(one) eSecurity

Readiness · Detection · Response

The complete cycle of Detection and Response in a single Retainer

One eSecurity's Retainer is much more than a contract: it is a dual-purpose agreement designed to protect your organization both in t**imes of crisis and during operational calm**.

In Times of Crisis

In the event of a cybersecurity incident, our DFIR and EIR teams act immediately. With SLAs of less than 2 hours, we offer a rapid response in detection, containment, eradication and recovery, minimizing the impact on your business.

In Peacetime

When there are no incidents, contracted hours can be used to improve your detection and response maturity through consulting projects, cyber crisis exercises, technical and strategic assessments, among others.

How does the One eSecurity retainer work?

On-demand response (SLA < 2h): When an incident occurs, our team of DFIR experts is immediately activated to contain, eradicate and recover systems, minimizing operational impact.

Flexible use of hours: You can use contracted hours for incident response as well as for consulting and maturity improvement projects in detection and response during peacetime.

Tailored to your business and threats: Scalable and customized according to your industry, maturity level and specific risks, always guaranteeing maximum return on value.
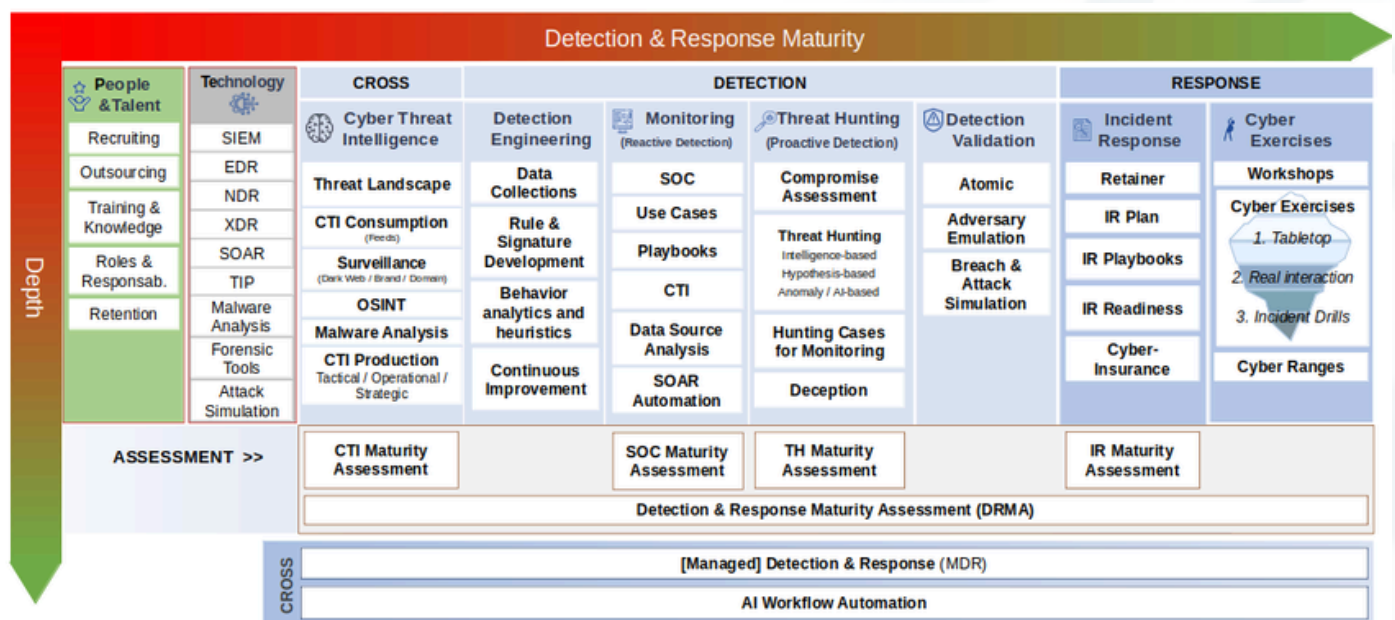

Turn peace into progress

Our Retainer is not only activated in emergencies, it also allows you to **build long-term resilience through strategic improvement projects**.

Assessments: Evaluate your starting point. From detection and response maturity analysis to technical diagnostics that will help you draw a clear improvement plan.

Cyber Intelligence: Understand who is behind the positives. Receive strategic reports on threat actors, relevant malware analysis and a threat landscape tailored to your industry.

Detection: Enable effective detection. Enhance your monitoring with detection engineering, SOAR automation, advanced use cases, threat hunting and technical validation of your capabilities.

Response: Get ready to act. Design and test real IR Plans and playbooks, and train your teams with workshops, tabletop exercises or advanced simulations with digital twins of your infrastructure.

Detection & Response Maturity

People & Talent	Technology	CROSS	DETECTION				RESPONSE	
Recruiting	SIEM	**Cyber Threat Intelligence**	**Detection Engineering**	**Monitoring** (Reactive Detection)	**Threat Hunting** (Proactive Detection)	**Detection Validation**	**Incident Response**	**Cyber Exercises**
Outsourcing	EDR	Threat Landscape	Data Collections	SOC	Compromise Assessment	Atomic	Retainer	Workshops
Training & Knowledge	NDR	CTI Consumption (Feeds)	Rule & Signature Development	Use Cases	Threat Hunting Intelligence-based Hypothesis-based Anomaly / AI-based	Adversary Emulation	IR Plan	Cyber Exercises 1. Tabletop
Roles & Responsab.	XDR SOAR	Surveillance (Dark Web / Brand / Domain)	Behavior analytics and heuristics	Playbooks		Breach & Attack Simulation	IR Playbooks	2. Real interaction
Retention	TIP Malware Analysis	OSINT Malware Analysis		CTI	Hunting Cases for Monitoring		IR Readiness	3. Incident Drills
	Forensic Tools Attack Simulation	CTI Production Tactical / Operational / Strategic	Continuous Improvement	Data Source Analysis SOAR Automation	Deception		Cyber-Insurance	Cyber Ranges

ASSESSMENT >>	CTI Maturity Assessment	SOC Maturity Assessment	TH Maturity Assessment	IR Maturity Assessment

Detection & Response Maturity Assessment (DRMA)

CROSS:
[Managed] Detection & Response (MDR)
AI Workflow Automation

Each initiative is tailored to your maturity model, ensuring that every hour spent delivers tangible progress.

(one)
eSecurity

Readiness · Detection · Response

Cybersecurity is not a list of hashes.
It is a dynamic strategy towards your maturity.

sales@one-esecurity.com

For incidents, please contact us:

+34 91 10 10 480

incident@one-esecurity.com