SecureTCU

South Korea-UK Collaborative R&D

SecureTCU Field Demonstration Report

Project Title	Securing TCU for Over-the-Air Updates for Automotive Applications (SecureTCU)
Project Duration	1 December 2022 – 31 October 2026
Consortium Partners	AUTOCRYPT, Beam Connectivity, Korea Automotive Technology Institute, Secure Elements
Test Date	9 June 2026

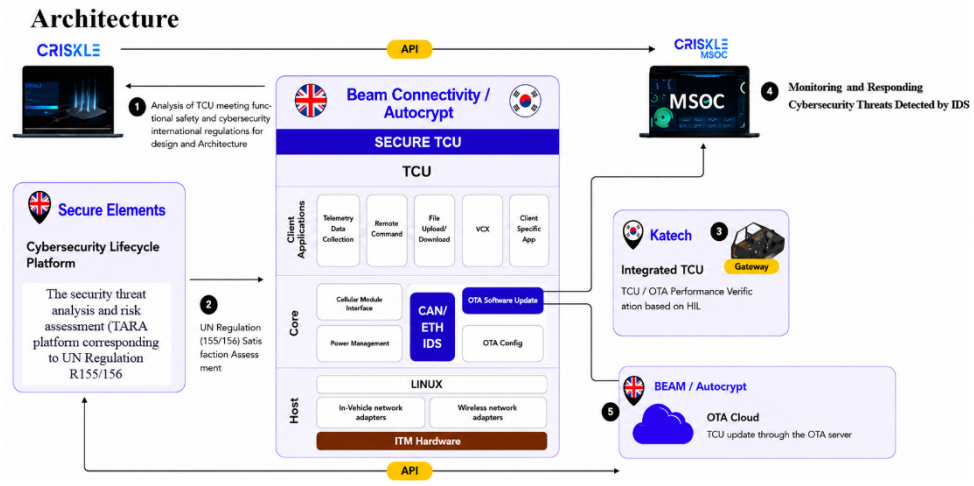
June 2026

Information security classification: PUBLIC

Table of Contents

I. Project Overview 1
II. Test Overview 2
III. Test Result 5

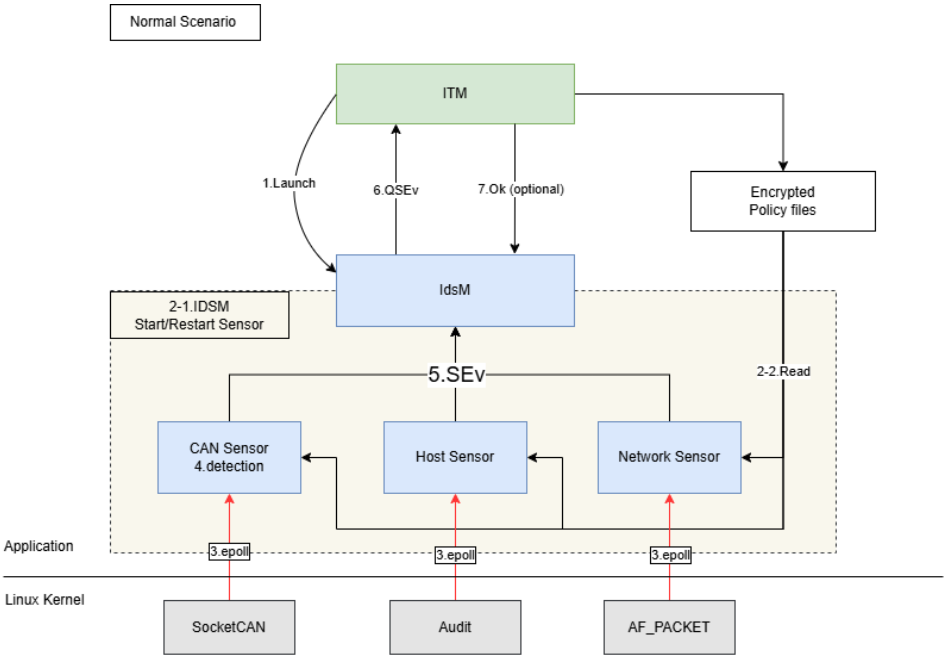
I. Project Overview

Project Title	Securing TCU for Over-the-Air Updates for Automotive Applications (SecureTCU)
Project Duration	1 December 2022 – 31 October 2026
Consortium Partners	AUTOCRYPT, Beam Connectivity, Korea Automotive Technology Institute, Secure Elements
Funding Agencies	Korea Institute for Advancement of Technology (KIAT), Innovate UK
Objective	To develop a cost-effective, integrated cybersecurity solution that enables real-time threat detection and rapid response for connected vehicles, supporting continuous compliance with global automotive cybersecurity regulations and standards, including UNECE R155/R156 and ISO/SAE 21434.
Key Deliverables	In Vehicle: • Next-generation TCU integrated with real-time Intrusion Detection Systems (IDS) • Over-the-air updates of IDS policies to address emerging threats and reduce false positives In Cloud: • Mobility SOC (MSOC) enabling automated incident response, continuous TARA, bidirectional traceability for cybersecurity and Automotive SPICE audits, and timely software and IDS policy updates.
Solution Architecture	

