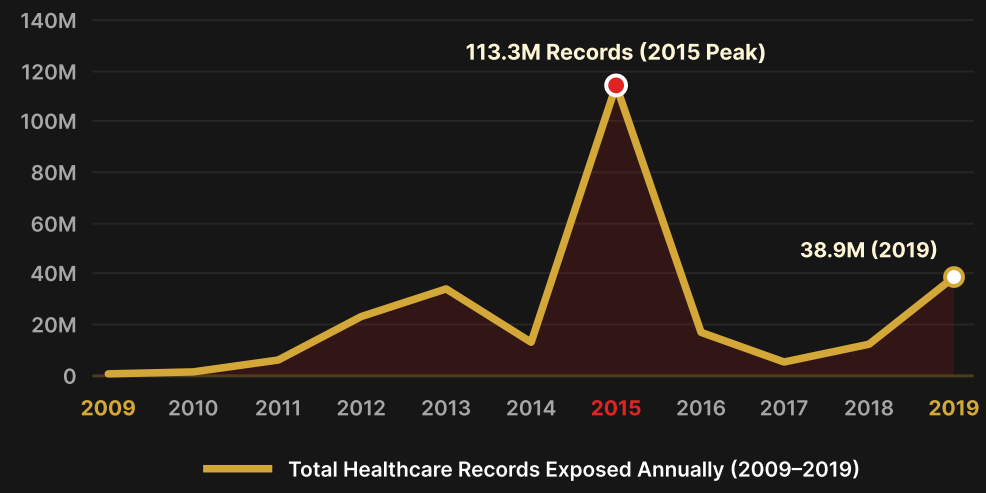


CHART 02: RECORD EXPOSURE SCALE (2009–2019)

Mega-Breach Spike (113M+ in 2015) & 2019 Resurgence



Global History of Medical Breaches (2020–2026)

2020

Düsseldorf & Vastaamo

Unpatched Citrix ransomware causes first recorded cyberattack fatality; Vastaamo therapy DB leaked for patient extortion.

2021–2022

Eye Care Leaders

Cloud myCare EHR ransomware cripples 40+ ophthalmology clinics and exposes 3.6M patient records.

2023–2024

HCA & Change Healthcare

11.2M records stolen at HCA; national clearinghouse crippled overnight via un-MFA'd Citrix portal.

2025–2026

TriZetto Cascade

Employee credential theft via infostealers triggers cascading partner shutdowns and clinic outages.

2020: The Year of Extortion & Clinical Disruption

Blackbaud, University Hospital of Düsseldorf, & Vastaamo Breaches

May 2020 — Sep–Oct 2020 — Late 2020

May 2020

Blackbaud Ransomware

Health group “TaskForce” compromised via third-party ransomware attack, exposing high-value donor and patient DBs.

Sep–Oct 2020

Düsseldorf & Vastaamo

Unpatched Citrix bug forces Düsseldorf ER shutdown and first cyberattack death; Vastaamo therapy notes extorted.

Late 2020

The Paradigm Shift

Adversaries realize medical attacks carry extreme psychological extortion leverage and life-or-death clinical impact.

2021–2022: EMR Supply Chain Fractures

Eye Care Leaders (ECL) Ransomware & Cascading Ophthalmology Practice Outages

Dec 4, 2021

Dec 2021 – Feb 2022

March – May 2022

Dec 4, 2021: Intrusion

Cloud EMR Strike

Ransomware actors breached Eye Care Leaders' myCare EHR platform, encrypting databases and exfiltrating patient records.

Dec 2021 – Feb 2022

Practice Paralysis

Ophthalmology clinics suffered weeks of EHR outages, losing access to surgical schedules, OCT imaging, and billing.

March – May 2022

3.6M+ Records Exposed

40+ eye clinics filed HHS OCR disclosures (Texas Tech: 1.29M; Wolfe Clinic: 542k)—driving ECL into Chapter 11 bankruptcy.

2023–2024: The Clearinghouse Crises

HCA, 23andMe, & Change Healthcare

HCA Breach (2023) — 23andMe Stuffing — Change Healthcare (2024)

2023

Massive Scale Dumps

11.2M records stolen from HCA; credential stuffing leverages reused passwords against 23andMe genetic profiles.

