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



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: 2026.06.09 06:59:52 +02'00'


pure | defense
CYBERSECURITY

delivered by
ECM MONITORY, spol. s r.o.
Process and enviromental monitoring systems

- Advnaced Threat Detection
- Expert & AI driven Investigation
- Rapid Threat Reaction
- Comprehensive Incident Reporting

# PRIDRUŽENÉ BEZPEČNOSTNÉ RIEŠENIA SLŽBY PURE|DEFENSE MDR

## Naš prístup

Našu prácu vnímame ako službu pre našich partnerov, s **poslaním** prinášať **špičkovú** kybernetickú bezpečnosť, dosahujúcu úrovne veľkých organizácií, **malým a stredným firmám**.

Predstavujeme unikátne prepojenie čistoty životného a digitálneho prostredia.

# PURE|DEFENSE MDM (MANAŽMENT MOBILNÝCH ZARIADENÍ) SLUŽBA

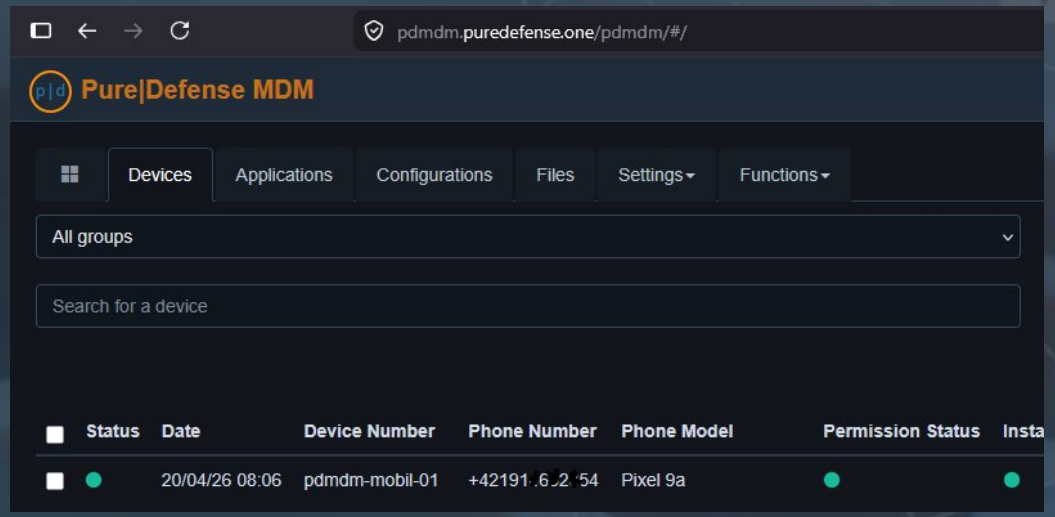
Manažment mobilných zariadení (**MDM**), ktorý je **riadený službou Pure|Defense MDR** rozširuje štandardný model správy mobilných zariadení z úrovne bežnej administrácie a prevádzkovej kontroly na kontinuálne monitorovanú bezpečnostnú službu. Popri uplatňovaní ⚠**bezpečnostných politík**, ⚠**správe konfigurácie**, ⚠**riadení aplikácií**, ⚠**vzdialenom nasadzovaní**, ⚠**šifrovaní** a ⚠**plnej správe životného cyklu** zariadení je úzko **prepojená** s ✖bezpečnostným **monitoringom**, ✖**detekciou** hrozieb a procesmi ✖**reakcie** na incidenty. Telemetria, bezpečnostné udalosti, indikátory správania a porušenia politík z riadených koncových zariadení sú **centrálne zhromažďované a vyhodnocované** s cieľom identifikovať škodlivú aktivitu, neoprávnený prístup, pokusy o kompromitáciu, podozrivé správanie aplikácií a nevyhovujúci bezpečnostný stav zariadení.

pure|defense CYBERSECURITY
delivered by ECM MONITORY, spol. s r.o. Process and environmental monitoring systems



