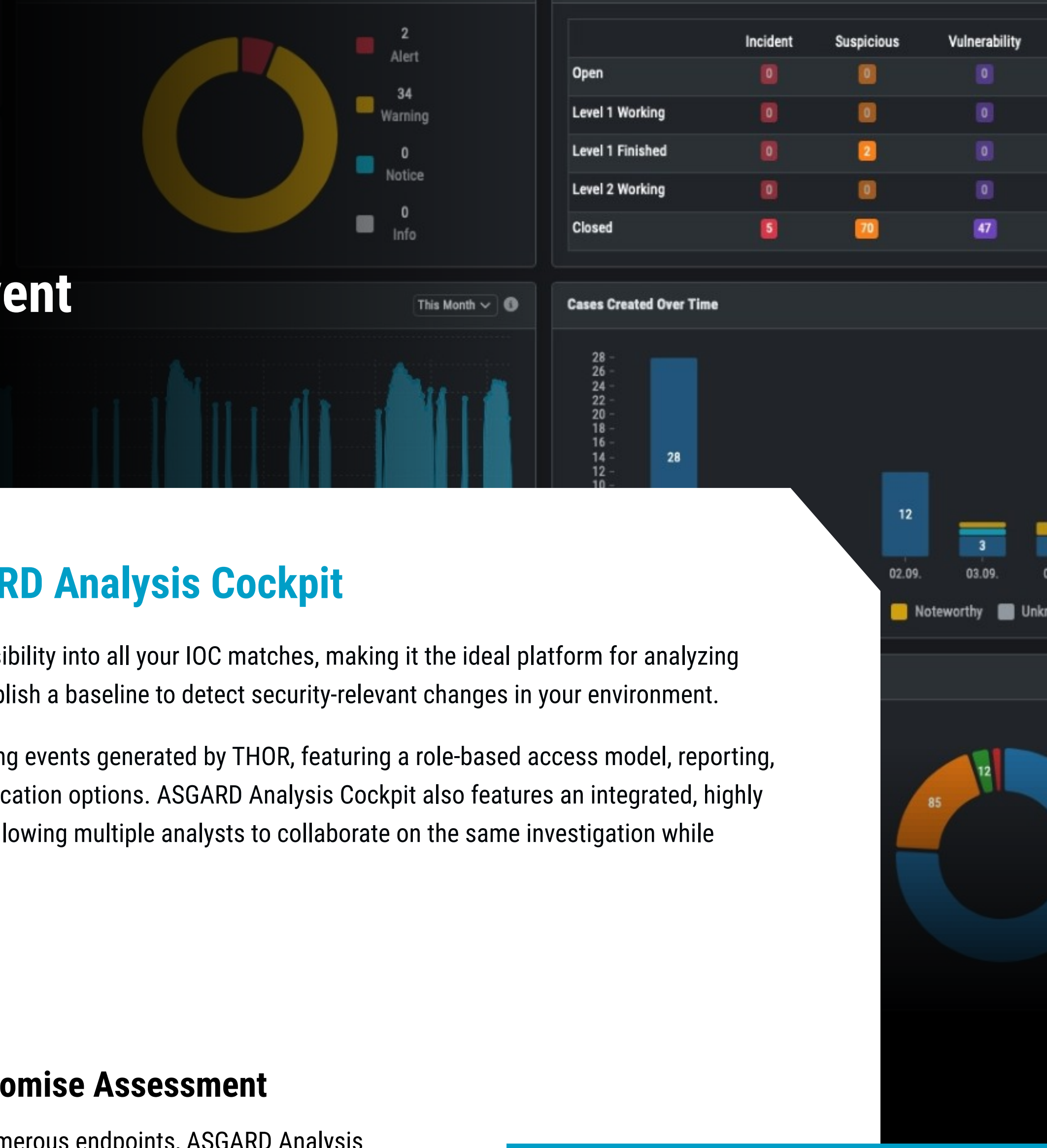
ASGARD
ANALYSIS COCKPIT

Optimized THOR Event Analysis at Scale



	Incident	Suspicious	Vulnerability
Open	0	0	0
Level 1 Working	0	0	0
Level 1 Finished	0	2	0
Level 2 Working	0	0	0
Closed	5	70	47

Cases Created Over Time

Full Visibility with ASGARD Analysis Cockpit

ASGARD Analysis Cockpit provides full visibility into all your IOC matches, making it the ideal platform for analyzing THOR scan results. It enables you to establish a baseline to detect security-relevant changes in your environment.

