IKARUS
security software

IKARUS
scan.engine

Datenblatt

Leistungsstarker Algorithmus zur komplexen Malware-Erkennung

Die **IKARUS scan.engine** ist eine der weltweit besten Carrier-grade Scan Engines und wird zu 100% von IKARUS betreut und entwickelt. Dank verschiedener mehrstufiger Abwehrtechnologien gegen Cyber-Bedrohungen und Malware aller Art findet, extrahiert, analysiert und eliminiert sie Schädlinge, Schwachstellen und Exploits in nahezu allen Dateisystemen, Archiven und Übertragungskanälen. Integrieren Sie die **IKARUS scan.engine** in Ihre bestehenden Produkte oder nutzen Sie sie zur Entwicklung eigener Security-Produkte: Die Möglichkeiten sind nahezu unbegrenzt.

Eine Plattform für viele Anwendungsmöglichkeiten

Die **IKARUS scan.engine** arbeitet mit hochentwickelten, leistungsstarken Scan-Technologien zur Analyse von Inhalten verschiedenster Art. Eine Besonderheit dabei ist die Multi-Architektur-Unterstützung für verschiedene Plattformen wie Linux, Windows und Android. Auch ohne Internet-Verbindung werden auf allen Systemen ausgezeichnete Erkennungsraten erreicht. Für Android-Umgebungen wurde ein SDK mit Optimierungen auf mobile Bedrohungen entwickelt.

Flexible Erkennungsmethoden für verschiedene Übertragungskanäle

Unter der Nutzung von flexibel ausgelegten mehrstufigen Verfahren, welche modular und daher unabhängig von verschiedenen Übertragungsarten anwendbar sind, arbeitet die **IKARUS scan.engine** autonom von Erscheinung, Größe oder Dateikennung von unterschiedlichsten Inhalten. Es werden alle möglichen Containertypen, wie Dateien, Dokumente und Archive bis hin zu Disk-Image-Formaten unterstützt. Um auch verschlüsselte Daten zu untersuchen ist es möglich, Formate wie PDF, Office-Dokumente und komprimierte Datenarchive, mit vorgegeben Passwortlisten zu entschlüsseln. Die **IKARUS scan.engine** ist dabei auch selbstständig in der Lage, Passwörter aus dem Inhalt einer Email zu extrahieren.

Mehrstufige Heuristik und erweiterte Sandbox-Analyse

Für die weitergehende Analyse verdächtiger Inhalte wird zusätzlich eine eigens entwickelte Sandbox-Umgebung eingesetzt. In diesem virtuellen, vollständig isolierten Umfeld werden bei Bedarf zusätzliche Überprüfungen durchgeführt und Verhaltensweisen sowie zusätzliche Ergebnisse analysiert, um mögliches schädliches Verhalten zu erkennen. Zusammen mit anderen Analysen wird somit eine umfassende Gesamtbewertung für die untersuchte Stichprobe erstellt. Wird die SDK-Version der **IKARUS scan.engine** eingesetzt, besteht auch die Möglichkeit, mehrstufige Detailinformationen der durchgeführten Analyse, z.B. erkannte Dateitypen und Prüfsummen, zu erhalten. Das IKARUS Analyse-Team ergänzt und entwickelt die Leistungsfähigkeit der **IKARUS scan.engine** laufend mit manuellen Analysen und Reverse-Engineering. Auch die weltweiten Bedrohungsdaten aus dem IKARUS SigQA (Signature Quality Assurance Program) und der laufende Austausch innerhalb der Antiviren-Industrie sorgen für eine verlässliche Erkennungsleistung.

Überzeugende Vorteile

- Plattformunabhängigkeit
- Flexibles Datenanalysemodul für verschiedenste Übertragungsraten
- Mehrstufige Heuristik & Sandbox-Analysemethoden
- Ressourcenoptimiert und besonders leistungsfähig

Optimierte Ressourcennutzung

Die **IKARUS scan.engine** ist von Grund auf in Richtung Skalierbarkeit und Ressourcenschonung entwickelt. Verschiedene Betriebsarten (Speicher oder Disk-optimiert) sowie eine nahezu lineare Steigerung der Leistungsfähigkeit durch Erhöhung der parallelen Threads resultieren in einem der leistungsfähigsten Gesamtsysteme am Markt.

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