Early 2024

Clearinghouse Strike

Ransomware targets Change Healthcare via an un-MFA'd Citrix portal, locking core clinical and billing systems.

Feb–March 2024

Systemic Paralysis

Prescription and claims networks crippled nationwide, forcing manual offline fallbacks for weeks.

2025–2026: Cascading Infostealers

TriZetto Provider Solutions & Beyond

Infostealer Infection — Ransomware Drop — Partner Cascade

Stage 01: Infostealers

The Infostealer Vector

Employee devices infected by stealer malware designed to harvest active browser session cookies and credentials.

Stage 02: Affiliate Drop

Affiliate Handoff

Initial access is rapidly brokered to ransomware syndicates for aggressive lateral movement and deployment.

Stage 03: Cascade

Cascading Failure

The breach blasts through partner trusts, paralyzing deeply integrated, dependent third-party clinics.

The Operational Catastrophe: Change Healthcare (2024)

Incident Overview: In February 2024, ransomware actors infiltrated Change Healthcare—processing 15 billion clinical and billing transactions annually—using stolen credentials on a remote Citrix portal without MFA. The attack forced core clearinghouse systems offline for weeks, halting prescriptions, eligibility checks, and practice cash flow nationwide.

The Security Failure

Stolen credentials on a legacy Citrix portal lacking multi-factor authentication (MFA) enabled lateral movement across core clearinghouse infrastructure.

Clinical Impact

Prescription filling, insurance verification, and doctor reimbursements ground to a halt nationwide overnight, forcing manual paper fallbacks.

The Lesson

Local clinic defense is useless if upstream clearinghouses and billing supply chains are compromised without offline continuity plans.

The Extortion Nightmare: Vastaamo Psychotherapy (2020)

Incident Overview: In 2020, attackers exfiltrated the patient database of Finland's Vastaamo Psychotherapy Center (40,000+ patients) after it was left exposed online without root authentication or firewall protection. When the clinic failed to pay, attackers emailed individual patients directly—threatening to publish their intimate therapy notes unless each paid a personal ransom.

The Security Failure

Clinical database left exposed directly to the internet due to misconfigured access controls, missing authentication, and absent firewall rules.

Clinical Impact

Hackers bypassed the clinic to blackmail thousands of vulnerable patients and minors directly using confidential psychotherapy session transcripts.

The Lesson

Medical data is deeply personal; a clinical leak represents an irreversible, catastrophic psychological violation of patient safety and trust.

University Hospital of Düsseldorf Ransomware Attack (2020)

Incident Overview: In September 2020, ransomware exploited an unpatched Citrix remote-access bug (CVE-2019-19781) at the University Hospital of Düsseldorf in Germany, locking 30 internal servers. Forced to close emergency admissions, the hospital rerouted an ambulance carrying a 78-year-old woman with an aortic aneurysm 20 km away to Wuppertal. The delay resulted in her death—the **first human death globally attributed to a cyberattack**.

The Security Failure

Ransomware exploited a known Citrix ADC / Gateway VPN vulnerability (CVE-2019-19781) left unpatched for months, encrypting 30 clinical servers.

Clinical Impact

Emergency care collapsed; an ambulance carrying a critically ill 78-year-old woman with a ruptured aneurysm was turned away and rerouted 20 km.

