Defensys

SENSE

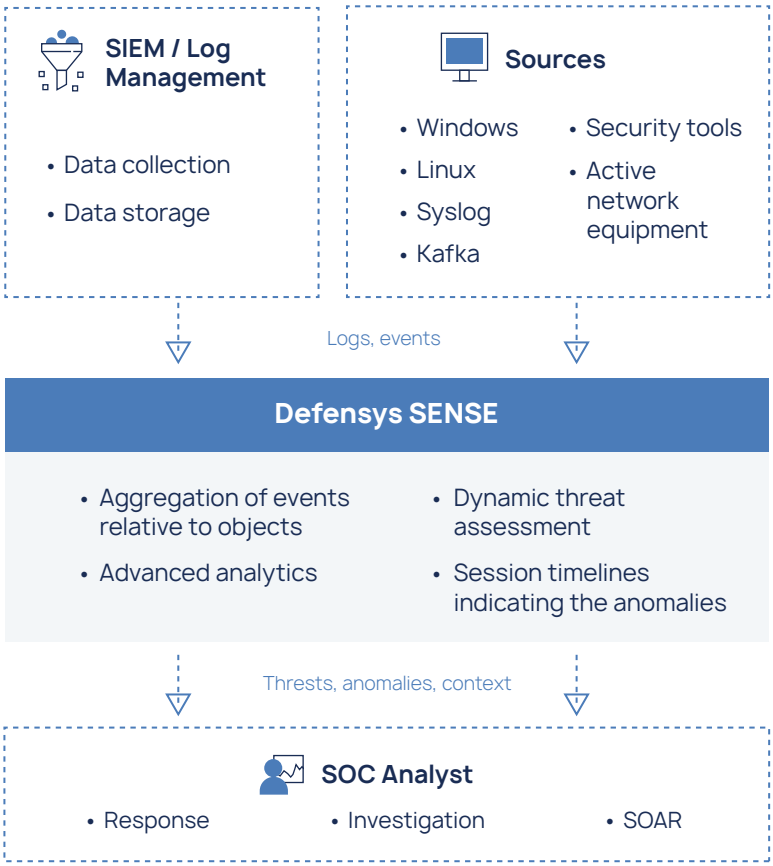
Cybersecurity analytics platform

Defensys

Defensys SENSE is a full-featured cybersecurity anomaly detection platform with the following capabilities:

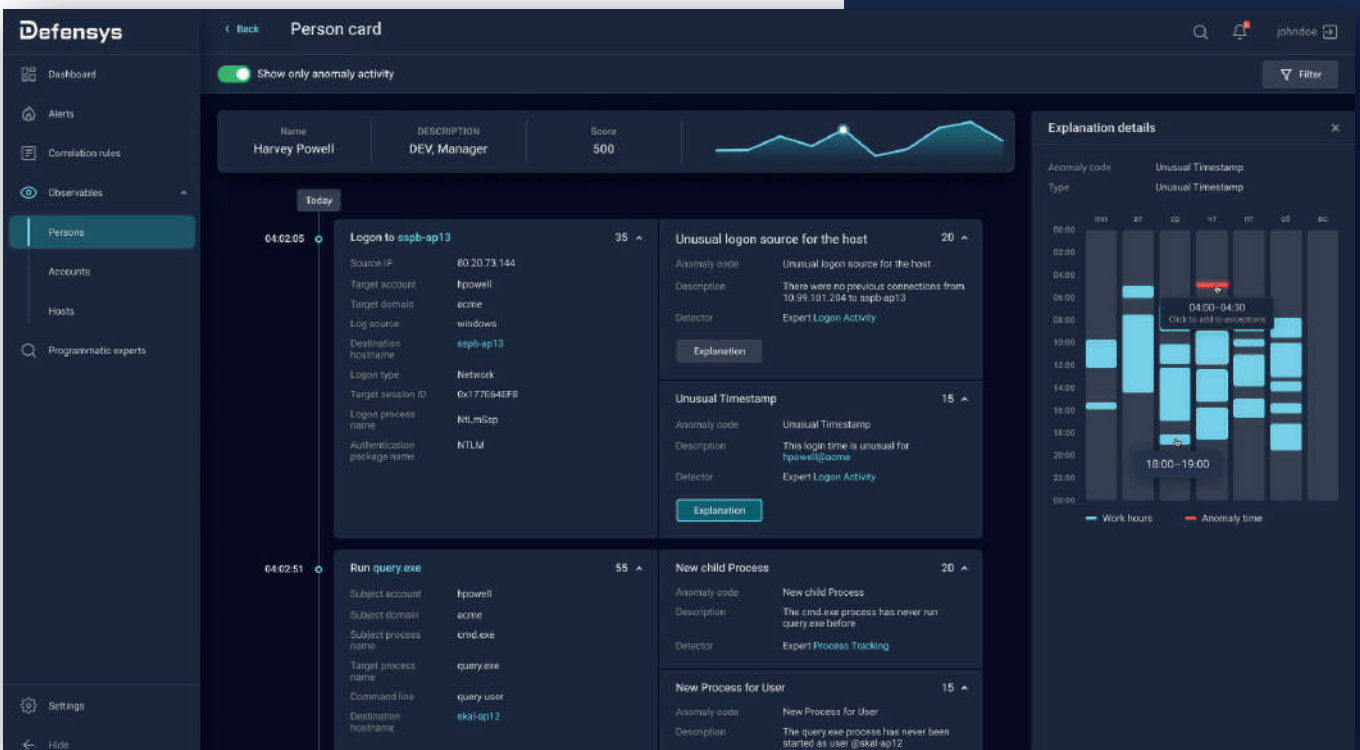
- ✓ Detecting abnormal system status changes.
- ✓ Identifying suspicious activity.
- ✓ Assessing threats and anomalies dynamically.

