new eagle

RAPTOR®
INNOVATION
SUMMIT 2025

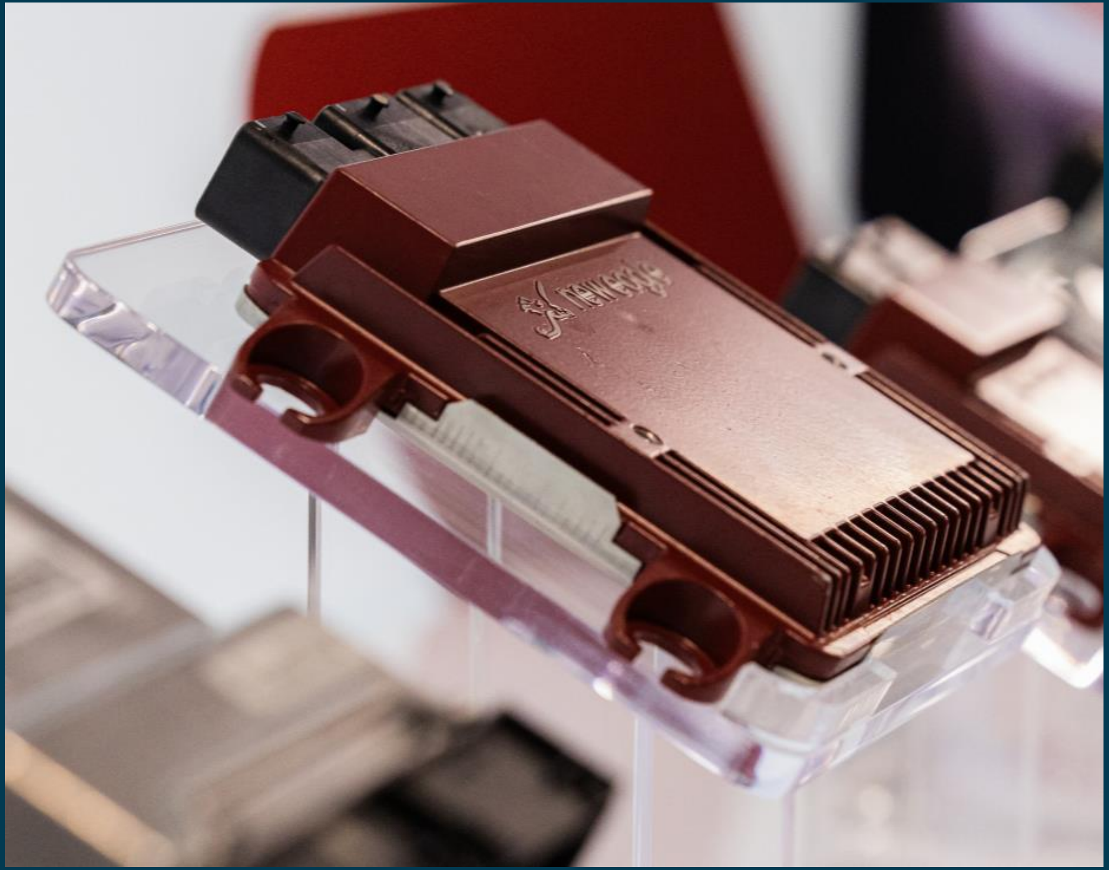
Exploring Approaches to Threat and Risk Assessment

Presented by:
Karen Boswell, Director System Safety and Quality, New Eagle
Rex Struble, Head of VxLabs North America, VxLabs

Exploring Approaches to TARA

Agenda

- Cybersecurity Management Process
- Raptor Secure Boundary and Application of the TARA
- Raptor-Secure
- Empower Raptor Users to create system TARA
- On-going collaboration with VxLab's AI-Powered Cybersecurity Platform – ThreatZ
- Mitigating cyber threats throughout the vehicle's lifecycle

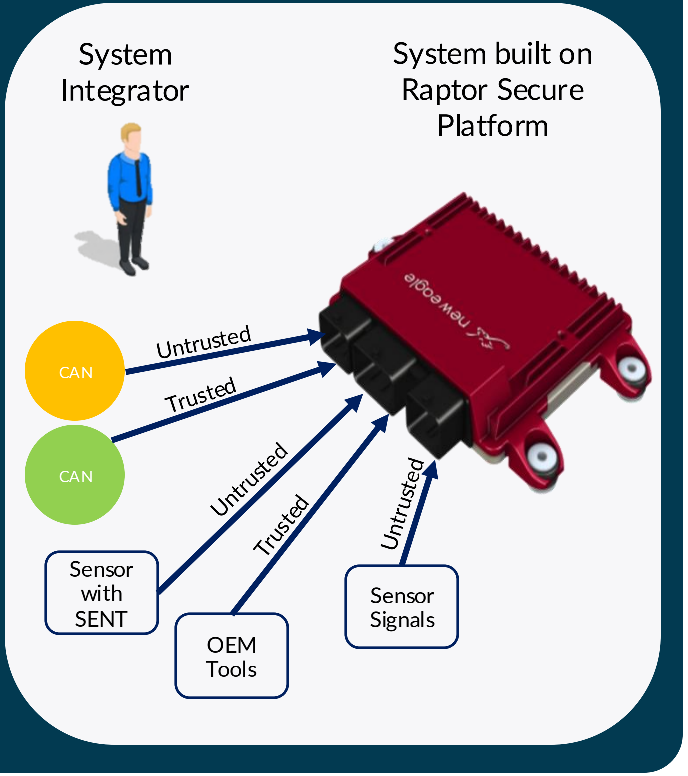


Structured TARA to Mitigate Cyber Threats

CHALLENGE

System Integrators able to use the Trust boundary of the New Eagle RCM Secured Platform Solution and achieve

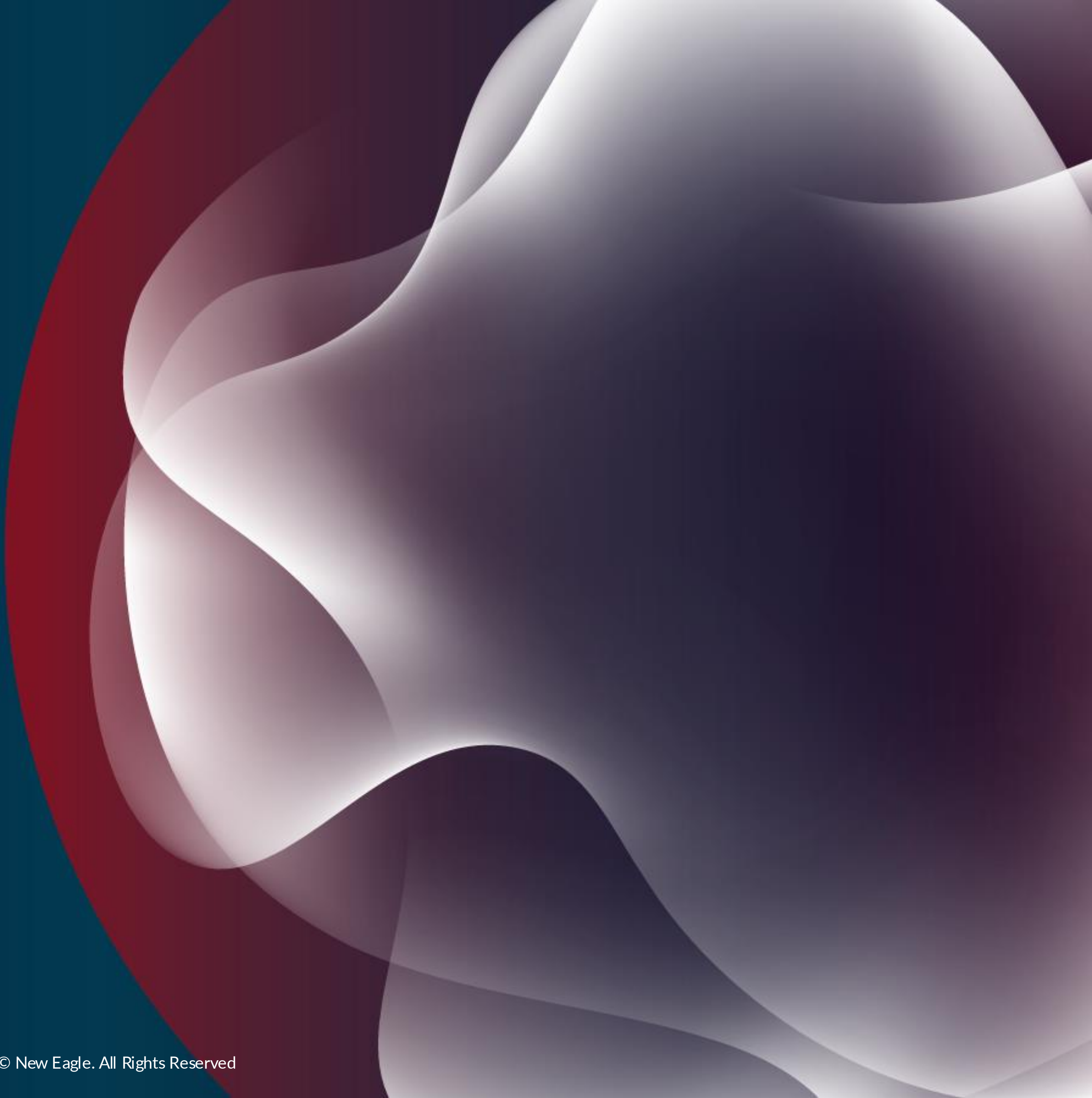
Cyber secure implementation through system lifecycle



SOLUTION

- ISO 21434 Execution
- Intuitive interface to the Raptor Secure Platform
- Lifecycle Management Support

Threat Analysis and Risk Assessment

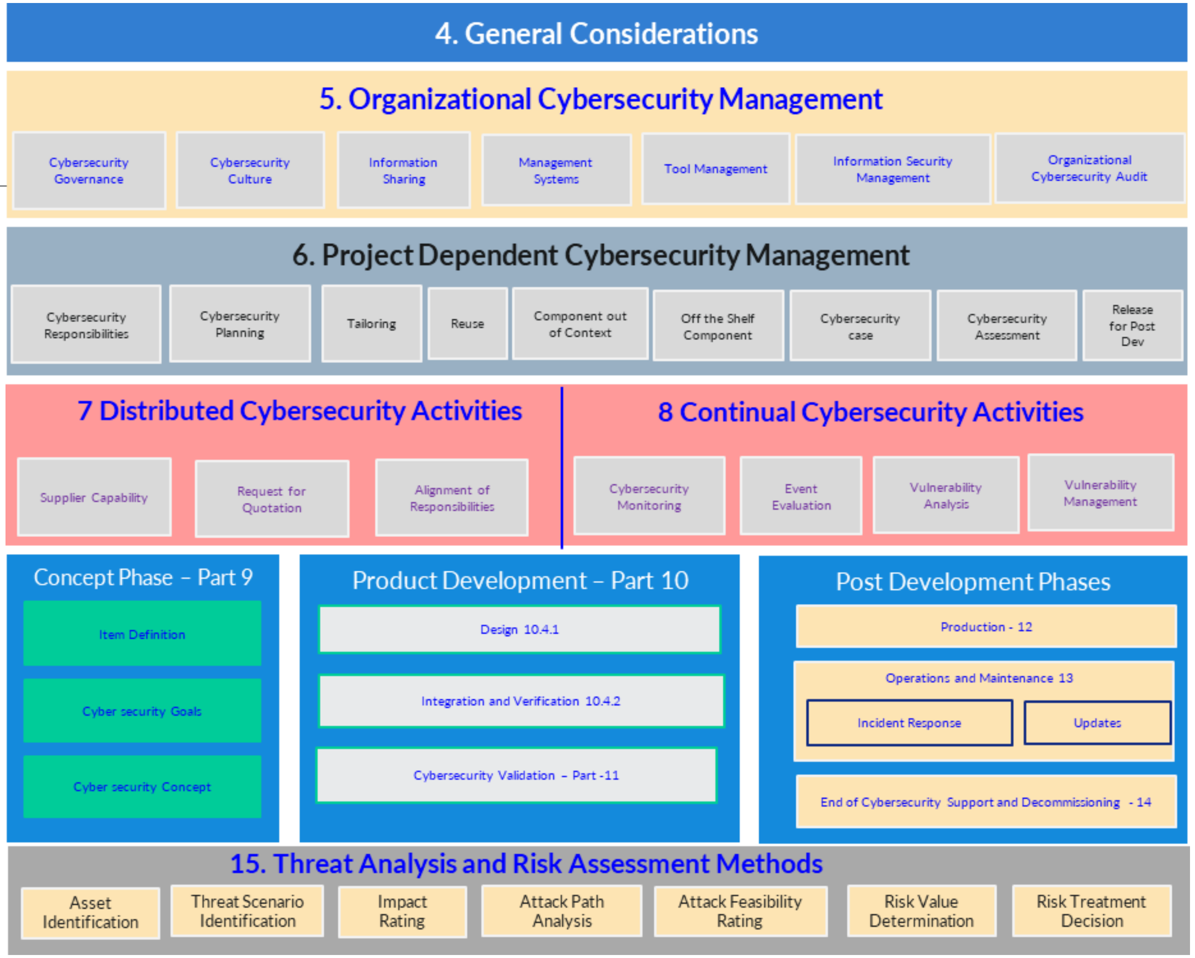


ISO 21434 – Road Vehicles Cybersecurity Engineering

Manage Cybersecurity Risks through the Lifecycle

- **Risk Management:** Comprehensive approach to identifying, assessing, and mitigating risks.
- **Cybersecurity Engineering:** Focuses on secure design, development, and testing of automotive systems.
- **Incident Response:** Guidelines for detecting, responding to, and recovering from cybersecurity incidents.

