BASE4
SECURITY

*We help building a
more secure digital ecosystem!*

CyberSOC

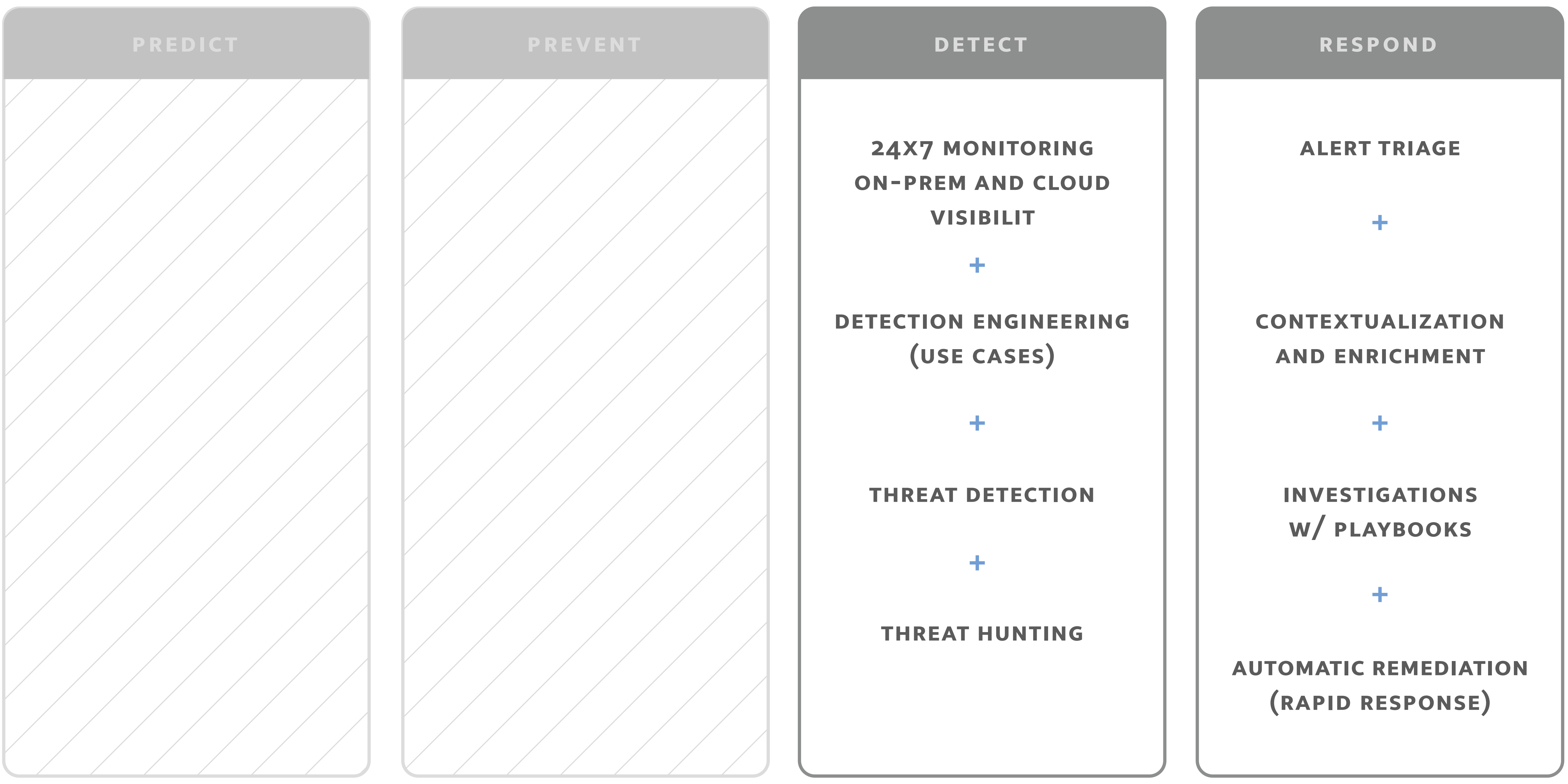
DATA SHEET

Managed Detection and Response (MDR)

MONITORING

24X7

The objective is to generate visibility on cyber threats that may affect the client's assets or critical information. The service performs the detection of possible incidents, which are enriched and contextualized in order to prioritize and respond to them with the possibility of automatic remediation. CyberSOC has extensive experience monitoring on-prem and cloud environments (SaaS, IaaS, PaaS).