The Lesson

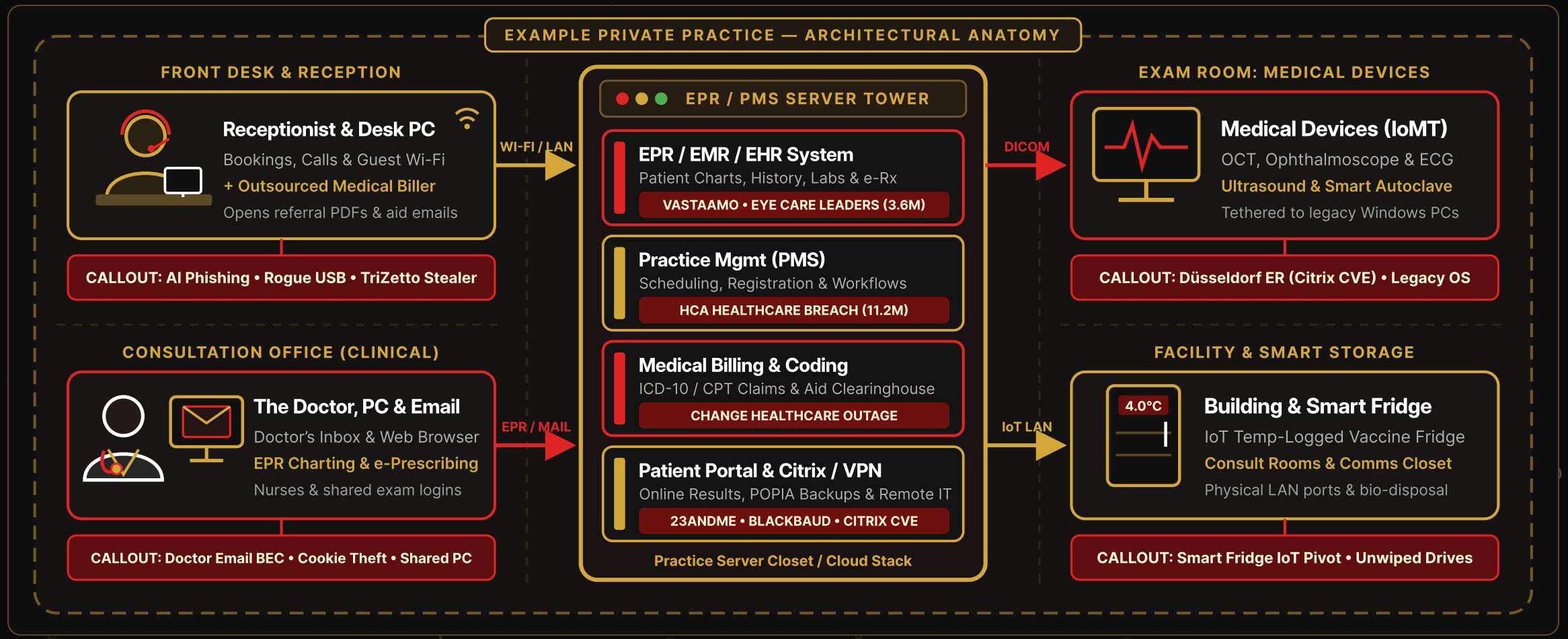
The treatment delay caused the first fatality tied directly to a cyberattack—proving remote-access edge patching is life-safety critical.

PART II

ROOT FAILURES & ANALYSIS

Anatomy of a Private Medical Practice: A Hacker's Map

Simplified practice architecture showing the Receptionist, Doctor & Email, EPR/PMS Tower, Devices, and Breach Callouts



Practice Anatomy: The 4 Core Pillars & Breach Callouts

How each pillar of a modern private medical practice maps to real-world cyber incidents

1. DIGITAL ECOSYSTEM

EPR, PMS & Billing Tower

Components: EPR/EMR charts, PMS scheduling, ICD-10 billing switch, Patient Portal & POPIA backups.

Breach Callouts: Vastaamo, Eye Care Leaders (3.6M), Change Healthcare & 23andMe.

2. STAFFING & HR

Doctor, Reception & Biller

Components: Doctor's PC & email, nurses (shared logins), receptionist desk, and outsourced billers.

Breach Callouts: TriZetto (infostealer cookies), Blackbaud & AI spear-phishing.

3. MEDICAL DEVICES

Diagnostic & Clinical Gear

Components: OCT scanners, ophthalmoscopes, ECG, ultrasound, autoclaves & legacy capture PCs.

Breach Callouts: Düsseldorf Hospital (Citrix CVE → ER lockout) & unwiped drives.

4. PHYSICAL FACILITY

Rooms & Smart Storage

Components: Reception/waiting Wi-Fi, consult rooms, smart vaccine fridges (IoT temp logs) & disposal.

Breach Callouts: Rogue front-desk USBs, open LAN ports & IoT fridge sensors.

Why is Medical Security Hard?

The intersection of clinical life-safety, legacy hardware, and strict statutory enforcement

CLINICAL MANDATE

Continuity & Privacy

Zero tolerance for clinical downtime combined with high-value patient records prized by extortionists.

HARDWARE REALITY

IoMT Ecosystems

Diagnostic devices operating with high clinical precision but running legacy OS builds with low fault tolerance.

