PENTESTERRA

ATTACK CHAIN ANALYSIS

Do Your Isolated Findings Hide an Attack Path?

Not a CVE list - a graph of how an attacker actually gets in, correlating network, web, code, and OSINT findings into verified attack paths.

IN SHORT

The correlation of individual security findings into multi-step attack paths - network, web/API, code, OSINT in one graph - instead of treating each finding as an isolated ticket. Every node is mapped to a MITRE ATT&CK tactic and technique.

5 Sources

Network, web, API, code, OSINT in one graph

ATT&CK

Every node mapped to a tactic and technique

Verified

Chains built from proven, not theoretical, steps

THE SITUATION TODAY

WHO YOU ARE

You're the CISO or security lead of an organization that wants to know not just which vulnerabilities exist, but how they combine into a real path to your critical data.

WHAT HAPPENED

Three separate teams each closed their own medium-severity ticket last quarter - none of them knew the three combined into one critical path.

WHY IT HURTS

A vulnerability report scores findings in isolation. An attacker doesn't - they chain them. That gap is exactly where a breach starts.

WHERE YOU WANT TO GET TO

DESIRED OUTCOME

You want to see, with concrete proof, how your isolated findings chain into a real attack path to your critical assets - not just a list sorted by CVSS.

THE SOLUTION

An Attack Chain Analysis service: cross-domain correlation of findings from network, web/API, code, and OSINT into a graph, with MITRE ATT&CK mapping and business-impact and compliance scoring for every path.

WHY IT'S DIFFERENT

You're not buying another CVSS-sorted vulnerability report. You're working with [YOUR COMPANY NAME] - a certified provider with a long track record in information security. You've likely worked with us already, directly or through someone you know. And up to 20 attack chains are computed per cycle, at depth up to 5 - every chain is built from findings verified with real exploits, not CVSS guesses: after a fix lands, the whole chain is re-run to confirm it is genuinely broken.

CONCRETE PROOF

The result is a complete, ready-to-deliver PDF report with every critical path mapped to MITRE ATT&CK and the single highest-leverage fix highlighted. If broader gaps come up, we propose additional services: penetration testing, vulnerability assessment, DevGuard code review.

Up to 20	Depth 5	Re-Verification
Attack chains computed per cycle	Multi-step paths, not single findings	Every chain re-run after a fix

WHAT'S ACTUALLY INCLUDED

Not a CVE list sorted by score - a real graph of how findings combine.

Cross-Domain Correlation

The engine pulls findings from every source and builds a graph of how they connect.

- Network + web + API + code + OSINT findings in one graph
- The artifact from step one is the input to step two
- Not a list of vulnerabilities - realistic exploitation routes
- Recomputed on every assessment cycle

MITRE ATT&CK Mapping

Every node in a chain is mapped to an ATT&CK tactic and technique.

- Per-node tactic and technique mapping
- Phase view from initial access to business impact
- Chain diff between cycles: new, closed, changed

Business Impact & Compliance Context

A chain that ends at a payment database matters more than one that ends at a marketing microsite.

- Business-process and asset-criticality scoring
- Compliance mapping: OWASP, PCI-DSS, GDPR, NIST, ISO
- Executive summary plus the single highest-leverage fix

Real Verification, Not Guesses

Chains are built from verified findings, not CVSS guesses.

- Every chain step backed by exploit verification
- Regression detection when a fixed step reopens
- Confirmed vs. potential separation, clear on real finding existence

PENTESTERRA

ATTACK CHAIN ANALYSIS

WHAT YOU GET

- ✓ A complete PDF report with every critical path mapped to MITRE ATT&CK
- ✓ Cross-domain correlation of findings from network, web, code, and OSINT
- ✓ Business-impact scoring and compliance mapping for every chain
- ✓ The single highest-leverage fix highlighted per path
- ✓ Automatic chain re-verification after every fix

HOW IT WORKS

1

We define the scope

The finding sources to correlate - network, web, code, OSINT.

2

We build the graph

We correlate existing findings into realistic attack paths.

3

We map to ATT&CK

Every node with tactic, technique, and business impact.

4

We deliver the report

A complete PDF with critical paths and the highest-leverage fix.

Discover the attack paths hidden in your findings

A complete report, ready to present to clients, auditors, or your board.

Request your Attack Chain Analysis →

info@pentesterra.com · pentesterra.com/attack-chain-analysis