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 features scan control and response functions, ASGARD Analysis Cockpit provides log analysis through pre-installed ELK and Splunk along with a base-lining agent that makes it easy to focus on differences between current and past scan results.

ASGARD Analysis Cockpit provides interfaces to customer's CMDBs, Vulnerability Management Systems and other inventories.

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, registry 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:

- **Log Analysis Services** - pre-installed ELK and Splunk for maximum convenience
- **Quarantine Service** - file quarantine via Bifrost protocol
- **Update Service** - automatic updates for THOR / SPARK scanners
- **License Service** - central registration and sub license generation
- **Asset Management Service** - central inventory and status dashboard

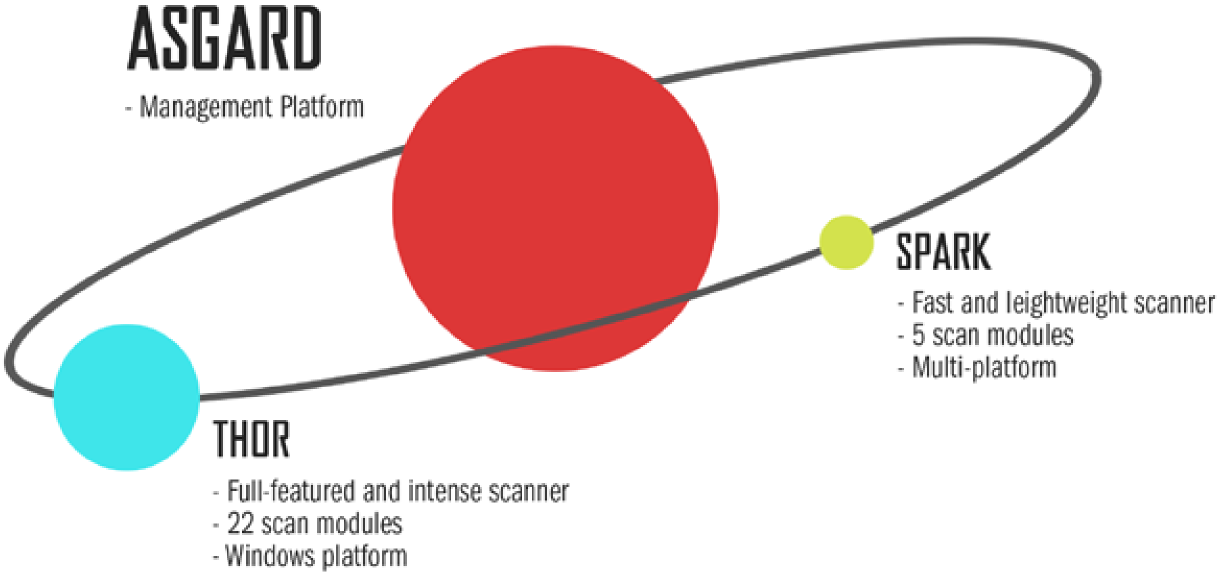
Manage scans from a central interface

Integrated Basic SIEM

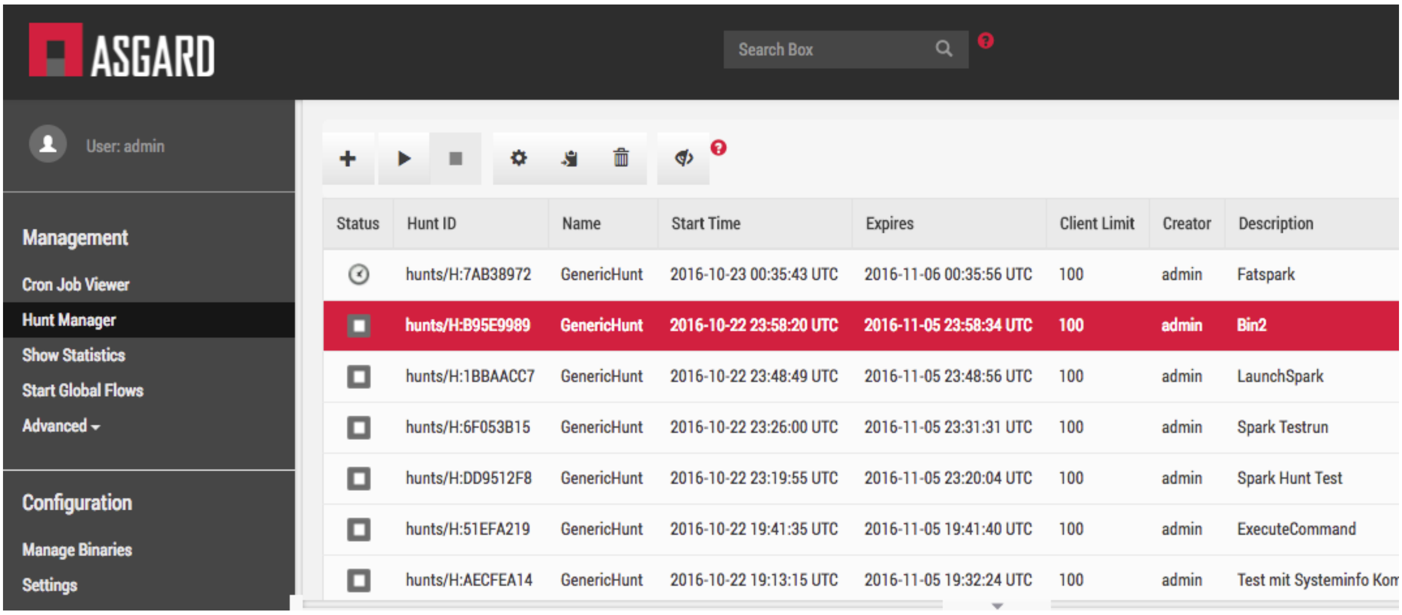
Multi-platform agents

Response and Remediation

Low resource footprint



ASGARD



Status	Hunt ID	Name	Start Time	Expires	Client Limit	Creator	Description
◷	hunts/H:7AB38972	GenericHunt	2016-10-23 00:35:43 UTC	2016-11-06 00:35:56 UTC	100	admin	Fatspark