THREAT ASYMMETRY

Regulatory Velocity

Static compliance standards cannot evolve as fast as nimble cybercrime syndicates and automated exploit brokers.

STATUTORY MANDATE

Compliance Pressure

POPIA Special Health Information rules, 2026 Health Regs, NHA s17 criminal liability, and HPCSA rules carry R10M fines.

What Organizations Got Wrong

Basic Control Failures

Missing MFA on remote portals, default administrative passwords, and delayed edge patching.

Blind Vendor Trust

Assuming third-party EMR and billing software vendors maintain rigorous security without auditing.

Human Factor Blindspots

Failing to defend staff against modern infostealers and AI-crafted spear-phishing campaigns.

PART III

EMERGING CHALLENGES

Emerging Challenges in MedSec

Three disruptive vectors reshaping clinical operational security and compliance requirements

CHALLENGE 01

AI-Adaptive Attacks

Automated vulnerability discovery and sub-24h zero-day weaponization across web stacks, plus deepfake phishing.

CHALLENGE 02

Post-Quantum Readiness

NIST 2027/FIPS compliance shifts and “Store Now, Decrypt Later” harvesting of long-lived patient records.

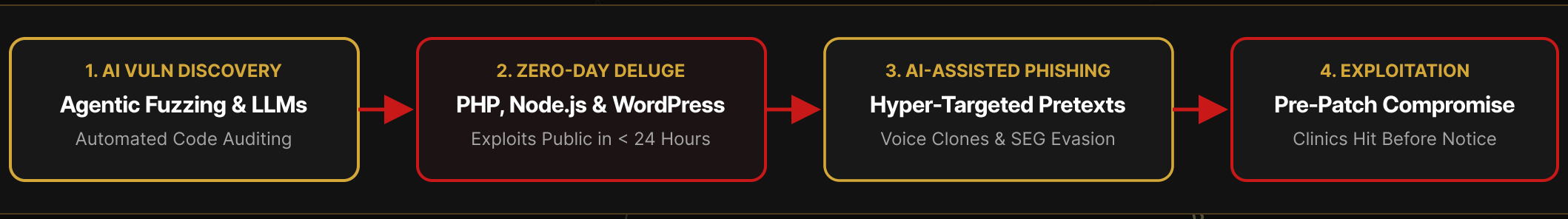
CHALLENGE 03

IoMT Device Lifecycle

Unencrypted device disposal, firmware patching vacuums, vendor opacity, and blocked security testing.

AI-Adaptive Attacks & Accelerated 0-Day Velocity

Autonomous fuzzing, polymorphic malware, and zero-days dropping before teams can patch



PREVALENCE VECTOR 01: SOCIAL ENGINEERING

Hyper-Realistic AI Phishing & Voice Clones

Flawless contextual spear-phishing and real-time voice cloning impersonating referring doctors or billing managers to bypass email gateways.

PREVALENCE VECTOR 02: ENDPOINT EVASION

AI-Generated Polymorphic Malware

Payloads dynamically mutating code structures and API calls at runtime to defeat heuristic EDR detection on clinical workstations.

PREVALENCE VECTOR 03: VULNERABILITY DELUGE

Automated 0-Days in PHP, Node.js & WordPress

AI models uncover critical bugs across PHP runtimes, Node.js packages, and WordPress booking plugins faster than clinics can patch or threat-model.

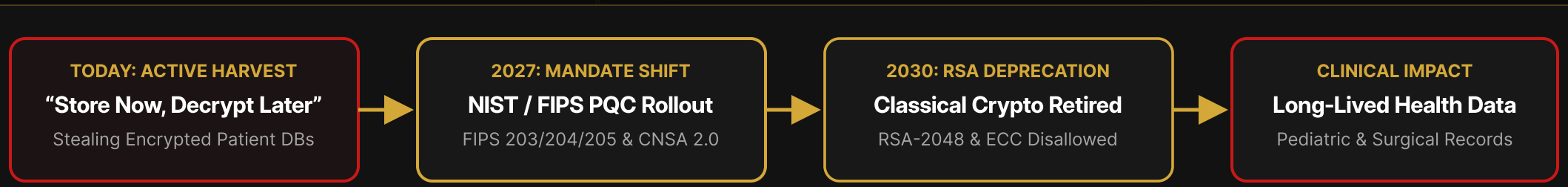
CLINICAL PRACTICE DEFENSE

Closing the Patch Latency Window

Defenses require phishing-resistant FIDO2 MFA keys, managed Web Application Firewalls (WAF), and automated 24-hour virtual patching.

