HarfangLab Guard feat. IKARUS

Endpoint Protection, Detection and Response-System made in Europe

Durch die zunehmende Komplexität moderner Angriffe stößt reine Antivirensoftware an ihre Grenzen. EDR-Features erweitern den Schutz, indem sie die oft subtil ineinandergreifenden Schritte einer Angriffskette in einen zeitlichen und inhaltlichen Kontext setzen. So lassen sich auch gezielte Bedrohungen schneller erkennen und abwehren.

Während Antivirensoftware bösartigen Code innerhalb von Millisekunden erkennen und blockieren kann, zielen EDR-Systeme (Endpoint Detection & Response) darauf ab, Vorgänge auf Endgeräten sichtbar zu machen und mögliche Anzeichen eines Angriffs zu melden. Sie sammeln Telemetriedaten von Clients und Servern, identifizieren Anomalien und decken Muster oder Korrelationen in Vorgängen auf, die auf Sicherheitsverletzungen hinweisen können. Zugleich geben sie Security-Analysen Werkezeuge an die Hand, um direkt auf Geräte und Systeme zuzugreifen, Prozesse zu analysieren und Angriffe abzuwehren.

Europäische EDR & EPP-Lösung für kritische Infrastruktur, GOs, Enterprises

- ✓ **Abwehr** neuer und bekannter Bedrohungen
- ✓ Umfassende **Visibilität** über Endgeräte (inkl. App Inventory)
- ✓ Automatisierbare **Echtzeit-Reaktionen** auf Sicherheitsvorfälle

HarfangLab Guard feat. IKARUS ist ein umfangreiches EDR und EPP-System, das von den Cybersicherheitsunternehmen HarfangLab aus Frankreich und IKARUS Security Software aus Österreich entwickelt wurde. Mit der Zusammenführung ihrer besten Technologien schaffen die Unternehmen ein ganzheitliches, europäisches System, das mit den Features und der Erkennungsleistung der internationalen Marktführer mithalten kann und zugleich die europäische Cybersouveränität bewahrt.

HarfangLab Guard feat. IKARUS identifiziert selbst gezielte Angriffe, warnt bei Anomalien, erkennt Angriffsmuster und blockiert Malware in Echtzeit. Ihr IT-Team kann sich auf die wirklich wichtigen Sicherheitsvorfälle konzentrieren – und über die Management-Konsole unmittelbar reagieren.

© IKARUS Security Software GmbH. All rights reserved.

Einzigartige Transparenz, Sicherheit und Daten-Souveränität

DEPLOYMENT

- ✓ **Cloud-Hosting** im Rechenzentrum in Österreich/Europa
- ✓ **On-Premises-Deployment** bei vollem Funktions- und Leistungsumfang
- ✓ **MDR-Option** (Managed Detection & Response) über IKARUS-Partner

HarfangLab Guard feat. IKARUS wird zu 100% in Europa entwickelt und gehostet. Der Fokus der Datenverarbeitung liegt auf den Bedürfnissen europäischer Organisationen und kritischer Infrastrukturen.

Organisationen behalten jederzeit die vollständige Kontrolle über alle Daten, die von HarfangLab Guard feat. IKARUS erhoben werden. Einzigartig ist außerdem der offene Einblick in das EDR-Regelwerk, sodass Security-Analysten Alarme nicht nur sehen, sondern auch nachvollziehen und verstehen können.

EPP und EDR in einem zentralen Interface

HarfangLab Guard feat. IKARUS besteht aus einem Agenten, der auf Clients oder Servern installiert wird, einer zentralen Management-Konsole sowie der integrierten IKARUS Malware Scan Engine. Damit vereint die Lösung leistungsstarke Malware-Erkennung und die Abwehr und Isolation erkannter Bedrohungen mit tiefreichenden Analyse- und Reaktionsmöglichkeiten.

» Der **Agent** untersuchen Ihre Clients und Server auf Malware und Anomalien. Er enthält die gesamte Logik für die Bedrohungserkennung, sodass der lokale Schutz auch bei getrennter Verbindung aufrecht bleibt. Außerdem sammelt und überträgt der Agent Telemetriedaten in Echtzeit an die Management-Konsole. Der Umfang der gesammelten Daten kann individuell festgelegt und jederzeit eingesehen werden.