# PURE|DEFENSE MDM SLUŽBA

## riadená Pure|Defense MDR




Komunikácia s riadiacim serverom


Network logy a security eventy posielané do MDR

Po korelácii a vyhodnotení závažnosti je vykonaná obranná (containmnet) akcia

## Pure|Defense MDR SIEM/SOAR

```
Apr 19, 2026 @ 18:25:12.330   android.security   arm64-v8a   BE4B.251210.005   dumpsys package com.google.android.gms

Apr 19, 2026 @ 17:30:55.392   android.network    arm64-v8a   BE4B.251210.005   Network connection from com.android.chrome to 2a02:2638:d::44:443
```

pure|defense CYBERSECURITY
delivered by ECM MONITORY, spol. s r.o. Process and environmental monitoring systems

# PURE|DEFENSE MDM SLUŽBA

## riadená Pure|Defense MDR (Security Incidet lifecycle)




Network logy a security eventy posielané do MDR

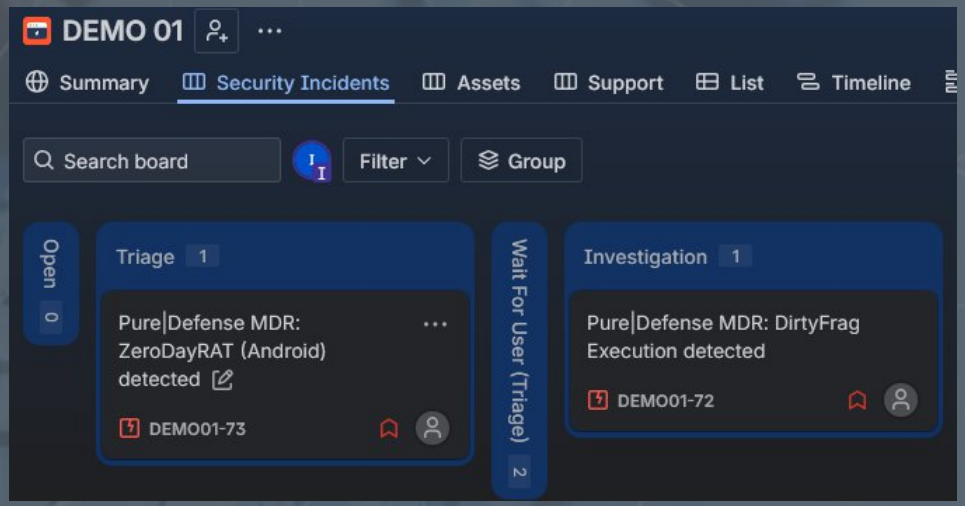
### Pure|Defense MDR SIEM/SOAR

| | | | | |
|---|---|---|---|---|
| Apr 19, 2026 @ 18:25:12.330 | android.security | arm64-v8a | BE4B.251210.005 | dumpsys package com.google.android.gms |
| Apr 19, 2026 @ 17:30:55.392 | android.network | arm64-v8a | BE4B.251210.005 | Network connection from com.android.chrome to 2a02:2638:d::44:443 |