II. Test Overview

Date	9 June 2026
Location	KATECH Proving Ground, Cheonan, Republic of Korea
Environment	Closed proving-ground environment for remotely operated vehicle testing
Objective	The objective of the field demonstration was to verify the end-to-end cybersecurity detection and response capabilities of the SecureTCU solution in a remotely operated vehicle environment.
Main Test System	• **SecureTCU:** An integrated telematics control unit equipped with Host IDS, CAN IDS, and Cellular IDS functions. • **CAN IDS:** Monitors in-vehicle CAN communications and detects abnormal or malicious CAN messages, including unknown IDs, signal-value violations, overflow and underflow conditions, and manipulated vehicle-status data. • **Cellular IDS:** Monitors cellular communication and network activity to detect abnormal traffic, unauthorized access attempts, flooding attacks, and other suspicious external communication events. • **Host IDS:** Monitors the Linux-based TCU host environment and detects unauthorized logins, policy-file tampering, abnormal process activity, and other suspicious system events. • **Remote Vehicle:** A remotely teleoperated test vehicle integrated with the SecureTCU and configured to transmit vehicle-status and security-event data to the RTOC and MSOC platform. • **RTOC:** Monitors the remote vehicle, displays vehicle-status information and cybersecurity warnings, and supports remote control and precautionary response actions during the test. • **CRISKLE MSOC Platform:** Receives, analyses, and manages cybersecurity events generated by the SecureTCU, and supports alert handling, incident response, playbook execution, and ticket creation. • **OTA System:** Delivers software, IDS policy, and configuration updates to the TCU and supports remediation after a cybersecurity event
Equipment	• Remotely teleoperated test vehicle • Integrated SecureTCU prototype • Remote Teleoperation Control Centre (RTOC) • Vector CANoe used by the test operator to inject and manipulate CAN messages • Attacker laptop

Integrated TCU-IDS Architecture



IDS Detection Test Items

- CAN IDS Detection Rules

Attack Type	Description and Example
Unknown ID Attack Detection	Detects transmission of CAN IDs not defined in the DBC (Database CAN) file.
	(Example) Attacker A injects an undefined CAN ID to manipulate the steering angle value.
Signal Space Violation Attack Detection	Detects manipulation of unauthorized bit fields or transmission of signal patterns outside the normal range (e.g., speed, gear, parking status).
	(Example) Attacker B transmits a CAN message with values outside the normally defined signal set range.
Signal Overflow Attack Detection	Detects transmission of abnormal values that exceed the permitted upper limit of a specific signal.
	(Example) Attacker C transmits a CAN message with a value exceeding the signal upper limit, disrupting vehicle operation.

- Cellular IDS Detection Rules

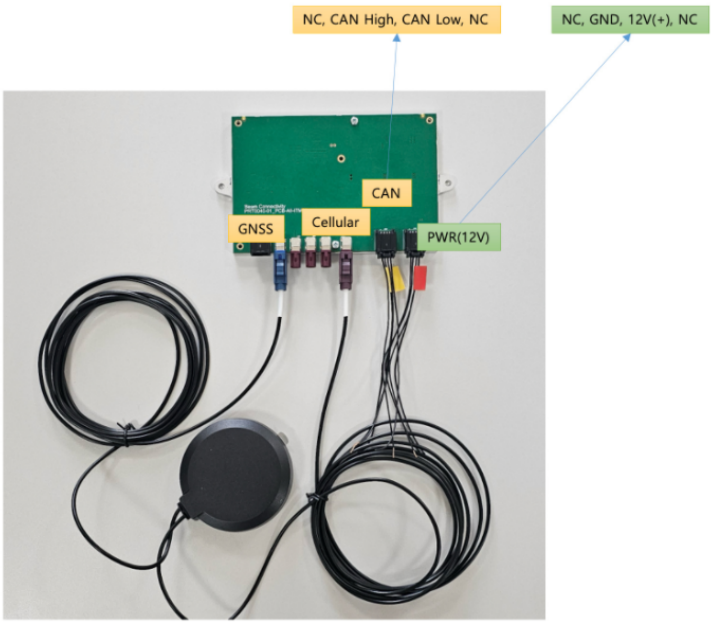
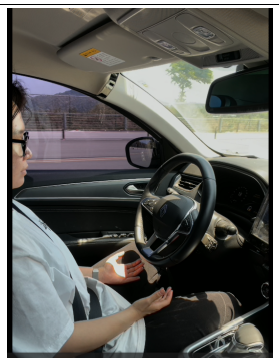
Attack Type	Description and Example
IP/Port Flooding Attack Detection (Layer 3)	Detects attacks that continuously send an excessive number of IP packets to a specific or random port, overloading the TCU network stack.
	(Example) Attacker A uses the RTOC or an external malicious server to send a large volume of packets to the TCU MQTT communication port, sharply increasing the TCU data load.

