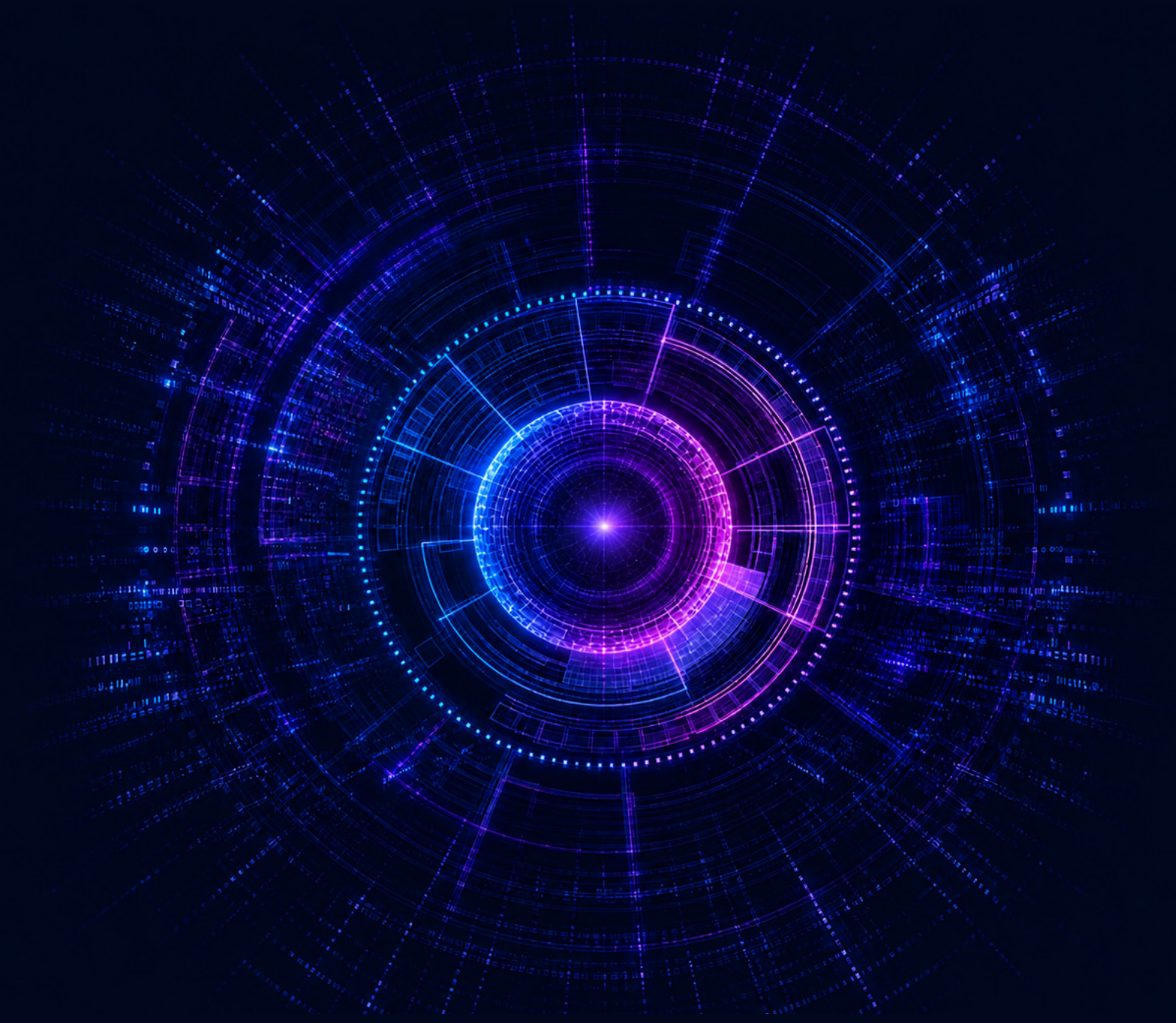
FREEDIVISION

HarfangLab



Ochrana koncových bodů, detekce a reakce

Systém vyvinutý a provozovaný v Evropě

ÚVOD

HarfangLab Guard feat. IKARUS je komplexní evropská platforma pro zabezpečení koncových bodů, která v jediném agentovi kombinuje Endpoint Protection (EPP), Endpoint Detection & Response (EDR) a volitelně Attack Surface Management (ASM). Řešení, vyvinuté a provozované v Evropě, splňuje požadavky středních a velkých podniků, vládních organizací a provozovatelů kritické infrastruktury na účinnost, transparentnost a datovou suverenitu.

