BASE4 SECURITY

Ajudando a construir um ecossistema digital mais seguro.

CyberSOC

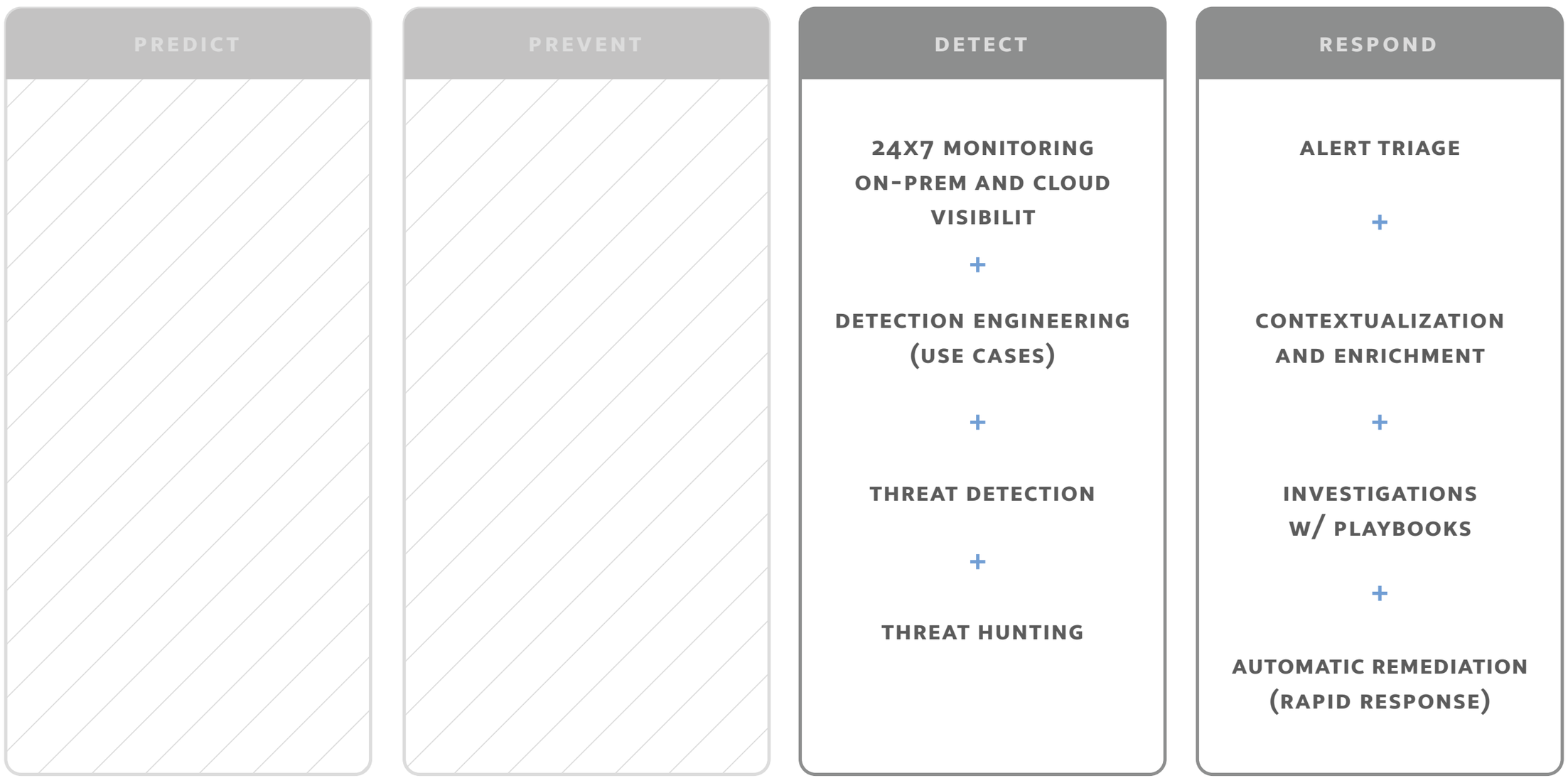
DATA SHEET

Managed Detection and Response (MDR)

MONITORAMENTO

24X7

O objetivo é gerar visibilidade das ameaças cibernéticas que podem afetar os ativos ou informações críticas do cliente. O serviço detecta possíveis incidentes, que são enriquecidos e contextualizados a fim de priorizar e responder a eles com a possibilidade de remediação automática. CyberSOC tem ampla experiência no monitoramento de ambientes on-prem e em nuvem (SaaS, IaaS, PaaS).