SENSE's advanced analytical features improves SOC performance and timely detect initial signs of an attack, and prioritize the most vital threats in the flow of events and incidents..



Key benefits

- **Continuous monitoring, anomaly detection** and early threat warning.
- **Detection of insider threats,** as well as previously unknown attacks.
- **Triage of threats and anomalies,** focusing on high-risk objects.
- **Reduced number of incidents** and false positives.
- **Simplified incident analysis** and event tracking.



Security state monitoring

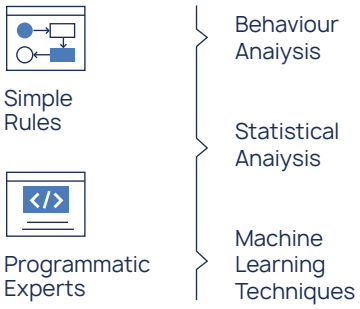
Defensys SENSE continuously monitors security events by analysing data from different sources: log management systems, SIEM, and others. The incoming data is analysed relating to particular system objects: users, workstations, files, accounts, services, etc.

By analyzing object behavior, Defensys SENSE builds normal behavior profiles while learning and detects suspicious activity in case of any inconsistency with a behavior profile.

Multi-level system of programmatic experts

The built-in system of programmatic experts provides comprehensive monitoring for better tasks and events control. The monitoring is carried out for:

- ✓ running processes and applications,
- ✓ logon requests,
- ✓ accessing to files by processes,
- ✓ VPN connections,
- ✓ DGA events and connection to look-alike domains,
- ✓ events connected with e-mail traffic,
- ✓ account switch events,
- ✓ security group management event,
- ✓ user account management events,
- ✓ and others.



Adaptive correlation of events

Defensys SENSE automatically advances its built-in anomaly detection analytics. With the new data sources and analysis rules introduced, programmatic experts automatically adapt them without the need to additionally tweak them.

Defensys SENSE has a universal data format for analysis, which provides flexibility to use analytical tools.

Dynamic threat and anomaly assessment

The SENSE's system for dynamic assessment of anomalies calculates the observable's threat rating. The rating score increases both in case of any suspicious activity and in case of exceeding user-defined values. Then a system analyst receives a corresponding notification to be able to immediately detect and respond to anomalies and threats.

Event timeline

Detailed information on observable's suspicious activity is saved in the timeline format. Each timeline contains detected behaviour anomalies and their context that build the corresponding time scale.

Timelines substantially simplify analysis of incidents and detection of security issues.

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/