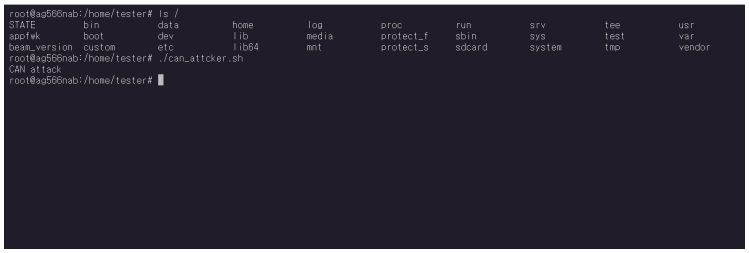
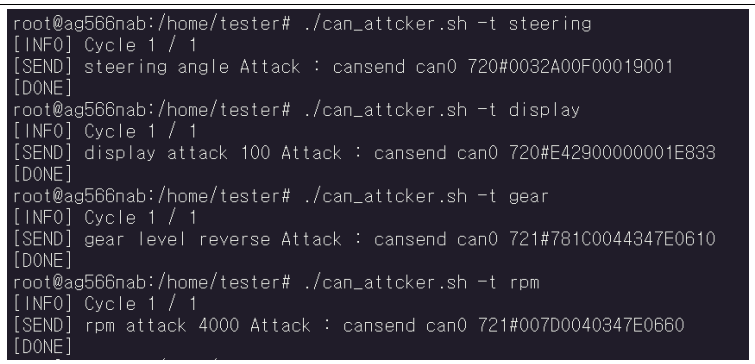
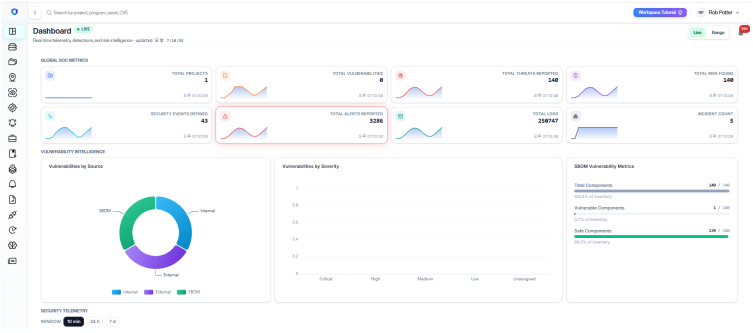
Outbound Error Detection (Layer 3) (IP Spoofing)	Detects attempts to alter normal network traffic into malicious traffic or cause the TCU to connect to an attacker-controlled server (MQTT broker).
	(Example) Attacker B manipulates the MQTT broker address so that the TCU attempts to connect to an attacker MQTT broker instead of the original Beam MQTT Broker (configuration tampering/malicious reconfiguration).

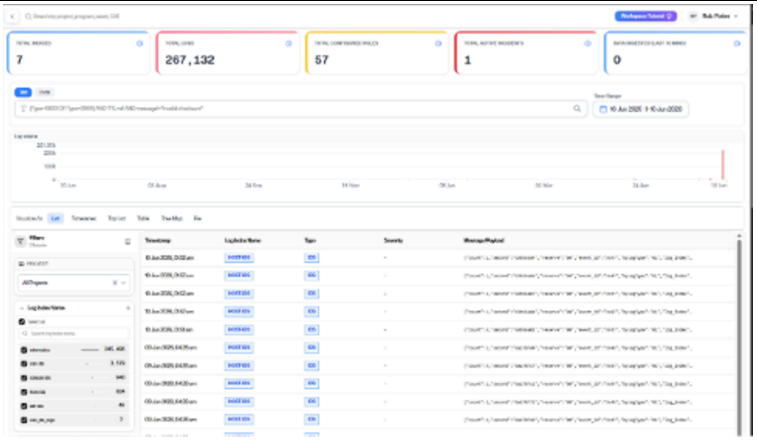
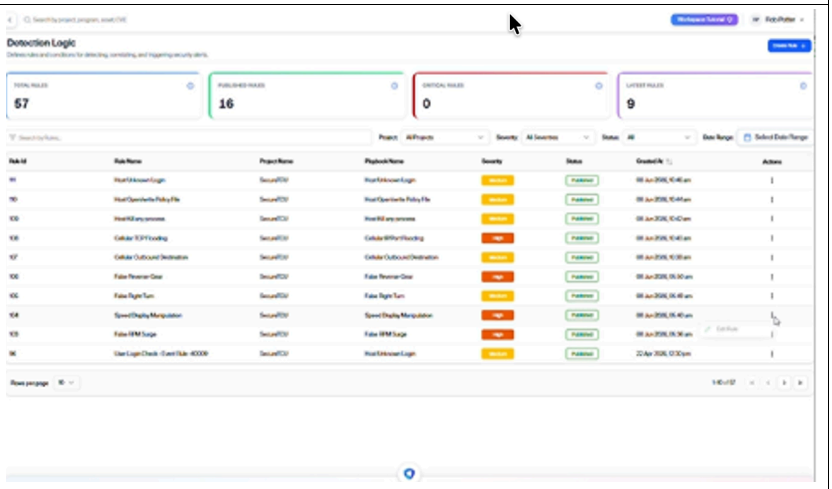
- Host IDS Detection Rules

