

Cyber Defense & Incident Response

When prevention is not enough — rapid response saves the business.

Effective cyber defense is not a product — it is a continuously maintained posture that evolves alongside the threat landscape. We design and deploy turnkey defensive architectures, integrate SIEM and IDS/IPS tooling, and stand ready to respond the moment an incident occurs. Our goal: minimize dwell time, contain damage, and restore normal operations rapidly — while preserving the forensic evidence you need.

21 min**BREAKOUT TIME**

average time for attacker lateral movement after gaining initial access

277**DAYS DWELL**

average days before detection without active continuous defense monitoring

70%**FASTER**

incident containment speed improvement with a pre-built response playbook

\$2.7M**SAVINGS**

average cost reduction when an IR plan is in place before a breach occurs

Our Defense Services

1

IDS / IPS Deployment

Intrusion Detection and Prevention Systems designed for your specific network topology — identifying and blocking threats at the earliest possible point before they spread.

3

DLP Implementation

Data Loss Prevention controls to monitor and block unauthorized movement of sensitive data — inside and outside your perimeter, detected and stopped in real time.

5

Incident Response

Structured methodology: triage, containment, root cause analysis, lateral movement mapping, evidence preservation, and systematic post-incident hardening.

2

SIEM Integration

Security Information and Event Management configured to correlate logs across your entire environment, surfacing the anomalies and patterns that matter most.

4

Cloud Security (AWS/Azure)

We harden cloud environments, configure IAM policies correctly, and integrate cloud-native monitoring into your overall unified security posture seamlessly.

6

Tabletop Exercises

We stress-test your response procedures through simulated breach scenarios before a real event forces the issue — building genuine muscle memory in your team.

Why Active Defense Is Non-Negotiable

Speed Is Everything

Every minute between detection and containment increases the blast radius. Mature defense architecture collapses response time from days to minutes consistently.

Attackers Move Fast

Modern threat actors achieve lateral movement in under 30 minutes. Without continuous monitoring, your team is always reacting too late to meaningfully limit damage.

Forensics Matter Legally

Poorly handled incidents destroy evidence. Our methodology preserves the full forensic chain of custody needed for legal proceedings, regulation, and insurance claims.

What You Gain

A

Faster Containment

Pre-built playbooks and rehearsed procedures mean your team acts in minutes — limiting damage and operational disruption from the very first moment of detection.

B

Operational Continuity

Our defensive architecture is designed to absorb attacks and keep critical systems running — not just to detect threats passively after significant damage is done.

C

Legal & Regulatory Cover

Documented incident response, preserved evidence, and timely DNSC notification protect your organization from secondary legal and regulatory liability after any event.

"

Their IR team was on a call with us within 40 minutes of the alert. Containment was achieved before business hours. We disclosed zero client data and avoided a NIS2 notification.
— IT Director, financial services firm — Incident Response client

Build your defense before you need it. Request a free posture review — no commitment required. secureintel.ro