Tel.:++421/55/622 85 82,84
e-mail: obchod@ecm-monitory.sk

Dodávka, montáž a servis priemyselných meracích prístrojov, analyzátorov a kontinuálnych monitorovacích systémov plynov, kvapalín a častíc pre ekologické a procesné aplikácie. Komplexné riešenia v oblasti kybernetickej bezpečnosti v súlade s požiadavkami NIS2.

Pure|Defense MDR Service for SMB

> **Pure|Defense MDR for SMB** je **spravovaná služba riadenej detekcie a organizovanej reakcie** na hrozby kybernetickej bezpečnosti, optimalizovaná pre malé a stredné spoločnosti (ďalej len MDR)

Autor projektu a garant riešenia

Igor Kapitančík

Digitally signed by Igor Kapitančík
DN: cn=Igor Kapitančík, c=SK, email=igor.kapitancik@igoo.sk
Reason: I am the author of this document
Date: 2025.04.01 09:30:14 +02'00'

Igor Kapitančík

SANS / GIAC Security Operations Manager (GSOM) — SANS / GIAC Certified Forensic Analyst (GCFA)

Security Service and Solution Architect
Certified Cybersecurity Operations Leader
Security Automation and Orchestration System Architect
Software Developer with Security Expertise
Senior Security & Monitoring Specialist / Analyst
Senior IT Administrator

MDR služba poskytuje nepretržité monitorovanie hrozieb, pokročilú detekciu a rýchlu reakciu na incidenty prostredníctvom riadenej analýzy s použitím **generatívnej umelej inteligencie** (ďalej len **AI**), expertného **aktívneho vyhľadávania hrozieb** (ďalej len **Threat Hunting**) a adaptívnych **protokolov reakcie** (ďalej len **playbook**) kybernetickej obrany, čím zabezpečuje rýchlu neutralizáciu hrozieb a proaktívne obmedzenie šírenia voči vyvíjajúcim sa kybernetickým hrozbám.

Ako poskytovateľ **MDR služieb** poskytujeme proaktívne riešenie kybernetickej bezpečnosti s využitím výstupov strategickej Threat Intelligence analýzy, ktoré je navrhnuté tak, aby nepretržite monitorovalo, detegovalo a okamžite reagovalo na vyvíjajúce sa kybernetické hrozby. Využitím analýz riadených umelou inteligenciou a odborníkmi, behaviorálnej detekcie hrozieb a vyšetrovania vedeného našim expertným tímom, zabezpečujeme okamžitý prehľad o bezpečnostných incidentoch, čo umožňuje rýchlu neutralizáciu bezpečnostných hrozieb v počiatočných fázach a okamžité zamedzenie šírenia incidentov. Náš prístup zabezpečuje, že hrozby sú eliminované ešte pred ich eskaláciou, čím sa minimalizujú prevádzkové výpadky a predchádza narušeniam bezpečnosti.

Naša služba funguje na základe adaptívneho bezpečnostného obranného a reakčného protokolu (palybooku) špecifického pre jednotlivé hrozby, ktorý zabezpečuje efektívne implementovanie karanténnych postupov počas incidentu a kontrolu šírenia hrozieb s cieľom zabrániť ich rozšíreniu. Integrujeme usmernenia a návody na riešenie incidentov, stratégie zmierňovania hrozieb a poradenstvo v oblasti riadenia rizík, čím zosúlaďujeme bezpečnostné operácie s požiadavkami regulačných autorít a osvedčenými priemyselnými postupmi. Vďaka našim 24/7 SOC (Security Operation Center / **Centrum operácií kybernetickej bezpečnosti**) operáciám, proaktívnemu Threat Huntingu a automatizovanou reakciou, zvyšujeme odolnosť voči kybernetickým hrozbám, poskytujeme komplexnú kontrolu hrozieb a neustále zlepšujeme bezpečnostnú úroveň organizácií, a tým im aktívne pomáhame brániť sa proti pokročilým kybernetickým protivníkom.

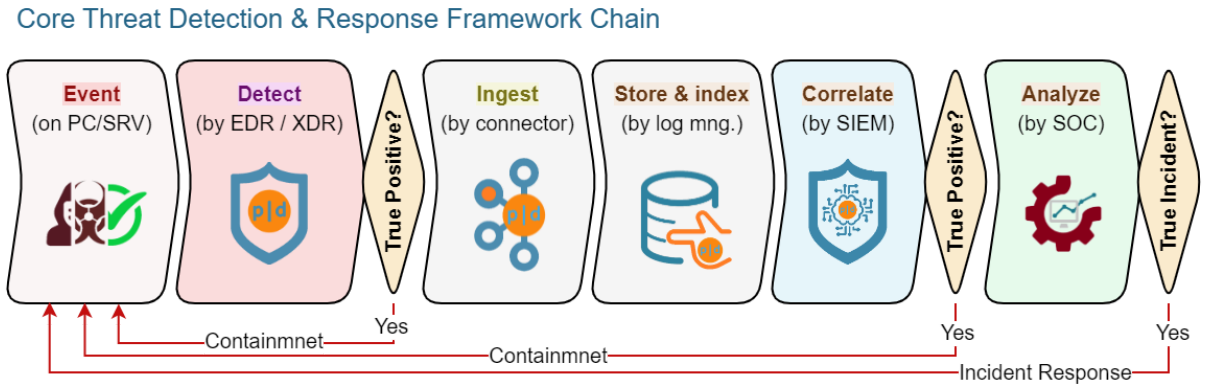
Core Threat Detection & Response Framework

