INFRASTRUCTURE SECURITY ASSESSMENT

Your IT infrastructure is the backbone of everything - this briefing maps the attack paths most organizations have never tested, and shows you the structured path to a validated, resilient posture.

CREST Registered Region - Global

VA

PEN TEST

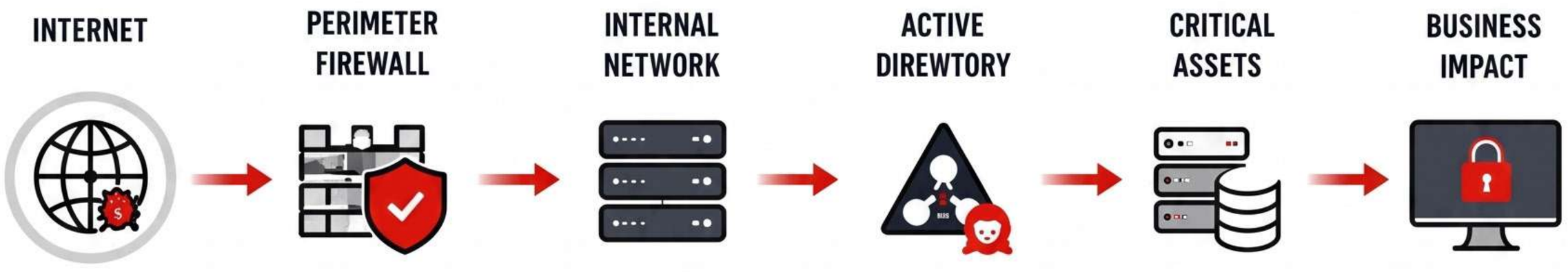
certin Empanelled

WHY INFRASTRUCTURE SECURITY MATTERS:

THE GAPS MOST ORGANIZATIONS HAVE NEVER TESTED

Current research reveals that 93% of enterprise networks can be fully penetrated by a skilled adversary within 48 hours. These are not theoretical risks – they are validated findings from real world assessments across enterprise environments globally.

THE ATTACK PATH: FROM OUTSIDE TO IMPACT



THE REALITY IN NUMBERS

93%

ENTERPRISE NETWORKS PENETRABLE

External attackers achieve full compromise

Positive Technologies

48 HOURS

AVERAGE RED TEAM BREAKOUT TIME

Average time to full internal compromise via AD misconfigurations

258 DAYS

AVERAGE BREACH DWELL TIME

Attacker maps, escalates, and plants backdoors undetected

IBM

$4.88M

AVERAGE GLOBAL BREACH COST

Network compromise is the highest-cost breach category

IBM

KEY INSIGHT

The consistent pattern across high-value breaches is not a single missing patch. It is a combination of network segmentation gaps, Active Directory misconfigurations, and trust assumptions built years ago that no longer reflect current threat actor capabilities.

WHERE INFRASTRUCTURE BREACHES ACTUALLY START

8 Critical Finding Categories Attackers Exploit

Attack entry points validated across enterprise network penetration tests and breach investigations. These are not theoretical — they are the findings our engineers document in every engagement.

01 EXTERNAL ATTACK SURFACE

Unpatched internet-facing services, exposed VPN endpoints, and open ports provide the initial foothold. 52% of significant breaches originate from external attack vectors.

02 FLAT NETWORK ARCHITECTURE

VLAN hopping and inter-segment routing gaps allow a single compromised host to reach finance, HR, and production systems simultaneously.

03 ACTIVE DIRECTORY MISCONFIGURATIONS

Kerberoasting, Pass-the-Hash, DCSyns, BloodHound path analysis, and GPO abuse enable escolation from standard uver to domain admin within hours.

04 NETWORK DEVICE HARDENING GAPS

Default predentials on routers and switches, exposed SNMP management planes, and unreviewed configurations expose the management layer to lateral movement.

05 PERMISSIVE FIREWALL RULES

Overly permissive outbound rules are exploited for data exfiltration and C2 communication. IDS/IPS evasion and WAF bypass are validated in every engagement.

