BASE4 SECURITY

Ayudando a construir un ecosistema digital más seguro.

CyberSOC

DATA SHEET

Managed Detection and Response (MDR)

MONITOREO

24X7

El objetivo es generar visibilidad sobre las ciberamenazas que puedan afectar los activos o información crítica del cliente. El servicio realiza la detección de posibles incidentes, los cuales son enriquecidos y contextualizados con el fin de priorizar y responder ante los mismos con posibilidad de remediación automática.

CyberSOC cuenta con una amplia experiencia monitoreando ambientes on-prem y cloud (SaaS, IaaS, PaaS).

PREDICT	PREVENT	DETECT	RESPOND
		24X7 MONITORING ON-PREM AND CLOUD VISIBILIT + DETECTION ENGINEERING (USE CASES) + THREAT DETECTION + THREAT HUNTING	ALERT TRIAGE + CONTEXTUALIZATION AND ENRICHMENT + INVESTIGATIONS W/ PLAYBOOKS + AUTOMATIC REMEDIATION (RAPID RESPONSE)

Threat Hunting

El objetivo del servicio es detectar ciberataques que pasan desapercibidos a los controles reactivos implementados en la organización, para esto se emplea un enfoque proactivo basado en MITRE ATT&CK, donde nuestros especialistas validarán hipótesis de ataques (TTPs) que podría estar ejecutando un atacante en búsqueda de evidencia que confirme la presencia de una amenaza aún no detectada.

Managed Detection and Response OT (MDR OT)

MONITOREO

24X7

El servicio realiza el monitoreo continuo de las redes industriales de la organización, detectando posibles incidentes, con el fin de investigarlos, enriquecerlos agregándoles información de contexto, priorizarlos y así, responder ante los mismos. El objetivo es generar visibilidad y dar respuesta ante ciberamenazas que puedan afectar a los activos industriales de la organización.

Se utilizan herramientas como Claroty para el monitoreo de las redes industriales, generando automáticamente un inventario de los activos presentes en las mismas y estableciendo una línea base de comportamiento, que luego es utilizada en búsqueda de vulnerabilidades, anomalías y/o indicadores de posibles ciberamenazas.

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

El objetivo es mantener informado y protegido al cliente de las nuevas amenazas cibernéticas que lo puedan llegar a afectar. Se realiza un seguimiento y monitoreo de ciberactores que estén atacando en la región y/o a la industria del cliente, investigando sus TTPs según MITRE ATT&ACK y recopilando IOCs en listas dinámicas que luego pueden ser integradas con las plataformas de seguridad del cliente para realizar detecciones y bloqueos proactivos.

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

Attack Surface Monitoring (ASM)

MONITOREO

24X7

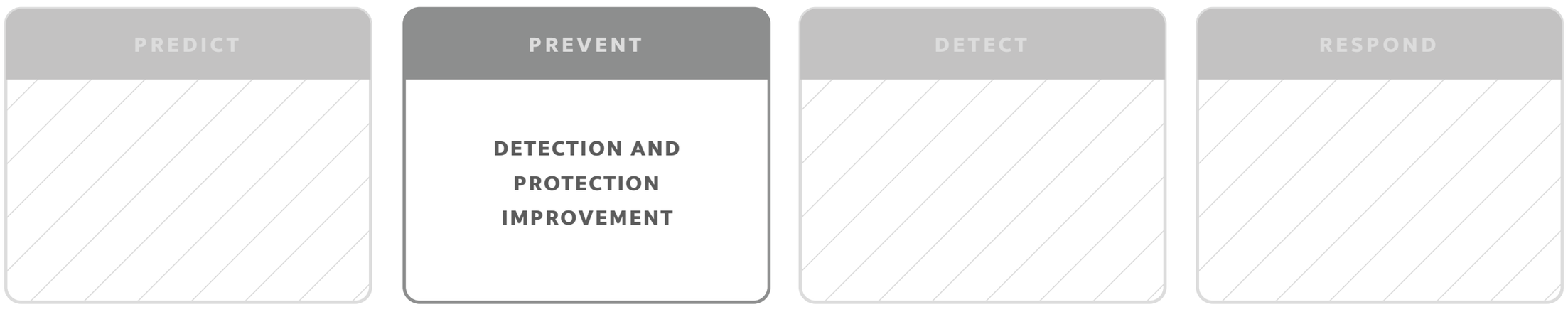
Monitoreo continuo 24x7 de la superficie de ataque externa del cliente en internet. El objetivo del servicio es predecir y detectar posibles vectores de ataque, como los vería un atacante lo antes posible, para así evitar un incidente de ciberseguridad.