> **Základný operačný rámec detekcie a reakcie na hrozby**

Základný operačný rámec detekcie a reakcie na hrozby predstavuje základný plán, ktorý definuje, ako moderné MDR služby systematicky identifikujú, vyšetrujú a reagujú na kybernetické hrozby v reálnom čase. Proces zvyčajne začína **udalosťou na hostiteľovi** (Event on Host), ako je neoprávnené spustenie procesu, podozrivý pokus o prihlásenie alebo anomálne správanie systému. Tieto udalosti sú najskôr detegované nástrojmi **XDR (Extended Detection and Response)**, ktoré nielen poskytujú rozsiahlu telemetriu naprieč koncovými zariadeniami, sieťami, cloudovým prostredím a identitami, ale tiež **automaticky vykonávajú zadržiavacie opatrenia pri známych hrozbách**, aby zabránili ich šíreniu a minimalizovali dopad ešte pred začiatkom následnej analýzy. Po detekcii sú základné telemetrické dáta alebo udalosti **prijaté konektorom do centralizovanej**

bezpečnostnej platformy, kde sú spracované a obohatené. Následne sú **uložené a indexované systémom pre správu logov (Log Management)**, čo zaručuje ich dostupnosť pre analýzu v reálnom čase aj retrospektívne hodnotenie. Takto štruktúrované dáta sú potom **korelované pomocou SIEM (Security Information and Event Management)**, ktorý aplikuje preddefinované detekčné pravidlá, **krížovo overuje informácie z threat intelligence feedov, behaviorálnych modelov a základných vzorcov**, ako aj **známe indikátory kompromitácie (IoCs)** na identifikáciu významných vzorcov správania.

Udalosti (Alert, Event), ktoré sú generované a obohatené prostredníctvom tejto korelácie, sú následne **analyzované tímom v Pure|Defense SOC**, kde analytici aplikujú **kontextuálne chápanie a metodiky aktívneho threat huntingu** na vyhodnotenie závažnosti, overenie nálezov, preskúmanie súvislostí a určenie, či upozornenie predstavuje skutočnú hrozbu, falošne pozitívny výstup, alebo potenciálne falošne negatívny prípad spôsobený medzerami v detekcii — a v prípade potreby **iniciujú reakčné opatrenia**. Tento rámec podporuje **plynulú integráciu s automatizovanými playbookmi, postupmi na zadržanie hrozieb a reportovaním riadeným súladom s reguláciami**, čím zabezpečuje **operačnú efektivitu aj regulačnú zhodu**. Zároveň umožňuje **nepretržité zlepšovanie prostredníctvom spätnej väzby**, čím zvyšuje **presnosť detekcie, efektivitu triedenia hrozieb a presnosť reakcií**. Využitím tohto viacvrstvového prístupu — od detekcie po reakciu — môžu organizácie signifikantne znížiť **priemerný čas potrebný na detekciu (MTTD)**, znížiť **dwell time (časový interval, počas ktorého je škodlivý softvér na kompromitovanom zariadení bez povšimnutia)** a zlepšiť svoj celkový **stav kybernetickej bezpečnosti a odolnosť voči hrozbám**. **Integráciou automatizovaného obohacovania, reakcií riadených playbookmi a eskalačných ciest,** rámec zabezpečuje, že hrozby sú **prioritizované, izolované a riešené** včas a systematicky — čím vytvára **operačný základ Pure|Defense MDR služby**.