MDR/SOC/SIEM/SOAR Security alert

### Pure|Defense MDR Containment


### Pure|Defense MDR Incident Management Portal




Po eradikácií je zariadenie opäť pripravené na použitie

# PURE|DEFENSE MDM SLUŽBA (SCHÉMA)

**Background (BG) Mode**

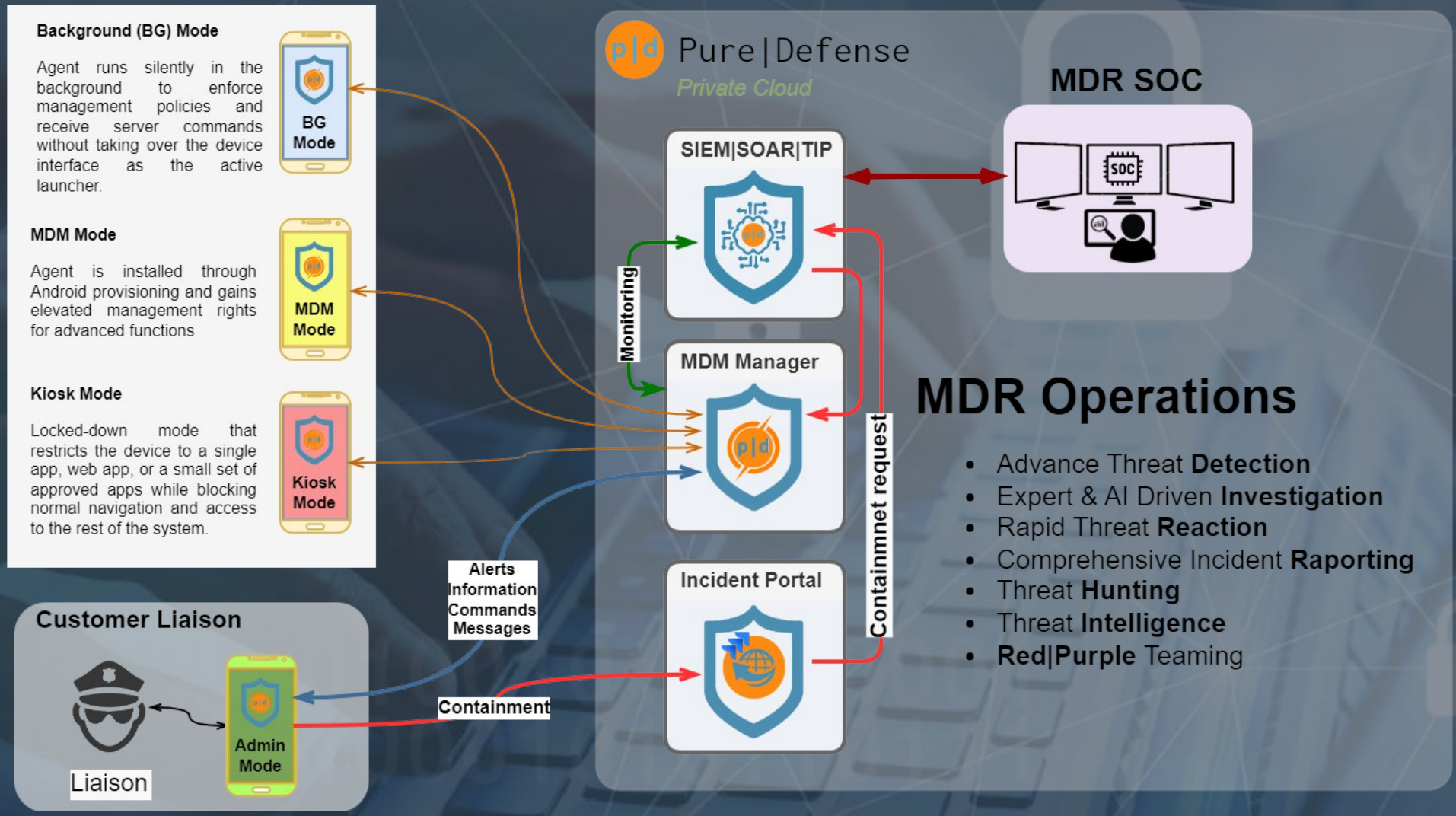
Agent runs silently in the background to enforce management policies and receive server commands without taking over the device interface as the active launcher.

**MDM Mode**

Agent is installed through Android provisioning and gains elevated management rights for advanced functions

**Kiosk Mode**

Locked-down mode that restricts the device to a single app, web app, or a small set of approved apps while blocking normal navigation and access to the rest of the system.




## MDR Operations

- Advance Threat **Detection**
- Expert & AI Driven **Investigation**
- Rapid Threat **Reaction**
- Comprehensive Incident **Raporting**
- Threat **Hunting**
- Threat **Intelligence**
- **Red|Purple** Teaming

# PURE|DEFENSE MDM OPERAČNÉ MÓDY

## ✖ Mód "Na pozadí" (Background mode)

Background mode ("Na pozadí) je režim, v ktorom MDM agent beží na zariadení na pozadí bez prevzatia úlohy predvoleného launcheru, pričom naďalej zabezpečuje správu zariadenia, uplatňovanie politík a základný dohľad nad jeho stavom.

## ✖ Mód "V popredí" (Foreground mode/MDM Mode)

MDM mód ("Na popredí") je režim, v ktorom je zariadenie zaregistrované ako plne spravované zariadenie (device owner), takže MDM riešenie môže uplatňovať rozšírené politiky, ticho inštalovať aplikácie a vykonávať širšiu správu a kontrolu zariadenia.