PREDICT

PREVENT

DETECT

24X7 MONITORING ON-PREM AND CLOUD VISIBILIT
+
DETECTION ENGINEERING (USE CASES)
+
THREAT DETECTION
+
THREAT HUNTING

RESPOND

ALERT TRIAGE
+
CONTEXTUALIZATION AND ENRICHMENT
+
INVESTIGATIONS W/ PLAYBOOKS
+
AUTOMATIC REMEDIATION (RAPID RESPONSE)

Threat Hunting

The objective of the service is to detect cyber-attacks that go unnoticed by the reactive controls implemented in the organization, using a proactive approach based on MITRE ATT&CK, where our specialists will validate attack hypotheses (TTPs) that an attacker could be executing in search of evidence that confirms the presence of an undetected threat.

Managed Detection and Response OT (MDR OT)

MONITORING

24x7

The service performs continuous monitoring of the organization's industrial networks, detecting possible incidents, in order to investigate them, enrich them by adding context information, prioritize them and thus respond to them. The objective is to generate visibility and respond to cyber threats that may affect the organization's industrial assets.

Tools such as Claroty are used to monitor industrial networks, automatically generating an inventory of the assets present in them and establishing a baseline of behavior, which is then used to search for vulnerabilities, anomalies and/or indicators of possible cyber threats.

PREDICT	PREVENT	DETECT	RESPOND
		24x7 Monitoring + OT Asset Visibility + Threat Detection + Vulnerabilites	ALERT TRIAGE + CONTEXTUALIZATION AND ENRICHMENT + INVESTIGATIONS W/ PLAYBOOKS

Cyber Threat Intelligence (CTI)

24x7

The objective is to keep the client informed and protected from new cyber threats that may affect them. We track and monitor cyber-actors that are attacking in the region and/or the client's industry, investigating their TTPs according to MITRE ATT&ACK and compiling IOCs in dynamic lists that can then be integrated with the client's security platforms for proactive detection and blocking.

PREDICT	PREVENT	DETECT	RESPOND
NEW VULNS AND EXPLOITS + NEW CYBERTHREATS W/ IOCS AND TTPS	IOCS BLOCKING AUTOMATION	IOCS CORRELATION	