- New Eagle integrates Cybersecurity Management into QMS and APQP



4. General Considerations

5. Organizational Cybersecurity Management

Cybersecurity Governance | Cybersecurity Culture | Information Sharing | Management Systems | Tool Management | Information Security Management | Organizational Cybersecurity Audit

6. Project Dependent Cybersecurity Management

Cybersecurity Responsibilities | Cybersecurity Planning | Tailoring | Reuse | Component out of Context | Off the Shelf Component | Cybersecurity case | Cybersecurity Assessment | Release for Post Dev

7 Distributed Cybersecurity Activities

Supplier Capability | Request for Quotation | Alignment of Responsibilities

8 Continual Cybersecurity Activities

Cybersecurity Monitoring | Event Evaluation | Vulnerability Analysis | Vulnerability Management

Concept Phase – Part 9

Item Definition | Cyber security Goals | Cyber security Concept

Product Development – Part 10

Design 10.4.1 | Integration and Verification 10.4.2 | Cybersecurity Validation – Part -11

Post Development Phases

Production - 12 | Operations and Maintenance 13 (Incident Response | Updates) | End of Cybersecurity Support and Decommissioning - 14

15. Threat Analysis and Risk Assessment Methods

Asset Identification | Threat Scenario Identification | Impact Rating | Attack Path Analysis | Attack Feasibility Rating | Risk Value Determination | Risk Treatment Decision

ISO 21434 – Threat Analysis and Risk Assessment (TARA)

new eagle
RAPTOR® INNOVATION SUMMIT 2025

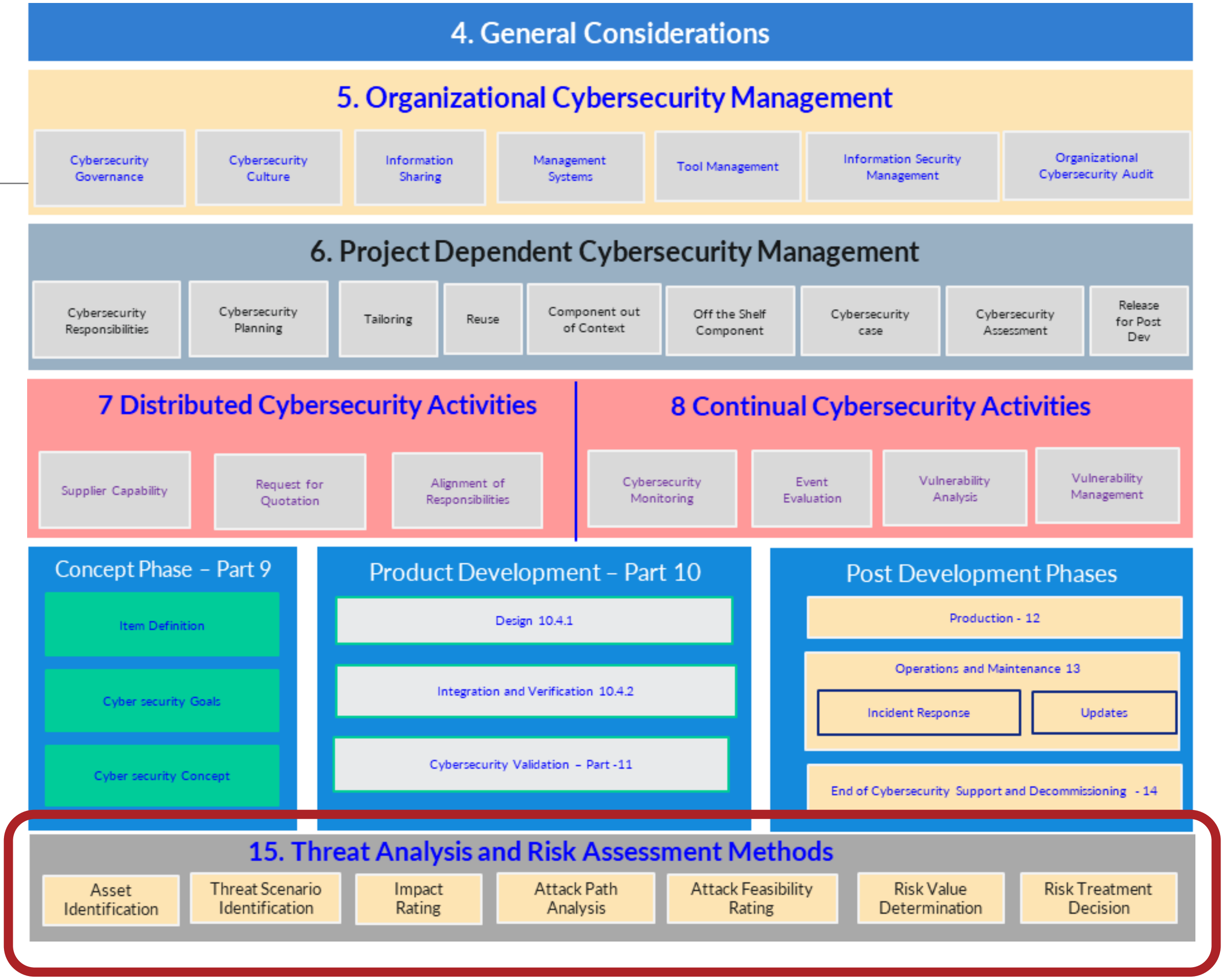
Risk-based approach to determine the extent to which a road user may be impacted by a threat scenario

Item Definition – Defined boundary, functions, architecture

TARA – Assess the risk and cyber damage scenarios

Cybersecurity Goals – Develop requirement to protect assets against a threat scenario

Cybersecurity Concept – Develop solution to achieve goals



4. General Considerations

5. Organizational Cybersecurity Management

Cybersecurity Governance | Cybersecurity Culture | Information Sharing | Management Systems | Tool Management | Information Security Management | Organizational Cybersecurity Audit

6. Project Dependent Cybersecurity Management

Cybersecurity Responsibilities | Cybersecurity Planning | Tailoring | Reuse | Component out of Context | Off the Shelf Component | Cybersecurity case | Cybersecurity Assessment | Release for Post Dev

7 Distributed Cybersecurity Activities

Supplier Capability | Request for Quotation | Alignment of Responsibilities

8 Continual Cybersecurity Activities

Cybersecurity Monitoring | Event Evaluation | Vulnerability Analysis | Vulnerability Management

Concept Phase – Part 9

Item Definition | Cyber security Goals | Cyber security Concept

Product Development – Part 10

Design 10.4.1 | Integration and Verification 10.4.2 | Cybersecurity Validation – Part -11

Post Development Phases

Production - 12

Operations and Maintenance 13: Incident Response | Updates

End of Cybersecurity Support and Decommissioning - 14

15. Threat Analysis and Risk Assessment Methods

Asset Identification | Threat Scenario Identification | Impact Rating | Attack Path Analysis | Attack Feasibility Rating | Risk Value Determination | Risk Treatment Decision

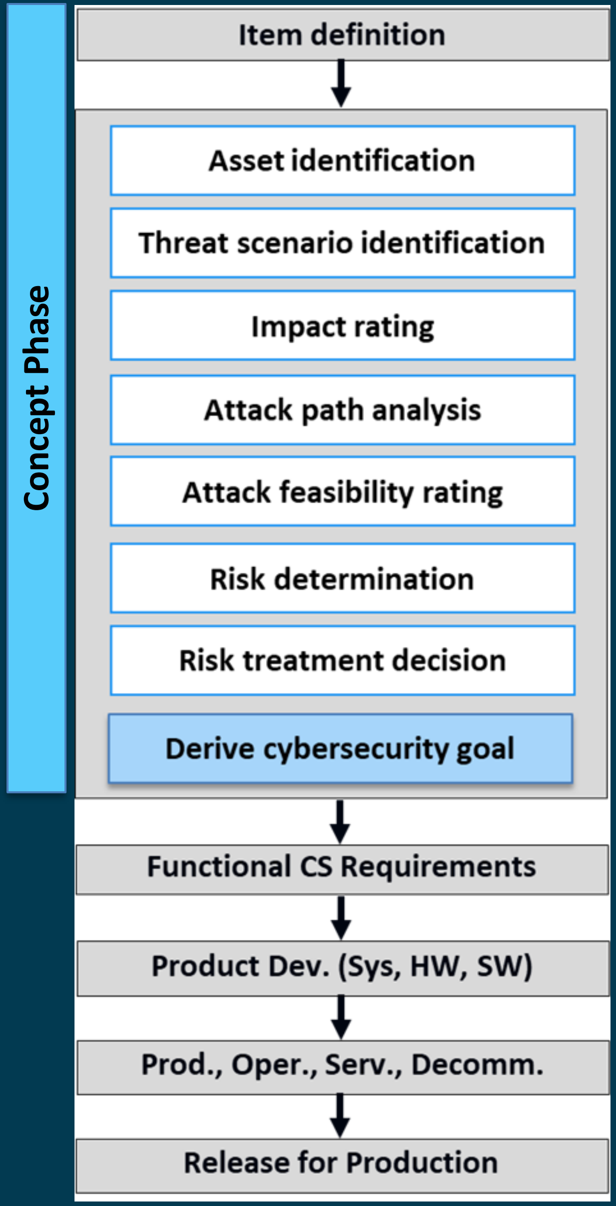
INNOVATE FASTER. SCALE SMARTER

TARA boundary defines the secure Raptor Base

Executing the TARA

Methodologies used within TARA

- **Threat Scenario identification**
    - STRIDE is a used to identify and analyze potential security threats to a system
    - STRIDE represents the following threats: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
- **Attack Feasibility Rating Methods**
    - Attack Potential-based approach
    - CVSS-base approach (Common Vulnerability Scoring System)
    - Attack vector-based approach
- **Risk Determination – Cybersecurity Assurance Level**