## ✖ "Výhradný" mód (Kiosk Mode)

Kiosk mode v MDM je režim, v ktorom je zariadenie uzamknuté na jednu alebo vopred povolenú skupinu aplikácií, pričom používateľ nemá prístup k nepovoleným funkciám, nastaveniam ani bežnému prostrediu zariadenia.

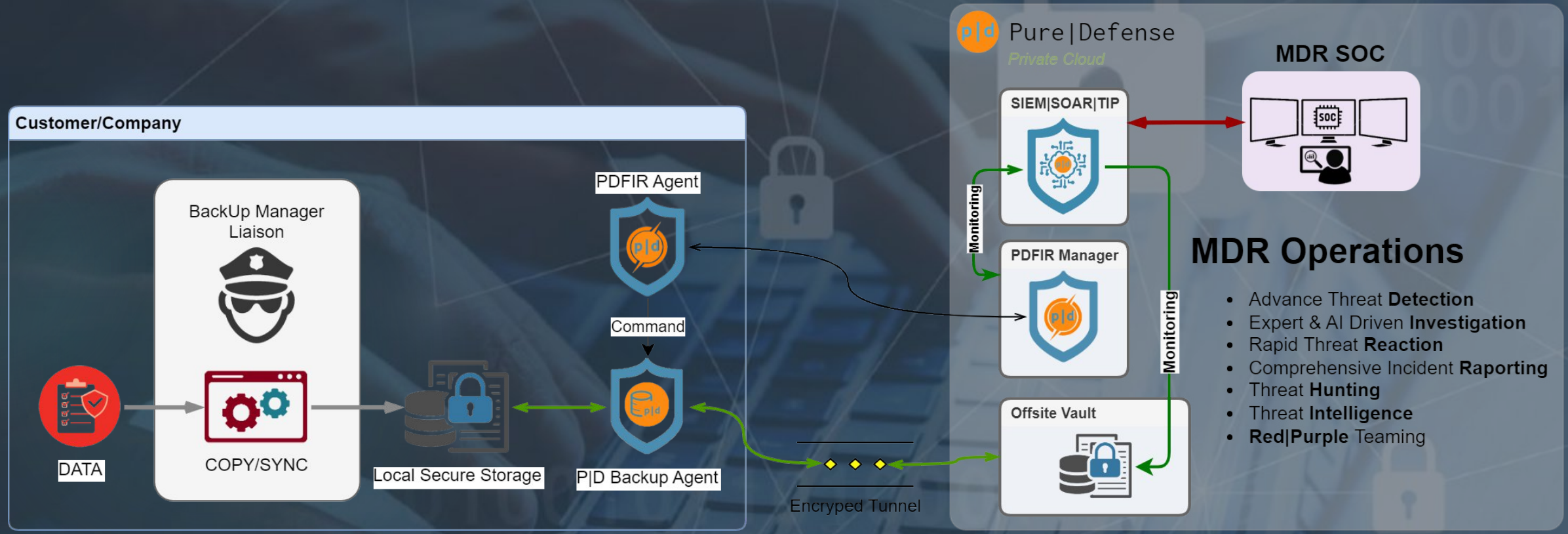
# PURE|DEFENSE MDM VLASTNOSTI A AKCIE

- ✖ Tichá inštalácia, aktualizácia a odinštalácia aplikácií.
- ✖ Správa politík zariadenia, napríklad Wi-Fi, Bluetooth, GPS, mobilných dát, hesiel a časového limitu obrazovky.
- ✖ Detailný inventár a informácie o stave zariadenia.
- ✖ Uvodné nastavenie pomocou QR kódu.
- ✖ Lokalizácia zariadení.
- ✖ Vzdialené uzamknutie zariadenia.
- ✖ Vzdialené obnovenie do výrobných nastavení alebo vymazanie zariadenia.
- ✖ Reštart zariadenia na diaľku.
- ✖ Blokovanie nechcených aplikácií.
- ✖ Zvýšenie kontroly nad zariadením pomocou kiosk režimu alebo obmedzenie USB, Wi-Fi, Bluetooth, GPS a mobilných dát.