Threat Hunting

O objetivo do serviço é detectar ciberataques que passam despercebidos pelos controles reativos implementados na organização, usando uma abordagem proativa baseada no MITRE ATT&CK, onde nossos especialistas validarão hipóteses de ataque (TTPs) que um atacante poderia estar executando em busca de evidências que confirmem a presença de uma ameaça não detectada.

Managed Detection and Response OT (MDR OT)

MONITORAMENTO

24X7

O serviço realiza um monitoramento contínuo das redes industriais da organização, detectando possíveis incidentes, a fim de investigá-los, enriquecê-los adicionando informações contextuais, priorizá-los e assim responder a eles. O objetivo é gerar visibilidade e responder a ameaças cibernéticas que possam afetar os ativos industriais da organização.

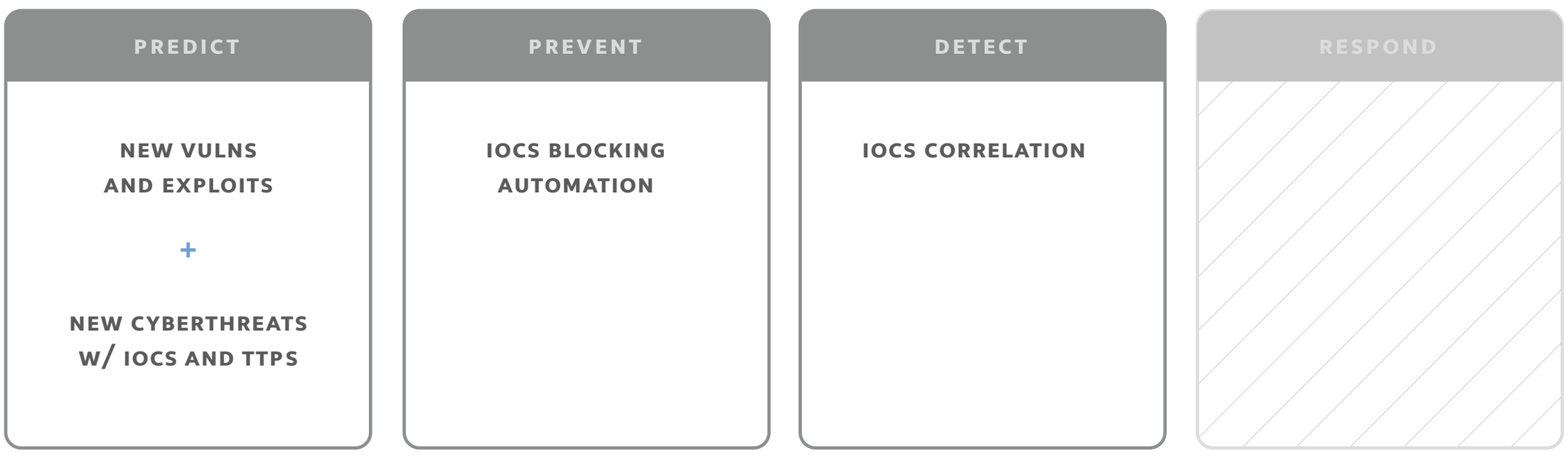
Ferramentas como Claroty são usadas para monitorar redes industriais, gerando automaticamente um inventário dos ativos presentes nelas e estabelecendo uma linha de base de comportamento, que é então usada para buscar vulnerabilidades, anomalias e/ou indicadores de possíveis ameaças cibernéticas.

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

O objetivo é manter o cliente informado e protegido de novas ameaças cibernéticas que possam afetá-lo. Rastreamos e monitoramos os ciberatores que estão atacando na região e/ou na indústria do cliente, investigando seus TTPs de acordo com o MITRE ATT&ACK e compilando IOCs em listas dinâmicas que podem então ser integradas com as plataformas de segurança do cliente para detecção e bloqueio proativos.



Attack Surface Monitoring (ASM)

MONITORAMENTO

24X7

Monitoramento contínuo 24x7 da superfície de ataque externo do cliente na Internet. O objetivo do serviço é prever e detectar possíveis vetores de ataque, como um atacante os veria o mais cedo possível, a fim de evitar um incidente de ciber-segurança.

Ele monitora ativos expostos, portas abertas, registros DNS, certificados, repositórios de código, entre outros, a fim de prever possíveis riscos digitais antes que eles sejam detectados por um atacante.

