

Incident Response

Planning, preparation, and coordinated response when security incidents occur.

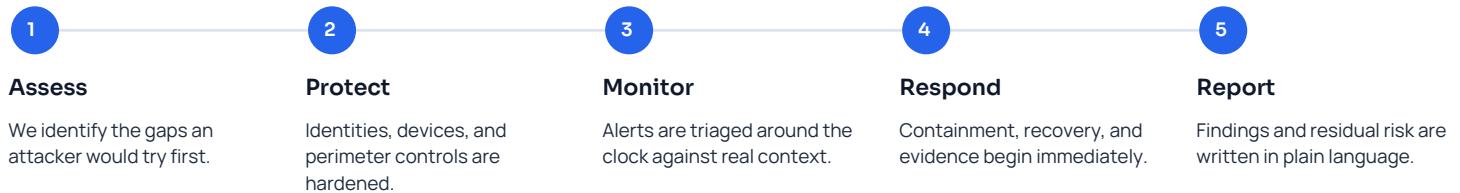


Service illustration • Cybersecurity

What this service addresses

- Increasingly targeted phishing and ransomware attacks
- Limited visibility into endpoint and identity threats
- Pressure from insurers, clients, and regulators

A clear path to delivery



Included capabilities & what they mean

Capability	Practical detail
Continuous threat detection and response	Review suspicious activity, investigate context, and coordinate containment and remediation.
Email and identity protection	Strengthen sign-in controls and email defenses against account misuse, phishing, and impersonation.
Vulnerability identification and remediation tracking	Identify exposure, prioritize fixes by risk, and track remediation rather than simply listing issues.
User awareness training	Help employees recognize suspicious messages and understand how to report them.
Incident response planning	Clarify decision makers, containment steps, recovery dependencies, and communications before an incident.

Business outcomes

- Reduced likelihood and impact of incidents
- Clear visibility into security posture
- Better-prepared employees

Before we begin

Do you guarantee we will never be breached? No responsible provider can. Our focus is reducing risk, detecting threats early, and responding quickly.

Scope and licensing vary by environment. Product availability and support terms are confirmed during planning.

CYBERSECURITY

Incident Response: a closer look

Planning, preparation, and coordinated response when security incidents occur.

From challenge to coverage

SIGNS IT IS TIME TO ACT

- 1 No agreed first move when something goes wrong
- 2 Nobody sure who is allowed to isolate a system
- 3 Notifications to insurers and clients left to the last minute
- 4 A plan written before the current staff joined

WHAT THE SERVICE COVERS

- Response plan and contact tree
- Role and authority definition
- Containment and recovery runbooks
- Communication templates for staff, clients, and insurers
- Tabletop exercise and after-action review

Decisions to settle before an incident

Area	What we review	Why it matters
Authority	Incident owner, escalation contacts and decision rights	Avoid uncertainty about who can authorize action.
Containment	Isolation procedures and evidence-preservation needs	Balance business continuity with investigation requirements.
Recovery	Restore priorities and communication plans	Coordinate technical recovery and stakeholder updates.

This assessment supports preparedness; it is not emergency incident response. Response services require agreed scope.

How an engagement runs

01

Discover

Review the current environment, priorities and constraints with your team.

02

Plan

Agree scope, owners, timing and how success will be reviewed.

03

Deliver

Carry out the agreed work with documented changes and checkpoints.

04

Review

Revisit results, open items and next priorities on an agreed cadence.

What good looks like

The results this service is designed to support. Actual results depend on your environment and the agreed scope.

A rehearsed response plan with named owners

Containment decisions made quickly and defensibly

Notifications handled on time

Lessons recorded and applied after each event

Questions clients ask

Do you respond to an active incident?

Yes, within the scope agreed in your service terms. Where a deeper forensic investigation is needed, we coordinate it and keep the evidence chain intact.

How often should the plan be tested?

At least annually, and whenever staff, systems, or suppliers change. A short tabletop exercise is usually enough to reveal what would break.

Your next step

Free self-assessment

Security Governance Self-Assessment

Review policies, ownership and risk practices.
massiveit.com/security-governance-assessment

Talk to an engineer

Book a consultation

Walk through your environment and get a scoped recommendation.
massiveit.com/consultation • (813) 518-5454

RELATED CYBERSECURITY SERVICES

Managed Detection and Response • Endpoint Detection and Response • Email Security • Security Awareness Training • Vulnerability Management • Security Assessments

Scope, licensing and service levels vary by environment and are confirmed in your agreement. This overview describes typical engagements, not guaranteed results.