Concept Phase
Item definition
Asset identification
Threat scenario identification
Impact rating
Attack path analysis
Attack feasibility rating
Risk determination
Risk treatment decision
Derive cybersecurity goal
Functional CS Requirements
Product Dev. (Sys, HW, SW)
Prod., Oper., Serv., Decomm.
Release for Production

new eagle

RAPTOR® INNOVATION SUMMIT 2025

Threat Analysis and Risk Assessment

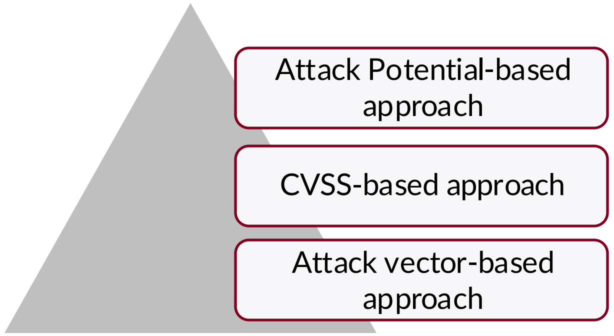
Threat Scenario Identification

One damage scenario can correspond to multiple threat scenarios

Threat modelling approaches based on frameworks such as **EVITA**, **TVRA**, **PASTA**, **STRIDE** (**S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, **E**levation of Privilege

STRIDE Threats	Explanation	Security Attribute	Threat Scenario **<STRIDE threat** mapped to security property> **to an asset**, which **may cause the damage scenario**
Spoofing	Attackers pretend to be someone or something else	Authentication: Freshness, imitation of something or someone different	***spoofed*** *messages may lead to messages at the wrong time*
Tampering	Attackers change data in transit or in a data store, attackers may change functions as well as implemented software, firmware or hardware	Integrity: Manipulation of data or code (network, CAN, memory,..)	***tampered*** *messages may lead to messages at the wrong time*
Repudiation	Attackers perform actions that cannot be traced back to them	Non-Repudiation Freshness, Claim something not to have done	***replay*** *of messages (jammer) which were intercepted before leads to messages at the wrong time*
Information Disclosure	Attackers get access to data in transit or in a data store	Confidentiality: Privacy, Disclosure of Information towards unauthorized people	***unauthorized disclosure*** *of messages which can enable reengineering and encryption of secrets*
Denial of Service	Attackers interrupt a system legitimate operation by overloading	Availability: Denial or degradation of a service towards valid user	***denial of service*** *of the communication channel which means that no commands can be transmitted*
Elevation of Privilege	Attackers perform actions they are not authorized to perform	Authorization Earn ability without authorization	***elevation of privilege*** *may result in unauthorized persons gaining access*

Attack Path and Attack Feasibility


Attack Potential-based approach

CVSS-based approach

Attack vector-based approach

Attack potential-based approach

Elapsed Time		Specialist Expertise		Knowledge of the Item		Window of Opportunity		Equipment	
Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value
< 1 week	0	Laymen	0	Public	0	Unlimited	0	Standard	0
< 1 month	1	Proficient	3	Restricted	3	Easy	1	Specialized	4
<= 6 month	4	Expert	6	Confidential	7	Moderate	4	Custom	7
<= 3 Years	10	Multiple Experts	8	Strictly Confidential	11	Difficult / None	10	Multiple Custom	9
> 3 Years	19	-	-	-	-	-	-	-	-

Value	Attack Feasibility
0 - 9	High
10 - 13	
14 - 19	Medium
20 - 24	Low
=> 25	Very Low

		Attack Feasibility Rating				Method
		Very Low	Low	Medium	High	Attack Feasibility Level
		Physical	Local	Adjacent	Network	Attack Vector
Impact Rating	Negligible	--	--	--	--	
	Moderate	CAL1	CAL1	CAL2	CAL3	
	Major	CAL1	CAL2	CAL3	CAL4	
	Severe	CAL2	CAL3	CAL4	CAL4	

Raptor-Secure

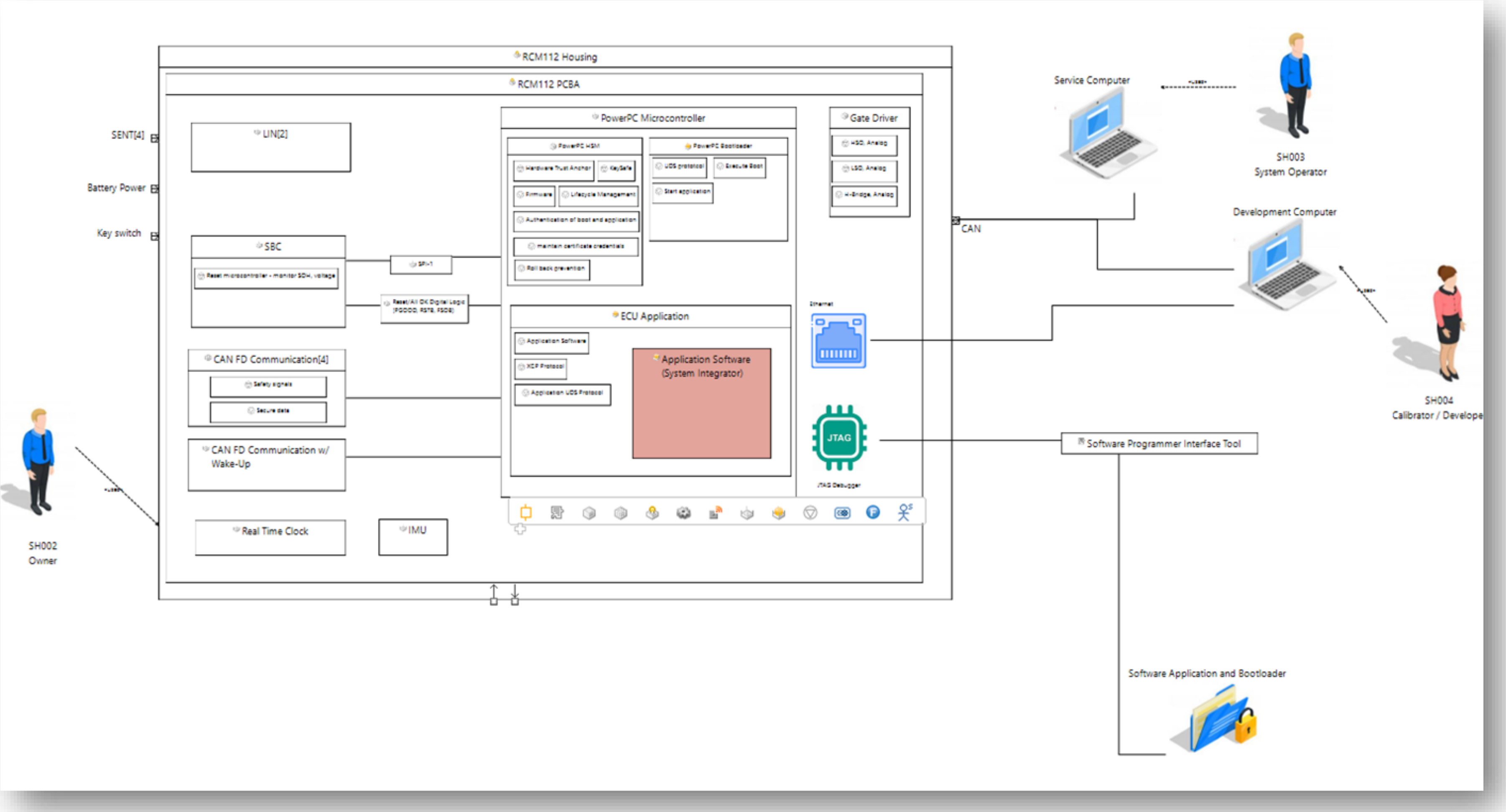
Item Definition for Security

RAPTOR Secure platform

New Eagle cybersecurity item definition does not include specific function, sensors, driven loads added to the item by System Integrator

Functions analyze align with SEooC

TARA of the Vehicle Level ITEM must be analyzed by the System Integrator

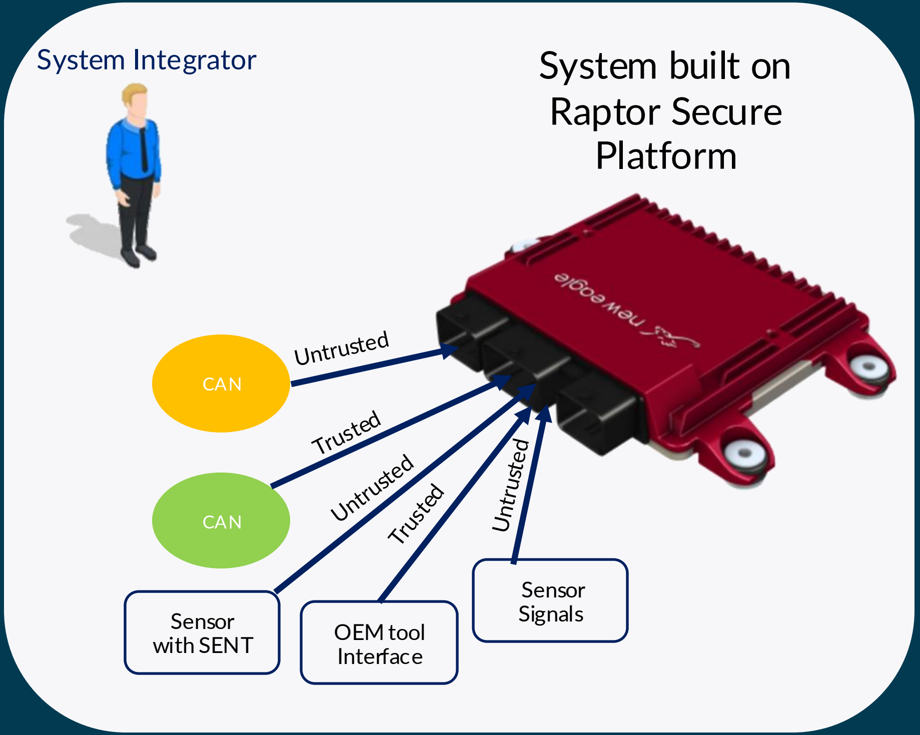


CCM112 Architecture

System Integrators are able to use the Trust boundary of the Secured Platform Solution

New Eagle Secure Platform

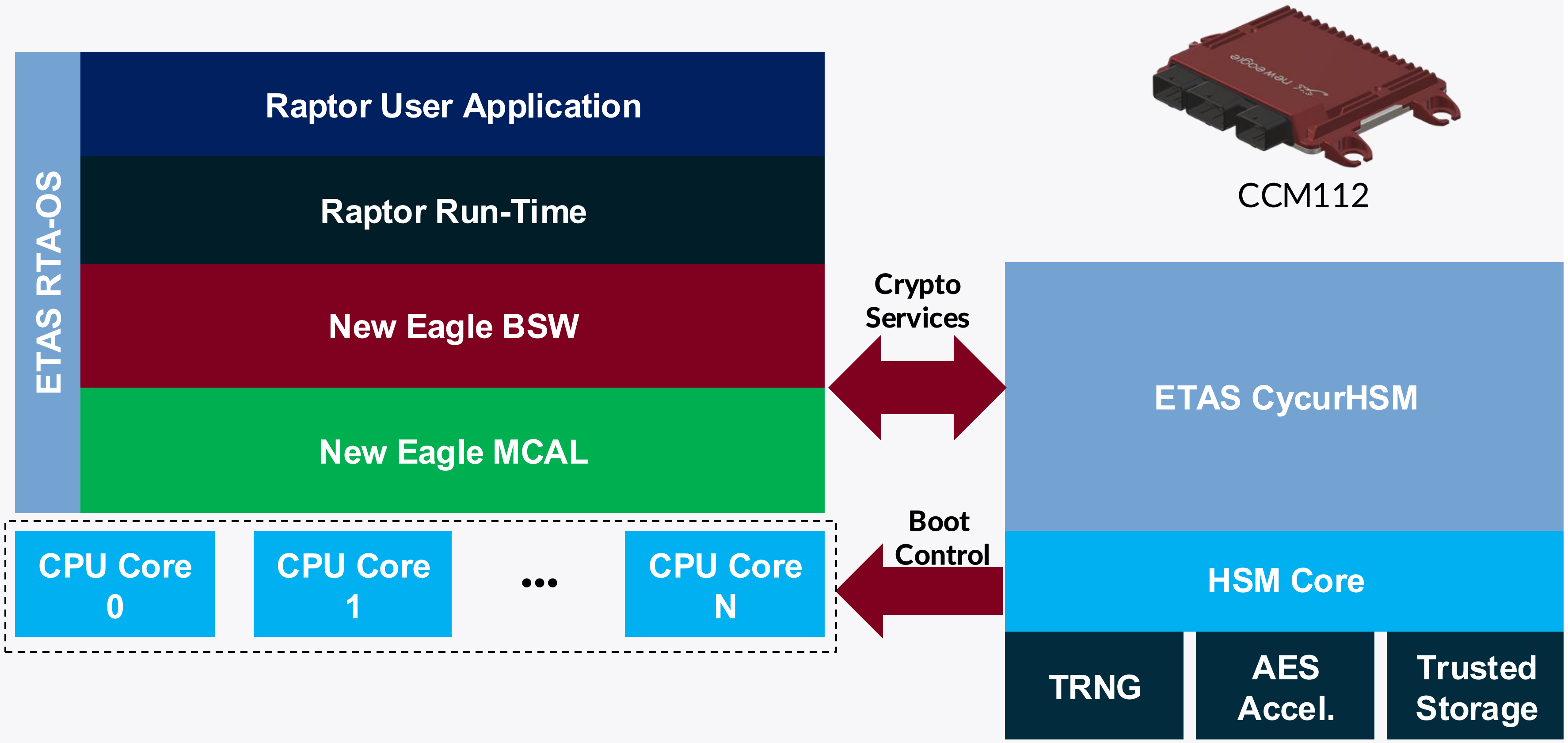
- Secure Boot
- Key safe through Hardware Security Module
- Rollback prevention
- Trusted cryptographic algorithms
- JTAG lockout
- Secure Programming
- UDS Services 27 and 29
- Secure on-board Communication
- Lifecycle management to establish privileges for production



