THE BLUEPRINT FOR CYBER RESILIENCE

A STRATEGIC DIAGNOSTIC OF EXTERNAL AND INTERNAL THREAT SIMULATIONS.

DWG NO. CYBER-RES-001 | SCALE: 1:100 | DATE: [CURRENT DATE] | ENGINEER: TACTICAL BLUEPRINT OPS

THE INEVITABILITY OF THE BREACH

ANONALY: EXTRENE

CRITICAL FAILURE

INTRUSION DETECTED

CRITICAL FAILURE

DATA EXFILTRATION

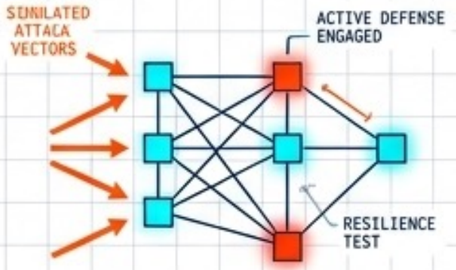
ANONALY: EXTRENE

"FOR BUSINESSES, A CYBER-ATTACK IS NOT A MATTER OF 'IF' BUT 'WHEN.'"

STATUS: MONITORING /
THREAT LEVEL: LOW /
SYSTEM: STABLE

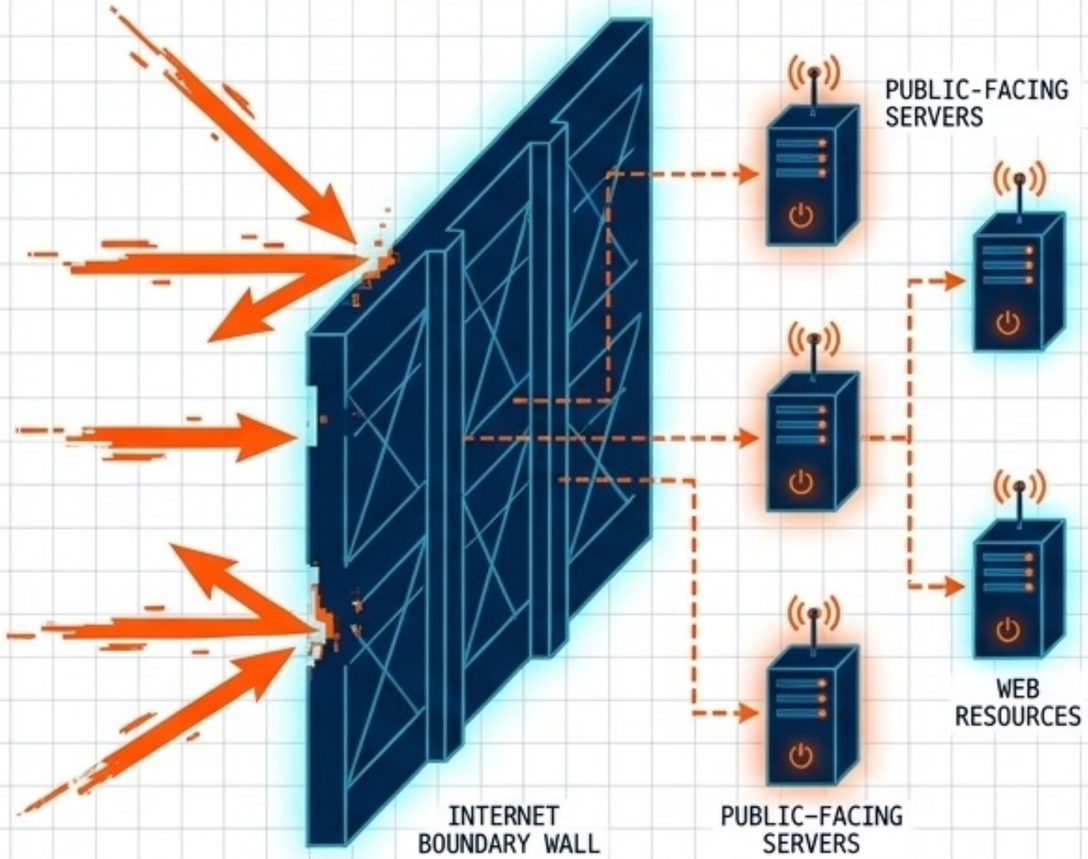
Startups and SMEs cannot rely on theoretical defenses.

Survival requires shifting from passive monitoring to active, simulated stress-testing of your own networks.