Attack Type	Description and Example
Unknown Login / Unauthorized System Intrusions Detection	Detects unauthorized or abnormal logins to the TCU based on audit logs.
	If a remote shell opened for debugging (such as SSH/ADB) is left open, Attacker A can use that session to log in to the TCU.
Policy File Tampering Detection	Detects unauthorized access to or modification of the IDS policy file (e.g., open/write actions) to prevent policy tampering attempts.
	After compromising a third-party software provider system, an attacker attempts to overwrite the IDS intrusion policy file in the TCU.
Process Manipulation Detection	Detects abnormal termination (kill) of critical running processes in the host or manipulation of PID values (Process ID Manipulation).
	Attacker C forcibly terminates a specific process or manipulates the PID value of a running process to disrupt normal operation.

III. Test Result

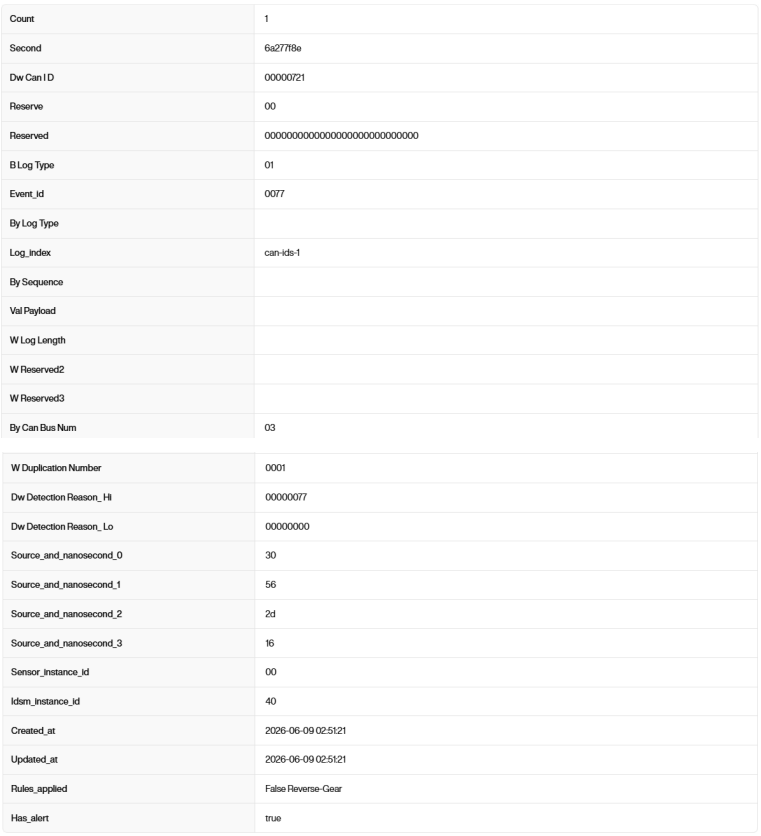
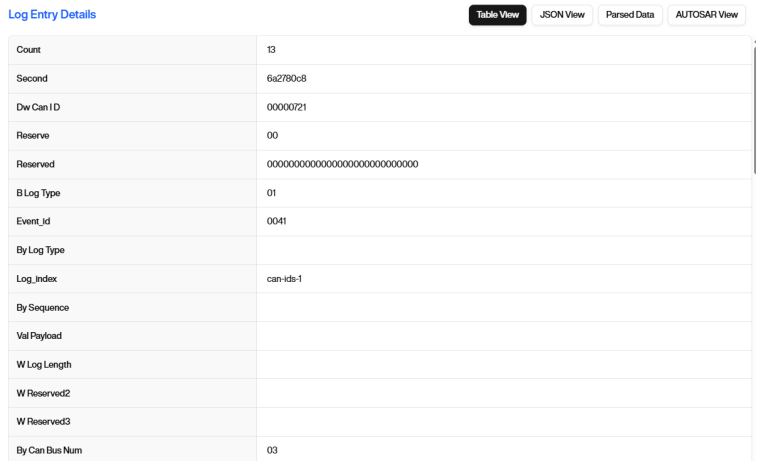
	Test	Result
	Integration and Driving Test of the Remote Vehicle and SecureTCU	 [SecureTCU: Integrated TCU with IDS]
		 [Remote Vehicle]
		 [Remote Vehicle]