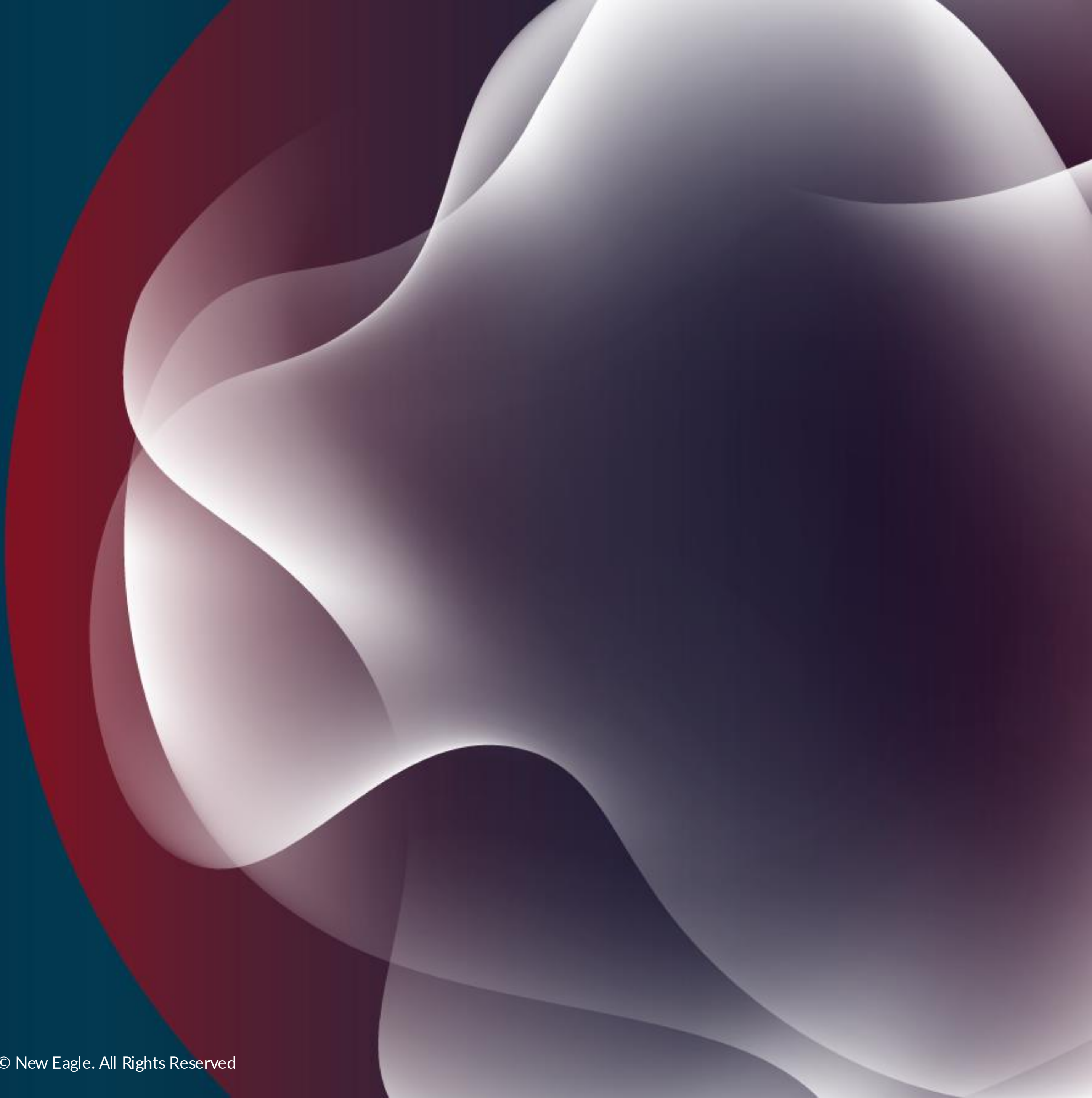
INNOVATE FASTER. SCALE SMARTER

CCM112 With Advanced Cybersecurity Functions Powered by ETAS

- Available on CCM112 in Q4 2025
- Initial feature set will focus on run-time cryptographic services for SecOc and J1939-91C
- Secure boot functionality available in H1 2026
- Makes full use of hardware security module of TC3XX MCU



Empower Raptor Users to Create System TARA



new eagle

RAPTOR®
INNOVATION
SUMMIT 2025

Enhancing Raptor-Secure

Ongoing Collaboration with VxLabs: Objectives

1) **Demonstrate the benefits of a Dynamic TARA across the tech-stack, supply-chain, and full vehicle lifecycle.**
   - New Eagle Device: CCM112 module block

2) **Enable customer Dynamic TARA Dev at the system level.**

3) **Enable interoperability between Raptor and ThreatZ (VxLabs' AI-powered CSMS Saas Module)**

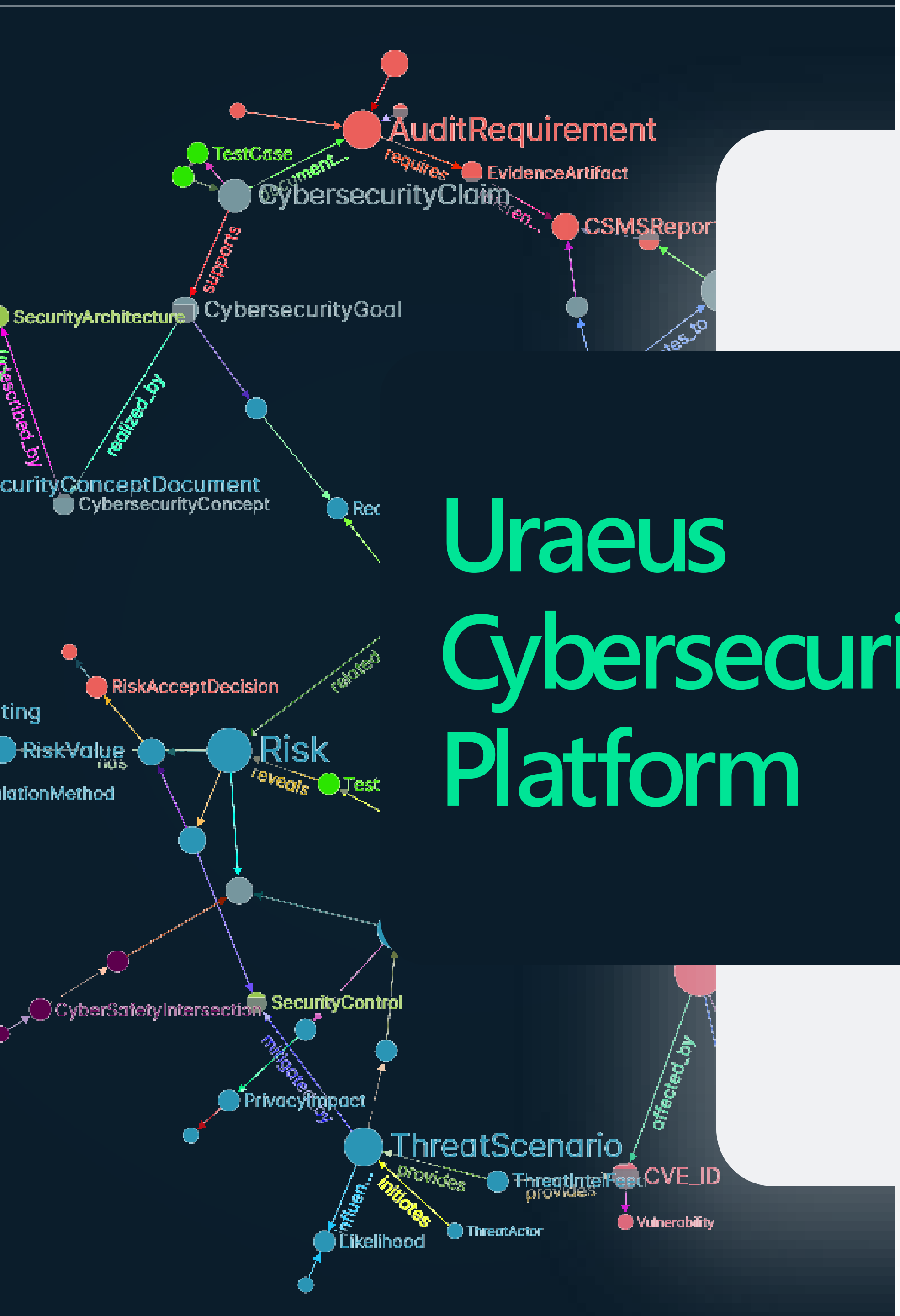
CSMS = Cybersecurity Management System

INNOVATE FASTER. SCALE SMARTER

VxLabs

Uraeus Cybersecurity Platform

VxLabs



Uraeus Cybersecurity Platform

Collaborative Security Ecosystem

Uraeus eliminates traditional security gaps by connecting development and operational domains through a common data model and security framework.