Podporované platformy

- Windows
- Linux
- macOS

Jedinečná transparentnost, bezpečnost a datová suverenita

Organizace si vždy zachovávají plnou kontrolu nad všemi daty shromažďovanými řešením HarfangLab Guard feat. IKARUS. Otevřená sada pravidel ve standardizovaných formátech, jako jsou YARA a Sigma, umožňuje transparentnost typu white-box: bezpečnostní týmy mohou dohledat a pochopit výstrahy a v případě potřeby pravidla odpovídajícím způsobem upravit.

EDR: Více kontextu, rychlejší reakce

EDR (Endpoint Detection & Response) zviditelňuje bezpečnostně relevantní aktivity na koncových bodech, detekuje anomálie a vzorce útoků a umožňuje rychlou reakci - od vyšetřování až po vzdálenou reakci na incidenty. Bezpečnostní týmy tak mohou prioritizovat incidenty, efektivně je vyšetřovat a cíleně odstraňovat hrozby.

V kombinaci s integrovaným IKARUS Malware Scan Engine řešení HarfangLab Guard feat. IKARUS spolehlivě blokuje malware ještě před spuštěním, čímž snižuje zatížení systémů i analytiků. Platforma detekuje i cílené útoky, koreluje anomálie do prakticky využitelných výstrah a díky přístupu white-box poskytuje úplnou dohledatelnost.

Nezávisle ověřeno

- **MITRE ATT&CK** Evaluations 2023 a 2024
- Certifikace **ANSSI** CSPN a kvalifikace ANSSI
- Certifikace **BSI** (BSI-DSZ-BSZ-0021-2025

Prevence, reakce a správa útočné plochy

Tři moduly v jediném lehkém agentovi

Endpoint Protection (EPP) - technologie IKARUS Malware Scan Engine

Vícevrstvá detekce malwaru spolehlivě blokuje škodlivý kód ještě před jeho spuštěním.

- Detekce malwaru v reálném čase dříve, než dojde ke škodě.
- Ochrana i v offline prostředích nebo sítích air-gap.
- Detekce malwaru napříč platformami.
- Nižší zatížení analytiků a systémů.

Endpoint Detection & Response (EDR) - technologie HarfangLab

EDR koreluje signály z koncových bodů do řetězců útoků a umožňuje rychle porozumět reálným útokům - podporuje rychlou analýzu a reakci.

- Telemetrie koncových bodů v reálném čase (procesy, síť, události).
- Detekce anomálií a korelace řetězců útoků.
- Threat hunting a vzdálená reakce na incident.
- Forenzní časové osy pro analýzu kořenové příčiny.
- Obohacení o threat intelligence (IOC, kontext).
- Vlastní ochrana agenta proti deaktivaci a manipulaci.

Attack Surface Management (ASM) - volitelný doplněk

ASM poskytuje nepřetržitý přehled o skutečné útočné ploše a pomáhá snižovat riziko ještě před zneužitím zranitelností - bez další infrastruktury nebo síťových skenů

- Přehled o CVE a expozicích pro každý koncový bod.
- Detekce shadow IT a nespravovaných aktiv.
- Prioritizace rizik podle kontextu a zneužitelnosti.
- Řešení založené na agentovi; není nutné další síťové skenování.

Flexibilní modely nasazení - konzistentní sada funkcí

Architektura

HarfangLab Guard feat. IKARUS kombinuje prevenci a izolaci identifikovaných hrozeb s možnostmi hloubkové analýzy a reakce.