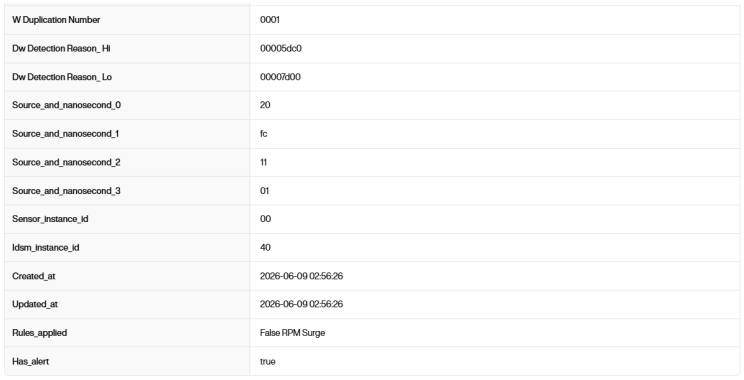
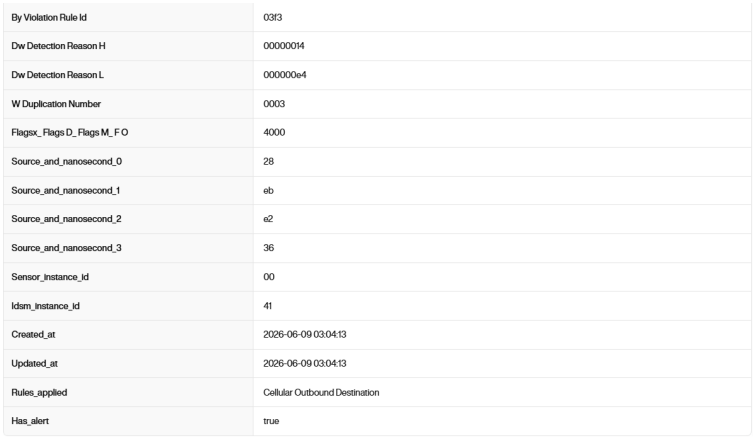
		 [Remote Teleoperation Center (RTOC)]
	The attacker gains remote access to the TCU through an exposed debug port	
	Attack Type: CAN Signal Overflow	
	CRISKLE MSOC Dashboard	

	MSOC SIEM (Security Information and Event Management): Collects, searches, and analyses all security events	
	MSOC Detection Logic	

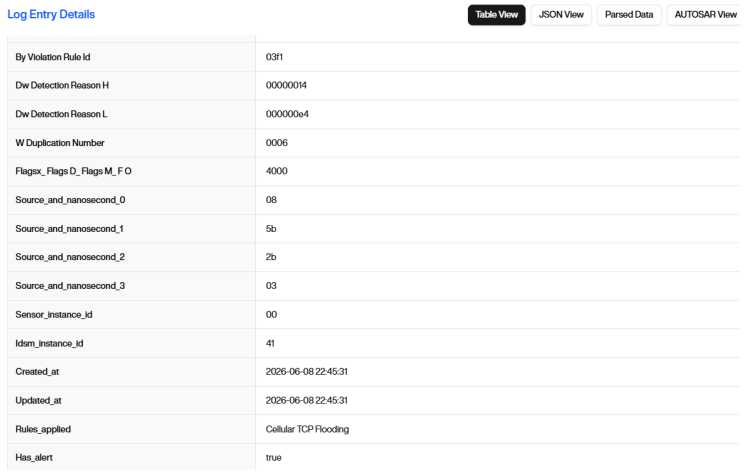
	CAN IDS Detection of a Signal Overflow Attack (Speed Value Exceeding the Upper Limit)	Log Entry Details Table View | JSON View | Parsed Data | AUTOSAR View Count: 2 Second: 6a278210 Dw Can I D: 00000720 Reserve: 00 Reserved: 00000000000000000000000000000000 B Log Type: 01 Event_id: 0041 By Log Type: Log_index: can-ids-1 By Sequence: Val Payload: W Log Length: W Reserved2: W Reserved3: By Can Bus Num: 03 W Duplication Number: 0001 Dw Detection Reason_ Hi: 00000320 Dw Detection Reason_ Lo: 000003e8 Source_and_nanosecond_0: 10 Source_and_nanosecond_1: 12 Source_and_nanosecond_2: 44 Source_and_nanosecond_3: 32 Sensor_Instance_id: 00 Idsm_Instance_id: 40 Created_at: 2026-06-09 03:01:54 Updated_at: 2026-06-09 03:01:54 Rules_applied: Speed Display Manipulation Has_alert: true [Verification of IDS Detection Logs in CRISKLE MSOC for the Signal Overflow Attack and Speed Manipulation]
	Confirmation of the IDS-Detected Signal Overflow Attack and Speed Manipulation in the RTOC, Followed by Appropriate Response Actions, Including Stopping the Vehicle	

	CAN IDS Detection of ENUM Error (Steering Manipulation)	Log Entry Details Table View | JSON View | Parsed Data | AUTOSAR View Count: 25 Second: 6a27821d Dw Can I D: 00000720 Reserve: 00 Reserved: 00000000000000000000000000000000 B Log Type: 01 Event_id: 0079 By Log Type: Log_index: can-ids-1 By Sequence: Val Payload: W Log Length: W Reserved2: W Reserved3: By Can Bus Num: 03 W Duplication Number: 0001 Dw Detection Reason_ Hi: 00000079 Dw Detection Reason_ Lo: 00000000 Source_and_nanosecond_0: 18 Source_and_nanosecond_1: 72 Source_and_nanosecond_2: 46 Source_and_nanosecond_3: 26 Sensor_instance_id: 00 Idsm_instance_id: 40 Created_at: 2026-06-09 03:02:12 Updated_at: 2026-06-09 03:02:12 Rules_applied: False Right-Turn Has_alert: true [Verification of IDS Detection Logs in CRISKLE MSOC for ENUM Error and Steering Manipulation]
	Confirmation of the IDS-Detected ENUM Error and Steering Manipulation in the RTOC, Followed by Appropriate Response Actions, Including Stopping the Vehicle.	