It offers advanced capabilities for analyzing events generated by THOR, featuring a role-based access model, reporting, asset overviews, an API, and flexible notification options. ASGARD Analysis Cockpit also features an integrated, highly configurable case management system, allowing multiple analysts to collaborate on the same investigation while maintaining a structured workflow.

Use Cases

Incident Response and Compromise Assessment

In case of a security incident involving numerous endpoints, ASGARD Analysis Cockpit ensures a clear overview. It allows to focus your attention on security-relevant findings across thousands of assets, providing a comprehensive view of the current situation through advanced case management capabilities.

For in-depth detection and analysis of security threats, ASGARD Analysis Cockpit leverages THOR. With over 30,000 handcrafted YARA signatures, 3,000 Sigma rules, numerous anomaly detection rules, and thousands of IOCs, THOR detects Advanced Persistent Threats (APTs) across IT and OT systems.

Furthermore, the seamless integration with ASGARD Management Center allows efficient coordination and management of your security operations. This integration facilitates a unified approach to threat detection and response, ensuring that all relevant data and findings are easily accessible and visible.

Continuous Compromise Assessment

By utilizing ASGARD Management Center to schedule and manage regular scans with THOR, and automatically forwarding THOR events to ASGARD Analysis Cockpit, security-relevant findings can be addressed at an early stage. Regular compromise assessments significantly increase the chances of mitigating damage by identifying hackers at an early stage. This proactive approach enables timely responses to potential threats.

By leveraging ASGARD Analysis Cockpit, specifically tailored to THOR Scanner results, large volumes of events can be quickly aggregated and correlated, rather than evaluating each event individually. Systematic management of security incidents enables companies to achieve a higher level of protection.

Key Benefits

Centralized Case Management

Grouping of correlating, security-relevant findings to accelerate coordinated analysis and response tasks.

Notifications

Define notifications in the form of SYSLOG, email, or webhooks for case updates or new events for previously closed cases.

Baselining Dashboard

Customize your view in the Baselining (or Events) section with user-specific dashboards. Set up and share tailored event views based on your needs.

Core Capabilities

Baselining Section Overview

Baselining Section: This section shows all IOC matches outside the current baseline – highlighting those findings that need attention. It offers advanced visualization and filtering tools, and auto-grouping to streamline analysis, categorization, and case creation.

ChatGPT-Integration: Use ChatGPT in your Baselining or All Events view to gain deeper insights into the events under investigation.

API-Integration - Powerful APIs

The Analysis Cockpit offers a comprehensive set of APIs for case management, threat intelligence, and sandbox integration.

Integrated Case Management

The integrated Case Management provides an intuitive interface for seamless collaboration among multiple analysts on shared IOC matches. It's highly configurable, allowing customizable workflows tailored to various analyst groups. The scalable two-level analyst model easily supports multi-tiered operations.

Rich Reporting Section

The reporting section offers a range of built-in reports covering IOC matches and case management activities. These reports provide general statistics on all activities and events within the cockpit. They also assist organizations in improving their processes by delivering KPIs for implemented workflows. Custom reports can be created and scheduled as needed. Additionally, external reporting engines can be integrated through scheduled exports of raw report data.

Start the conversation today!

Whether you're interested in a strategic conversation, compromise assessment, or technical demo, our team can't wait to speak with you! Reach out to us directly at

info@nextron-systems.com

Learn more about the ASGARD Analysis Cockpit and how it can work for your business at

www.nextron-systems.com/asgard-ac

Nextron Systems, a German technology company, is at the forefront of providing innovative security solutions for Compromise Assessments. With a client base exceeding 500 enterprise customers and risk-conscious mid-sized businesses from over 30 countries, our cutting-edge scanning solutions, THOR and ASGARD, are trusted and recommended by security agencies. Security professionals and forensic analysts appreciate our tools for safeguarding their data and systems amidst a rapidly evolving threat landscape.

We detect hackers.

Over 500 Customers around the Globe
Trust Nextron Systems.

nextron systems