Post-Quantum Readiness & The 2027 Compliance Shift

Why 2027 NIST/FIPS mandates and “Store Now, Decrypt Later” make quantum defense urgent today



REGULATORY TIMELINE: 2027 MANDATE

NIST FIPS & CNSA 2.0 Compliance Deadlines

NIST finalized FIPS 203, 204, and 205 PQC standards; NSA CNSA 2.0 mandates quantum-resistant upgrades for software and cloud vendors starting in 2027.

IMMEDIATE THREAT VECTOR

“Store Now, Decrypt Later” (SNDL)

Syndicates harvest encrypted clinical databases and retinal imaging archives today to decrypt once quantum hardware matures.

MEDICAL RETENTION DISPARITY

Record Longevity vs. Crypto Expiry

HPCSA Booklet 9 requires keeping patient records 6+ years (and pediatric records to age 21)—outliving classical RSA-2048 security.

PRACTICE ACTION

Cryptographic Agility & Vendor Roadmaps

Audit external VPN/TLS gateways and require hybrid post-quantum encryption roadmaps from cloud EMR, PACS, and clearinghouse vendors.

IoMT Device Lifecycle & Vendor Transparency Gaps

Secure disposal risks, update vacuums, and third-party opacity across diagnostic hardware

1. PROCUREMENT OPACITY
No SBOM / No Certs
Zero Security Verification

→

2. THE UPDATE VACUUM
Obsolete Embedded OS
Patches Blocked by Recertification

→

3. VENDOR GOVERNANCE
Who Manages Support?
Unmonitored Remote Backdoors

→

4. RETIREMENT RISKS
Unencrypted Disposal
Recoverable Scans on Drives

LIFECYCLE CHALLENGE 01: DISPOSAL

Secure Disposal & Decommissioning

Trading in or retiring OCT scanners and fundus cameras with unencrypted drives leaves gigabytes of patient scans recoverable on resale markets.

LIFECYCLE CHALLENGE 02: MAINTENANCE

The Firmware & Patching Vacuum

Diagnostic units run legacy Windows/Linux builds where OS updates void clinical calibration or stall for months awaiting vendor recertification.

LIFECYCLE CHALLENGE 03: GOVERNANCE

Who Manages the Vendor Relationship?

Support is often left to third-party technicians using persistent, unmonitored AnyDesk/TeamViewer logins with zero POPIA operator agreements.

LIFECYCLE CHALLENGE 04: ASSURANCE

Zero Transparency or Security Testing Access

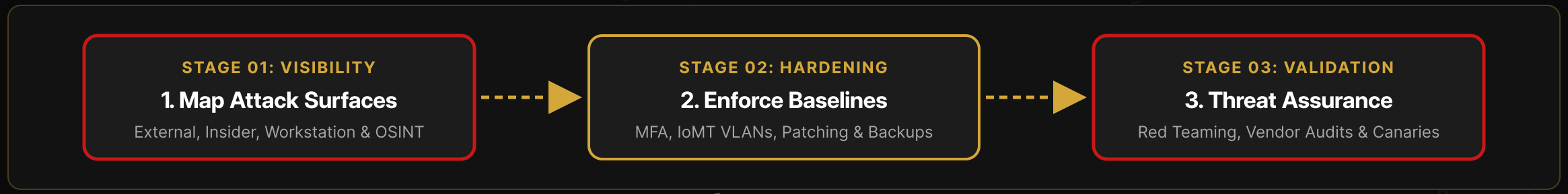
Practices lack firmware transparency, Software Bills of Materials (SBOMs), or access to independent penetration test certifications prior to purchase.

PART IV

PRAGMATIC PRACTICE DEFENSE

A Pragmatic Approach for Practices

Three sequential pillars moving clinical practices from blind exposure to verified resilience



1. Map Attack Surfaces

Catalog every connected diagnostic machine, remote access portal, workstation, staff OSINT exposure, and vendor pathway.