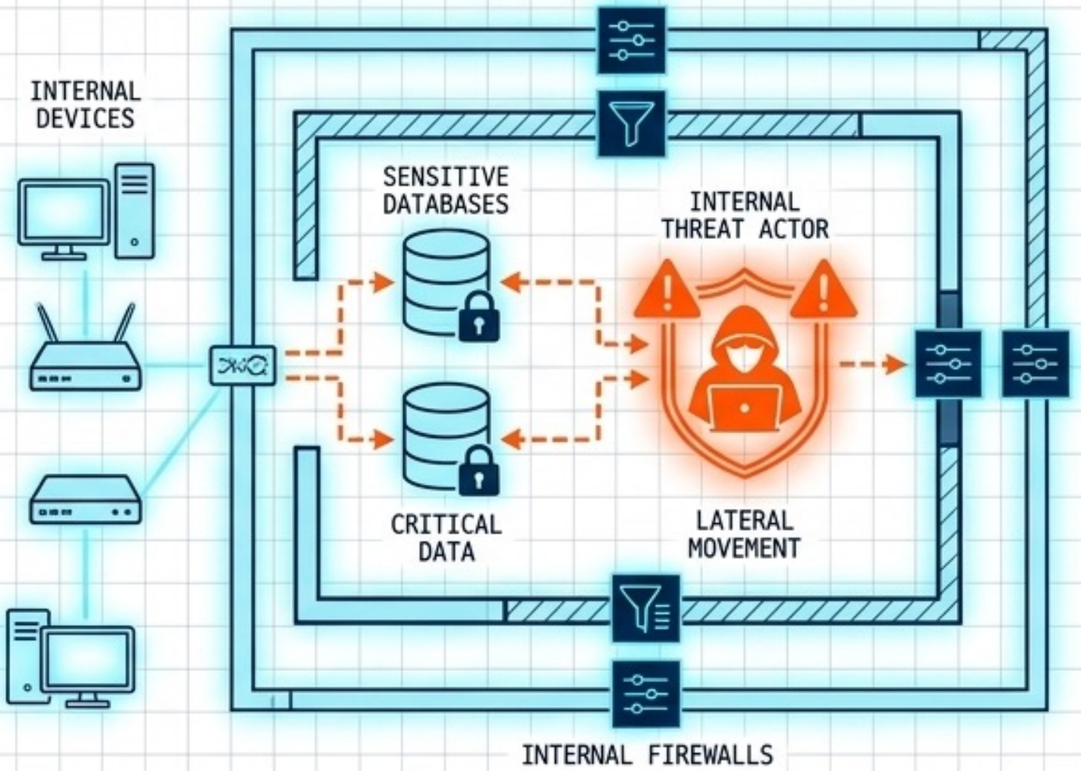
TWO BATTLEGROUNDS: THE PERIMETER AND THE CORE

EXTERNAL SIMULATION

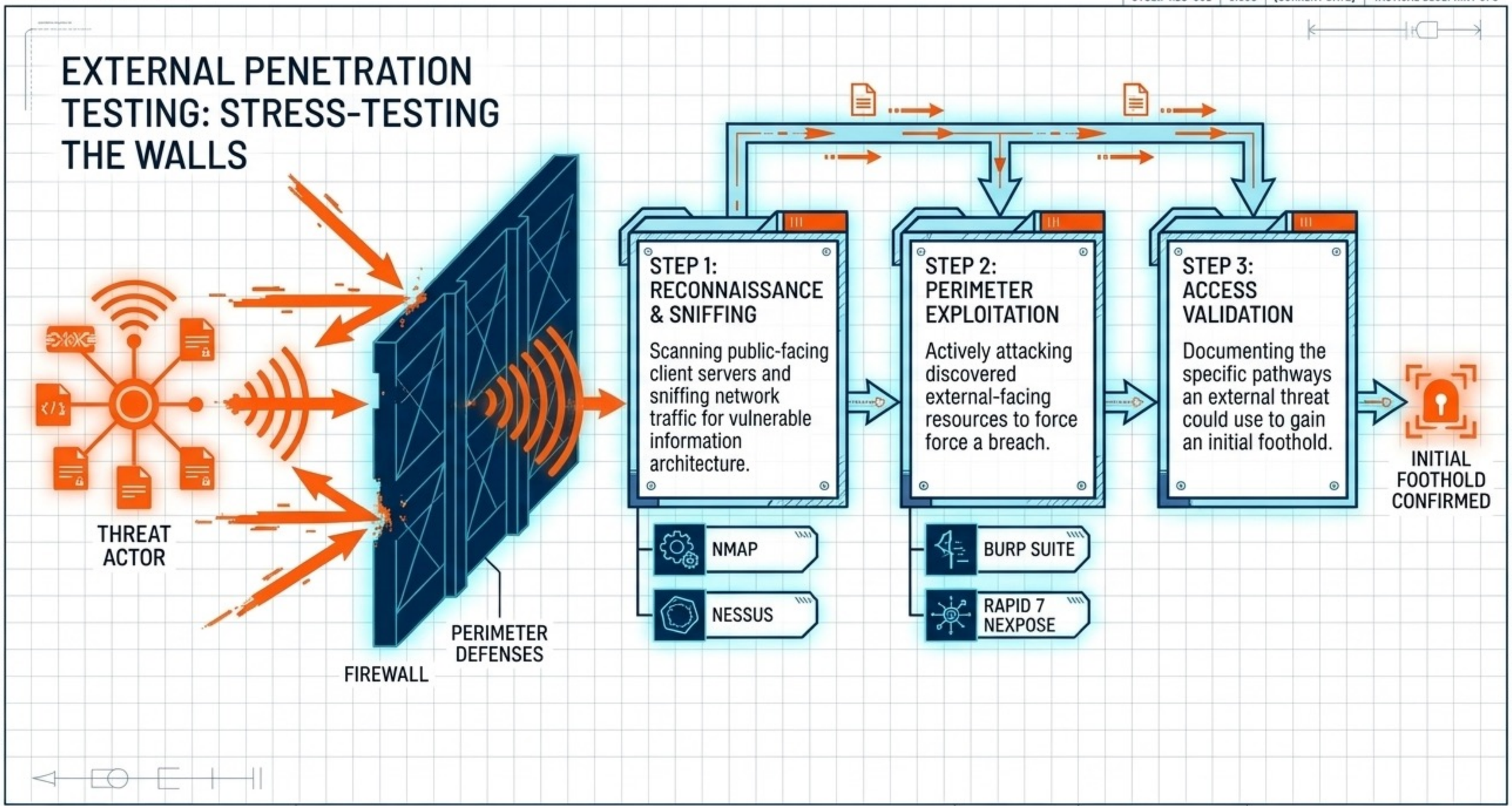


Simulating outside threats attempting to breach the network walls by searching for public-facing servers and exploiting external resources.

INTERNAL SIMULATION



Simulating threats that have already bypassed the perimeter, attempting to access sensitive data while evading internal firewalls.