» Die **IKARUS Malware Scan Engine** erweitert die Funktionen des Endpoint Detection and Response Systems um die Vorteile einer leistungsstarken Antiviren-Lösung: Malware wird, unabhängig von der Plattform, für die sie geschrieben wurde, sofort erkannt und noch vor ihrer Ausführung geblockt. Damit werden die Ressourcen des EDR-Systems und der Security-Analysten geschont und fokussiert. Ein zusätzlicher Antiviren-Client ist überflüssig.

» Über die **Management-Konsole** können Security-Teams Sicherheitseinstellungen anpassen, Vorfälle untersuchen und Probleme unmittelbar beheben. Echtzeit-Warnungen können über alle betroffenen Endpunkte gleichzeitig bearbeitet oder Reaktionen automatisiert werden. Die grafische Darstellung von Ereignissen und Prozessen erleichtert die Rekonstruktion und Analyse von Sicherheitsvorfällen.

Für optimale Leistung und Stabilität wurden die EDR-Agenten in der Programmiersprache RUST entwickelt. Zusammen mit der IKARUS Malware Scan Engine, die mit Fokus auf Schnelligkeit und Verlässlichkeit entwickelt wurde, stellt HarfangLab Guard feat. IKARUS ein außerordentlich effizientes, skalierbares System dar.

Die Kapazität einer Instanz oder einer Datenbank kann problemlos und ohne Serviceunterbrechung erhöht werden. Die Installation von Agenten erfordert keinen Neustart, sodass Administratoren das Netzwerk unkompliziert erweitern und anpassen können.

© IKARUS Security Software GmbH. All rights reserved.

Hauptmerkmale

- ✓ **Erkennen und Blockieren bekannter und unbekannter Gefahren:** Durch die Integration der IKARUS Malware Scan Engine und die Erkennung von IOCs und Anomalien bietet HarfangLab Guard feat. IKARUS einen umfassenden Endpoint-Schutz, der die Vorteile einer starken Antiviren-Lösung mit den Features eines EDR-Systems vereint. Da sich die gesamte Erkennungslogik am Endpoint-Agenten befindet, sind Ihre Geräte und Server selbst bei getrennter Verbindung geschützt. Das offene Regelwerk ermöglicht IT-Security-Analysten nachzuvollziehen, welche Ereignisse zu einer Warnmeldung geführt haben.
- ✓ **Untersuchen und Beheben von Sicherheitsvorfällen:** Sicherheitsteams erhalten alle notwendigen Werkzeuge und Informationen, um Warnungen zu qualifizieren und nachzuverfolgen sowie Threat Hunting-Kampagnen zu starten, um auch gezielte Angriffe frühzeitig zu stoppen. Dazu können Endgeräte einzeln oder zusammen isoliert, Files runtergeladen, Prozesse, geplante Tasks oder Services anhand bestimmter Kriterien gestoppt und Dateien oder die Registrierungsdatenbank von Infektionen bereinigt werden. Eine Bedrohung wird mit ihrer Kritikalität, der Anzahl der Sicherheitsereignisse pro Agenten und einer Ansicht der MITRE ATT&CK Matrix dargestellt.
- ✓ **Umfassende Telemetriedaten der Endgeräte:** Telemetriedaten können kontinuierlich („live“) oder basierend auf Warnungen übermittelt werden, um Echtzeit-Ermittlungen und die Suche nach Indikatoren zu ermöglichen. Auch der Umfang der übermittelten Telemetrie-Daten kann individuell und granular über Policies eingestellt werden.
- ✓ **Grafische Darstellung von Security Events oder Prozessen:** Für jeden Sicherheitsvorfall wird eine Timeline erstellt, die alle relevanten Telemetrie-Daten sowie für Endpoints alle gestarteten Prozesse, Netzwerkverbindungen, Event Logs und Warnungen auflistet und den sofortigen Beginn der Analysen ermöglicht. Dadurch wird der Gesamtkontext des Vorfalls bzw. der einzelnen Prozessschritte einsehbar. Maßnahmen zur Untersuchung oder Behebung sind direkt über die Grafik erreichbar.
- ✓ **Individuelles Sicherheitsmanagement:** Ein detailliertes Whitelist-Management-System ermöglicht es, anhand spezifischer Kriterien Ausnahmen zu Erkennungsregeln oder -heuristiken zu definieren und dadurch False Positives zu reduzieren. Auch die Ansicht im Management-Portal kann durch personalisierbare Dashboards angepasst werden, indem basierend auf Security-Vorfälle, Metadaten von Binärdateien oder Drivern, Untersuchungsergebnisse, Telemetriedaten oder Ereignisprotokolle von Agenten spezifische Reports erstellt werden. Für Alarme, die gesamte Telemetrie, zu Analysezwecken und für das Threat Hunting stehen vorkonfigurierte Dashboards zur Verfügung.
- ✓ **Threat Intelligence-Integration:** HarfangLab Guard feat. IKARUS nutzt signaturbasierte Malwareerkennung, YARA- und SIGMA-Regeln, Driver IOCs, Künstliche Intelligenz sowie verhaltensbasierten Erkennung. Zusätzliche Threat Intelligence-Feeds können durch Uploads (manuell oder via API), Erstellen von Regeln, über den MISP-Konnektor oder über Playbooks via SOARs integriert werden. Die IKARUS TIP verfügt für die schnelle und einfache Integration über eine geeignete Schnittstelle.

