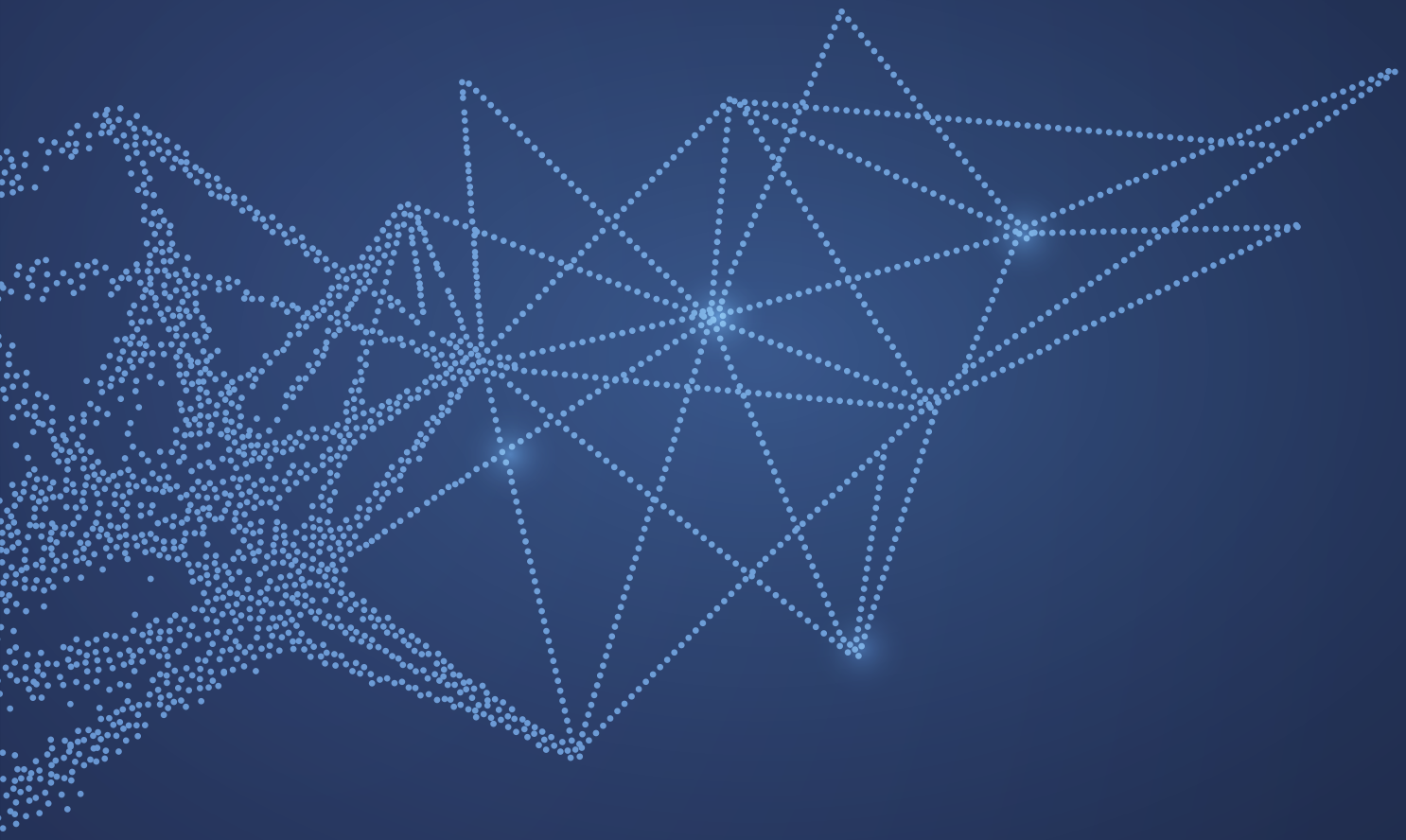
Defensys Threat Intelligence Platform

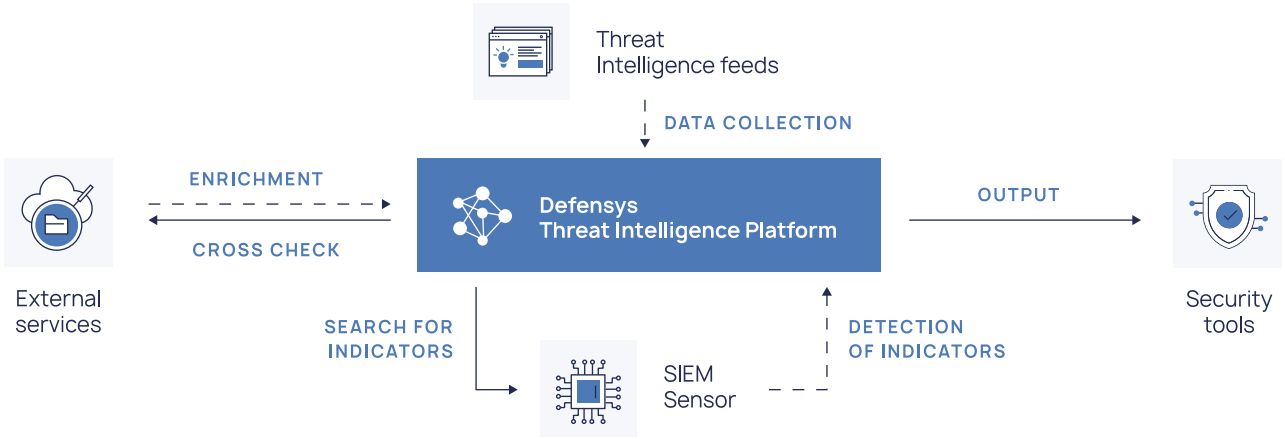
Platform for Threat Intelligence