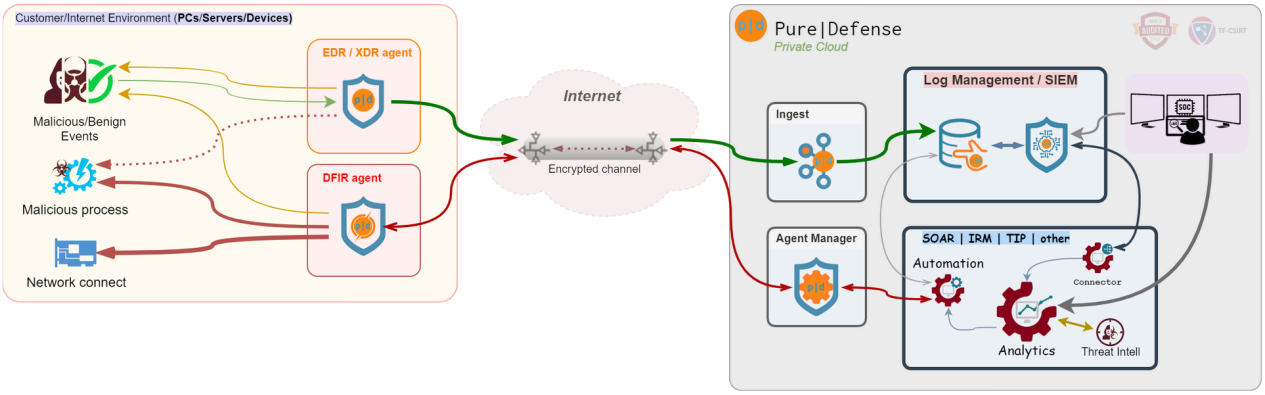


Pure|Defense MDR Service Delivery Models

> **Prevádzkové modely Pure|Defense MDR služby**

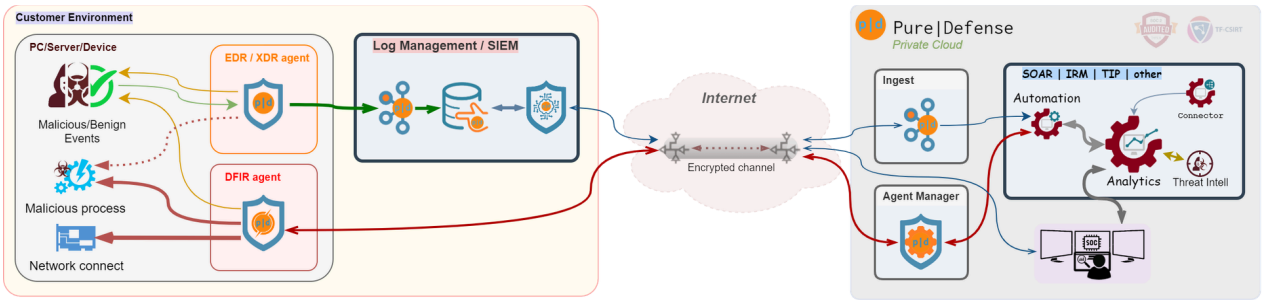
Modely poskytovania služby **Managed Detection and Response (MDR)** definujú **štrukturálny a technologický prístup**, prostredníctvom ktorého sú **kybernetické bezpečnostné služby nasadzované, prevádzkované a integrované do prostredia organizácie**.

Základným modelom je **Pure|Defense MDR postavený na privátnom cloudovom móde (Private Cloud-Based MDR)**, kde sú všetky komponenty — od spracovania detekcie hrozieb, príjmu telemetrie, korelácie udalostí až po orchestráciu reakcií — **bezpečne hosťované v dedikovanej cloudovej infraštruktúre**. Tento prístup zabezpečuje **vysokú dostupnosť, škálovateľnosť a centralizované threat intelligence**, pričom zároveň zachováva **prísnu kontrolu nad ochranou údajov**. Je obzvlášť vhodný pre organizácie, ktoré chcú využiť **pokročilú bezpečnostnú analytiku a nepretržité 24/7 monitorovanie**, a to bez potreby rozsiahlej vlastnej infraštruktúry.



Pure|Defense MDR v móde privátneho cloudu

Pre organizácie s **prísnymi požiadavkami na lokálne umiestnenie dát, regulačnými obmedzeniami alebo potrebou lokálnej kontroly**, je možné MDR službu rozšíriť o službu "**On-Premises Cybersecurity Analytics Platform"**. Tým vzniká **hybridný model MDR (Hybrid Cloud/On-Premises)**, ktorý spája **flexibilitu cloudovej analytiky** s **kontrolou a dátovou suverenitou** on-premise (lokálne) implementovanou časťou. V tomto modeli sú **citlivé telemetrické dáta a logy spracovávané a uchovávané lokálne**, pričom organizácia zároveň profituje z **cloudových korelačných nástrojov, globálneho threat intelligence a centralizovanej podpory zo strany Pure|Defense SOC**. Tento hybridný prístup predstavuje **vyvážené riešenie**, ktoré ponúka **operačnú flexibilitu, zvýšenú kontrolu nad údajmi a potrebný súlad s požiadavkami národných regulátorov**, a je preto ideálne najmä pre **komplexné podnikové prostredia alebo sektory podliehajúce prísnym reguláciám**.



Pure|Defense v hybridnom móde

Pure|Defense Cyber Operations Process Flow

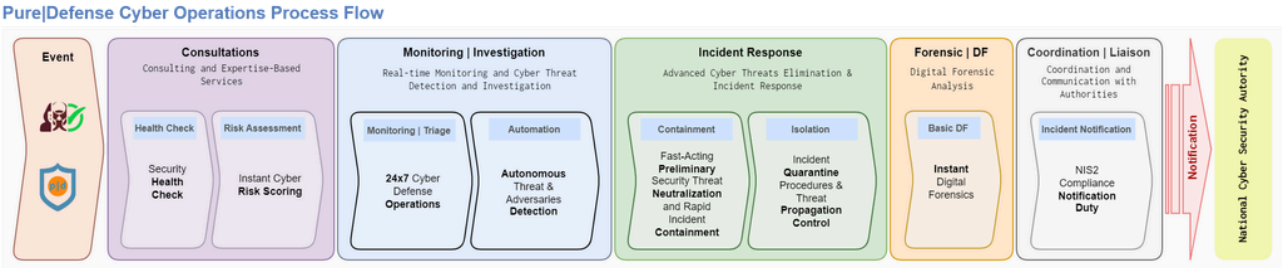
> **Architektúra operačných procesov kybernetickej bezpečnosti služby Pure|Defense MDR**

Architektúra operačných procesov kybernetickej bezpečnosti služby Pure|Defense MDR (Pure|Defense Cyber Operations Process Flow) definuje **štruktúrovanú, end-to-end metodológiu**, prostredníctvom ktorej organizácie **nepretržite monitorujú, detegujú, analyzujú a reagujú na kybernetické hrozby** efektívnym a odolným spôsobom.

Jadrom tohto procesu je prevádzka **24/7 kybernetickej obrany (24x7 Cyber Defense Operations)**, ktorú tvorí kombinácia **autonómnej detekcie hrozieb a protivníkov (Autonomous Threat & Adversaries Detection)** a odborníkmi vedených **operácií okamžitého a nepretržitého aktívneho vyhľadávania hrozieb (Live Cyber Threat Hunting Operations)**. Táto **nepretržitá ostražitosť v reálnom čase** umožňuje bezpečnostným tímom včas identifikovať **anomálne správanie** a okamžite vykonať **predbežné neutralizačné opatrenia (Fast-Acting Preliminary Security Threat Neutralization)**, čím sa predchádza eskalácii hrozieb.