Agent nepřetržitě kontroluje klientské stanice a servery na malware a anomálie. Obsahuje kompletní logiku detekce hrozeb, takže lokální ochrana zůstává aktivní i při přerušení konektivity. Zároveň v reálném čase shromažďuje a přenáší telemetrická data do konzole pro správu. Volitelný modul ASM používá stejnou telemetrii ke zviditelnění expozic a CVE - bez další infrastruktury. Rozsah shromažďovaných dat lze individuálně definovat a je vždy plně transparentní.

- **Cloudový hosting** v EU v datových centrech v Rakousku / Evropě.
- **On-premises nasazení** ve vlastní infrastruktuře.
- Podpora **air-gap / offline** režimu pro izolované systémy.
- **Možnost MDR** prostřednictvím partnerů poskytujících spravované služby.

IKARUS Malware Scan Engine rozšiřuje systém Endpoint Detection & Response o silné stránky vysoce výkonné antivirové vrstvy: malware je detekován okamžitě - bez ohledu na platformu, pro kterou byl vytvořen - a zablokován před spuštěním. Tím se snižuje zatížení EDR systému i bezpečnostních analytiků a není potřeba další antivirový klient.

Prostřednictvím **management konzole** bezpečnostní týmy konfigurují politiky, vyšetřují incidenty a spouštějí vzdálené reakční akce. Výstrahy v reálném čase lze řešit současně na všech dotčených koncových bodech nebo lze reakce automatizovat. Grafická zobrazení procesů a událostí podporují forenzní analýzu a hledání původu příčiny.

Integrace do stávajících pracovních postupů SOC

- Konektory pro **SIEM / SOAR / NDR / Threat Intelligence** a prostředí pro analýzu souborů.
- Podpora **API / API-ready** (automatizovatelné a rozšiřitelné pro vlastní případy použití).

Lehké, efektivní a škálovatelné

Pro vysoký výkon a stabilitu je EDR agent vyvíjen v jazyce Rust. V kombinaci s IKARUS Malware Scan Engine, navrženým s důrazem na rychlost a spolehlivost, poskytuje HarfangLab Guard feat. IKARUS mimořádně efektivní a škálovatelný systém. Kapacitu instance nebo databáze lze zvýšit bez přerušení služby. Instalace agenta nevyžaduje restart, takže správci mohou prostředí snadno rozšiřovat a přizpůsobovat.

Klíčové funkce

Detekce a prevence

Detekce a blokování známých i neznámých hrozeb: IKARUS Malware Scan Engine v kombinaci s detekcí IOC/anomálií spojuje silnou prevenci s kontextem EDR. Detekční logika v agentovi zajišťuje ochranu i při přerušení konektivity. Otevřená sada pravidel umožňuje dohledatelnost výstrah.

Vlastní ochrana a odolnost proti manipulaci: Ochrana proti odinstalaci, deaktivaci a manipulaci; pokusy o obejití ochrany jsou detekovány a hlášeny. Komunikace mezi konzolí a agentem je šifrovaná a založená na certifikátech.

Attack Surface Management (ASM) – volitelně: Přehled o expozicích a zranitelnostech pro jednotlivé koncové body, včetně nespravovaných aktiv a prioritizace podle kontextu/zneužitelnosti. Využívá telemetrii agenta – nejsou nutné další síťové skeny.

Vyšetřování, Threat Hunting a reakce na incidenty

Vyšetřování a náprava incidentů: Kvalifikace výstrah, sledování cest útoku a threat hunting. Izolace koncových bodů, stahování souborů, zastavování procesů/úloh/služeb a náprava dotčených systémů.

Vizuální analýza incidentů (časové osy): Časové osy s procesy, síťovými připojeními, protokoly událostí a výstrahami; akce pro vyšetřování a nápravu lze spouštět přímo ze zobrazení.

Telemetrie pro vyšetřování v reálném čase: Živě nebo na základě událostí (např. při výstrahách) pro podporu vyšetřování a práce s IOC. Rozsah a granularita jsou řízeny politikami.

Provoz, integrace a řízení

Granulární správa zabezpečení: Správa whitelistů/výjimek snižuje počet falešně pozitivních nálezů; dashboardy, reporty a předkonfigurovaná zobrazení pro výstrahy, telemetrii, analýzu a threat hunting.