□	hunts/H:B95E9989	GenericHunt	2016-10-22 23:58:20 UTC	2016-11-05 23:58:34 UTC	100	admin	Bin2
□	hunts/H:1BBAACC7	GenericHunt	2016-10-22 23:48:49 UTC	2016-11-05 23:48:56 UTC	100	admin	LaunchSpark
□	hunts/H:6F053B15	GenericHunt	2016-10-22 23:26:00 UTC	2016-11-05 23:31:31 UTC	100	admin	Spark Testrun
□	hunts/H:DD9512F8	GenericHunt	2016-10-22 23:19:55 UTC	2016-11-05 23:20:04 UTC	100	admin	Spark Hunt Test
□	hunts/H:51EFA219	GenericHunt	2016-10-22 19:41:35 UTC	2016-11-05 19:41:40 UTC	100	admin	ExecuteCommand
□	hunts/H:AECFEA14	GenericHunt	2016-10-22 19:13:15 UTC	2016-11-05 19:32:24 UTC	100	admin	Test mit Systeminfo Kom

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, memory, disk image and registry collection
- **Remediation**
  with ASGARD's remote execution and automated counteractive measures
- **Log Collection and Analysis**
  with preinstalled Splunk and ELK services
- **Asset Inventory**
  with the Security Cockpit feature (Q2/2017)

ASGARD's features are:

- Flexible and modern web interface
- Extensive response capabilities
- Cross-platform agents (Windows, Linux and macOS)
- Live remote memory analysis via Rekall framework
- 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 VMWare Image or Hardware Appliance
- Customizable platform / open to feature requests
- Direct contact to the developers / Security Made in Germany