2. Enforce Baselines

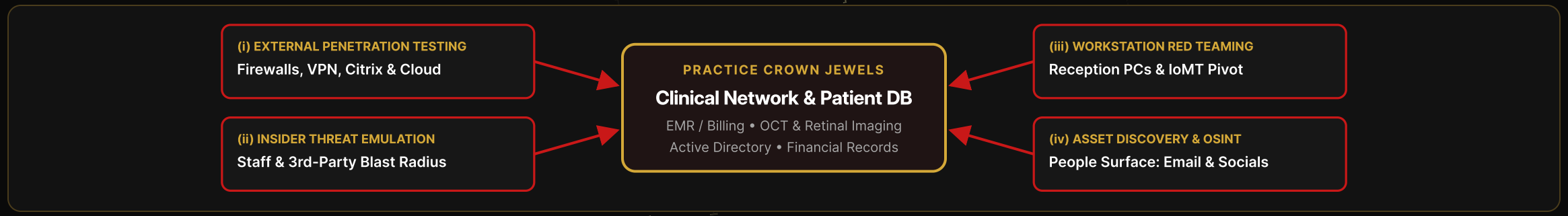
Enforce phishing-resistant MFA across all portals, VLAN segmentation for legacy IoMT, rapid patching, and immutable backups.

3. Threat Assurance

Move beyond static compliance checklists to proactive technical security validation, adversary emulation, and downtime drills.

1. Map Attack Surfaces: Clinical Practice Discovery

Four practical exercises to uncover how adversaries see and infiltrate a modern medical practice



(I) EXTERNAL NETWORK SURFACE

Practice Network External Penetration Testing

Probing public IPs, clinic Wi-Fi edges, VPN/RDP/Citrix gateways, and booking portals for unpatched vulnerabilities.

(II) INTERNAL BLAST RADIUS

Insider Threat Emulation (Staff & Third Parties)

Quantifying how much damage a compromised receptionist, locum, or billing vendor can cause—and verifying RBAC containment.

(III) CLINICAL ENDPOINTS

Workstation Red Teaming

Testing front-desk and diagnostic PCs against session theft, USB drop attacks, and pivoting into connected OCT imaging units.

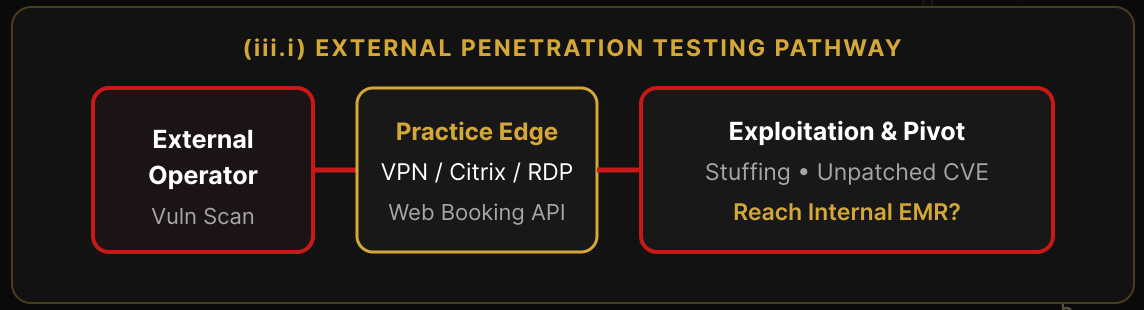
(IV) HUMAN & DIGITAL FOOTPRINT

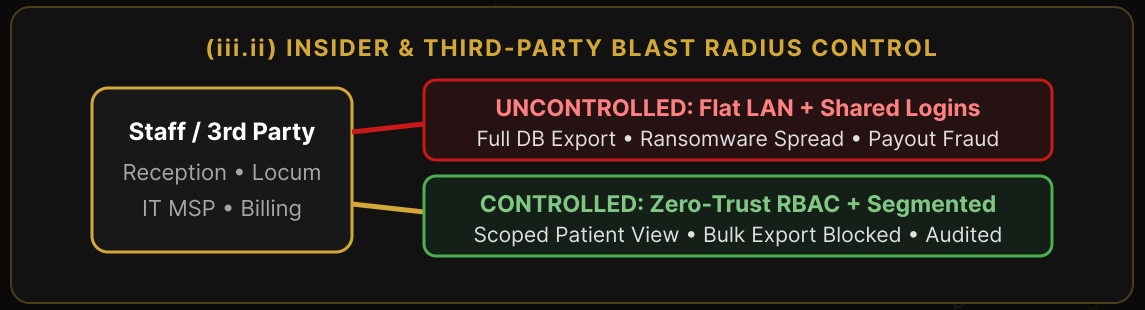
Asset Discovery & People OSINT Exercises

Mapping staff emails, credential breach dumps, LinkedIn/social media, and shadow IoMT assets before spear-phishers strike.