06 SCADA / ICS BOUNDARY EXPOSURE

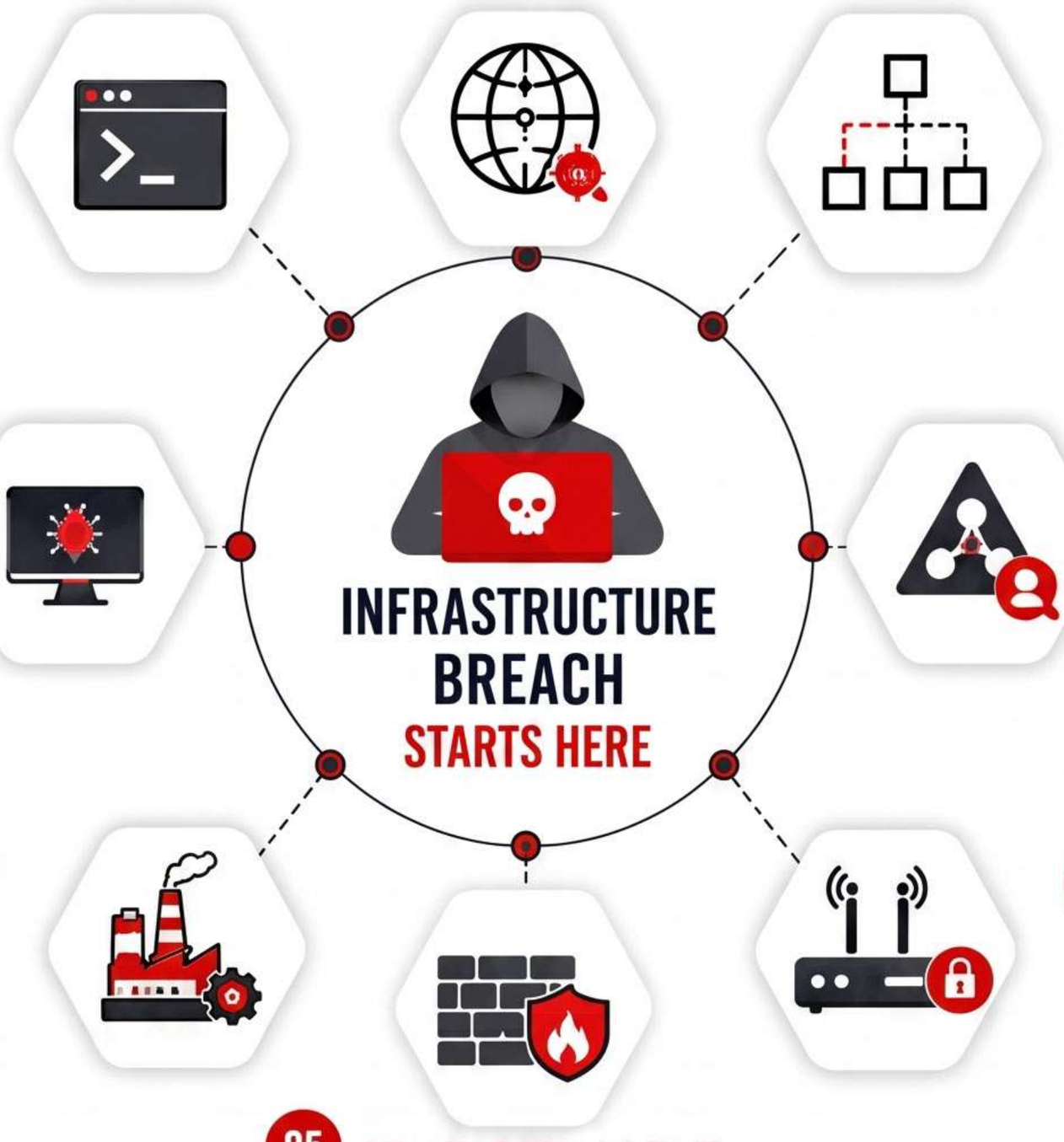
IT-to-OT pivot paths, Modbus and DNP3 protocol vulnerabilities, and HMI access gaps allow production system disruption via IT network compromise.

07 POST-EXPLOITATION BLIND SPOTS

Privilege escolation chains, lateral movement documentation, and SIEM evasion paths remain unknown until a real incident reveals the full attacker blast radius.

08 LIVING-OFF-THE-LAND TECHNIQUES

Attackers using native Windows tools — PowerShell, WMI, PeExec — generate no alerts in standard EDR or SIEM configurations. 25–35% of breaches have an insider threat component.



DID YOU KNOW?

Active Directory is cited in the majority of high-value breach lateral movement chains. BloodHound analysis routinely reveals privilage escalation paths that have existed undetected for 2–5 years in enterprise environments.