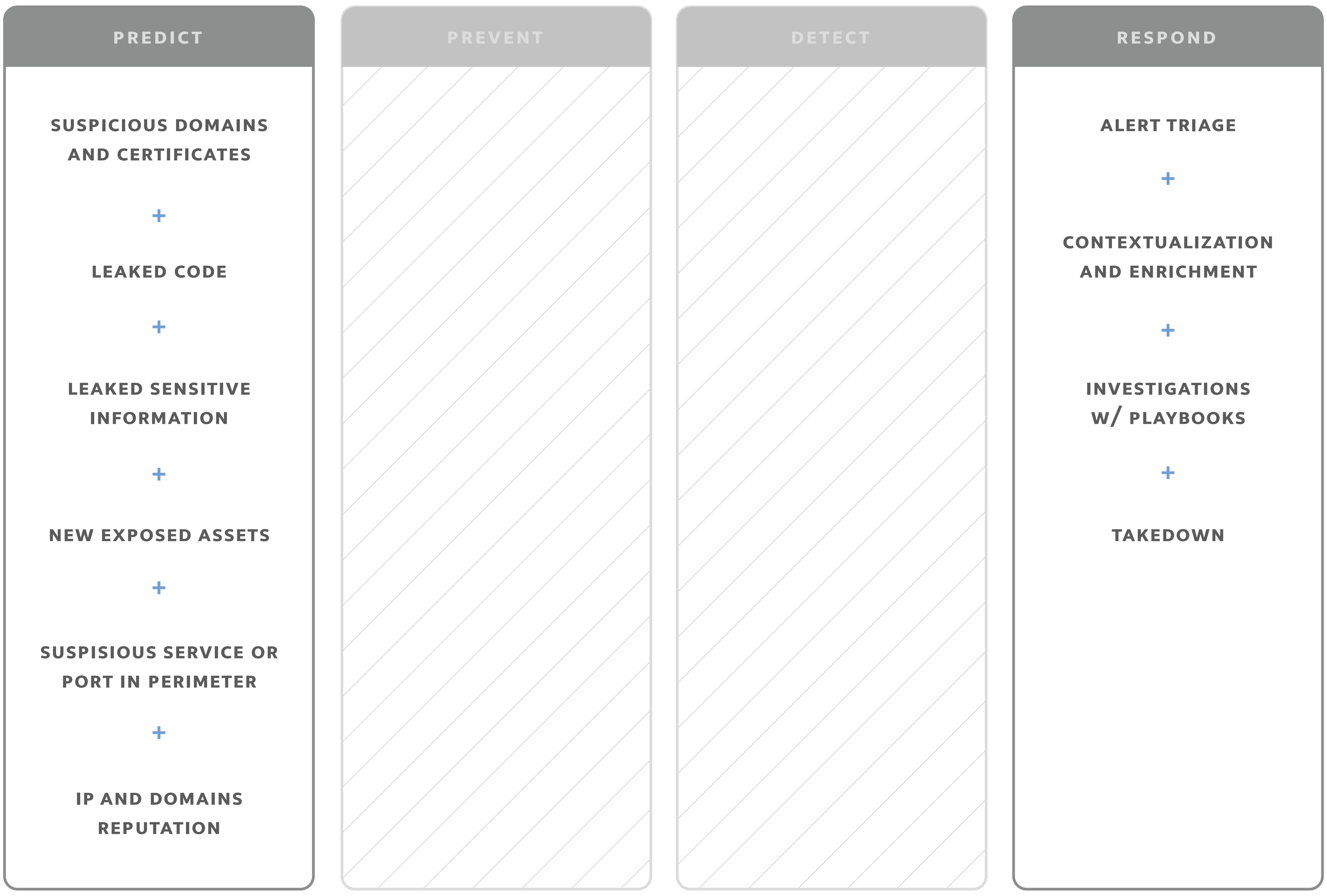
Attack Surface Monitoring (ASM)

MONITORING

24x7

Continuous 24x7 monitoring of the customer's external attack surface on the Internet. The objective of the service is to predict and detect possible attack vectors, as an attacker would see them as soon as possible, in order to avoid a cybersecurity incident.

Exposed assets, open ports, DNS records, certificates, code repositories, among others, are monitored in order to predict possible digital risks before they are detected by an attacker.



PREDICT

SUSPICIOUS DOMAINS AND CERTIFICATES
+
LEAKED CODE
+
LEAKED SENSITIVE INFORMATION
+
NEW EXPOSED ASSETS
+
SUSPISIOUS SERVICE OR PORT IN PERIMETER
+
IP AND DOMAINS REPUTATION