Regulatory Compliance

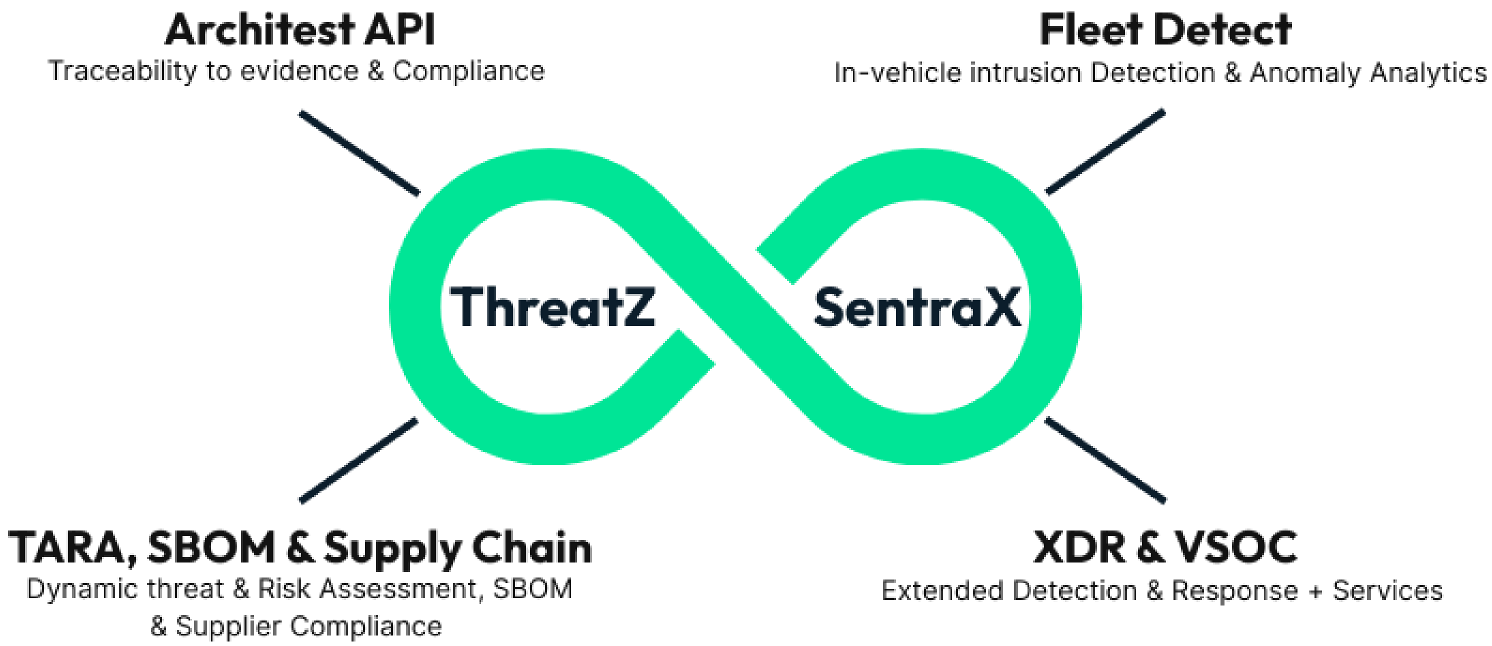
Built specifically to address ISO/SAE 21434 UNECE R155 and R156 requirements, Uraeus automates compliance documentation, verification, and reporting.

AI-Driven Intelligence

At the core of Uraeus is a sophisticated knowledge graph that contextually links threats, vulnerabilities, assets, and compliance requirements.

Uraeus Cybersecurity Platform

AI-Powered Knowledge Graph for Continuous Traceability & Compliance


Architest API
Traceability to evidence & Compliance
Fleet Detect
In-vehicle intrusion Detection & Anomaly Analytics
ThreatZ
SentraX
TARA, SBOM & Supply Chain
Dynamic threat & Risk Assessment, SBOM & Supplier Compliance
XDR & VSOC
Extended Detection & Response + Services

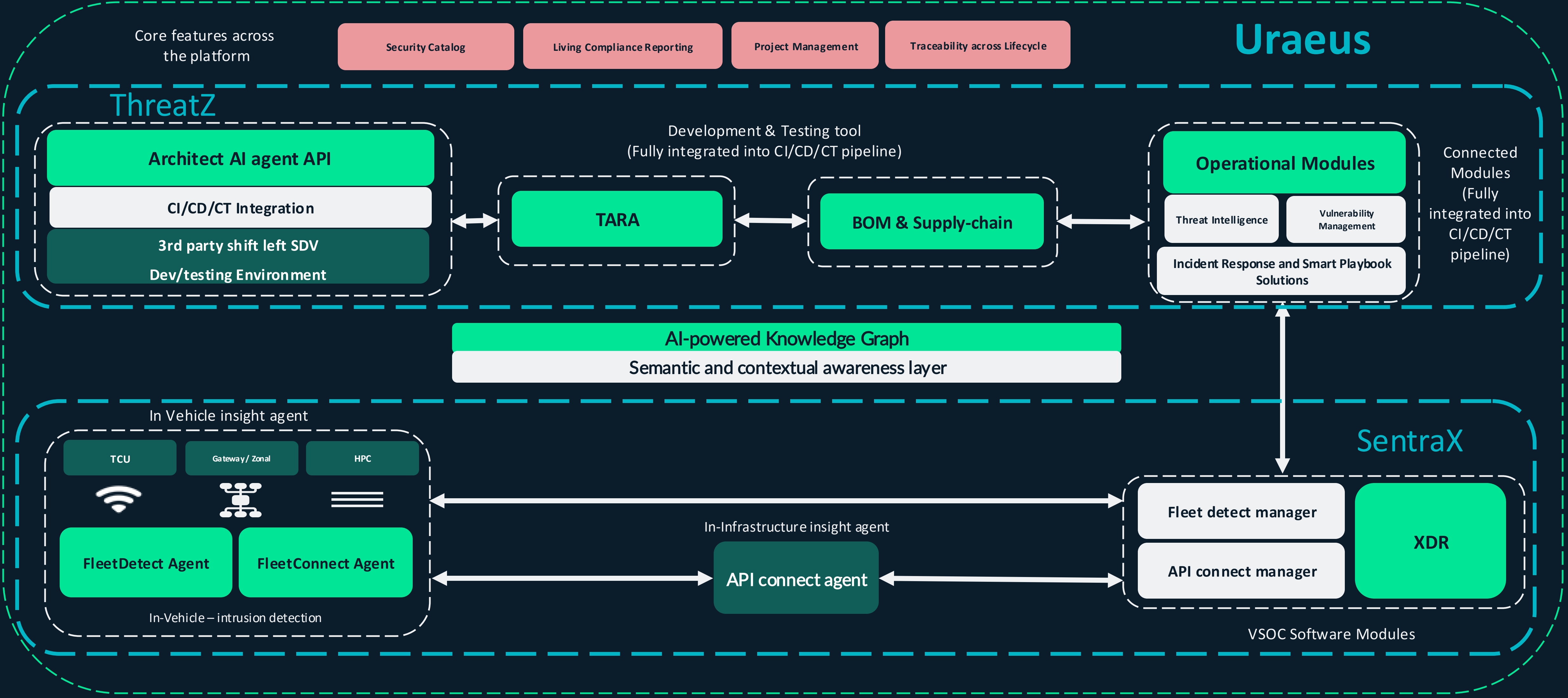
Uraeus is a modular cybersecurity platform whose **AI knowledge graph** unifies requirements, risks, SBOMs, controls, tests, evidence, and incidents into a single source of truth—**maintaining traceability & compliance** across the lifecycle via **open APIs** to PLM/ALM/DevOps and in-vehicle telemetry.

It includes **pre-built templates, libraries, and catalogs** aligned to ISO 21434 & UNECE R155, enabling teams to **build and reuse** a digital security library delivering faster with greater **consistency, speed and efficiency**.

Uraeus Cybersecurity Platform

VxLabs

AI-powered Knowledge Graph - Enabled



Uraeus

Core features across the platform

Security Catalog

Living Compliance Reporting

Project Management

Traceability across Lifecycle

ThreatZ

Architect AI agent API

CI/CD/CT Integration

3rd party shift left SDV Dev/testing Environment

Development & Testing tool (Fully integrated into CI/CD/CT pipeline)

TARA

BOM & Supply-chain

Operational Modules

Threat Intelligence

Vulnerability Management

Incident Response and Smart Playbook Solutions

Connected Modules (Fully integrated into CI/CD/CT pipeline)

AI-powered Knowledge Graph

Semantic and contextual awareness layer

SentraX

In Vehicle insight agent

TCU

Gateway / Zonal

HPC

FleetDetect Agent

FleetConnect Agent

In-Vehicle – intrusion detection

In-Infrastructure insight agent

API connect agent

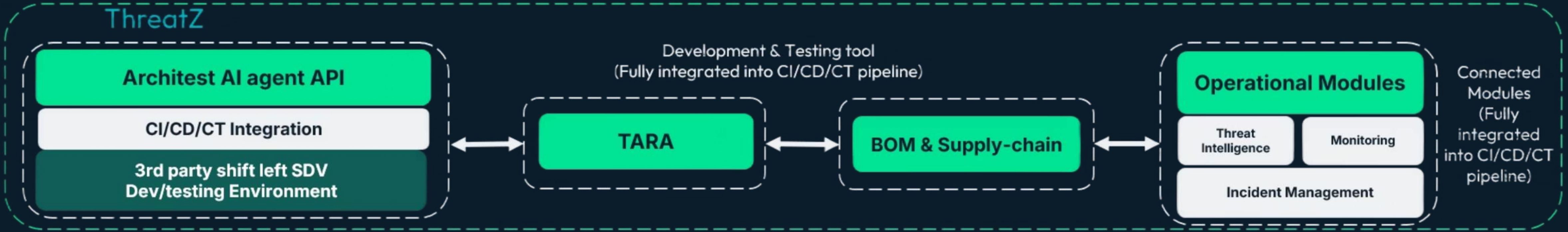
Fleet detect manager

API connect manager

XDR

VSOC Software Modules

ThreatZ: Core Sub-Modules


ThreatZ
Architest AI agent API
CI/CD/CT Integration
3rd party shift left SDV Dev/testing Environment
Development & Testing tool (Fully integrated into CI/CD/CT pipeline)
TARA
BOM & Supply-chain
Operational Modules
Threat Intelligence
Monitoring
Incident Management
Connected Modules (Fully integrated into CI/CD/CT pipeline)

TARA Module – Threat Analysis & Risk & Risk Assessment

- System modeling: Define assets, components, interfaces, and data flows.
- Threat & risk modeling aligned with ISO 21434.
- CAL (Cybersecurity Assurance Level) assignment.
- Security goals, claims, and concepts generation.
- Damage scenarios, attack paths, and vulnerability mapping. mapping.

BOM & Supply Chain Module

- SBOM (Software Bill of Materials) import and versioning. versioning.
- Vulnerability (CVE) tracking and VEX status management. management.
- Supplier risk profiling and compliance monitoring.
- Open-source license tracking.
- Delta tracking across SBOM versions.
- AI-driven analytics for prioritizing threats and risks.

Operations Module – Incident Monitoring & Response

- Real-time incident intake from VSOC via API.
- In-vehicle and backend incident correlation.
- Root cause analysis and mitigation tracking.
- Integration with threat intelligence feeds.
- Audit-ready incident reports.

Compliance Reporting Module

- Generate and manage all ISO 21434 and UNECE R155 reports.
- Grouped by report type, version, and generation date. date.
- Filters for checklist vs. formal reports.
- Export formats: PDF, Excel, JSON.
- Report history, versioning, and expiry notifications.