Se monitorea activos expuestos, puertos abiertos, registros DNS, certificados, repositorios de código, entre otros, en búsqueda de predecir posibles riesgos digitales antes de que los detecte un 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

El objetivo del servicio es la mejora continua de la postura de seguridad, con un enfoque de ciberinteligencia simularemos ciberataques según las Tácticas, Técnicas y Procedimientos (TTPs) de los ciberactores que podrían atacar a su organización, con el fin de mejorar las detecciones y protecciones de su organización para prevenir futuros incidentes



Cyber Deception

Es un servicio de práctica defensiva que tiene como objetivo engañar a los atacantes mediante la distribución de una serie de trampas y señuelos en la infraestructura de la organización para imitar activos genuinos, de forma que si un intruso los utiliza, se puedan detectar y monitorear los vectores de ataque (IOCs y TTPs) utilizados durante el período del ataque. Este servicio amplía las capacidades de detección de atacantes internos (insiders) y/o externos y facilita la producción de métricas e indicadores confiables en torno a IOCs y TTPs reales que utilizan los atacantes para intentar vulnerar a la organización, que luego pueden utilizarse para mejorar las capacidades de detección y prevención mejorando así la postura de seguridad de la misma.

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

Digital Risk Monitoring (DRM)

MONITOREO

CONTINUO

24X7

Monitoreo de la superficie de ataque externa del cliente en internet, deep y dark web. El objetivo del servicio es predecir y detectar posibles vectores de ataque como los vería un atacante lo antes posible, para así evitar un incidente de ciberseguridad. Se monitorean redes sociales, marketplaces, sitios de paste y de código, registros DNS, certificados, entre otros, en búsqueda de posibles fraudes a la marca, leaks de información y/o potenciales riesgos digitales.

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)

MONITOREO

24X7

Escaneo y gestión de vulnerabilidades basados en la mejor tecnología del mercado. CyberSoc ayuda a proteger tus activos críticos on-premise y en cloud, también aporta su experiencia y mejores prácticas a la hora de recomendar mitigaciones para prevenir futuros ciberataques.

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

Vulnerability Management Services (VMS)

Servicio 24x7 de escaneo y gestión de vulnerabilidades, basados en la mejor tecnología del mercado. CyberSoc ayuda a proteger tus activos críticos on-premise y en cloud, también aporta su experiencia y mejores prácticas a la hora de recomendar mitigaciones para prevenir futuros ciberataques.

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

CSIRT

Incident Response Assistance (IRA)

Responde de forma inmediata a los incidentes de ciberseguridad que afecten a tu organización e impacten al negocio. Servicio ejecutado por un equipo multidisciplinario de CSIRT que aplica a ataques del tipo Ransomware y a los incidentes de ciberseguridad urgentes, incluidos robo de identidades, robo de datos, espionaje informático, entre otros.

PREDICT	PREVENT	DETECT	RESPOND
			INCIDENT INVESTIGATION + ROOT CAUSE ANALYSIS + INCIDENT FORENSICS + CONTAINMENT, ERRADICATION AND RECOVERY

Table Top Exercise (TTX)

Evalúa un plan de respuesta a incidentes cibernéticos a través de un escenario simulado.

El ejercicio de simulación evalúa los procesos, las herramientas y la capacidad de su organización a la hora de responder a ciberataques, tanto desde el punto de vista ejecutivo y estratégico como técnico de la respuesta ante incidentes. Durante cada ejercicio, se presentan varios escenarios basados en experiencias del mundo real en un entorno de mesa redonda para observar las acciones y las decisiones simuladas de la organización.

BASE4
SECURITY

www.base4sec.com

© 2023 BASE4 Security S.A.
Todos los derechos reservados.