ASGARD

ASGARD is the central management platform for THOR and SPARK scans. It manages distributed THOR/SPARK scans on thousands of systems, collects, forwards and analyzes logs. Furthermore, ASGARD can control and execute complex response tasks if needed.

ASGARD comes in two variations: While ASGARD Management Center (MC) features scan control and response functions, ASGARD Analysis Cockpit (AC) provides log analysis with the help of a base-lining agent that makes it easy to focus on differences between current and past scan results.

ASGARD Analysis Cockpit provides our own web frontend that helps to group, evaluate, filter and work on log data that were collected by our scanners.

The hardened, Linux-based ASGARD appliance is a powerful, solid and scalable response platform with agents for Windows, Linux and macOS. It provides essential response features like the collection of file system or memory evidence, malware process termination, remote file system browsing and other counteractive measures.

It features templates for scan runs and lets you plan and schedule distributed sweeps with the lowest impact on system resources. Other services are:

- **Evidence Collection** - collect files, folders or a system's main memory
- **Scanner Updates** - automatic updates for THOR / SPARK scanners
- **Quarantine** - sample quarantine via Bifrost protocol
- **Asset Management** - central inventory and status dashboard
- **Log Analysis** - with ASGARD Analysis Cockpit

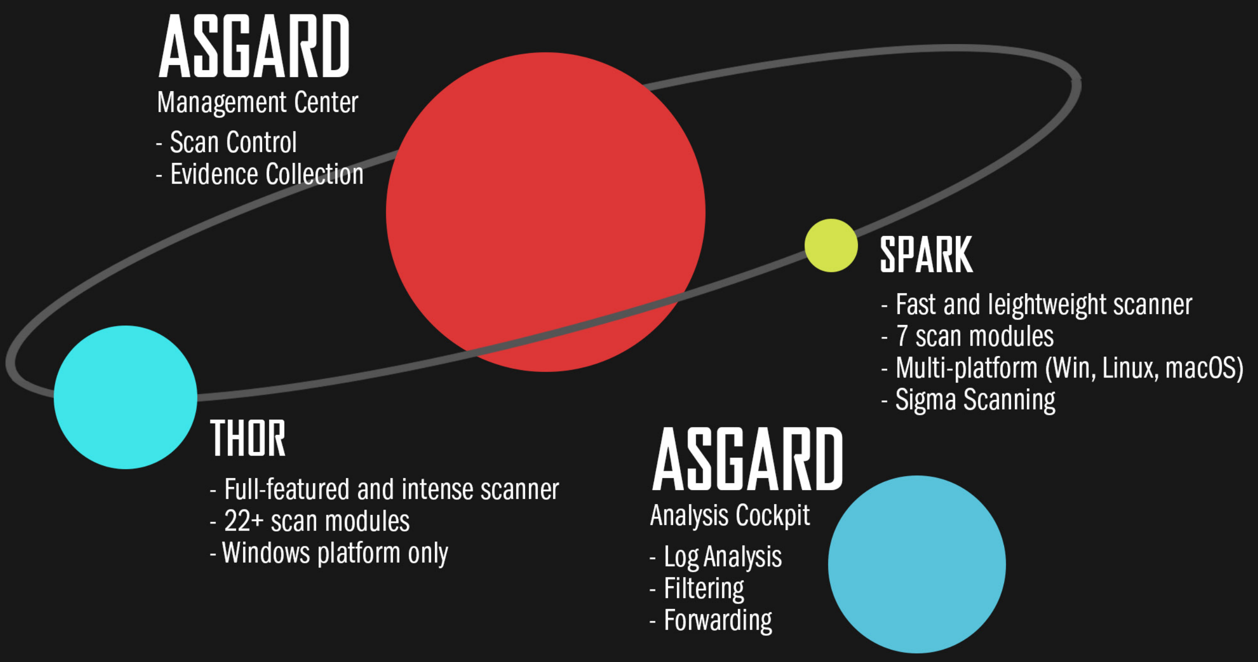
Manage scans from a central interface

Integrated Basic SIEM

Multi-platform agents

Response and Remediation

Low resource footprint



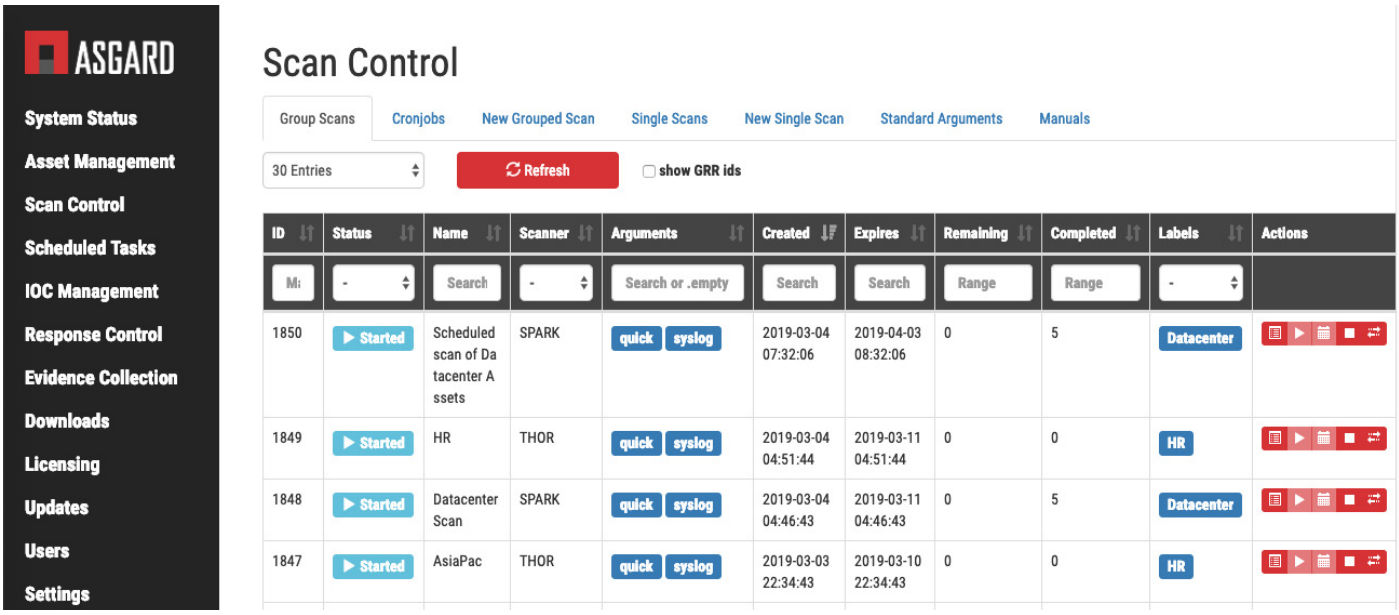
ASGARD
Management Center
- Scan Control
- Evidence Collection

SPARK
- Fast and leightweight scanner
- 7 scan modules
- Multi-platform (Win, Linux, macOS)
- Sigma Scanning

THOR
- Full-featured and intense scanner
- 22+ scan modules
- Windows platform only

ASGARD
Analysis Cockpit
- Log Analysis
- Filtering
- Forwarding

ASGARD Management Center



Scan Control

ID	Status	Name	Scanner	Arguments	Created	Expires	Remaining	Completed	Labels	Actions
Mi	-	Search	-	Search or .empty	Search	Search	Range	Range	-	
1850	▶ Started	Scheduled scan of Datacenter Assets	SPARK	quick syslog	2019-03-04 07:32:06	2019-04-03 08:32:06	0	5	Datacenter	▤ ▶ ▦ ■ ⇄
1849	▶ Started	HR	THOR	quick syslog	2019-03-04 04:51:44	2019-03-11 04:51:44	0	0	HR	▤ ▶ ▦ ■ ⇄
1848	▶ Started	Datacenter Scan	SPARK	quick syslog	2019-03-04 04:46:43	2019-03-11 04:46:43	0	5	Datacenter	▤ ▶ ▦ ■ ⇄
1847	▶ Started	AsiaPac	THOR	quick syslog	2019-03-03 22:34:43	2019-03-10 22:34:43	0	0	HR	▤ ▶ ▦ ■ ⇄

Typical incident response scenarios consists of different stages, whereas each stage has its own challenges and required tools. The ASGARD platform completes our tool-set universe and supports every stage of the incident response process.