DWG NO. CY8E8-955-001 | SCALE: 1:100 | DATE: (CURRENT DATE) | ENGINEER: TACTICAL BLUEPRINT OPS

INTERNAL PENETRATION TESTING: THE INSIDER PIVOT

THE SCENARIO

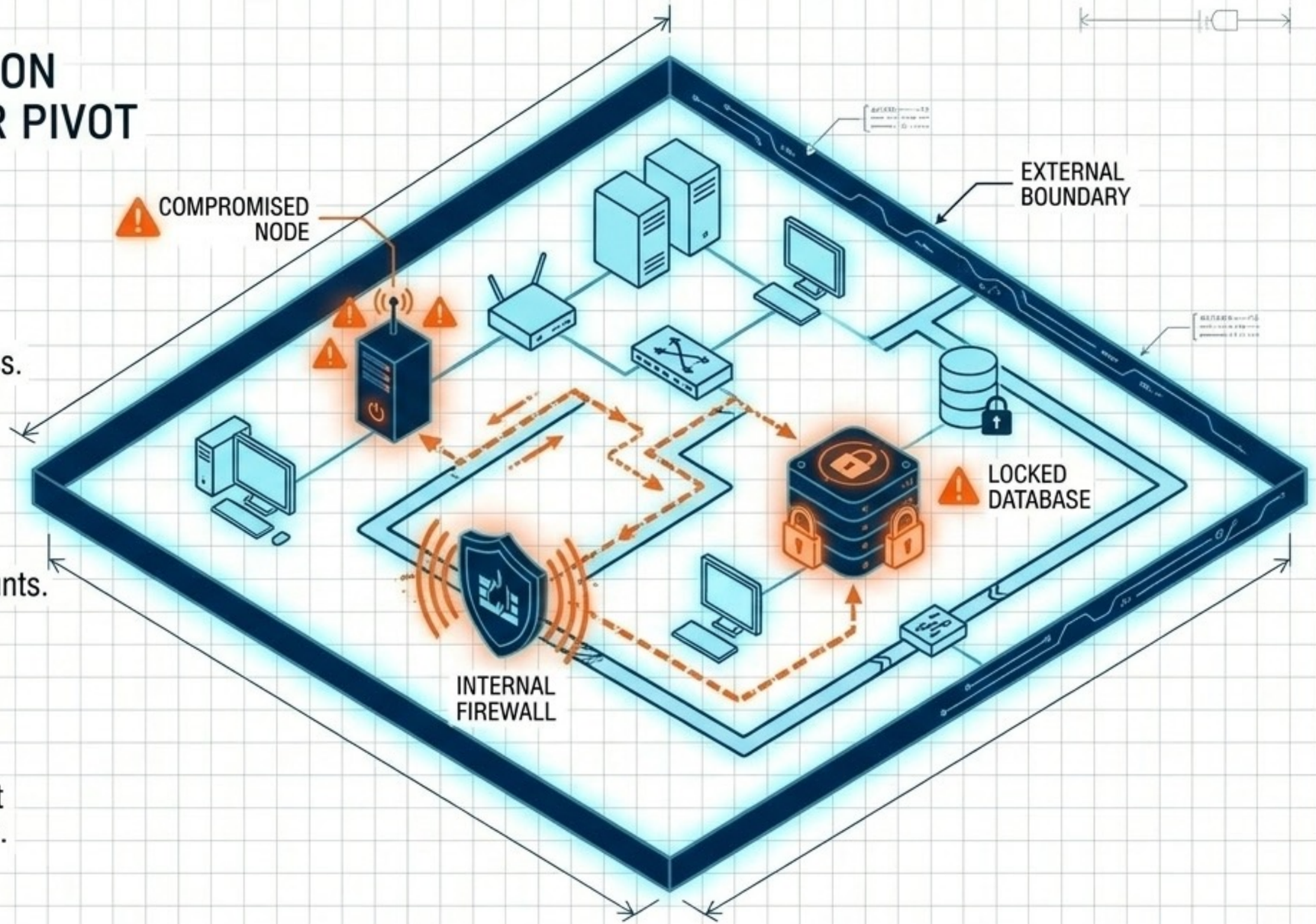
The perimeter is breached, or the threat originates internally. The objective shifts from entry to access.

PRIMARY VECTORS

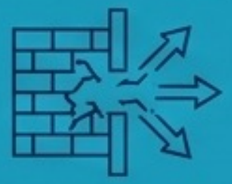
Deploying targeted `phishing` campaigns or local `malware` to compromise authorized user accounts.