External Penetration Testing & Insider Threat Emulation

Validating perimeter entry points and controlling internal staff / third-party blast radius





(III.I) PERIMETER & CLOUD BOUNDARY TESTING

Practice Network External Penetration Testing

- **Remote Gateways:** Audit VPNs, Citrix portals, AnyDesk/TeamViewer, and firewalls for missing MFA or unpatched CVEs.
- **Cloud EMR & Booking APIs:** Test intake forms, portals, and cloud buckets for broken auth and IDOR leaks.
- **Wireless Isolation:** Verify guest Wi-Fi cannot bridge into clinical VLANs or OCT imaging subnets.

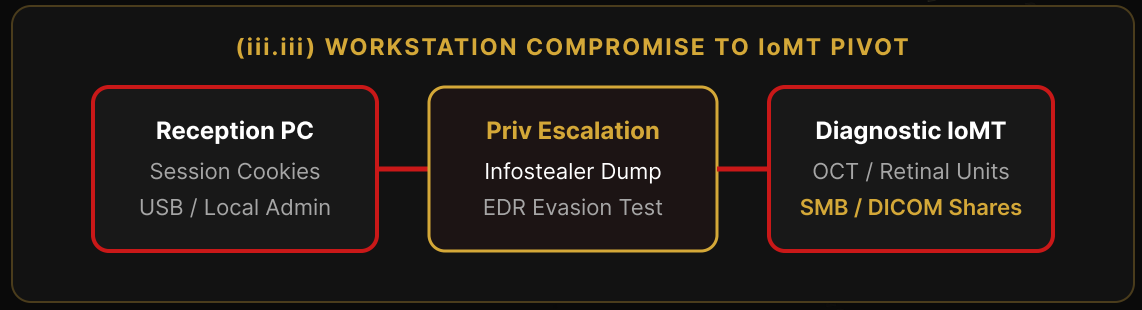
(III.II) STAFF & VENDOR BLAST RADIUS

Insider Threat Emulation: Is Damage Controlled?

- **Staff Blast Radius:** Emulate a compromised receptionist login to test if they can bulk-export the patient DB or alter bank details.
- **Third-Party & MSP Access:** Audit remote support tools used by IT vendors, OCT technicians, and billing bureaus.
- **Containment Controls:** Enforce least-privilege RBAC, ban shared front-desk logins, and alert on bulk queries.

Workstation Red Teaming & OSINT Asset Discovery

Hardening clinical endpoints and mapping the human attack surface across email and social media





(III.III) ENDPOINT RESILIENCE

Workstation Red Teaming

- **Session Hijacking:** Test if infostealers on reception PCs can steal active EMR/clearinghouse browser cookies bypassing MFA.
- **Privilege & USB Ports:** Test whether clinical users can escalate to Local Admin, run binaries, or mount rogue USBs.
- **Diagnostic PC Bridges:** Audit Windows PCs tethered to OCT and visual field instruments running legacy OS builds.