	CAN IDS Detection of Gear Manipulation	 [Verification of IDS Detection Logs in CRISKLE MSOC for Gear Manipulation]
	Confirmation of the IDS-Detected Gear Manipulation in the RTOC, Followed by Appropriate Response Actions, Including Stopping the Vehicle	
	CAN IDS Detection of a Signal Overflow Attack (RPM Signal Value Exceeding the Upper Limit)	

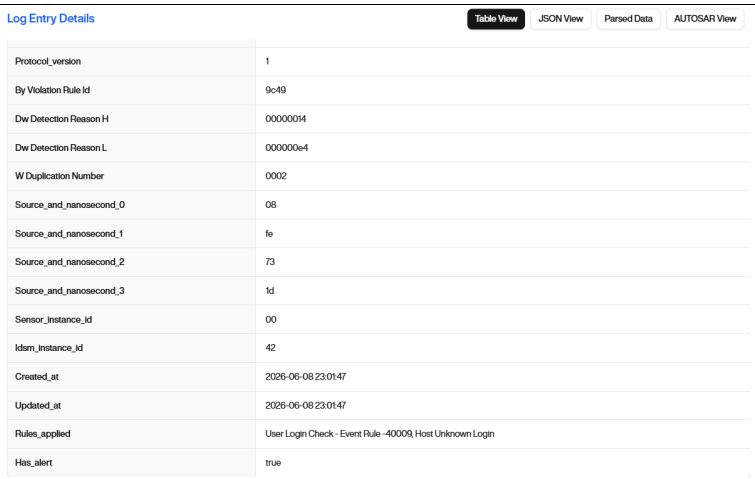
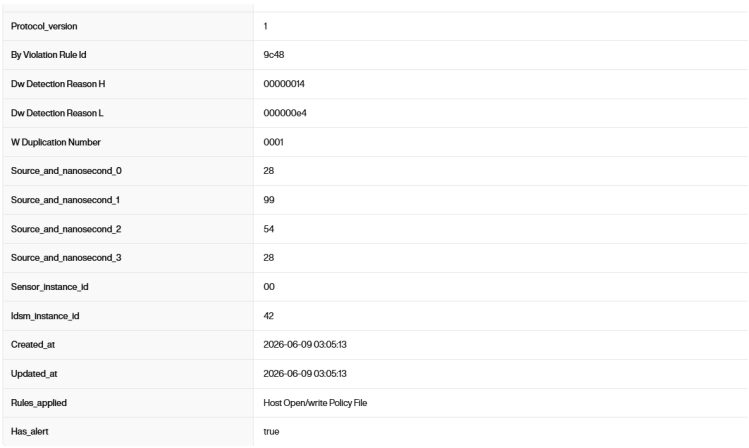
		 [Verification of IDS Detection Logs in CRISKLE MSOC for the Signal Overflow Attack and RPM Manipulation]
	Cellular IDS Detection of an Outbound Layer 3 Error	  [Verification of Cellular IDS Detection Logs in CRISKLE MSOC for an Outbound Layer 3 Error]