Security Catalog

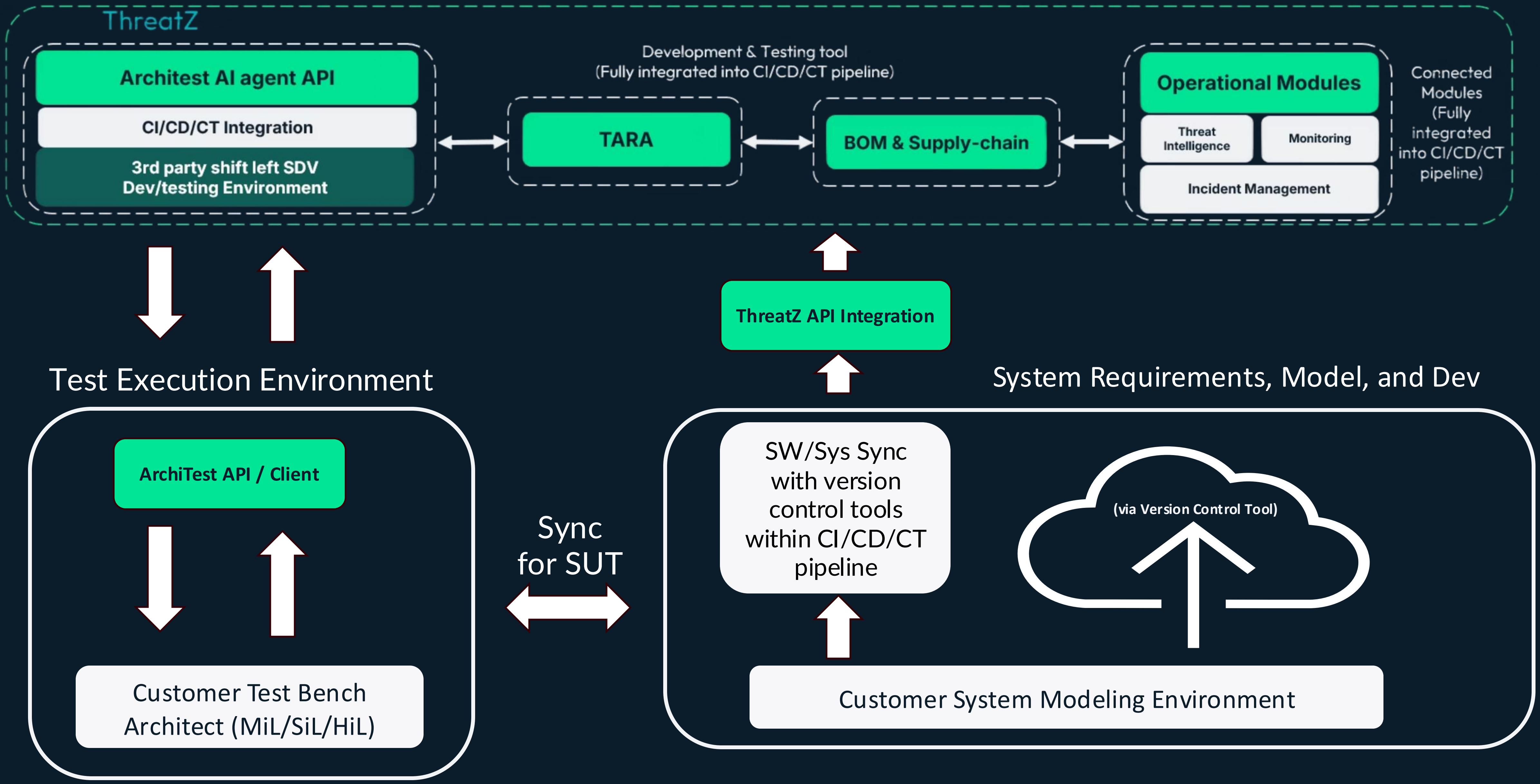
- Reusable library of threats, assets, goals, controls, and claims.
- Template-based security requirements.
- Shared across projects for consistency and traceability.

Policy Manager

- Define and enforce cybersecurity policies across projects.
- Manage accepted risk treatments and allowed/denied security states.
- Align policies with compliance and internal governance

ThreatZ: Integration Eco-system

VxLabs



ThreatZ

Architest AI agent API

CI/CD/CT Integration

3rd party shift left SDV Dev/testing Environment

Development & Testing tool
(Fully integrated into CI/CD/CT pipeline)

TARA

BOM & Supply-chain

Operational Modules

Threat Intelligence

Monitoring

Incident Management

Connected Modules (Fully integrated into CI/CD/CT pipeline)

ThreatZ API Integration

Test Execution Environment

System Requirements, Model, and Dev

ArchiTest API / Client

Customer Test Bench Architect (MiL/SiL/HiL)

Sync for SUT

SW/Sys Sync with version control tools within CI/CD/CT pipeline

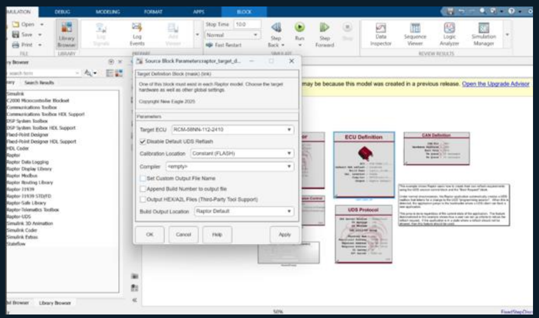
(via Version Control Tool)

Customer System Modeling Environment

Interoperability with Raptor

VxLabs

ThreatZ: Interoperability w/ Ecosystem

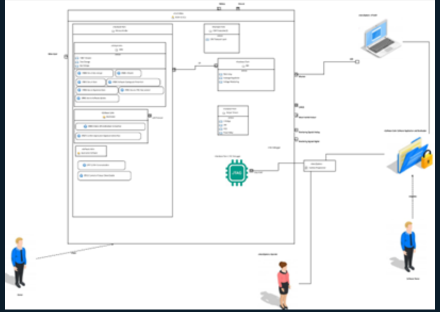


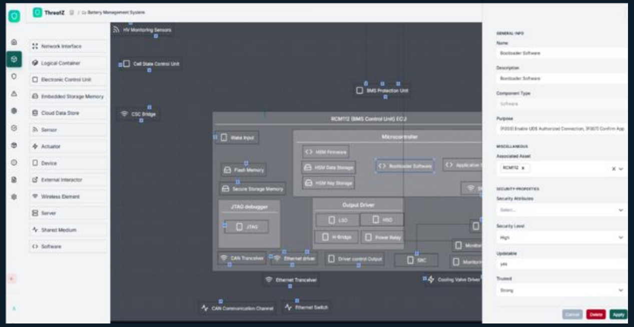
1

Raptor Simulink Plug-in Software Library – CCM112

2

New Eagle CCM 112 Item Definition Boundary Diagram



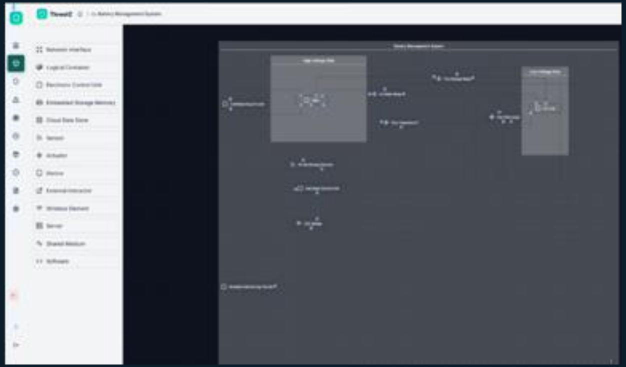


Import, Map, and Config CCM 112 Security Properties into ThreatZ

3

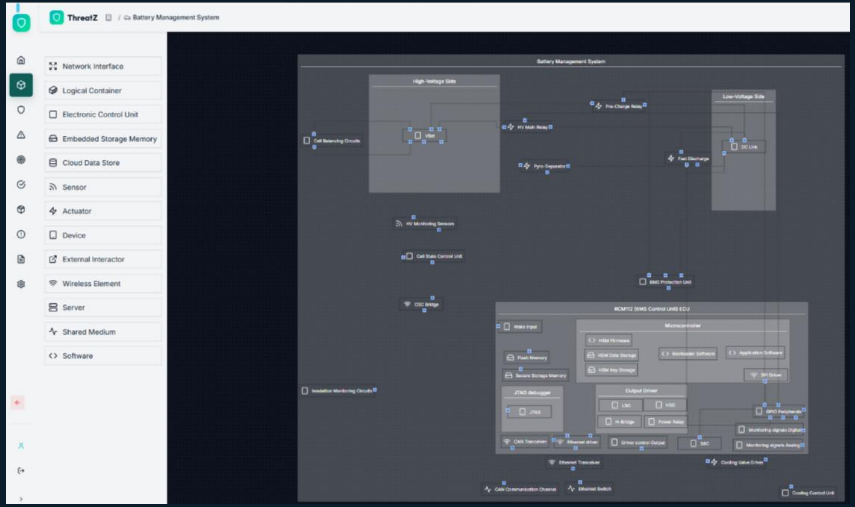
4

ThreatZ Native Models AND/OR Import 3rd Party Device Models



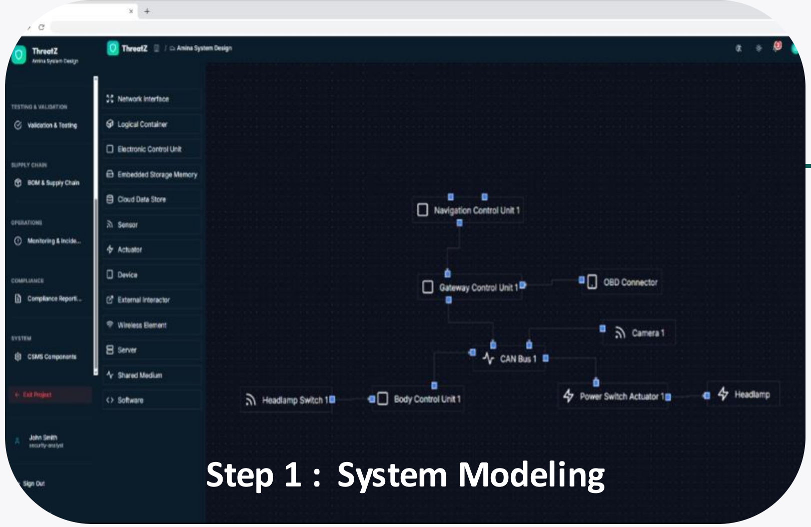
5

Full System Model with identification of System Assets & Interfaces

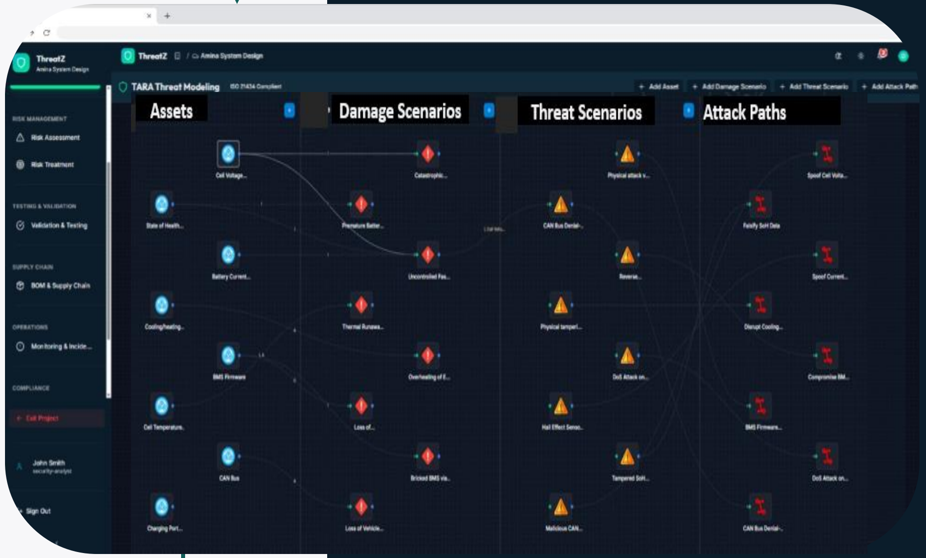


TARA

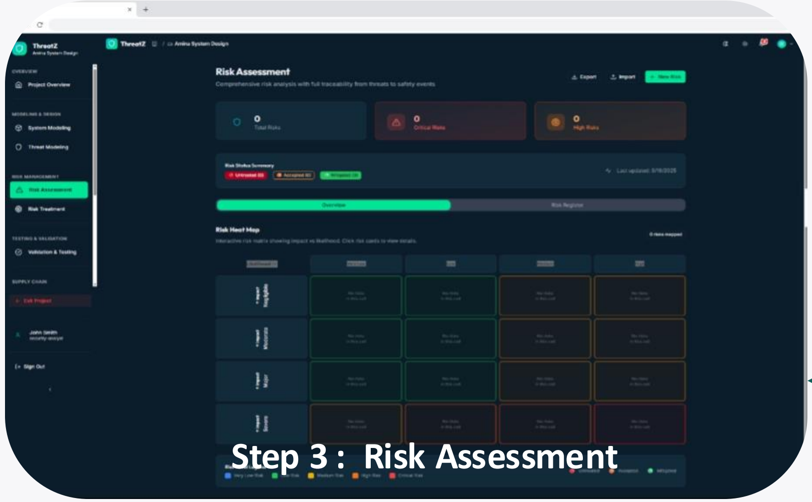
Graph-Based Risk Visualization



Step 1 : System Modeling



Step 2 : Threat Modeling



Step 3 : Risk Assessment

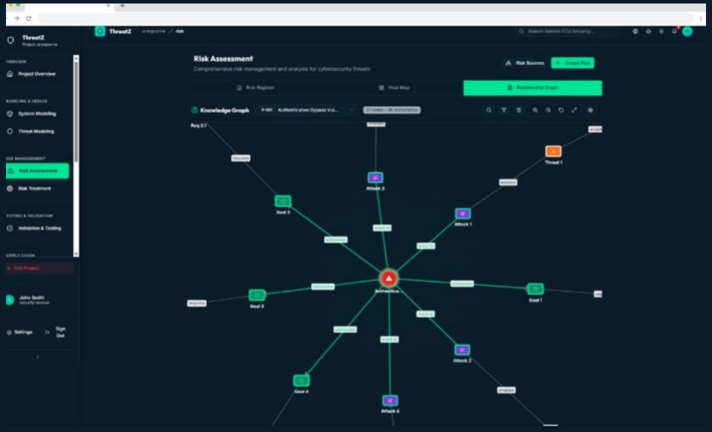
Key Features

- Drag-and-Drop System Modeling
- Risk Traceability
- Auto/Recommender AI Agent
- Extensive Security Catalog
- Tool chain Integration
- Risk Tracking over Time