EVASION TACTICS

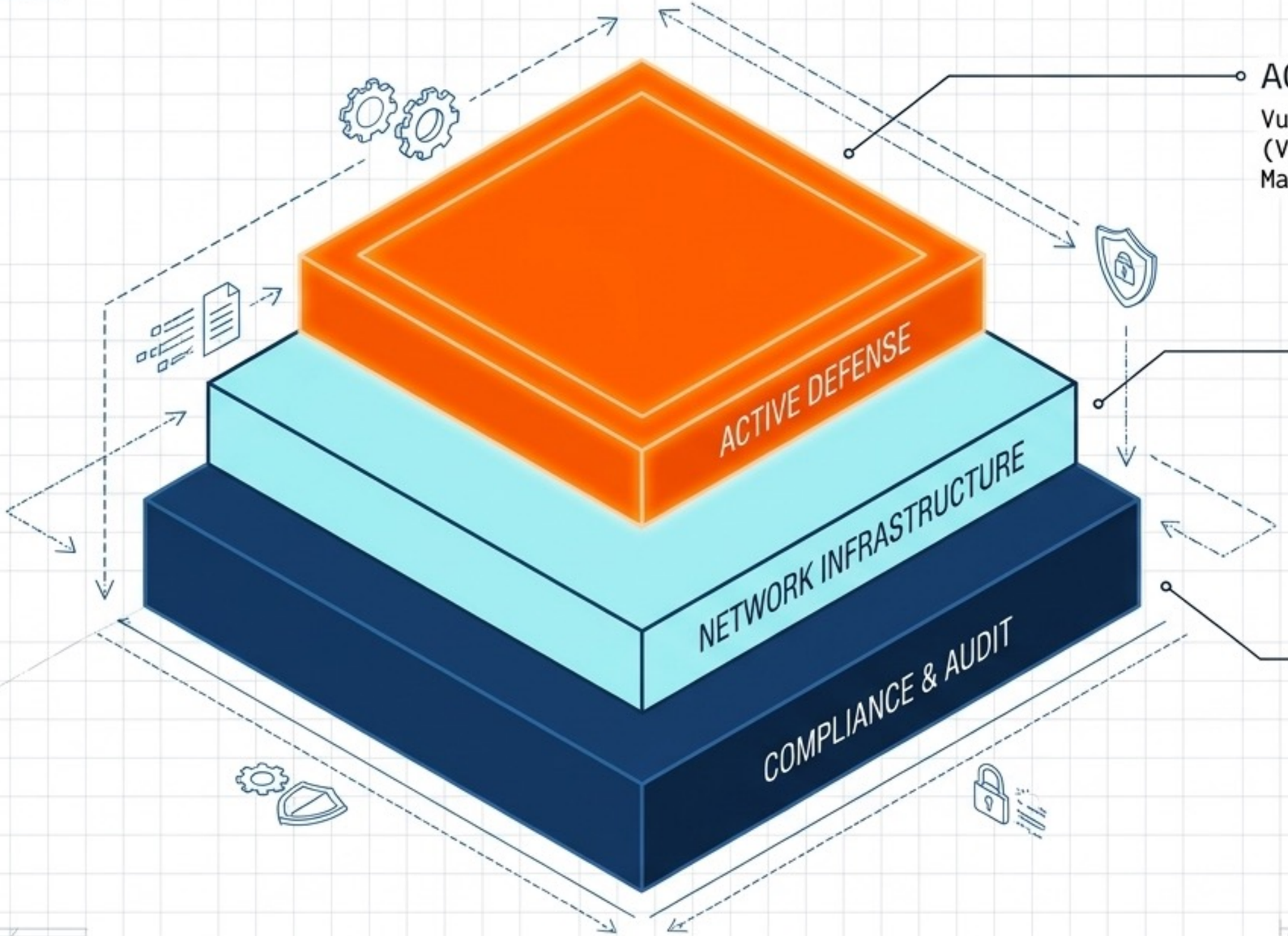
Navigating through the client's internal network resources and bypassing internal firewalls without triggering internal detection alarms.



DIAGNOSTIC MATRIX: EXTERNAL VS. INTERNAL METHODOLOGIES

	EXTERNAL	INTERNAL
OBJECTIVE	Breach the perimeter. 	Access sensitive information laterally. 
TARGET ASSETS	Public-facing servers, external network traffic. 	Internal network resources, proprietary databases. 
SIMULATED ACTOR	Anonymous outsider without credentials. 	Rogue employee or attacker with an initial internal foothold. 
ARSENAL & TACTICS	Port scanning, payload delivery (NMap, BURP). 	Privilege escalation, Phishing, Malware deployment, firewall evasion. 

THE FULL-STACK SECURITY ECOSYSTEM



ACTIVE DEFENSE

Vulnerability & Penetration Testing (VAPT), Web-Application Security, Malware clean-up.

NETWORK INFRASTRUCTURE

Network Security Management, powered by enterprise-class hardware (Authorized Partner for pfsense).

COMPLIANCE & AUDIT

Information Systems Audit, GDPR (EU), DPDP (India), SOC 1 & 2, ISO 27001 readiness, CSA STAR Registry, HECVAT (Education).

‘PEOPLE PATCHING’: THE HUMAN FIREWALL

THE CONCEPT

Technical barriers fail if human behavior is easily exploited. People must become the strongest line of defense for the organization.

THE EXECUTION

Upgrading employee know-how through hands-on workshops, contextual Security Education Training Awareness (SETA), and simulated Social Engineering Campaigns.

THE CYBERYOG ADVANTAGE

WHO WE ARE

A cybersecurity start-up founded in 2017, headquartered in India, uniquely focused on curating solutions for startups and SMEs.

KNOW YOUR CYBERSCORE (KYC)

We assess and validate your cybersecurity maturity against peer organizations and leading industry frameworks.

THE OUTCOME

You get a definitive score and a proven roadmap leading to a stronger security posture.

INITIATE YOUR DIAGNOSTIC

We would love to hear from you. Built in the City of Joy for your security needs.

LOCATION:	Kolkata, India
DIRECT LINE:	+91 9051 234 233
EMAIL:	info@cyberyog.com
WEB ECOSYSTEM:	www.cyberyog.com | pfsense.cyberyog.com training.cyberyog.com