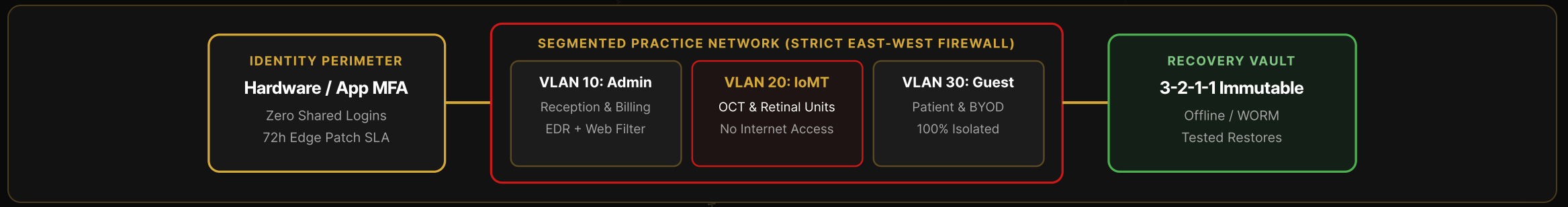
(III.IV) HUMAN & DIGITAL RECONNAISSANCE

Asset Discovery: People Attack Surface & OSINT

- **Email & Breach Exposure:** Audit practice emails against dark-web stealer logs and breach dumps to stop password reuse.
- **Social Media Profiling:** Review what doctors and staff expose on LinkedIn/Instagram (vendors used, badge photos, travel).
- **Shadow IT & Domain Hygiene:** Uncover forgotten subdomains, unmonitored WhatsApp workflows, and weak DMARC rules.

2. Enforce Baselines: Clinical Architecture & Controls

Containing breaches through identity hardening, VLAN segmentation, rapid patching, and immutable backups



BASELINE 01: IDENTITY

Phishing-Resistant MFA Everywhere

Enforce FIDO2/authenticator MFA across all EMR logins, remote portals, email, and clearinghouses; ban shared front-desk logins.

BASELINE 02: ARCHITECTURE

Clinical IoMT Network Segmentation

Isolate legacy diagnostic equipment (OCT scanners, fundus cameras, DICOM servers) into restricted VLANs with zero internet access.

BASELINE 03: HYGIENE

Automated Patching & Endpoint Hardening

Enforce a 72-hour patching SLA for edge appliances, deploy managed EDR on all clinical PCs, and block untrusted USB storage.

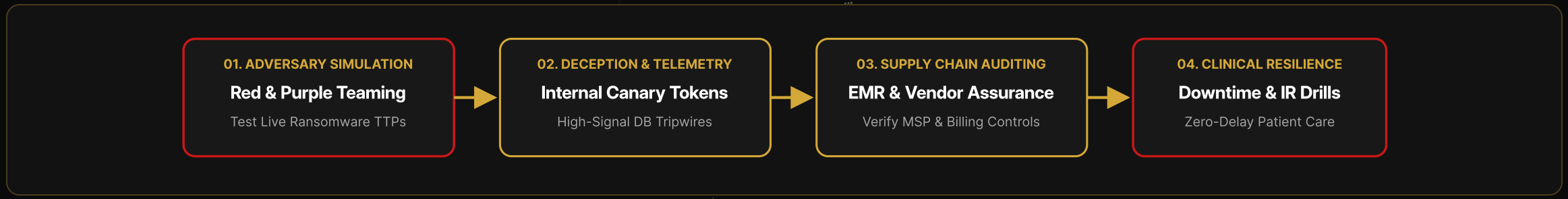
BASELINE 04: CONTINUITY

Immutable Backups & Offline Fallbacks

Maintain encrypted, immutable (WORM) offline backups of patient schedules and imaging with quarterly restoration drills.

3. Threat Assurance: Continuous Technical Validation

Moving beyond static POPIA/HIPAA paper checklists to continuous adversarial verification



ASSURANCE 01: CONTINUOUS VALIDATION

Purple Teaming & Control Verification

Continuously verify that EDR, firewall rules, and alerts actually block live credential dumping, lateral movement, and exfiltration.

ASSURANCE 02: EARLY WARNING

Canary Deployment & Tripwires

Place decoy patient records, honey-credentials, and canary listeners inside practice subnets to detect intruders within minutes.

ASSURANCE 03: THIRD-PARTY GOVERNANCE

Vendor & Supply Chain Security Audits

Mandate POPIA operator agreements, MFA proof, and pen-test attestations from EMR vendors, clearinghouses, and IT MSPs.

ASSURANCE 04: LIFE-SAFETY CONTINUITY

Clinical Incident Response Tabletop Drills

Rehearse ransomware isolation, offline chart fallback, emergency triage continuity, and POPIA/HIPAA breach reporting.

KMSEC (PTY) LTD

OMG PRIVATE PRACTICE BUSINESS WEEKEND 2026

Questions & Discussion

kmsecurity.co.za | secure@kmsecurity.co.za