VxLabs

A Dynamic and Living Risk Assessment

ThreatZ Platform Overview



Risk Assessment

Comprehensive risk management and analysis for cybersecurity threats

Dynamic Risk Relationship Graph

TARA Graph Modeling

- ❑ Graph-based links: Assets → Threats → Attack Paths → Controls.
- ❑ AI gap alerts for goals/controls.
- ❑ CAL, assumptions, and claims kept in sync

SBOM as Living Assets

- ❑ Continuos SBOM graph: components, versions, licences, suppliers.
- ❑ CVE/License feeds with instant impact.
- ❑ Policy gates and delta tracking across releases

Validation & Test

- ❑ End-to-end traceability: requirement → test → evidence
- ❑ Risk-based coverage + attack/ fault simulation hooks
- ❑ Auto-reports for ISO 21434 / UNECE R155

Operational Module

- ❑ Signals : XDR/VSOC, incidents, supplier disclosures.
- ❑ Closed loop: incidents update likelihood/exposure in risk model.
- ❑ Playbooks and timelines tied to policies.

Outcome

95%

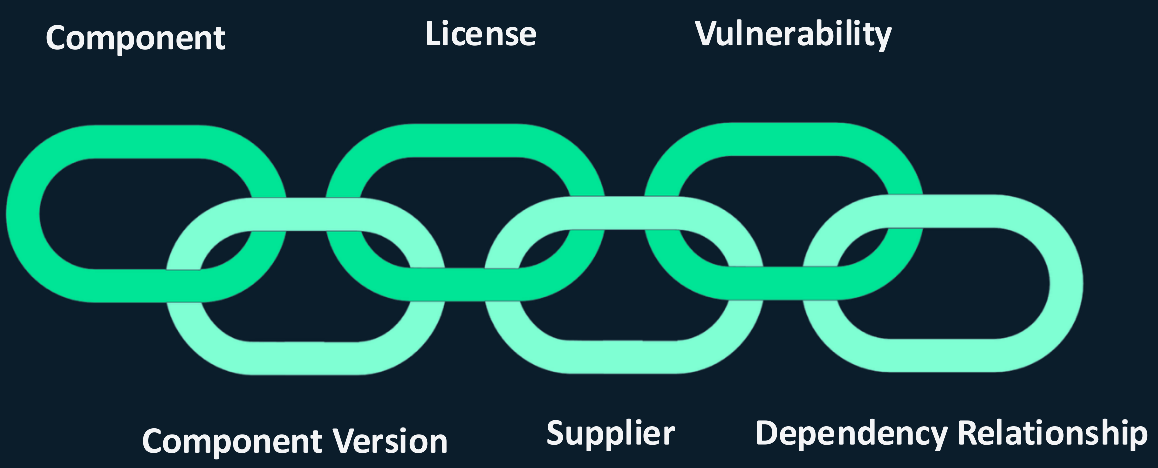
	Time-to-Impact after CVE	⬆ Minutes not days
SBOM Coverage	-40-60% ⬇	Incident MTTR

VxLabs

BOM & Supply Chain Module

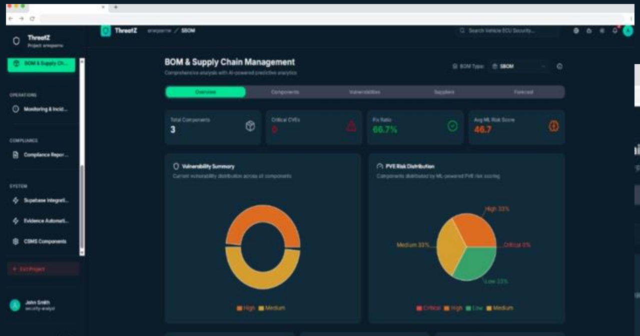
Empowers OEMs and Tier 1 suppliers to proactively mitigate risks across supply chain

- **Manage** bill of materials (BOM) – hardware and software
- **Track** third-party components
- **Monitor** supplier-related risks
- **Ensure traceability** of vulnerabilities, licenses, and VEX (Vulnerability Exploitability exchange) status.



BOM Management
License Compliance
Supplier Risk Monitoring
Cross-Module Linking

Vulnerability Tracking
Impact Propagation
AI-Powered Analytics
VEX Integration



BOM & Supply Chain Management

Comprehensive analysis with AI-powered predictive analytics

Total Components 3

Critical CVEs 0

Fix Ratio 66.7%

Avg ML Risk Score 46.7

Vulnerability Summary

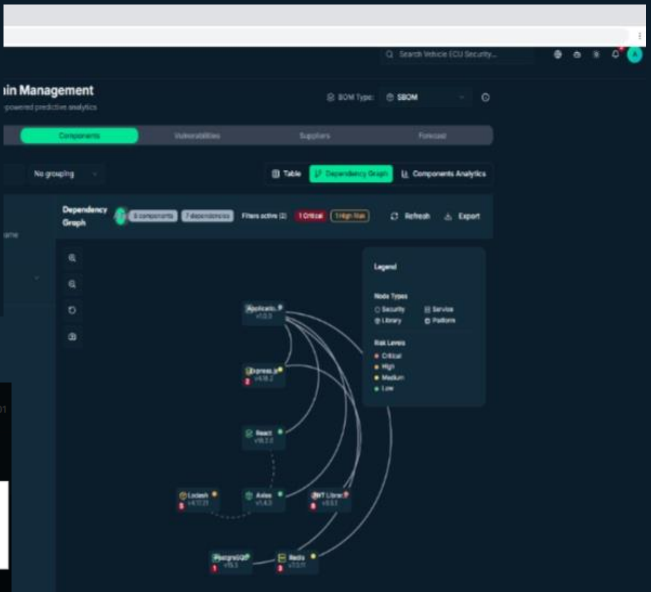
Current vulnerability distribution across all components

PVE Risk Distribution

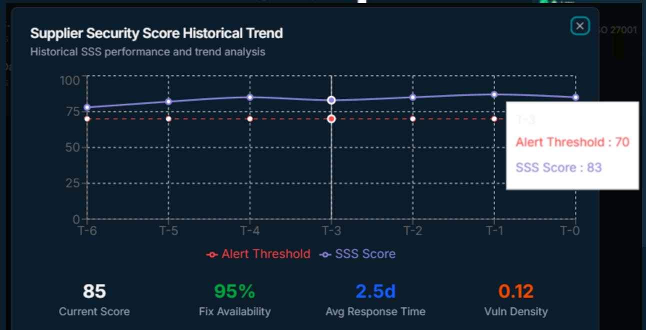
Components distributed by ML-powered PVE risk scoring

Exploit Likelihood 36.7%

SBOM Dashboard



Component Dependency Graph



Supplier Security Score Historical Trend

Historical SSS performance and trend analysis

85 Current Score

95% Fix Availability

2.5d Avg Response Time

0.12 Vuln Density

Supplier Security Score

Operations Module

Threat Intelligence & Incident Management

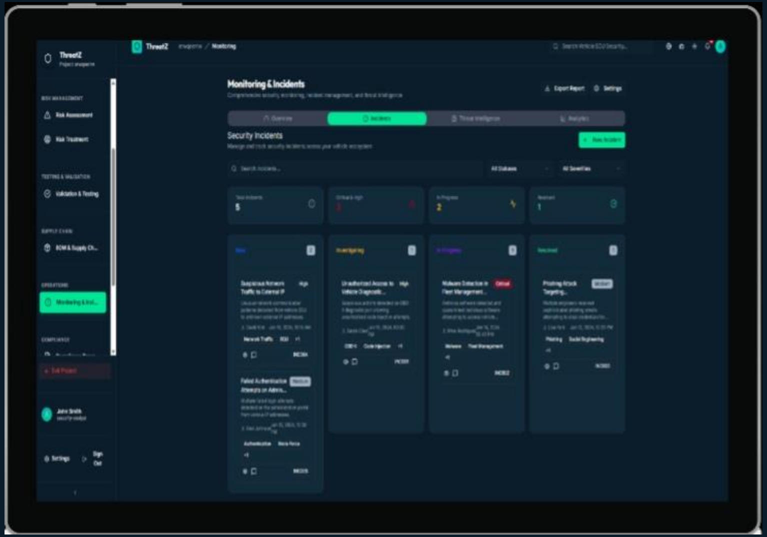
The **Operations Module** of **ThreatZ** is built to meet **ISO 21434 and UNECE R155 standards**, helping OEMs and Tier 1 suppliers manage cybersecurity incidents across the vehicle lifecycle. It focuses on specific ECUs or subsystems and integrates with OEM **VSOCs via APIs** to exchange relevant incident data in real time.

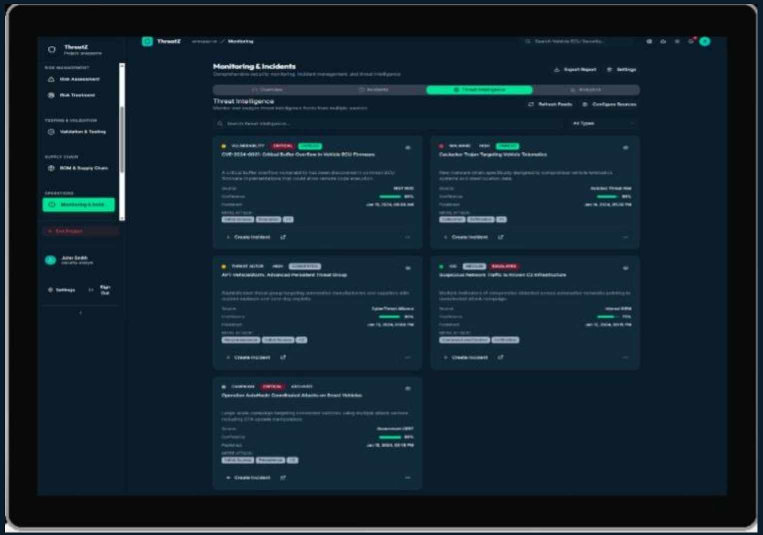
Kanban Incident Management

The incident manager features an intuitive kanban board visualization that transforms incident handling into a streamlined streamlined workflow process. Security teams can instantly view view the status of all security incidents across four key stages. stages.