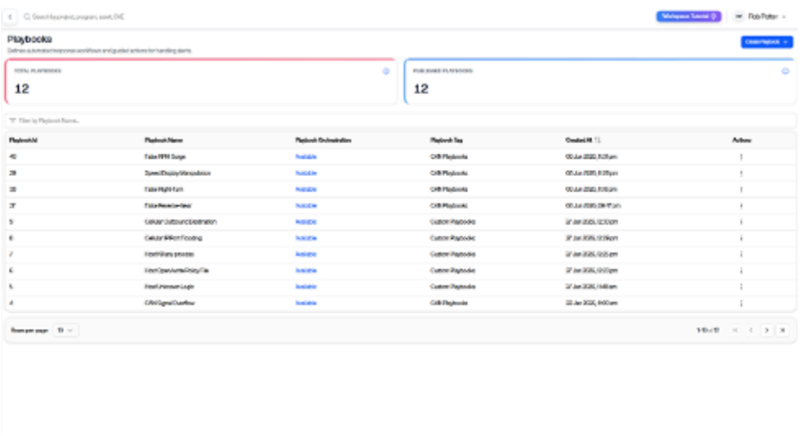
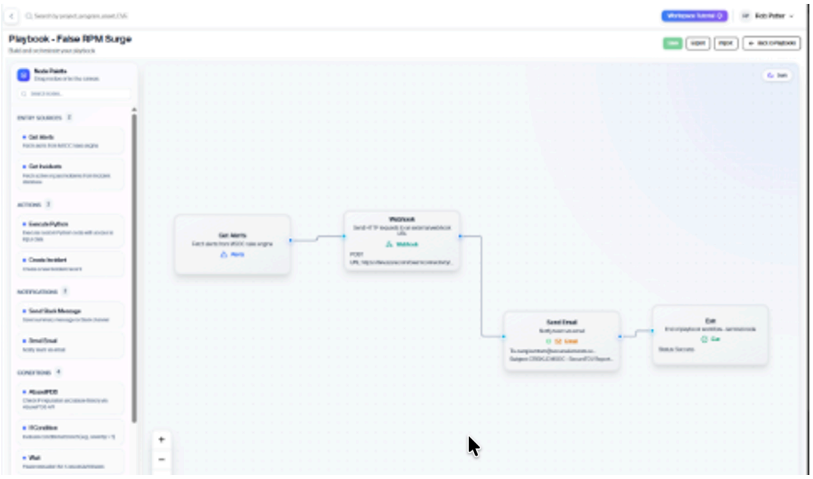
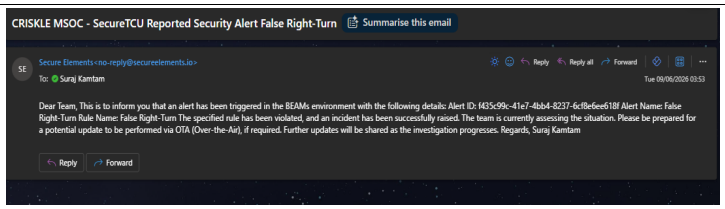
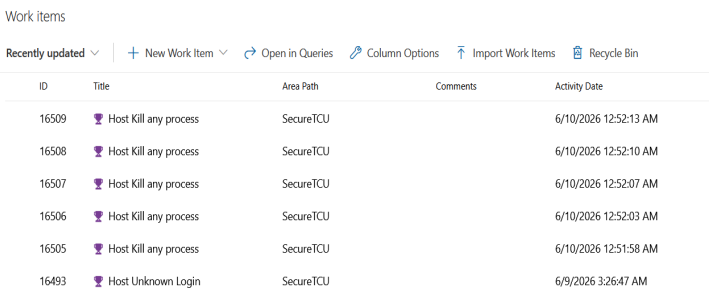

```
rules_applied: [
  {
    "rule_id": 107,
    "rule_name": "Cellular Outbound Destination",
    "alert_id": 3876,
    "alert_uuid": "44b6365a-590b-47ce-a5e8-61ae35d4fbb9",
    "alert_created_at": "2026-06-09 03:04:13",
    "alert_ttp": [
      {
        "config_type": "AUTOMOTIVE_ISAC",
        "tactic": "Manipulate Environment",
        "technique": "3"
      }
    ],
    "fields_applied_on": [
      {
        "field": "byViolationRuleId",
        "operator": "equal",
        "expected_value": "03f3",
        "actual_value": "03f3"
      }
    ],
    "severity": "medium"
  }
]
```

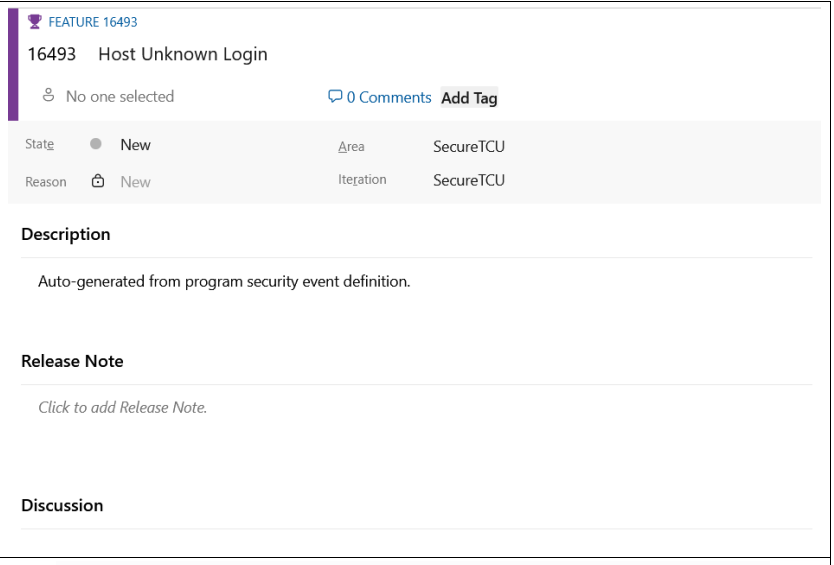
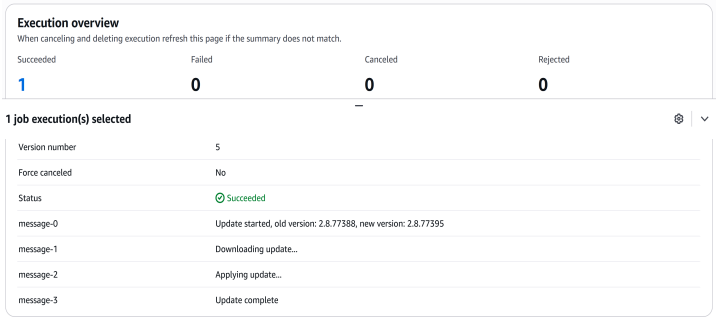
	Cellular IDS Detection of Layer 3 IP/Port-Based Flooding Attacks	rules_applied: [{ "rule_id": 108, "rule_name": "Cellular TCP Flooding", "alert_id": 3435, "alert_uuid": "b3b57ad3-380a-4db2-93df-7484576316ec", "alert_created_at": "2026-06-08 22:45:31", "alert_ttp": [{ "config_type": "AUTOMOTIVE_ISAC", "tactic": "Manipulate Environment", "technique": "2" }], "fields_applied_on": [{ "field": "byViolationRuleId", "operator": "equal", "expected_value": "03f1", "actual_value": "03f1" }], "severity": "high" }]  Log Entry Details Table View JSON View Parsed Data AUTOSAR View By Violation Rule Id: 03f1 Dw Detection Reason H: 00000014 Dw Detection Reason L: 000000e4 W Duplication Number: 0006 Flagsx_Flags D_Flags M_F O: 4000 Source_and_nanosecond_0: 08 Source_and_nanosecond_1: 5b Source_and_nanosecond_2: 2b Source_and_nanosecond_3: 03 Sensor_Instance_Id: 00 Idsm_instance_id: 41 Created_at: 2026-06-08 22:45:31 Updated_at: 2026-06-08 22:45:31 Rules_applied: Cellular TCP Flooding Has_alert: true [Verification of Cellular IDS Detection Logs in CRISKLE MSOC for Layer 3 IP/Port-Based Flooding Attacks]