Po potvrdení hrozby sa proces presúva do fázy **rýchlej izolácie incidentu (Rapid Incident Containment)**, počas ktorej sa využívajú **postupy separácie aktív zahrnutých do incidentu (Incident Quarantine Procedures)** a **kontrola šírenia hrozby (Threat Propagation Control)** na izolovanie postihnutých aktív a zastavenie laterálneho pohybu útočníka. Tieto kroky sú koordinované cez "**Cyber Defense & Incident Response Hub" (MDR Portál)**, ktorý poskytuje **prehľad a operačné riadenie** pomocou **panelov kľúčových výkonnostných ukazovateľov a metrík kybernetickej obrany (Cyber Defense Key Performance Indicators & Metrics Dashboards)**.

Celý proces je podporovaný **riadením životného cyklu bezpečnostného incidentu v reálnom čase a eskaláciou (Real-Time Security Incident Life-Cycle Management & Escalation)**, čo zaručuje **včasnú reakciu, zmiernenie dopadov a súlad s regulačnými povinnosťami**, ako je napríklad "**NIS2 Compliance Notification Duty", t.j. povinnosť včasne a bezodkladne informovať národné autority**. V počiatočnej fáze nasadenia Pure|Defense MDR služby sa zároveň realizujú **kontroly stavu bezpečnosti (Security Health Check)** a **rýchle posúdenie rizík (Risk Assessment)**, ktoré slúžia na **overenie pripravenosti organizácie a posilnenie jej kybernetickej odolnosti**. Tento **dynamický a adaptívny proces** zabezpečuje, že organizácie zostávajú **odolné a v súlade s predpismi aj v podmienkach neustále sa vyvíjajúcich kybernetických hrozieb**.



MDR Service Features & Capabilities

> Vlastnosti, parametre a schopnosti služby Pure|Defense MDR

MDR Service Features & Capabilities odkazujú na kľúčové funkcionality a pokročilé bezpečnostné opatrenia, ktoré umožňujú nepretržité monitorovanie hrozieb, proaktívnu detekciu útokov, rýchlu odozvu na incidenty a automatizované zamedzenie šírenia hrozieb.

Služba **Pure|Defense MDR pre SMB** je založená na proaktívnom a AI riadenom prístupe ku kybernetickej bezpečnosti, poskytujúcom nepretržité monitorovanie hrozieb, pokročilú detekciu a rýchlu odozvu na incidenty, aby sme ochránili organizácie pred sofistikovanými kybernetickými hrozbami. Naše operácie využívajú analýzy vytvárané s pomocou AI a vedené odborníkmi, **spravodajskú analýzu kybernetických hrozieb** (ďalej len **Threat Intelligence**) generovanú priebežne v reálnom čase a Threat Hunting, čo umožňuje rýchlu neutralizáciu bezpečnostných hrozieb v počiatočných fázach a okamžitú izoláciu incidentov, aby sa zabránilo eskalácii narušenia. Vďaka automatizovaným mechanizmom detekcie a reakcie dávame bezpečnostným tímom možnosť rýchlo identifikovať, vyšetrovať a riešiť bezpečnostné incidenty s minimálnym dopadom na prevádzkové činnosti organizácie.

Tel.:++421/55/622 85 82,84
e-mail: obchod@ecm-monitory.sk

Dodávka, montáž a servis priemyselných meracích prístrojov, analyzátorov a kontinuálnych monitorovacích systémov plynov, kvapalín a častíc pre ekologické a procesné aplikácie. Komplexné riešenia v oblasti kybernetickej bezpečnosti v súlade s požiadavkami NIS2.

Real-time Monitoring and Cyber Threat Detection and Investigation

Monitoring kybernetickej bezpečnosti v reálnom čase, detekcia kybernetických hrozieb a následná došetrenie podozrivých udalostí

Monitoring | Detekcia | Investigácia

Real-time monitoring and cyber threat detection zabezpečujú nepretržitú viditeľnosť a proaktívnu mitigáciu rizík. Analýzy vytvorené s použitím AI ako aj expertmi, analytikmi a odborníkmi umožňujú rýchlu detekciu hrozieb, hodnotenie rizík a efektívne zvládnutie incidentov. Strategické sledovanie aktív a hodnotenie rizík v reálnom čase posilňujú bezpečnosť, pričom sú v súlade so štandardmi ISO 27001, smernicou NIS2 (vrátane odvodených zákonov a nariadení, napr. §69/2018 Z. z.) a ďalšími normami pre kybernetickú bezpečnosť, reakciu na incidenty, riadenie rizík a podobne.