PREVENT

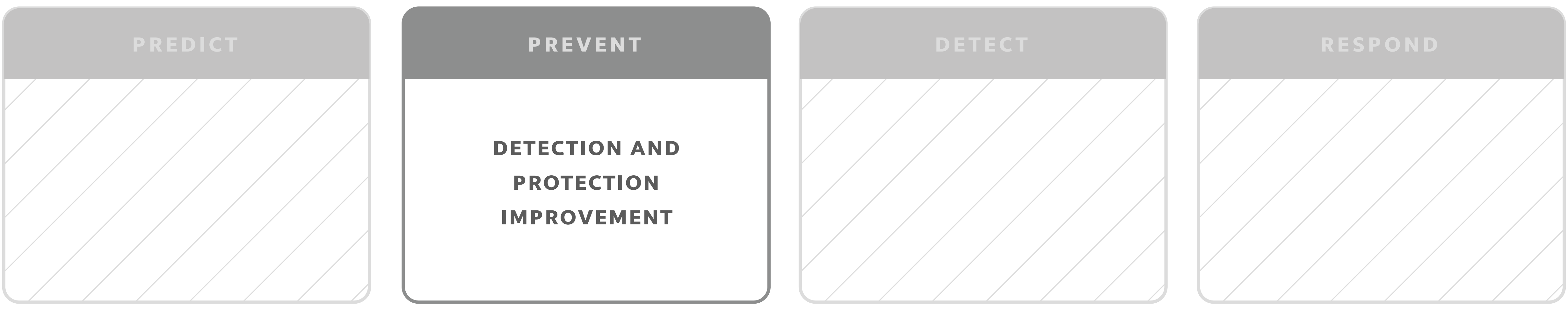
DETECT

RESPOND

ALERT TRIAGE
+
CONTEXTUALIZATION AND ENRICHMENT
+
INVESTIGATIONS W/ PLAYBOOKS
+
TAKEDOWN

Purple Teaming

The objective of the service is the continuous improvement of the security posture, with a cyber intelligence approach we will simulate cyber-attacks according to the Tactics, Techniques and Procedures (TTPs) of the cyber-actors that could attack your organization, in order to improve your organization's detections and protections to prevent future incidents.



PREDICT

PREVENT

DETECTION AND PROTECTION IMPROVEMENT

DETECT

RESPOND

Cyber Deception

It is a defensive practice service that aims to deceive attackers by distributing a series of traps and lures in the organization's infrastructure to mimic genuine assets, so that if an intruder uses them, the attack vectors (IOCs and TTPs) used during the period of the attack can be detected and monitored. This service extends the detection capabilities of internal (insiders) and/or external attackers and facilitates the production of reliable metrics and indicators around real IOCs and TTPs used by attackers to attempt to breach the organization, which can then be used to improve detection and prevention capabilities thus improving the security posture of the organization.

PREDICT	PREVENT	DETECT	RESPOND
▨	HONEYPOT PROJECT DEVELOPMENT + IOCS BLOCKING AUTOMATION	THREAT DETECTION + IOC RECOLECTION	▨

