


# Security Analyst 22.3

## Release Notes



**YAKINDU  
SECURITY ANALYST**

**Security Analyst 22.3**  
Build #SECA-193.1623, built on October 13, 2022

**Licensed to itemis AG**  
No distribution without prior written consent.  
itemis staff Floating license for yt-dataaccess-serna  
License type: LMX\_TYPE\_NETWORK from: vm1f:6200  
Valid until 2023-08-31 23:59

Runtime version: 11.0.9+11-b944.49 amd64  
VM: OpenJDK 64-Bit Server VM by JetBrains s.r.o.

Powered by [open-source software](#)

Copyright © 2018–2022 itemis AG

LM-X License Server Support	2
Assisted License Import	2
<b>Threat Scenario and Assistant Improvements</b>	<b>3</b>
Derived Compromised Assets	3
Explicit Compromised Assets	3
Impact on Damage Scenario Assignment Assistant	4
New Assistant for Explicit Compromised Assets	4
Improved Support for Large Models	5
<b>Enhanced Damage Scenario Rating</b>	<b>6</b>
New Impact Rating Editor Layout	6
Improved Completion Menu Sorting	6
Various Fixes and Improvements	6
Version Mapping	7

# LM-X License Server Support

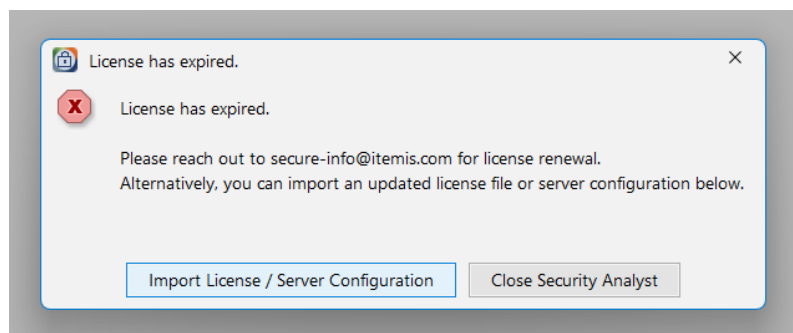
In addition to the local license files, with Security Analyst 22.3 we support license checks that require a centralized license server. With this in place, we now support floating licenses powered by [LM-X License Manager](#).

**Licensed to itemis AG**  
No distribution without prior written consent.  
itemis staff Floating license for yt-dataaccess-serna  
License type: LMX\_TYPE\_NETWORK from: vm1f:6200  
Valid until 2023-08-31 23:59

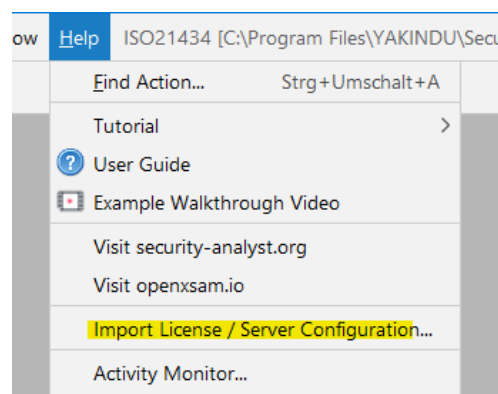
The server is configured via a properties file to configure the server endpoint. Details can be found in the user guide and the attached setup guide. The above mentioned license server needs to be installed accordingly by your administrators.

## Assisted License Import

Updating or importing licenses has been streamlined a lot. You no longer need to mess with your file system. Instead, when a missing or invalid license is detected, you can easily import it with the following dialog. Security Analyst will take care of the rest. change, a lot of error messages and workflows with regard to licenses have been improved.



Furthermore, you can initiate an import at any time from the help menu:



# Threat Scenario and Assistant Improvements

## Derived Compromised Assets

Threat Scenarios, especially the compromised assets, can now be tailored to your needs. By default, Security Analyst takes care of deriving recommended compromised assets based on the acted on elements and the "Production Rules Engine", which can be customized as part of the Method Configuration.