Integrace threat intelligence: Integrace pravidel YARA/SIGMA a IOC; feedy prostřednictvím nahrání/API, konektorů (např. MISP) nebo SOAR/playbooků.

SIEM/SOAR a interoperabilita: Integrace do stávajících pracovních postupů SOC prostřednictvím konektorů a rozhraní; telemetrii lze využít i pro vlastní analytiku a specifické případy použití.

Závěr

HarfangLab Guard feat. IKARUS představuje ucelený přístup k ochraně koncových bodů, který propojuje prevenci, detekci, vyšetřování a reakci v jednom řešení. Organizace tak získává konzistentní pohled na dění na pracovních stanicích a serverech a může bezpečnostní události řešit s potřebným kontextem.

Kombinace technologií HarfangLab a IKARUS, evropský vývoj a provoz, transparentní práce s daty a otevřenost vůči existujícím bezpečnostním nástrojům vytvářejí nejen základ pro nasazení v různých typech prostředí, ale i jistotu v kompatibilitě s vývojem regulatoních požadavků v rámci prostoru Evropské unie. Řešení lze přizpůsobit konkrétním požadavkům organizace, včetně on-premises, cloudového i izolovaného provozu.

FreeDivision.io

Řešení HarfangLab Guard feat. IKARUS tvoří v rámci FreeDivision.io technologický základ služby **FreeDivision.io Essential**. Technologie je zde součástí řízené ochrany koncových zařízení, kterou FreeDivision doplňuje o své odborné kapacity, monitoring, vyhodnocování událostí a reakci na bezpečnostní incidenty. Výsledkem je služba typu MDR, která organizacím umožňuje využívat pokročilou ochranu koncových bodů bez nutnosti budovat a provozovat vlastní SOC.

O společnosti FreeDivision

Ve FreeDivsion stavíme již od roku 2005 kybernetickou bezpečnost na odbornosti, kontinuálním vzdělávání a sledování nejnovějších bezpečnostních trendů, které přinášíme do praxe v České republice. Naše služby jsou navržené tak, aby výrazně zvyšovaly schopnost organizací včas odhalit a účinně čelit kybernetickým hrozbám, aniž by bezpečnost omezovala běžný chod firmy. Naším cílem je zajištění kontinuity podnikání, ochrana klíčových dat a systémů a vytvoření takového bezpečnostního prostředí, které podporuje růst a stabilitu byznysu. Současně reflektujeme rostoucí regulatorní požadavky a klademe důraz na kvalitní reporting, auditovatelnost a dlouhodobou udržitelnost bezpečnostních procesů.

O společnosti IKARUS

IKARUS Security vyvíjí a provozuje špičková řešení kybernetické bezpečnosti od roku 1986. Vlastní vývoj společnosti se zaměřuje na renomovaný IKARUS Malware Scan Engine, efektivní cloudová řešení a ochranu kritické infrastruktury. Společně s vybranými technologickými partnery nabízí IKARUS další bezpečnostní služby pro společnosti všech velikostí a odvětví i pro kritickou infrastrukturu. Ty sahají od modulární platformy IKARUS Threat Intelligence Platform s lokální a mezinárodní CTI přes služby Incident Response a Advanced Threat Protection až po integraci inovativních senzorů pro zabezpečení OT.

O společnosti HarfangLab

HarfangLab je francouzská společnost v oblasti kybernetické bezpečnosti, která se specializuje na výkonné technologie pro ochranu a detekci na koncových bodech. HarfangLab byl prvním EDR certifikovaným agenturou ANSSI a dnes má velké množství zákazníků, včetně úřadů, společností a mezinárodních organizací působících ve vysoce citlivých odvětvích. Jeho řešení se vyznačují otevřeností a bezproblémovou integrací s dalšími bezpečnostními komponentami, transparentností díky přístupnosti zpracovávaných dat a strategickou autonomií díky možnosti volby hostingu - v cloudu nebo ve vlastní infrastruktuře.

ADRESA

FreeDivision s.r.o.
Rektorská 50/52
108 00 Praha 10 – Malešice
Česká republika

KONTAKT

sales@freedivision.com
+420 220 972 426

www.freedivision.io