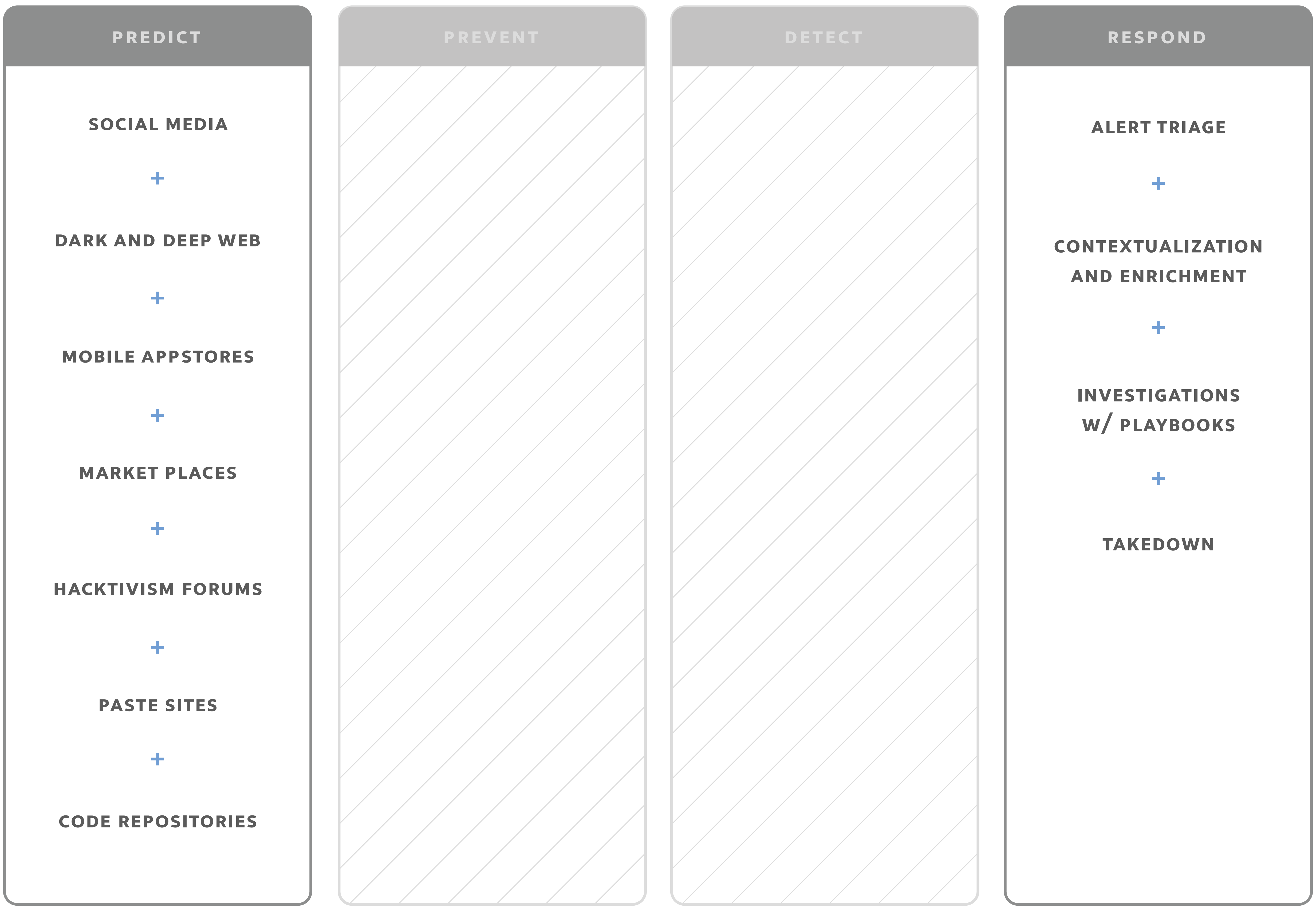
Digital Risk Monitoring (DRM)

MONITORING

CONTINUOUS

24X7

Monitoring of the client’s external attack surface on the internet, deep and dark web. The objective of the service is to predict and detect possible attack vectors as an attacker would see them as soon as possible, in order to avoid a cybersecurity incident. Social networks, marketplaces, paste and code sites, DNS records, certificates, among others, are monitored in search of possible brand fraud, information leaks and/or potential digital risks.



PREDICT

SOCIAL MEDIA
+
DARK AND DEEP WEB
+
MOBILE APPSTORES
+
MARKET PLACES
+
HACKTIVISM FORUMS
+
PASTE SITES
+
CODE REPOSITORIES