# PURE|DEFENSE MDR SLUŽBA KRÍZOVÉHO DÁTOVÉHO TREZORA

MDR služba krízového záložného dátového trezora je bezpečnostne orientovaná služba poslednej inštancie určená na **uchovanie obmedzeného objemu najcennejších** a prevádzkovo **najkritickejších dát** organizácie pred ransomvérom, deštruktívnymi útokmi, neoprávnenou manipuláciou a ďalšími formami nepriateľskej činnosti. Hlavná **hodnota služby** nespočíva iba v chránenom off-site úložisku, ale najmä v **bezpečnostných kontrolách** uplatňovaných v celom reťazci správy a ochrany dát. Prostredie vzdialeného trezora je prevádzkované **pod dohľadom Pure|Defense MDR** služby a chránené nepretržitým bezpečnostným monitoringom, riadením prístupov, oddelením rolí, proti manipulácii odolnými politikami zálohovania

# PURE|DEFENSE MDR SLUŽBA KRÍZOVÉHO DÁTOVÉHO TREZORA (SCHÉMA)




## MDR Operations

- Advance Threat **Detection**
- Expert & AI Driven **Investigation**
- Rapid Threat **Reaction**
- Comprehensive Incident **Raporting**
- Threat **Hunting**
- Threat **Intelligence**
- **Red|Purple** Teaming

# PURE|DEFENSE MDR SLUŽBA KRÍZOVÉHO DÁTOVÉHO TREZORA

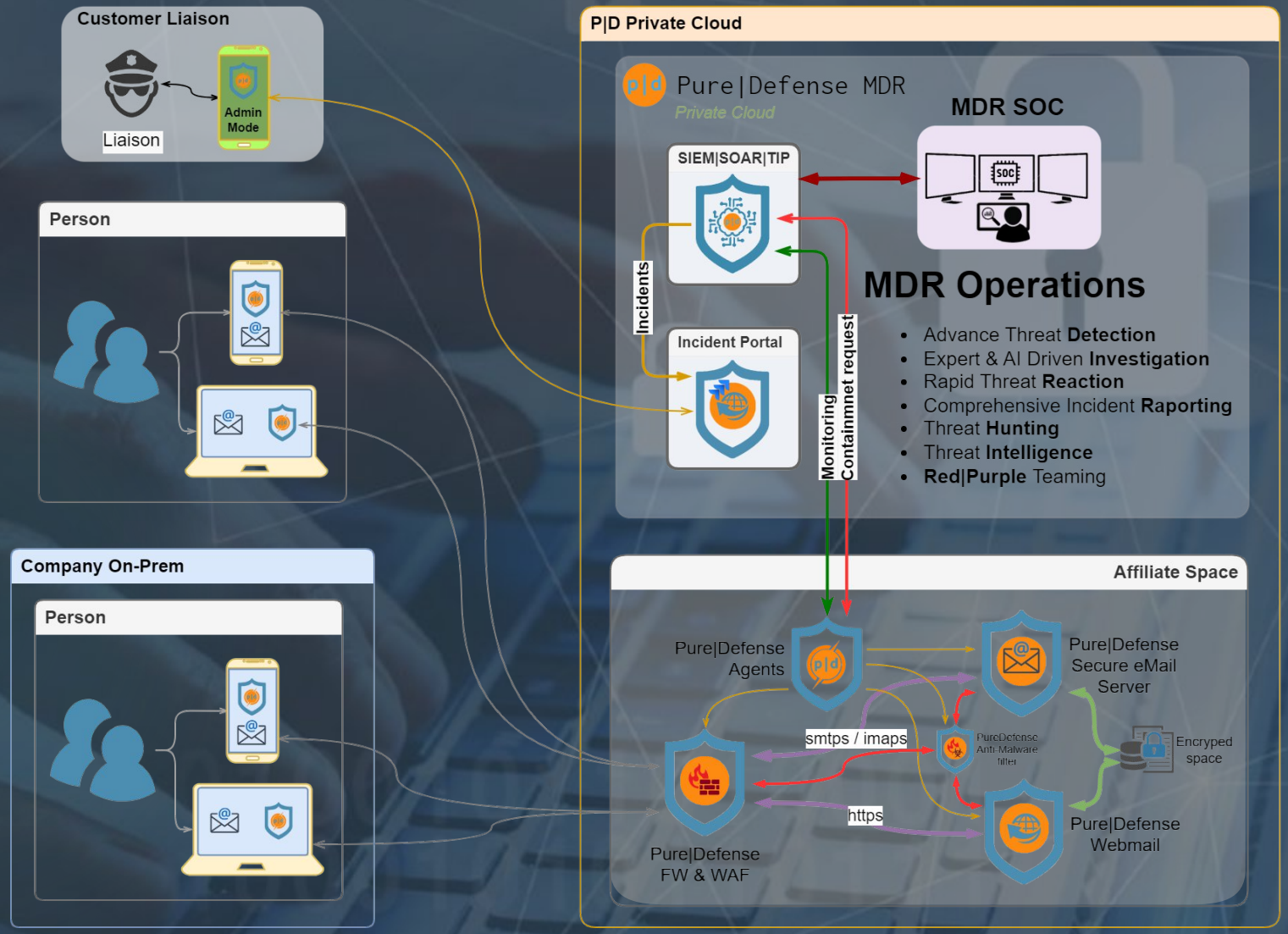
- ✖ Núdzové úložisko poslednej inštancie
- ✖ Bezpečné off-site uloženie dát
- ✖ Pravidelný automatizovaný prenos záloh
- ✖ Šifrovanie počas prenosu dát
- ✖ Šifrovanie uložených dát
- ✖ Prísne riadenie prístupových práv
- ✖ Nepretržitý bezpečnostný monitoring
- ✖ Detekcia anomálneho prístupus