WHAT WE ASSESS

8 LAYERS OF INFRASTRUCTURE SECURITY

Comprehensive. In-Depth. **Beyond Vulnerability Scans.**

LAYER 01

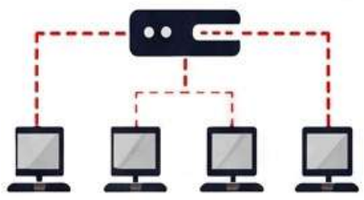
EXTERNAL ATTACK SURFACE

- Open ports • Exposed services • VPN testing
- Firewall bypass • Subdomain discovery
- Credential look validation

LAYER 02

INTERNAL NETWORK SEGMENTATION

- VLAN hopping • Inter-segment routing policy
- Fiat network identification • Lateral movement path mapping



LAYER 03

ACTIVE DIRECTORY SECURITY

- Kerberoasting • Pass-the-Hash • DCSync
- BloodHound analysis • GPO ahuse
- ACL misconfiguration • Trust relationship review

LAYER 04

NETWORK DEVICE HARDENING

- Router & switch config review • SNMP testing
- Default credential sweep • Management piane exposure assessment

LAYER 05

FIREWALL & PERIMETER CONTROLS

- Rule review • Egress filtering • IDS/IPS evasion
- WAF bypass • DMZ architecture review
- C2 channel testing

LAYER 06

SCADA / ICS BOUNDARY

- IT-To-OT pivot testing • Protocol assessment (Modbus, DNP3) • HMI access validation
- IEC 62443 compliance alignment

LAYER 07

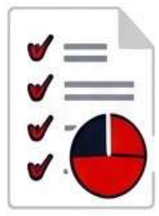
POST-EXPLOITATION VALIDATION

- Privilege escalation chains • Lateral movement path mapping • SIEM & EDR evasion validation
- Attacker hlast radius quantification
- Persistent backdoor identification

LAYER 08

COMPLIANCE & FRAMEWORK MAPPING

- MITRE ATT&CK technique mapping
- CVSS scoring with exploitability context
- Regulatory gap analysis • SSAFE score
- Risk-ranked remediation roadmap



ASSESSMENT METHODOLOGY

FROM FOOTHOLD TO FIX

01

RECONNAISSANCE

Information gathering, OSINT, asset discovery, and threat modeling

02

EXTERNAL SURFACE TESTING

Identify entry points and validate external attack vectors

03

INTERNAL NETWORK ASSESSMENT

Map network, validate segmentation and lateral movement opportunities

04

AD ATTACK CHAIN ANALYSIS

Exploit AD misconfigurations to assess privilage escolation paths

05

POST-EXPLOITATION VALIDATION

Simulate real attacker behavior to measure blest radius and impact

06

REMEDIATION GUIDANCE & RETEST

Prioritize remediation roadmap and retest to validate closure

COMPREHENSIVE COVERAGE

Most organizations test only their external perimeter. Layers 2 to 7 — internal segmentation, Active Directory, device hardening, and post-exploitation — are where attackers operate and where most assessments stop.

OUTCOME YOU CAN TRUST

Actionable findings. Validated risk.
Compliance evidence.
A stronger infrastructure security posture.

YOUR DECISION TODAY.
YOUR SECURITY TOMORROW.

Two Infrastructure Security Postures. One Clear Choice.

WITHOUT PROACTIVE INFRASTRUCTURE VAPT

UNKNOWN ATTACK PATHS
Internal attack paths remain hidden until an adversary maps them.

ACTIVE DIRECTORY WEAKNESSES
AD misconfigurations stay undetected for months or years.

SEGMENTATION GAPS
One compromised host can reach sensitive segments and critical systems.

COMPLIANCE BASED ON DOCUMENTS
Posture is based on documentation, not on validated exploitability.

HIGHER INSURANCE COSTS
Lack of VAPT evidence leads to higher premiums.

NO CLARITY FOR THE BOARD
You can't answer: How far could an attacker reach today?

INEFFECTIVE PATCH PRIORITIZATION
Patching is based on CVSS scores, not real-world exploitability.

LONGER DWELL TIME, HIGHER RISK
258-day average dwell time before breach detection.

VS

WITH ANNUAL BRISKINFOSEC INFRASTRUCTURE VAPT

VALIDATED SECURITY POSTURE
All attack paths from external entry to domain admin documented and closed.

AD HARDENING ROADMAP
Active Directory risks identified and prioritized with real exploitability evidence.

SEGMENTATION VALIDATION
Network segmentation gaps identified, remediated, and validated through testing.

COMPLIANCE BACKED BY EVIDENCE
Penetration test evidence and remediation records strengthen compliance postore.