Multi-Source Threat Intelligence Integration

- **Telegram/Social Media Monitoring**
- **Dark Web Scanning**
- **CERT/CC Advisors**
- **ASRG Feeds**
- **TLP GREEN: Auto-ISAC**

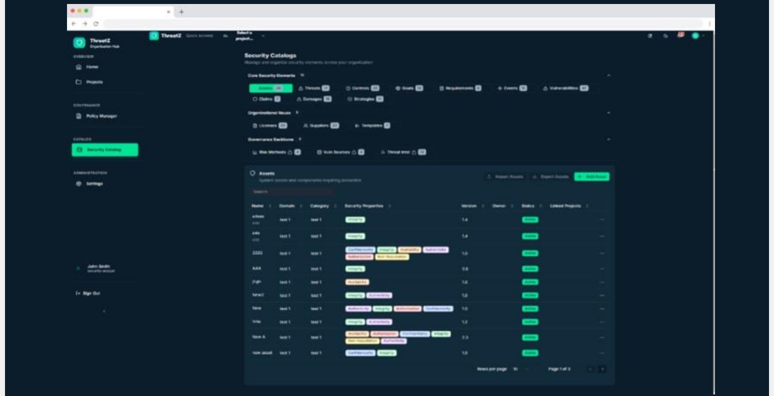




Basic Platform Modules

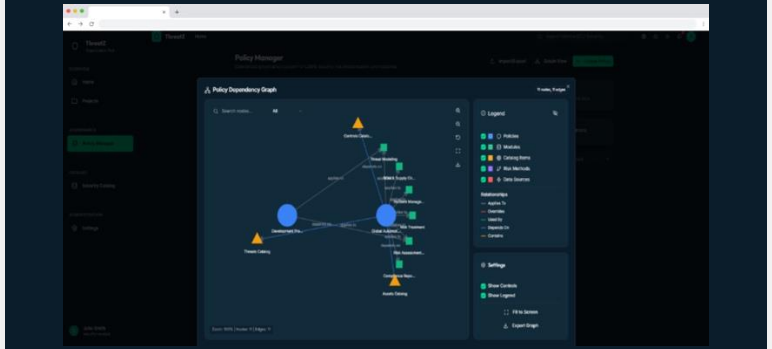
Security Catalog

A comprehensive repository of security assets and components that serve as building blocks for your security architecture. This centralized catalog contains essential elements for threat modeling and risk management.



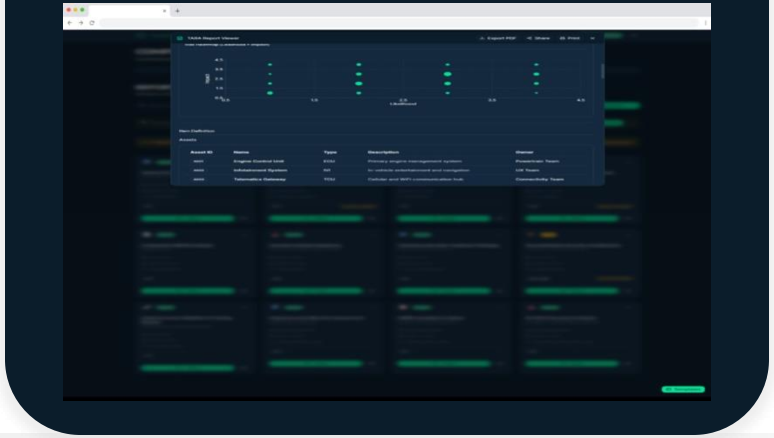
Policy Manager

An Organization's security governance framework through customizable policy controls. This module enables you to establish clear guidelines for allowed and disallowed actions within your Cyber Security Management System (CSMS).



Compliance Reporting

Automatic generation and manage all necessary compliance documentation through a centralized reporting engine. This module streamlines the creation of standardized reports required by regulatory frameworks and internal stakeholders.



Validation & Testing

1

Test Catalog

Import comprehensive test cases from company Test dictionary, manually or using AI-Suggestions

2

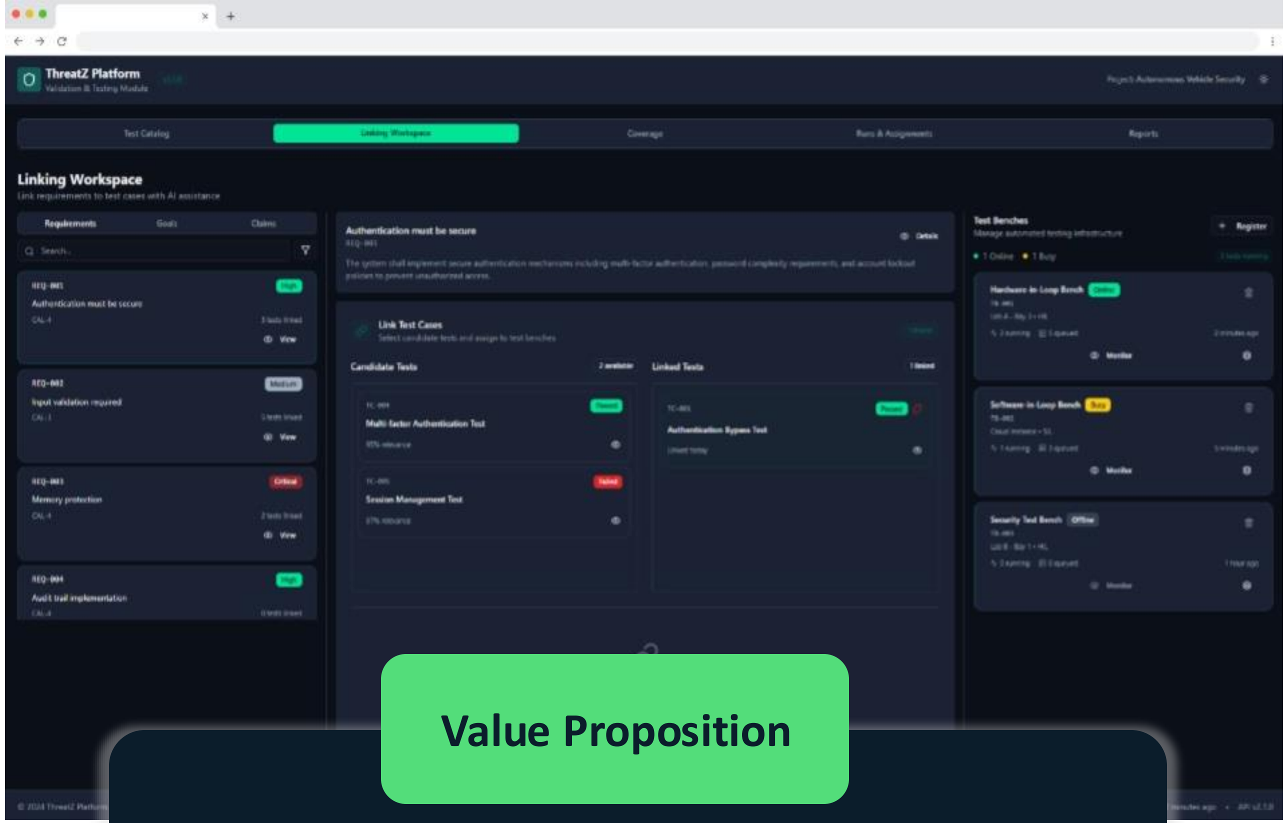
Linking

Map test cases to Requirements, Goals, Claims, and Risks for full traceability

3

Execution

Run test cases by bench configuration, schedule automation, and view real-time results



ThreatZ Platform
Validation & Testing Module

Project: Autonomous Vehicle Security

Linking Workspace
Link requirements to test cases with AI assistance

REQ-001 High
Authentication must be secure
CAL-4 3 tests linked
View

REQ-002 Medium
Input validation required
CAL-3 1 tests linked
View

REQ-003 Critical
Memory protection
CAL-4 2 tests linked
View

REQ-004 High
Audit trail implementation
CAL-4 0 tests linked

Authentication must be secure
REQ-001
The system shall implement secure authentication mechanisms including multi-factor authentication, password complexity requirements, and account lockout policies to prevent unauthorized access.

Link Test Cases
Select candidate tests and assign to test benches

Candidate Tests 2 available

TC-004 Passed
Multi-factor Authentication Test
95% relevance

TC-005 Failed
Session Management Test
87% relevance

Linked Tests 1 linked

TC-001 Passed
Authentication Bypass Test
Linked today

Test Benches
Manage automated testing infrastructure

● 1 Online ● 1 Busy

Hardware-in-Loop Bench Online
2 running 1 queued 2 minutes ago
Monitor

Software-in-Loop Bench Busy
TB-002
1 running 3 queued 5 minutes ago
Monitor

Security Test Bench Offline
1 hour ago
Monitor

Value Proposition

- ✓ Full traceability across Req/Goals/Claims/Risks
- ✓ Live evidence of validation
- ✓ Bridges AI suggestions with manual control
- ✓ Audit-ready outputs for ISO/SAE 21434 and UNECE R155

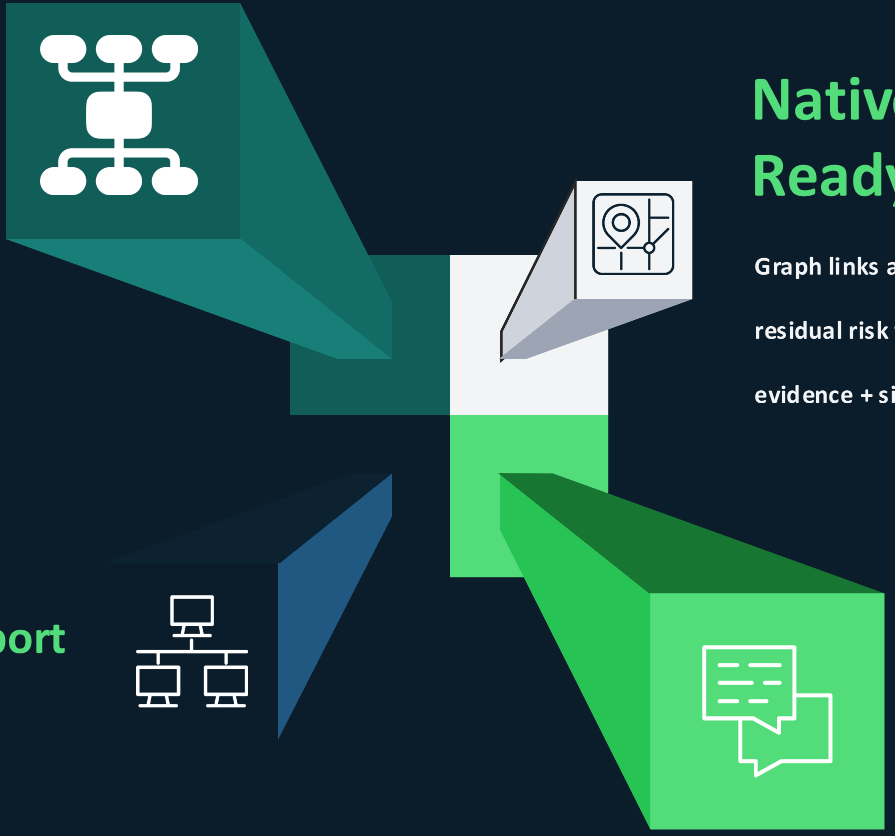
VxLabs

ThreatZ

Key Takeaways

AI & Automation

LLM + graph AI maps SBOM → threats/controls, Suggests policies & tests, and scores assisting the human expert / operator. Impact so CVE→impact is minutes, not days.



Native Risk & Compliance Ready Graph

Graph links assets ⇄ threats ⇄ controls ⇄ tests ⇄ Incidents; computes residual risk for CI gates, and auto-generates ISO 21434 / UN R155 evidence + signed release snapshots.

Interoperability by Default Open APIs + model import/export

Eco-system with bi-directional sync to keep evidence continuous across the lifecycle.

Live Ops Feedback

Incidents, SEVs, and threat intel continuously update likelihoods and back-propagate to assets/requirements; recalculating the risk with each change

Continue the discussion……

new eagle

Karen Boswell

Director – System Safety and Quality

Email: kboswell@neweagle.net

VxLabs

Rex Struble

Head of VxLabs North America

Email: rex.struble@vxlabs.de

INNOVATE FASTER. SCALE SMARTER

theNEST

Learn More About the CCM112 in the NEST

Scan the QR code to access related resources, technical content, and additional insights.

new eagle

RAPTOR®
INNOVATION
SUMMIT 2025