- Auditné logovanie operácií ✖
- Overovanie integrity záloh ✖
- Ochrana proti neoprávnenej manipulácii ✖
- Kontrola dát na škodlivý kód ✖
- Ochrana pred ransomvérom a sabotážou ✖
- Preddefinované postupy obnovy ✖
- Podpora obnovy po kybernetickom incidente ✖
- Dohľad a custody pod MDR tímom ✖

# PURE|DEFENSE MDR RIADENÝ BEZPEČNÝ EMAIL SERVER

MDR riadený **e-mailový server** je spravovaná, **bezpečnostne orientovaná služba elektronickej komunikácie** a spolupráce, ktorá spája **podnikové e-mailové funkcionality** s **nepretržitou ochranou**, **monitoringom** a **reakciou** na incidenty zabezpečovanými tímom MDR. Slžba je určená na podporu každodennej prevádzkovej komunikácie aj prostredí s vyššími požiadavkami na spoľahlivosť a bezpečnosť. **Hlavná pridaná hodnota** služby spočíva v jej bezpečnostnom **modeli riadenom MDR službou**. E-mailové prostredie je nasadené a prevádzkované ako riadená komunikačná platforma **pod dohľadom MDR**, s dôrazom na dôvernosť, integritu, dostupnosť a rýchlu detekciu škodlivej aktivity.

# PURE|DEFENSE MDR RIADENÝ BEZPEČNÝ EMAIL SERVER (SCHÉMA)



# PURE|DEFENSE MDR RIADENÝ BEZPEČNÝ EMAIL SERVER VLASTNOSTI

- ✖ Bezpečný podnikový e-mail
- ✖ Kalendáre a kontakty
- ✖ Distribučné skupiny
- ✖ Delegovaná administrácia
- ✖ Centrálna správa služby
- ✖ Politiky pre používateľov
- ✖ Viacfaktorová autentifikácia
- ✖ Šifrovanie prenosu aj uloženia

- Nepretržitý bezpečnostný monitoring ✖
- Detekcia prevzatia účtu ✖
- Ochrana proti phishingu ✖
- Kontrola príloh a URL ✖
- Aktívna reakcia MDR tímu ✖
- Zdieľané schránky ✖
- Mobilný prístup k pošte ✖
- Kontrola cieľeného (spear) phishingu ✖

pure | defense
CYBERSECURITY

delivered by
ECM MONITORY, spol. s r.o.
Process and enviromental monitoring systems

- Advnaced Threat Detection
- Expert & AI driven Investigation
- Rapid Threat Reaction
- Comprehensive Incident Reporting

# Ďakujeme za pozornosť!

V prípade akýchkoľvek otázok nás môžete kontaktovať na nižšie uvedených adersách.

https://www.puredefense.net | info@puredefense.net