	Host IDS Detection of Process Manipulation	rules_applied: [{ "rule_id": 109, "rule_name": "Host Kill any process", "alert_id": 3464, "alert_uuid": "4085df92-8804-40b8-b470-42700e3c6498", "alert_created_at": "2026-06-08 22:51:40", "alert_ttp": [{ "config_type": "MITRE_EMBEDDED", "tactic": "Application software", "technique": "71" }], "fields_applied_on": [{ "field": "byViolationRuleId", "operator": "equal", "expected_value": "9c47", "actual_value": "9c47" }], "severity": "medium" }] Log Entry Details Table View | JSON View | Parsed Data | AUTOSAR View Protocol_version: 1 By Violation Rule Id: 9c47 Dw Detection Reason H: 00000014 Dw Detection Reason L: 000000e4 W Duplication Number: 0001 Source_and_nanosecond_0: 18 Source_and_nanosecond_1: 30 Source_and_nanosecond_2: 82 Source_and_nanosecond_3: 09 Sensor_instance_id: 00 Idsm_instance_id: 42 Created_at: 2026-06-08 22:51:40 Updated_at: 2026-06-08 22:51:40 Rules_applied: Host Kill any process Has_alert: true [Verification of Host IDS Detection Logs in CRISKLE MSOC for Process Manipulation]

	Host IDS Detection of Unknown Login Attempts and Unauthorized System Intrusions	rules_applied: [
		{
		"rule_id": 96,
		"rule_name": "User Login Check - Event Rule -40009",
		"alert_id": 3469,
		"alert_uuid": "be591416-fbb7-4110-a59d-fbb8bc67cbe4",
		"alert_created_at": "2026-06-08 23:01:47",
		"alert_ttp": [
		{
		"config_type": "MITRE_ATTACK",
		"tactic": "Credential Access",
		"technique": "Password Cracking"
		}
		],
		"fields_applied_on": [
		{
		"field": "byViolationRuleId",
		"operator": "equal",
		"expected_value": "9c49",
		"actual_value": "9c49"
		}
		],
		"severity": "medium"
		},
		{
		{
		"rule_id": 111,
		"rule_name": "Host Unknown Login",
		"alert_id": 3470,
		"alert_uuid": "9624e224-23b6-492a-b78f-76432590848b",
		"alert_created_at": "2026-06-08 23:01:47",
		"alert_ttp": [
		{
		"config_type": "MITRE_EMBEDDED",
		"tactic": "Networking",
		"technique": "76"
		}
		],
		"fields_applied_on": [
		{
		"field": "byViolationRuleId",
		"operator": "equal",
		"expected_value": "9c49",
		"actual_value": "9c49"
		}
		],
		"severity": "medium"
		}
		]

		Log Entry Details Table View | JSON View | Parsed Data | AUTOSAR View  [Verification of Host IDS Detection Logs in CRISKLE MSOC for Unknown Login Attempts and Unauthorized System Intrusions]
	Host IDS Detection of Policy File Tampering	 Log Entry Details Table View | JSON View | Parsed Data | AUTOSAR View  [Verification of Host IDS Detection Logs in CRISKLE MSOC for Policy

		File Tampering]
	MSOC Playbooks: CRISKLE MSOC executes predefined playbooks to automatically trigger appropriate response actions based on the event type and risk level.	
	MSOC Playbook Orchestration	 [Playbook for retrieving alerts, transmitting event information through a webhook, notifying responsible personnel by email, and completing the response workflow upon detection of a security event]
	MSOC Email Notification of ticket Creation	
	Tickets Created for developers	

	Details of ticket	
	Success full OTA issued to resolve ticket	
	Attacker login failed	