### Threat Scenario TS.1: Spoofing on CAN Bus

<no description> <a href="#">Edit</a>	IL	Severe
{	AFL	Very Low
Cause of Compromise TC.1: Spoofing	RL	2
Acts on Ch.1: CAN Bus		
Compromises C: Confidentiality, I: Integrity, A: Availability (Derived)		
Threatens +		
Attack Tree AS.1		
Realizes DS.1: Headlamp turns off unexpectedly DS.2: Headlamps turns on unexpectedly		
Lessened by <no assumptions>		
Risk Level 2		
}		








If you are interested in the derived elements, you can expand the following detailed list:

<b>Compromises</b>	C: Confidentiality of DF.6: OnMsg, OffMsg: BodyECU -> PowSwitAct [CAN]
	C: Confidentiality of DF.7: OnMsg, OffMsg: GateECU -> PowSwitAct [CAN]
	C: Confidentiality of OffFunc: Switch Headlamp Off
	C: Confidentiality of OffMsg: Headlamp Off Message
	C: Confidentiality of OnFunc: Switch Headlamp On
	C: Confidentiality of OnMsg: Headlamp On Message
	I: Integrity of DF.6: OnMsg, OffMsg: BodyECU -> PowSwitAct [CAN]
	I: Integrity of DF.7: OnMsg, OffMsg: GateECU -> PowSwitAct [CAN]
	I: Integrity of OffFunc: Switch Headlamp Off
	I: Integrity of OffMsg: Headlamp Off Message
	I: Integrity of OnFunc: Switch Headlamp On
	I: Integrity of OnMsg: Headlamp On Message
	A: Availability of DF.6: OnMsg, OffMsg: BodyECU -> PowSwitAct [CAN]
	A: Availability of DF.7: OnMsg, OffMsg: GateECU -> PowSwitAct [CAN]
	A: Availability of OffFunc: Switch Headlamp Off
	A: Availability of OffMsg: Headlamp Off Message
	A: Availability of OnFunc: Switch Headlamp On
	A: Availability of OnMsg: Headlamp On Message

## Explicit Compromised Assets

In some instances, you might want to override this default and add or remove specific entries. Derived Compromised Assets can be "inlined" and made Explicit Compromised Assets via an intention (default: <ALT> + <ENTER>).

### Threat Scenario TS.1: Spoof:

Intentions	
 Add External Ids	▶
 Add Flag 'Explicitly Not Modeled'	▶
 Add Sibling Threat Scenario	▶
 <b>Inline Compromised Assets from Acts on</b>	▶
 Show paths in inspector	▶
TODOs	
 Add Todo	▶
 Hide Todos	▶

After inlining, the compromised assets can be tailored to your needs. In the following example, all qualified assets related to integrity or availability have been removed.

**Compromises**

- C: Confidentiality of DF.6: OnMsg, OffMsg: BodyECU -> PowSwitAct [CAN]
- C: Confidentiality of DF.7: OnMsg, OffMsg: GateECU -> PowSwitAct [CAN]
- C: Confidentiality of OffFunc: Switch Headlamp Off
- C: Confidentiality of OffMsg: Headlamp Off Message
- C: Confidentiality of OnFunc: Switch Headlamp On
- C: Confidentiality of OnMsg: Headlamp On Message

## Impact on Damage Scenario Assignment Assistant

If a Damage Scenario concerns a Derived Compromised Asset of a Threat Scenario, it will be suggested in the Damage Scenario Assignment Assistant for the Damage Scenario. Instead of using the Derived Compromised Assets for a Threat Scenario you can also define Explicit ones.

DS.1: Headlamp turns off unexpectedly threatened by [ TS.1: Spoofing on CAN Bus Reset  
TS.2: Tampering on Gateway ECU, White... Accept Reject ]

## New Assistant for Explicit Compromised Assets

The new assistant suggests Explicit Compromised Assets based on the "Causing Assets" of the Threat Scenario and the Production Rules Engine. If an Explicit Compromised Asset is selected but not suggested by the Production Rules Engine, the assistant suggests to Remove that Compromised Asset. The "Causing Assets" are derived from the Threat Scenario Class and the Acts On relation of the Threat Scenario.