PREVENT

DETECT

RESPOND

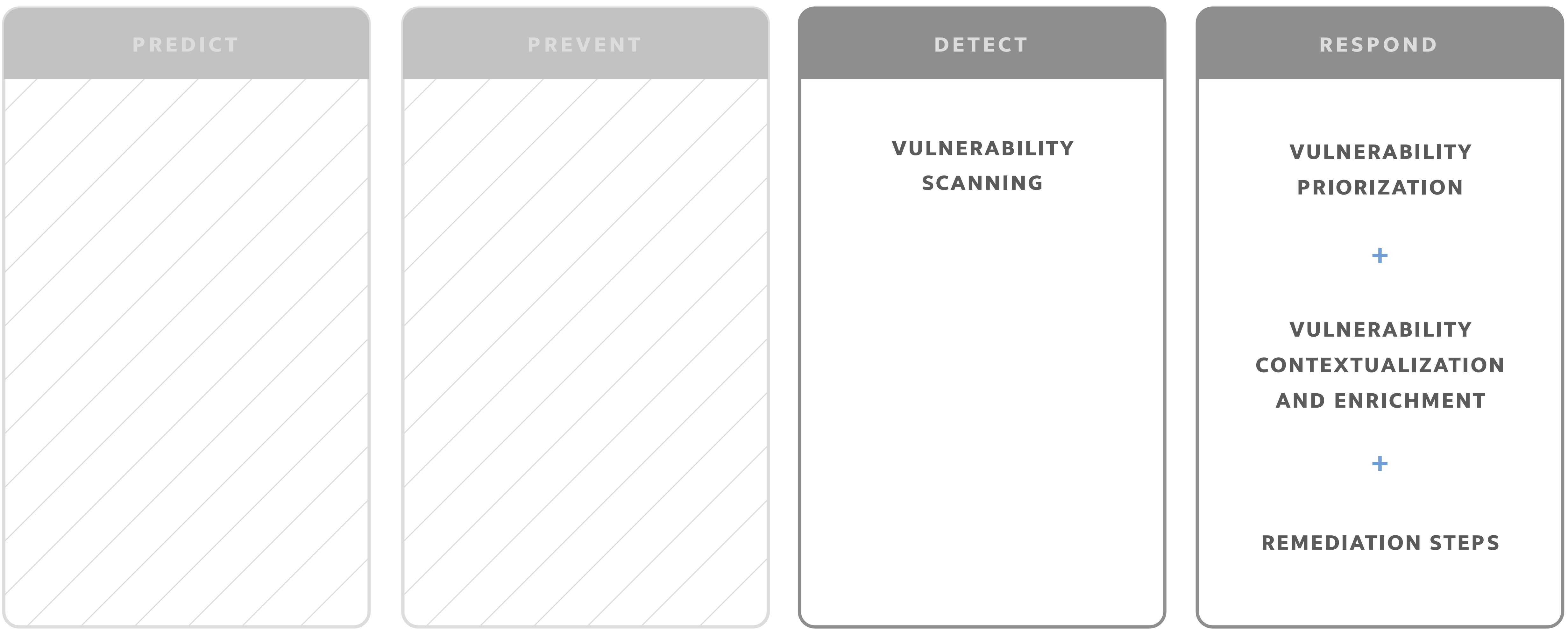
ALERT TRIAGE
+
CONTEXTUALIZATION AND ENRICHMENT
+
INVESTIGATIONS W/ PLAYBOOKS
+
TAKEDOWN

Continuous Cloud Security Assessment (CCSA)

MONITORING

24X7

Vulnerability scanning and management based on best-of-breed technology. CyberSoc helps protect your critical assets on-premise and in the cloud, and also provides expertise and best practices when recommending mitigations to prevent future cyber-attacks.



PREDICT	PREVENT	DETECT	RESPOND
		VULNERABILITY SCANNING	VULNERABILITY PRIORIZATION + VULNERABILITY CONTEXTUALIZATION AND ENRICHMENT + REMEDIATION STEPS

Vulnerability Management Services (VMS)