PREDICT	PREVENT	DETECT	RESPOND
SUSPICIOUS DOMAINS AND CERTIFICATES + LEAKED CODE + LEAKED SENSITIVE INFORMATION + NEW EXPOSED ASSETS + SUSPISIOUS SERVICE OR PORT IN PERIMETER + IP AND DOMAINS REPUTATION			ALERT TRIAGE + CONTEXTUALIZATION AND ENRICHMENT + INVESTIGATIONS W/ PLAYBOOKS + TAKEDOWN

Purple Teaming

O objetivo do serviço é a melhoria contínua da postura de segurança, com uma abordagem de inteligência cibernética simularemos ciberataques de acordo com as Táticas, Técnicas e Procedimentos (TTPs) dos ciberatores que poderiam atacar sua organização, a fim de melhorar as detecções e proteções de sua organização para prevenir futuros incidentes.

PREDICT	PREVENT	DETECT	RESPOND
	DETECTION AND PROTECTION IMPROVEMENT		

Cyber Deception

É um serviço de prática defensiva que visa enganar os atacantes, distribuindo uma série de armadilhas e iscas na infra-estrutura da organização para imitar os ativos genuínos, para que, se um intruso os utilizar, os vetores de ataque (IOCs e TTPs) utilizados durante o período do ataque possam ser detectados e monitorados.

Este serviço amplia as capacidades de detecção de invasores internos (internos) e/ou externos e facilita a produção de métricas e indicadores confiáveis em torno de IOCs e TTPs reais usados por invasores para tentar violar a organização, que podem então ser usados para melhorar as capacidades de detecção e prevenção, melhorando assim a postura de segurança da organização.

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

Digital Risk Monitoring (DRM)

MONITORAMENTO

CONTINUO

24X7

Monitoramento da superfície de ataque externo do cliente na internet, em rede profunda e escura. O objetivo do serviço é prever e detectar possíveis vetores de ataque como um atacante os veria o mais cedo possível, a fim de evitar um incidente de ciber-segurança. Redes sociais, mercados, sites colados e codificados, registros DNS, certificados, entre outros, são monitorados quanto a possíveis fraudes de marca, vazamentos de informações e/ou potenciais riscos digitais.

PREDICT	PREVENT	DETECT	RESPOND
SOCIAL MEDIA + DARK AND DEEP WEB + MOBILE APPSTORES + MARKET PLACES + HACKTIVISM FORUMS + PASTE SITES + CODE REPOSITORIES			ALERT TRIAGE + CONTEXTUALIZATION AND ENRICHMENT + INVESTIGATIONS W/ PLAYBOOKS + TAKEDOWN

Continuous Cloud Security Assessment (CCSA)

MONITORAMIENTO

24X7

Vulnerabilidade de escaneamento e gerenciamento com base na melhor tecnologia de ponta. O CyberSoc ajuda a proteger seus ativos críticos no local e na nuvem, além de fornecer experiência e melhores práticas na recomendação de mitigações para evitar futuros ciberataques.

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

Vulnerability Management Services (VMS)

Serviço de varredura e gerenciamento de vulnerabilidade 24x7, com base na melhor tecnologia do mercado. O CyberSoc ajuda a proteger seus ativos críticos no local e na nuvem, e também fornece sua experiência e melhores práticas ao recomendar mitigações para evitar futuros ciberataques.

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

CSIRT

Incident Response Assistance (IRA)

Responda imediatamente aos incidentes de segurança cibernética que afetam sua organização e impactam seus negócios. Serviço executado por uma equipe multidisciplinar CSIRT que se aplica a ataques do tipo Ransomware-type e incidentes urgentes de cibersegurança, incluindo roubo de identidade, roubo de dados, espionagem cibernética, entre outros.

PREDICT	PREVENT	DETECT	RESPOND
			INCIDENT INVESTIGATION + ROOT CAUSE ANALYSIS + INCIDENT FORENSICS + CONTAINMENT, ERRADI-CATION AND RECOVERY

Table Top Exercise (TTX)

Avalia um plano de resposta a incidentes cibernéticos através de um cenário simulado.

O exercício de simulação avalia os processos, ferramentas e capacidade de sua organização em responder a ataques cibernéticos, tanto do ponto de vista executivo, estratégico e técnico de resposta a incidentes. Durante cada exercício, vários cenários baseados em experiências do mundo real são apresentados em um ambiente de mesa redonda para observar as ações e decisões simuladas da organização.

BASE4
SECURITY

www.base4sec.com