LOWER INSURANCE PREMIUMS
20–40% reduction in premiums with VAPT certification and proof.

CLEAR ANSWERS FOR THE BOARD
Attacker blast radius validated and bounded.

EXPLOITABILITY-DRIVEN PRIORITY
Patching prioritized based on actual risk to your environment.

CONTINUOUS VISIBILITY & IMPROVEMENT
LURA portal for tracking, retesting, and continuous remediation.

3 STEPS TO A VALIDATED INFRASTRUCTURE POSTURE

1 BOOK A STRATEGY BRIEFING
45-minute confidential discussion to review your infrastructure posture and identify the right assessment scope.

2 RECEIVE YOUR SCUPED PROPOSAL
Detailed assessment plan with methodology, timeline, compliance mapping, and engagement tier options within 48 hours.

3 PARTNER ON EXECUTION
Phased delivery with LURA portal tracking from findings to remediation validation and compliance sign-off.

What Happens Next?

Client Breaches
Post-assessment security record

Start With Zero Commitment

Understanding your unique security challenges begins with a conversation. We offer a no-obligation consultation to assess your current posture and identify immediate risk areas.

Our Team Holds Industry-Leading Certifications

We invest heavily in our team's continuous education because the threat landscape never stops evolving. Neither do we.

OSCP | OSWE | CISSP | CISA | CEH

CREST Accredited

Internationally certified penetration testing excellence

CERT-IN Empanelled

Government-recognized trusted cybersecurity assessment provider

ISO 27001 : 2022 Certified

Our own security practices are independently audited and verified annually

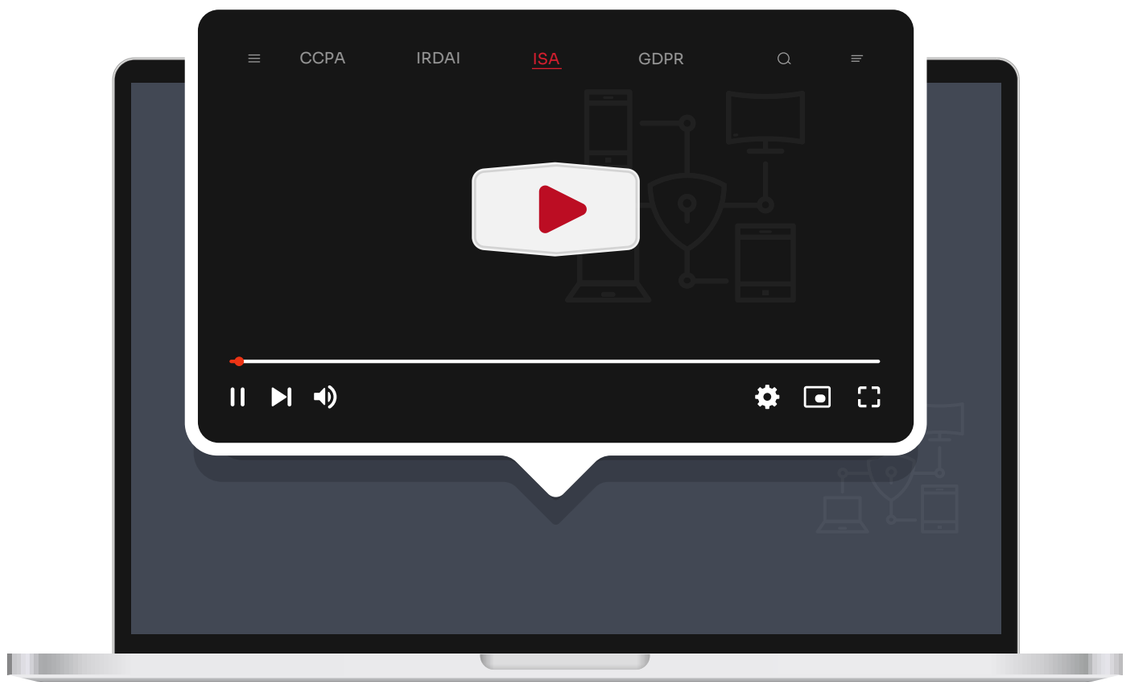
25+
Countries Client Portfolio

67%
Logic flaws missed by bots

98%
Client retention

640+
Successful Customers

5600+
Delivered in 24 countries



Reach us for FREE

consultation

Book Now

sales@briskinfosec.com
www.briskinfosec.com

Our Geographical Presence

India UAE