Funkcia	Pure|Defense SMB	Popis
24x7 Cyber Defense Operations Prevádzka kybernetickej obrany v mode 24/7 Monitoring | Triedenie	OBSAHUJE	Zabezpečuje nepretržité monitorovanie hrozieb, rýchlu odozvu na incidenty a proaktívne zmierňovanie rizík, aby chránil organizácie pred vyvíjajúcimi sa kybernetickými hrozbami v reálnom čase.
Autonomous Threat & Adversaries Detection Automatická detekcia hrozieb a nepriateľských subjektov Automatizácia	OBSAHUJE	Bezpečnostný prístup riadený umelou inteligenciou, ktorý využíva strojové učenie, behaviorálnu analytiku a spravodajstvo o hrozbách na identifikáciu, analýzu a reakciu na kybernetické hrozby a nepriateľské aktivity v reálnom čase bez manuálneho zásahu.
Cyber Security Expert-Driven Cyber Threat Detection Pokročilé vyhľadávanie hrozieb vedené odborníkmi Investigácia	8X5	Kombinuje ľudskú inteligenciu, skúsenosť expertov, pokročilú analytiku kybernetických hrozieb a Threat Intelligence na analýzu komplexných vzorcov útokov, identifikáciu sofistikovaných hrozieb a vykonávanie rýchleho aj hĺbkového forenzného vyšetrovania, čím zabezpečuje presnú a adaptívnu reakciu na incidenty.
Root Cause & Origin Analysis Analýza počiatku a primárnej príčiny kybernetického útoku Analýzy	ADD-ON	Identifikácia primárnej príčiny, vstupného bodu útoku a vektorov hrozieb pri bezpečnostnom incidente s cieľom umožniť efektívnu nápravu a prevenciu budúcich rizík.
Strategic Asset Cyber Surveillance & Extended Monitoring Rozšírené monitorovanie kritických asetov Monitoring kritických asetov	ADD-ON	Proaktívny bezpečnostný proces, ktorý zabezpečuje nepretržitý dohľad, detekciu hrozieb a hodnotenie rizík kritických aktív s cieľom predchádzať kybernetickým hrozbám a udržiavať operačnú odolnosť.

Tel.:++421/55/622 85 82,84
e-mail: obchod@ecm-monitory.sk

Dodávka, montáž a servis priemyselných meracích prístrojov, analyzátorov a kontinuálnych monitorovacích systémov plynov, kvapalín a častíc pre ekologické a procesné aplikácie. Komplexné riešenia v oblasti kybernetickej bezpečnosti v súlade s požiadavkami NIS2.

Advanced Cyber Threats Elimination & Incident Response

Reakcia na incidenty a rozšírená aktívna eliminácia kybernetických hrozieb

Reakcia na incidenty

Proaktívny prístup riadený výstupmi z Threat Intelligence procesu, ktorý využíva detekciu hrozieb riadenú AI, expertnú analýzu a automatizované mechanizmy reakcie na rýchlu identifikáciu, izoláciu a neutralizáciu sofistikovaných kybernetických hrozieb. Integráciou hodnotenia rizík v reálnom čase, forenzných vyšetrovaní a adaptívnych zmierňovacích stratégií zabezpečuje minimálny dopad na prevádzku, operačnú odolnosť a neustále zlepšovanie bezpečnostného postavenia organizácie.

Funkcia	Pure|Defense SMB	Popis
Fast-Acting Preliminary Security Threat Neutralization and Rapid Incident Containment Okamžitá eliminácia bezpečnostných hrozieb Rýchla obranná reakcia Containment | Obranná reakcia	OBSAHUJE	Proaktívny proces kybernetickej bezpečnosti, ktorý zabezpečuje okamžité potlačenie hrozieb, rýchlu izoláciu incidentov a ich zmiernenie, aby sa zabránilo eskalácii a minimalizoval sa dopad na prevádzku. Využitím automatizovaných mechanizmov reakcie a analýzy riadenej odborníkmi umožňuje efektívne zvládnutie incidentov a zrýchlenú obnovu prevádzky po kybernetických útokoch.
Threat-Specific Adaptive Cyber Defense & Response Playbooks Protokoly reakcie explicitne definované pre konkrétne hrozby Playbooks | Protokoly reakcie	OBSAHUJE	Dynamické bezpečnostné protokoly vytvárané expertmi s využitím AI, ktoré poskytujú prispôsobené zmierňovanie hrozieb, rýchlu odozvu na incidenty a adaptívne obranné stratégie šité na mieru konkrétnym kybernetickým hrozbám.
Incident Quarantine Procedures & Threat Propagation Control Izolácia asetu a hrozby v prípade kompromitácie Izolácia	OBSAHUJE	Kritické kybernetické bezpečnostné opatrenia, ktoré izolujú kompromitované systémy a zabraňujú laterálnemu pohybu prostredníctvom automatizovaných mechanizmov reakcie, čím zabezpečujú minimálny dopad a rýchlu neutralizáciu hrozieb.
Incident Handling Guidelines, Threat Mitigation Strategies & Risk Mitigation Advisory Návody a postupy pri detegovaní závažného incidentu Návody | Postupy	ADD-ON	Poskytuje štruktúrované reakčné protokoly, proaktívne opatrenia na zadržiavanie hrozieb a strategické usmernenia na zníženie rizík, čím zabezpečuje efektívne riadenie incidentov, minimálny dopad a zvýšenú odolnosť voči kybernetickým hrozbám.

Tel.:++421/55/622 85 82,84
e-mail: obchod@ecm-monitory.sk

Dodávka, montáž a servis priemyselných meracích prístrojov, analyzátorov a kontinuálnych monitorovacích systémov plynov, kvapalín a častíc pre ekologické a procesné aplikácie. Komplexné riešenia v oblasti kybernetickej bezpečnosti v súlade s požiadavkami NIS2.

Presentation, Reporting, Integration and Notification (*of Detection, Incident and Response*)

Prezentácia, reporty, integrácie a notifikácie detekcií, incidentov a reakcií na incidenty

Portal | Reporty | Notifikácie

Zabezpečuje viditeľnosť hrozieb v reálnom čase, efektívnu reakciu na incidenty a bezpečnostné zlepšenia založené na dátach. Prostredníctvom Centra kybernetickej obrany a reakcie na incidenty využívajú bezpečnostné tímy kľúčové ukazovatele výkonnosti (KPI), riadenie životného cyklu incidentov a kontextovo orientované notifikácie, aby prioritizovali hrozby, zlepšili zdieľanie spravodajských informácií a automatizovali nápravu, čím posilňujú odolnosť voči kybernetickým hrozbám a operačnú pripravenosť.