- **Quick Preventive Scanning**
  with the lightweight SPARK scanner or THOR in quick mode
- **Intense Triage Scans**
  with THOR and custom case-based indicators to determine the extend of the incident
- **Evidence Collection**
  with THOR's quarantine feature or ASGARD's file, folder or memory collection
- **Remediation**
  with ASGARD's remote execution and counteractive measures
- **Log Collection and Analysis**
  with ASGARD Analysis Cockpit
- **IOC Management**
  Manage a custom set of IOCs and YARA rules

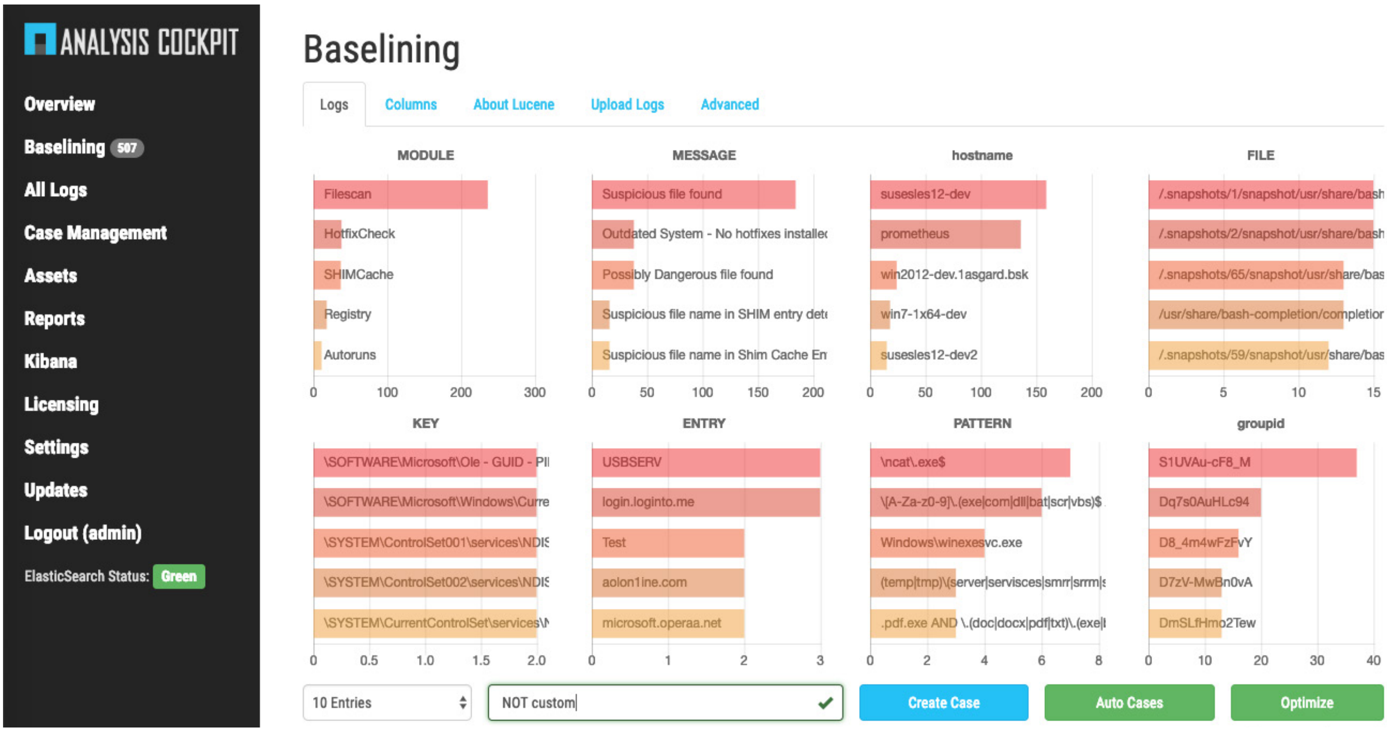
ASGARD Managements Center's features are:

- Flexible and modern web interface
- Extensive response capabilities
- Cross-platform agents (Windows, Linux and macOS)
- Automatic agent updates
- Detailed monitoring of client CPU, memory and IO usage and self-imposed limits
- Task Scheduler
- Fully scalable back-end to handle very large deployments

Further advantages / features are:

- Shipped as Soft or Hardware Appliance
- Customizable platform / open to feature requests
- Direct contact to the developers / Security Made in Germany
- Control multiple instances of ASGARD with Master ASGARD

ASGARD Analysis Cockpit


ANALYSIS COCKPIT
Overview
Baselining 507
All Logs
Case Management
Assets
Reports
Kibana
Licensing
Settings
Updates
Logout (admin)
ElasticSearch Status: Green
Baselining
Logs
Columns
About Lucene
Upload Logs
Advanced
MODULE
Filescan
HotfixCheck
SHIMCache
Registry
Autoruns
0
100
200
300
MESSAGE
Suspicious file found
Outdated System - No hotfixes installed
Possibly Dangerous file found
Suspicious file name in SHIM entry dete
Suspicious file name in Shim Cache En
0
50
100
150
200
hostname
susesles12-dev
prometheus
win2012-dev.1asgard.bsk
win7-1x64-dev
susesles12-dev2
0
50
100
150
200
FILE
/.snapshots/1/snapshot/usr/share/bash
/.snapshots/2/snapshot/usr/share/bash
/.snapshots/65/snapshot/usr/share/bas
/usr/share/bash-completion/completior
/.snapshots/59/snapshot/usr/share/bas
0
5
10
15
KEY
\SOFTWARE\Microsoft\Ole - GUID - PI
\SOFTWARE\Microsoft\Windows\Curre
\SYSTEM\ControlSet001\services\NDIS
\SYSTEM\ControlSet002\services\NDIS
\SYSTEM\CurrentControlSet\services\N
0
0.5
1.0
1.5
2.0
ENTRY
USBSERV
login.loginto.me
Test
aolon1ine.com
microsoft.operaa.net
0
1
2
3
PATTERN
\ncat\.exe$
\[A-Za-z0-9]\.(exe|com|dll|bat|scr|vbs)$
Windows\winexesvc.exe
(temp|tmp)\(server|servisces|smrr|srrm|s
.pdf.exe AND \.(doc|docx|pdf|txt)\.(exe|
0
2
4
6
8
groupid
S1UVAu-cF8_M
Dq7s0AuHLc94
D8_4m4wFzFvY
D7zV-MwBn0vA
DmSLfHmo2Tew
0
10
20
30
40
10 Entries
NOT custom
Create Case
Auto Cases
Optimize

ASGARD Analysis Cockpit offers the best way to group, filter, evaluate and forward events generated by our scanners. It feature a base lining, case management, role based access model, reporting, asset overview and flexible notification options.

Used to process the scan result of periodic scans or as filtering platform that forwards only the most relevant findings to your SIEM system.

- **Case Management**
  Automatically create cases for a set of events and evaluate them collaboratively
- **Notifications**
  Define notifications in the form of SYSLOG, Email or Web Hooks for case changes or new incoming events for already closed cases
- **Reporting**
  Generate comprehensive reports on started / completed scans, coverage and findings

ASGARD Analysis Cockpit's features are:

- Flexible web interface
- Role-based access control
- Full audit trail of user activity
- Fast ElasticSearch database
- Integrated reporting (HTML/JSON)
- Multiple ways to import logs (file/SYSLOG)
- LDAP authentication

Further advantages / features are:

- Shipped as soft appliance
- Customizable platform / open to feature requests
- API access
- Optional Kibana frontend