Data Management



Defensys

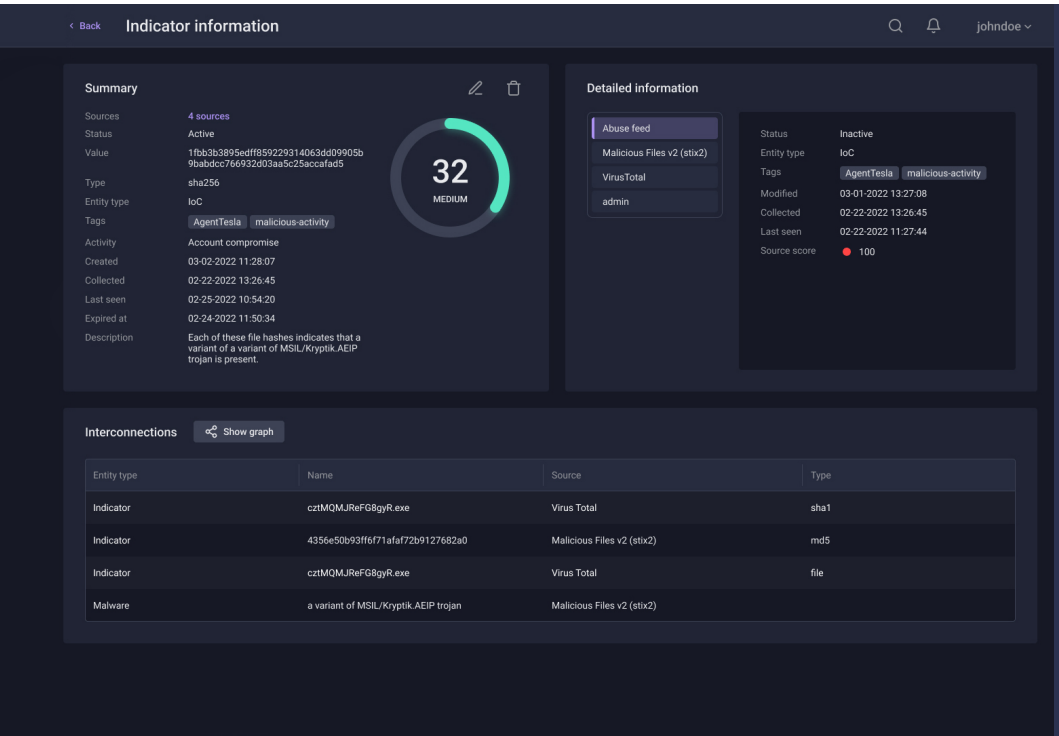
The Defensys Threat Intelligence Platform ensures:

- ✓ automatic collection, normalization and enrichment of IoCs (indicators of compromise) from multiple sources, which include Defensys own feed and open source feeds as well
- ✓ sending the processed data directly to internal security tools
- ✓ searching and detecting IoCs in the company's internal infrastructure using SIEM sensors



Key benefits:

- **Simpler TI data management** with continuous collecting, normalizing, enriching, and storing data from multiple feeds and sources in a single database
- **Easier detection of hidden threats** with automatic monitoring relevant IoCs in SIEM with sensors
- **Faster investigations** with rapid information sourcing and automating key playbooks
- **Timely threats blocking and risk mitigation** with automatic uploading of processed data directly to the block lists of security tools, such as IDS
- **Less false positives** with ranking IoCs in a scoring model
- **Quicker IoCs collection for geographically distributed infrastructure** with using SIEM sensors



The indicator card contains all available information:

- ✓ raw data from the TI provider
- ✓ enrichment results
- ✓ reports, malware, vulnerabilities, and other related indicators
- ✓ detection and update history

Functionality

Threat Intelligence data collection

The Defensys Threat Intelligence Platform automatically collects threat intelligence data from a variety of feeds. It has native integration with threat intelligence exchange solutions:

- IBM X-Force Exchange
- AT&T Open Threat Exchange (OTX)
- Defensys feed
- Group-IB Threat Intelligence
- Kaspersky Threat Intelligence
- RST Threat Feed
- ESET Threat Intelligence
- Shadowserver
- Open source feeds
- Other sources may also be connected

Processing and enrichment

During processing, IoCs are normalized and aggregated into a single representation model, duplicate indicators are linked and merged. You can rate each IoC and define its expiration policies. Defensys TIP supports the IoCs enrichment with additional context to complete the feed providers' data. Supported enrichment services:

- VirusTotal
- Hybrid Analysis
- Whois
- RiskIQ
- Ipgeolocation.io
- ThreatCrowd
- MaxMind
- Shodan
- OPSWAT Metadefender
- And others

Interconnections analysis

Interconnection analysis helps the cybersecurity experts correctly interpret the data and build a comprehensive threat picture. Defensys TIP collects the IoC information available from the feed provider, as well as and related data on:

- Analytical Reports
- Malware
- Vulnerabilities
- MITRE mapping
- Other context

Extrapolation on security tools

Pre-processing ensures a less number of false positives, which often occur with raw data. After processing, the data is automatically sent to available internal information security tools:

- Cisco
- McAfee
- Palo Alto Networks
- Other tools

Additionally, it is possible to exchange data using common formats: STIX 2.1, CSV, JSON.

Search and discovery in the IT infrastructure

Using sensors, Defensys TIP proactively searches for relevant IoCs in SIEM events. Once detected, the IoCs alerts are sent via different channels.

Playbooks automation

The platform ensures IoC workflows set up. After configuring a sequence of rules, you can fully automate data processing playbook from its collection to blocking.

Easy bulletins building

The easy-to-use bulletin builder helps you generate information on threats and vulnerabilities, send bulletins to target organizations, and export to external systems using APIs.

Defensys

About Defensys

Defensys is an award-bearing and nationally acknowledged vendor of cybersecurity solutions. Since 2011, we have been fostering government agencies and private-sector companies to confidently withstand modern cyber threats and ensure reliable security management worldwide.

Defensys technologies are embedded in financial, public, oil and gas, energy, metal industry, and other sectors.

sales@defensys.com

Cybersecurity Digest:
defensys.com/blog/