Funkcia	Pure|Defense SMB	Popis
Cyber Defense & Incident Response Hub Centrum kybernetickej obrany a reakcií na incidenty Portal	OBSAHUJE	Centralizovaná platforma pre bezpečnostné operácie, ktorá integruje detekciu hrozieb v reálnom čase, riadenie incidentov a automatizované reakčné procesy. Umožňuje komunikáciu a efektívne zmierňovanie hrozieb, rýchle riešenie incidentov a neustále zlepšovanie kybernetickej bezpečnosti v rámci organizácie.
Cyber Defense Key Performance Indicators & Metrics Dashboards Prehľady výkonnosti a metrík kybernetickej bezpečnosti Prehľady | Dashboards	OBSAHUJE	Agregovaním kľúčových kybernetických metrík tieto panely (dashboardy) umožňujú proaktívne hodnotenie rizík, monitorovanie výkonnosti a sledovanie súladu s predpismi, čím zabezpečujú rozhodovanie založené na dátach a neustále zlepšovanie bezpečnosti.
Cybersecurity Performance & Metrics Regular Review Pravidelné reporty o stave bezpečnosti Reporty	OBSAHUJE MESAČNE	Štruktúrovaný hodnotiaci proces a výstup, ktorý posudzuje a prezentuje efektivitu detekcie hrozieb, účinnosť reakcie na incidenty a celkové bezpečnostné postavenie na základe kľúčových ukazovateľov výkonnosti (KPI) a metrík v reálnom čase. Analýzou historických trendov, úspešnosti nápravných opatrení a dodržiavania predpisov môžu organizácie identifikovať medzery, optimalizovať bezpečnostné stratégie a posilniť svoju odolnosť voči vyvíjajúcim sa kybernetickým hrozbám.
Real-Time Security Incident Life-Cycle Management (include Escalation) Riadenie životného cyklu kybernetického incidentu Eskalácia Životný cyklus Incidentu | Eskalácia	OBSAHUJE	Štruktúrovaný, komplexný prístup k detekcii, analýze, izolácii a riešeniu bezpečnostných incidentov v reálnom čase. Integráciou automatizovanej detekcie, analýzy s využitím AI a eskalačných protokolov zabezpečuje rýchlu prioritizáciu incidentov, efektívnu koordináciu reakcie a minimálne prevádzkové narušenie, čím posilňuje celkovú kybernetickú odolnosť organizácie.

Tel.:++421/55/622 85 82,84
e-mail: obchod@ecm-monitory.sk

Dodávka, montáž a servis priemyselných meracích prístrojov, analyzátorov a kontinuálnych monitorovacích systémov plynov, kvapalín a častíc pre ekologické a procesné aplikácie. Komplexné riešenia v oblasti kybernetickej bezpečnosti v súlade s požiadavkami NIS2.

Cyber Threat Hunting

Aktívne expertné vyhľadávanie hrozieb

Threat Hunting | TH

Proaktívny, Threat Intelligence riadený prístup, ktorý využíva pokročilé profilovanie hrozieb na zmiernenie rizík, cielené operácie Threat Hunting a nepretržitý celosvetový taktický prehľad nad kybernetickými útokmi na detekciu a neutralizáciu sofistikovaných kybernetických hrozieb. Využitím operácií Threat Huntingu v reálnom čase a hĺbkovej forenznej analýzy hrozieb môžu bezpečnostné tímy identifikovať taktiky útočníkov, analyzovať stopy útokov a zmierňovať riziká v reálnom čase. Tento nepretržitý proces riadený expertmi posilňuje kybernetickú odolnosť, skracuje čas zotrvania hrozby v systéme a zvyšuje proaktívnu obranu proti vyvíjajúcim sa hrozbám.

Function	pure|defense SMB	Description
Live Cyber Threat Hunting Operations Operatívne vyhľadávanie kybernetických hrozieb Operatívny TH	OBSAHUJE	Proaktívny bezpečnostný prístup, ktorý využíva pokročilú Threat Intelligence, behaviorálnu analytiku a detekciu anomálií riadenú umelou inteligenciou na identifikáciu a neutralizáciu kybernetických hrozieb v okamihu ich vzniku. Integráciou nepretržitého monitorovania, forenzného vyšetrovania a rýchlych reakčných mechanizmov a protokolov umožňuje okamžitú detekciu, izoláciu a zmiernenie sofistikovaných nepriateľských aktivít, čím skracuje čas zotrvania hrozby v systéme a posilňuje kybernetickú odolnosť organizácie.

Cyber Threat Intelligence

Spravodajská analýza kybernetických hrozieb

Threat Intelligence | CTI

Proaktívny, spravodajský a riadený prístup, ktorý využíva atribúciu útočníkov a kontextualizáciu incidentov na identifikáciu, analýzu a zmiernenie vyvíjajúcich sa kybernetických hrozieb. Integráciou monitorovania hrozieb na dark webe, ako aj iných hodnotných zdrojov, vrátane interných zdrojov kybernetickej Threat Intelligence získavajú organizácie viditeľnosť hrozieb v reálnom čase, zlepšené detekčné schopnosti a posilnenú kybernetickú odolnosť voči nepriateľským taktikám a novým útočným vektorom.