WEITERE KUNDENVORTEILE

- ✓ **Offenes Regelwerk,** um Alarme nicht nur sehen, sondern auch verstehen zu können
- ✓ Werkzeug für **Threat Hunting** und tiefgehende Analysemöglichkeiten
- ✓ Integration mit **SIEM/SOAR** und Threat Intelligence
- ✓ **On-Premises-Deployment** bei vollem Funktions- und Leistungsumfang
- ✓ **Effizient, robust** und kompatibel mit Windows, Linux und MacOS
- ✓ Persönlicher und lokaler **deutschsprachiger Support** durch IKARUS

Informationen und persönliche Beratung:

IKARUS Security Software GmbH
Telefon: +43 1 58995-500
E-Mail: sales@ikarus.at

© IKARUS Security Software GmbH. All rights reserved.

Unabhängige Tests durch MITRE ATT&CK Evaluations

Die MITRE ATT&CK Evaluations testen die Wirksamkeit verschiedener Lösungen anhand realitätsnaher Angriffs-szenarien. Sie bestätigen HarfangLab starke Leistungen sowohl bei der Erkennung einzelner Angriffsschritte (Detection) als auch beim Schutz durch Blockieren der Bedrohungen (Protection).

MITRE ATT&CK Evaluations Enterprise 2024
MIRTE ATT&CK Evaluations Enterprise 2023 - Turla

Über IKARUS

IKARUS Security Software entwickelt und betreibt seit 1986 führende Cybersicherheitslösungen. Die Eigenentwick-lungen des Unternehmens konzentrieren sich auf die anerkannte IKARUS Malware Scan Engine, effiziente Cloud-Lösungen sowie den Schutz kritischer Infrastrukturen. Gemeinsam mit ausgewählten Technologiepartnern bietet IKARUS neben den Kerntechnologien eine breite Palette an Sicherheitsdienstleistungen für Unternehmen aller Größen und Branchen sowie für kritische Infrastrukturen an. Diese reichen von der modularen IKARUS Threat Intelligence Platform, die lokale und internationale Bedrohungsinformationen aggregiert und verarbeitet, über Incident Response Services und Advanced Threat Protection bis hin zur Integration innovativer OT Security Sensoren.

Über HarfangLab

HarfangLab ist ein französisches Cybersecurity-Unternehmen, das auf EDR-Technologien spezialisiert ist, die Cyber-angriffe erkennen, neutralisieren und ein besseres Verständnis der IT-Infrastruktur ermöglichen. HarfangLab war das erste EDR, das von der französischen Behörde für Cybersicherheit ANSSI zertifiziert wurde, und verfügt heute über zahlreiche Kunden, darunter Verwaltungen, Unternehmen und internationale Organisationen, die in hochsensiblen Bereichen tätig sind. HarfangLabs Lösungen zeichnen sich durch ihre Offenheit und ihre nahtlose Integration mit anderen Sicherheitskomponenten, ihre Transparenz durch die Zugänglichkeit der verarbeiteten Daten und die strategische Autonomie durch die Wahl des Hostings – Cloud oder eigene Infrastruktur – aus.

IKARUS Sales Team | sales@ikarus.at | +43 1 589 95-500
IKARUS Support Team | support@ikarus.at | +43 1 589 95-400

© IKARUS Security Software GmbH. All rights reserved.