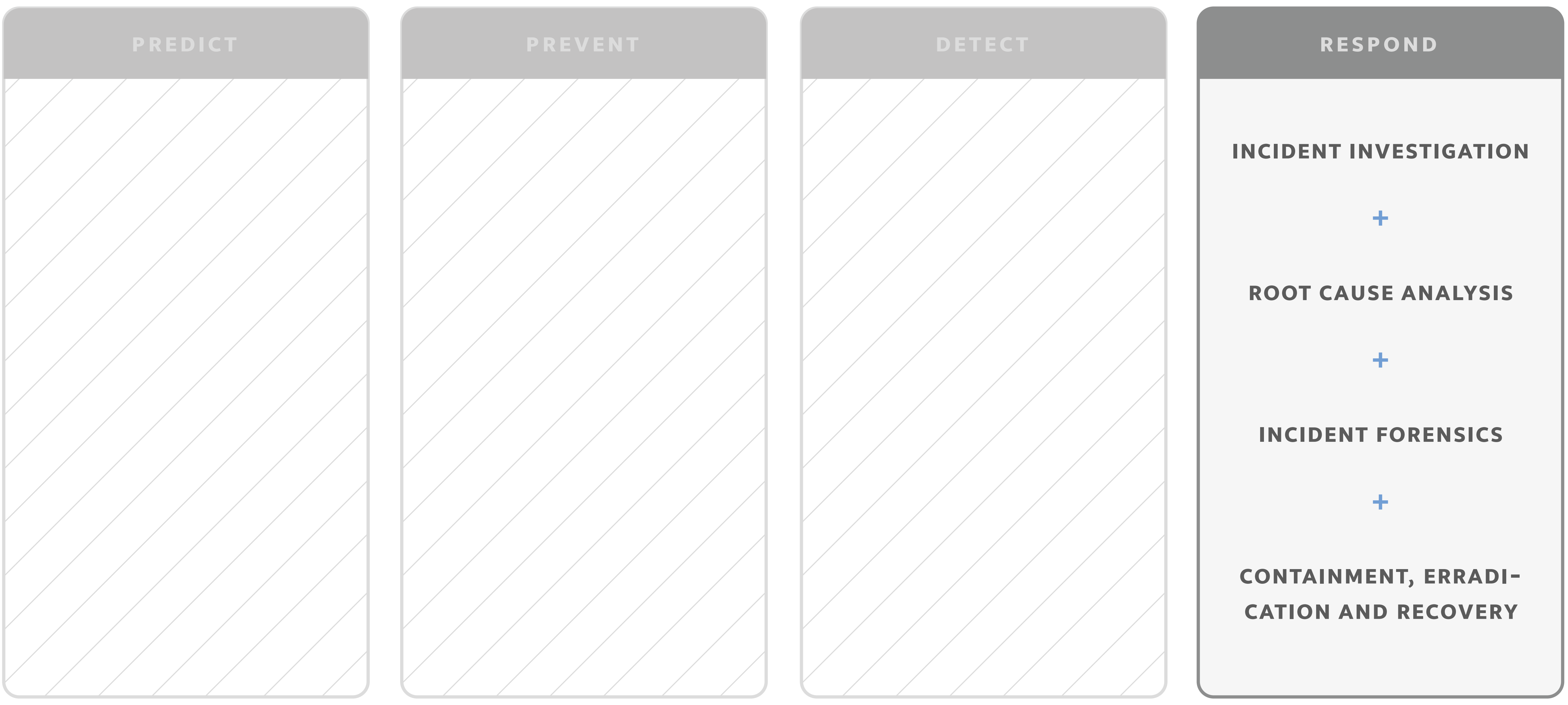
24x7 vulnerability scanning and management service, based on the best technology in the market. CyberSoc helps protect your critical assets on-premise and in the cloud, also provides expertise and best practices when recommending mitigations to prevent future cyber-attacks.

PREDICT	PREVENT	DETECT	RESPOND
	CLOUD CONFIGURATION COMPLIANCE	CLOUD MISSCONFIGURATION IDENTIFICATION	FINDING PRIORIZATION + REMEDIATION STEPS

CSIRT

Incident Response Assistance (IRA)

Respond immediately to cybersecurity incidents that affect your organization and impact your business. Service executed by a multidisciplinary CSIRT team that applies to Ransomware-type attacks and urgent cybersecurity incidents, including identity theft, data theft, computer espionage, among others.



PREDICT

PREVENT

DETECT

RESPOND

INCIDENT INVESTIGATION

+

ROOT CAUSE ANALYSIS

+

INCIDENT FORENSICS

+

CONTAINMENT, ERRADICATION AND RECOVERY

Table Top Exercise (TTX)

Evaluates a cyber incident response plan through a simulated scenario.

The simulation exercise evaluates your organization’s processes, tools and capabilities when responding to cyber-attacks, both from an executive, strategic and technical incident response standpoint. During each exercise, several scenarios based on real-world experiences are presented in a roundtable environment to observe the organization’s simulated actions and decisions.

BASE4
SECURITY

www.base4sec.com