Function	pure|defense SMB	Description
Proactive Intelligence-Driven Threat Management Proaktívna správa kybernetických hrozieb založená na spravodajských analýze CTI	OZNÁMENIE	Využíva Threat Intelligence v reálnom čase, profilovanie nepriateľských subjektov pôsobiacich v danom hospodárskom segmente a automatizovanú detekciu na predvídanie, identifikáciu a zmiernenie kybernetických hrozieb ešte pred ich eskaláciou, čím zabezpečuje včasné zníženie rizík a adaptívne obranné stratégie. V prípade aktuálnej hrozby MDR dohodnutým spôsobom informuje konštituenta o danej hrozbe.

Tel.:++421/55/622 85 82,84
e-mail: obchod@ecm-monitory.sk

Dodávka, montáž a servis priemyselných meracích prístrojov, analyzátorov a kontinuálnych monitorovacích systémov plynov, kvapalín a častíc pre ekologické a procesné aplikácie. Komplexné riešenia v oblasti kybernetickej bezpečnosti v súlade s požiadavkami NIS2.

Digital Forensic Analysis

Digitálne forenzné analýzy

Forenzná analýza | DF

Digitálna forenzná analýza je systematický proces zhromažďovania, skúmania a interpretácie digitálnych dôkazov na vyšetrovanie kybernetických incidentov, únikov dát a škodlivých aktivít. Využitím rýchlej digitálnej forenznej analýzy, základnej analýzy malvéru a komplexnej a právne prípustnej digitálnej forenznej analýzy môžu bezpečnostné tímy rýchlo identifikovať hrozby, zabezpečiť integritu dôkazov a podporiť právne procesy a reakcie na incidenty.

Function	pure|defense SMB	Description
Instant Digital Forensics Rýchla forenzná analýza Základná DF	OBSAHUJE	Prístup riedený Threat Intelligence na rýchlu analýzu v reálnom čase, identifikáciu a reakciu na bezpečnostné incidenty. Využitím techník digitálnej forenznej analýzy v reálnom čase môžu bezpečnostné tímy okamžite extrahovať a analyzovať digitálne dôkazy, definovať indikátory kompromitácie (IoC) a indikátory útoku (IoA) a urýchliť zadržanie hrozieb a nápravné opatrenia. Táto činnosť je nevyhnutná na splnenie povinnosti notifikácie a spolupráci v prípade závažného incidentu definovanej v direktíve NIS2 (vrátane zákonov implementujúcich danú direktívu, §69/2018 Z. z.)
Fundamental Malware Analysis Fundamentálna analýza malvéru Reverse Engineering	PHISH-FORENSICS	Základný proces kybernetickej bezpečnosti, ktorý zahŕňa analýzu škodlivého kódu s cieľom identifikovať jeho správanie, schopnosti a dopad. Využitím statických a dynamických analytických techník môžu bezpečnostné tímy detegovať indikátory kompromitácie (IoC), odhaliť útočné vektory a posúdiť potenciálne riziká, čím umožňujú efektívne zmierňovanie hrozieb a rýchlu reakciu. V službe pre malé a stredné podniky je zahrnutá iba služba pre analýzu phishing útokov, t.j. konštituent zašle vzorku phishingoveho e-mailu dohodnutým spôsobom a následne dostane vyjadrenie či je daný e-mail maliciózny, resp. benígny. V prípade požiadavky na analýzu malvéru je potrebné kontaktovať obchodného reprezentanta.

Tel.:++421/55/622 85 82,84
e-mail: obchod@ecm-monitory.sk

Dodávka, montáž a servis priemyselných meracích prístrojov, analyzátorov a kontinuálnych monitorovacích systémov plynov, kvapalín a častíc pre ekologické a procesné aplikácie. Komplexné riešenia v oblasti kybernetickej bezpečnosti v súlade s požiadavkami NIS2.

Coordination and Communication with Authorities

Koordinácia a komunikácia s autoritami v oblasti kybernetickej bezpečnosti v prípade incidentu

Koordinácia (v prípade incidentu) | **Zástupca** (v komunikácií s autoritami)

Koordinácia a komunikácia s úradmi a autoritami v oblasti kybernetickej bezpečnosti označuje štruktúrovanú spoluprácu medzi tímom kybernetickej bezpečnosti organizácie a konštituenta a príslušnými vládnymi, regulačnými a právnymi orgánmi. Tento proces zabezpečuje súlad s právnymi požiadavkami, uľahčuje zdieľanie spravodajských informácií o hrozbách, umožňuje včasné hlásenie incidentov a podporuje riadenie krízových situácií. Efektívna koordinácia pomáha zmierniť riziká, skrátiť reakčné časy a posilniť celkovú kybernetickú odolnosť organizácie.