Compromised Asset Identification Refresh

---

What's this?

Threat Scenarios with Explicit Compromised Assets

What's this?  
TS.1: Spoofing on CAN Bus

compromises		
C: Confidentiality of DF.6: OnMsg, OffMsg: BodyECU -> PowSwitAct [CAN]	<span>Accept</span>	<span>Reject</span>
C: Confidentiality of DF.7: OnMsg, OffMsg: GateECU -> PowSwitAct [CAN]	<span>Accept</span>	<span>Reject</span>
C: Confidentiality of OffFunc: Switch Headlamp Off	<span>Accept</span>	<span>Reject</span>
C: Confidentiality of OffMsg: Headlamp Off Message	<span>Accept</span>	<span>Reject</span>
C: Confidentiality of OnFunc: Switch Headlamp On	<span>Accept</span>	<span>Reject</span>
C: Confidentiality of OnMsg: Headlamp On Message	<span>Accept</span>	<span>Reject</span>

# Improved Support for Large Models

Since Security Analyst calculates all possible attack paths throughout the modeled attack graph, large models pose a tough challenge. It is not trivial to keep Security Analyst responsive while calculating thousands of attack paths and damage transformations. With Version 22.3 we introduce major improvements under the hood to improve the performance by a large magnitude which means in other words: support for even larger models. The following picture says more than many words:



# Enhanced Damage Scenario Rating

## New Impact Rating Editor Layout

The layout of the impact rating editor has been improved. The rather complex tree structure has been replaced with a tabular-like representation to do the impact analysis per damage scenario. The rational field per rating has been moved to the inspector.

### Impact

S: Safety	RU.S3: Life-threatening injuries	3	RU
F: Financial	RU.F0: Negligible losses	0	RU
O: Operational	RU.O2: Important function impaired	2	RU
P: Privacy	RU.P0: No or negligible consequences	0	RU

## Improved Completion Menu Sorting

The order of security properties in the completion menu has been aligned with the order of declaration in the method configuration.

Impact Category S: Safety	⇒	Ⓢ S: Safety	Impact Model (MethodConfiguration)
Impact Category F: Financial		Ⓡ F: Financial	Impact Model (MethodConfiguration)
Impact Category O: Operational		Ⓞ O: Operational	Impact Model (MethodConfiguration)
Impact Category P: Privacy		Ⓟ P: Privacy	Impact Model (MethodConfiguration)

## Various Fixes and Improvements

- “Concerns” column is now editable in damage scenario table
- “Concerns” column sorting in damage scenario table is now alphabetical
- Feasibility options show its own description in the inspector
- When installing Security Analyst, sometimes existing files have not been overwritten correctly. This has been fixed.
- Security fix: Mitigated log4j vulnerabilities
- Method Configuration imports did sometimes result in broken references. This has been fixed.
- Fixed an issue where report generation was not possible due to an out of bound exception.
- New optional feasibility aggregator “geometric mean”
- CVSS-based risk matrices can be edited now

# Version Mapping

The following table can be used to determine the Security Analyst version based on the internal plugin version "com.moraad.core" that is stored in the .msd file of every solution:

```
<language slang="l:2bca1aa3-c113-4542-8ac2-2a6a30636981:  
com.moraad.core" version="<com-moraad-core-version>" />
```

com.moraad.core version	Security Analyst version
81	22.3
80	22.2
78	22.1
74	21.3
73	21.2
72	21.1.1
71	21.1
64	20.4
63	20.3.1
61	20.3
59	20.2.1
58	20.2
55	20.1.1
54	20.2.1
49	19.4.1
48	19.4
46	19.3.1
44	19.3
41	19.2
37	2.5.1