Function	pure|defense SMB	Description
NIS2 Compliance Notification Duty Notifikačná povinnosť definovaná v NIS2 Notifikačná povinnosť	OBSAHUJE	Povinná požiadavka podľa smernice NIS2, ktorá vyžaduje, aby organizácie promptne hlásili významné kybernetické bezpečnostné incidenty príslušným úradom. Táto povinnosť zabezpečuje transparentnú komunikáciu, rýchle obmedzenie šírenia hrozieb a súlad s regulačnými predpismi, čo umožňuje úradom vyhodnotiť riziká, koordinovať reakcie a zmierniť potenciálne narušenia kritickej infraštruktúry a základných služieb.
NIS2 Regulatory & Cybersecurity Compliance Liaison Zástupca pre komunikáciu s úradmi a autoritami Zástupca (pre koordináiu a koordináciu)	ADD-ON	Určený zástupca zodpovedný za zabezpečenie súladu so smernicou NIS2, riadenie hlásenia incidentov, regulačnej komunikácie a správy kybernetickej bezpečnosti. Táto rola zabezpečuje koordináciu s úradmi, dohliada na povinnosť oznamovania v súlade s NIS2 a zabezpečuje dodržiavanie právnych a best-practice požiadaviek na kybernetickú bezpečnosť pre daný hospodársky segment, čím posilňuje stav kybernetickej bezpečnosti organizácie a jej odolnosť voči kybernetickým hrozbám.
Dedicated Incident Response Commander Vyhradený veliteľ v pri reakcii na incident Vyhradený veliteľ	AD-HOC CONTACT SALES	Seniorný bezpečnostný líder, ktorý je zodpovedný za dohľad a koordináciu všetkých aspektov reakcie na kybernetické incidenty. Táto rola zabezpečuje rýchle zadržanie hrozieb, súlad s regulačnými požiadavkami a bezproblémovú komunikáciu s internými tímami a externými úradmi. Zahŕňa tiež plnenie povinnosti oznamovania v súlade so smernicou NIS2 a riadenie núdzových horúcich liniek pre reakciu na incidenty, aby sa minimalizoval dopad na prevádzku a posilnila kybernetická odolnosť organizácie.

Tel.:++421/55/622 85 82,84
e-mail: obchod@ecm-monitory.sk

Dodávka, montáž a servis priemyselných meracích prístrojov, analyzátorov a kontinuálnych monitorovacích systémov plynov, kvapalín a častíc pre ekologické a procesné aplikácie. Komplexné riešenia v oblasti kybernetickej bezpečnosti v súlade s požiadavkami NIS2.

Consulting and Expertise-Based Services

Konzultácie a služby poskytované špecialistami na kybernetickú bezpečnosť

Konzultácie

Špecializované kybernetické poradenstvo, hodnotenie rizík a strategické usmernenia, ktoré pomáhajú organizáciám posilniť bezpečnostné postavenie, zmierniť hrozby a dosiahnuť súlad s nariadeniami regulačných orgánov. Využitím bezpečnostných kontrol (Security Health Checks), okamžitého hodnotenia kybernetických rizík (Instant Cyber Risk Scoring) a analýzy náchylnosti systému na zneužitie zraniteľností v reálnom čase (Live Exploitability Analysis) a ostatných funkcií MDR poskytujú bezpečnostní experti prispôsobené riešenia na implementáciu bezpečnostného rámca s ohľadom na súladom (Compliance-Driven Security Framework Implementation), integráciu riadenia kybernetických ritík (Cybersecurity Governance Integration) a prevádzky SOC, čím zabezpečujú proaktívnu obranu a odolnosť voči vyvíjajúcim sa kybernetickým hrozbám v infraštruktúre konštituenta.

Function	pure|defense SMB	Description
Security Health Check Detekcia úrovne odolnosti systému z pohľadu kybernetických hrozieb Odolnosť systému	OBSAHUJE	Komplexné hodnotenie kybernetickej bezpečnosti organizácie, ktoré identifikuje zraniteľnosti, nesprávne konfigurácie a potenciálne riziká. Využitím okamžitého hodnotenia kybernetických rizík (Instant Cyber Risk Scoring), analýzy exploitov v reálnom čase (Live Exploitability Analysis) a implementácie bezpečnostného rámca súladu (Compliance-Driven Security Framework Implementation) poskytuje praktické odporúčania na posilnenie obrany, zvýšenie odolnosti voči hrozbám a zabezpečenie súladu s regulačnými požiadavkami.
Instant Cyber Risk Scoring Okamžitá kvantifikácia kybernetických rizík v realnom-čase Hodnotenie rizík	OBSAHUJE	Počiatočné hodnotenie bezpečnostného stavu organizácie, ktoré analyzuje zraniteľnosti, vystavenie hrozbám a exploitovateľnosť s cieľom poskytnúť okamžitú kvantifikáciu rizík. Využitím analýzy exploitov v reálnom čase (Live Exploitability Analysis), bezpečnostných kontrol (Security Health Checks) a implementácie bezpečnostného rámca súladu (Compliance-Driven Security Framework Implementation) umožňuje organizáciám prioritizovať zmierňovacie opatrenia, posilniť odolnosť voči hrozbám a udržiavať súlad s požiadavkami regulátora a ostatných autorít pod ktoré koštituent spadá.
On-Prem Cybersecurity Analytics Platform Monitorovacia a analytická platforma v priestoroch koštituenta Lokálny SIEM	CONTACT SALES	Lokálne nasadené bezpečnostné riešenie (SIEM - Security Information and Event Management), ktoré umožňuje organizáciám analyzovať hrozby, detegovať anomálie a reagovať na incidenty v reálnom čase v rámci ich vlastnej infraštruktúry. Využitím analýzy exploitov v reálnom čase (Live Exploitability Analysis), implementácie bezpečnostného rámca riadeného súladom (Compliance-Driven Security Framework Implementation) a integrácie s podnikovým bezpečnostným operačným centrom (Enterprise Security Operations Center – SOC) zabezpečuje úplnú kontrolu nad údajmi, regulačný súlad a pokročilú hrozbovú inteligenciu, pričom minimalizuje závislosť od externých cloudových bezpečnostných služieb.