black hat ARSENAL

Attack Knowledge Base for Automotive

ATHENA: Advanced THreat knowlEdge-base for Networked Automotive

Tien-Chih Lin@CyCraft

Tien-Chih Lin(Dange)

- Senior Cyber Security Researcher of CyCraft
- Focus on Car Security, Cloud Security
- Certified Automotive Cyber-Security Professional by SGS
- HITCON Speaker
- dange.lin@cycarrier.com

CYCRAFT

black hat
USA 2023
AUGUST 9-10, 2023
BRIEFINGS

IR-on-MAN: InterpRetable Incident Inspector Based ON Large-Scale Language Model and Association miNing

Sian-Yao Huang, Cheng-Lin Yang, Chung-Kuan Chen

CYCRAFT

#BHUSA @BlackHatEvents

Large Language Models

black hat
USA 2020
AUGUST 5-6, 2020
BRIEFINGS

Operation Chimera - APT Operation Targets Semiconductor Vendors

by Chung-Kuan Chen + Shang-De Jiang + Inndy Lin

#BHUSA @BLACKHATEVENTS

APT Investigation

SANS
BLUE TEAM
SUMMIT & TRAINING

Don’t Relay Me: Empirically Diagnose Privilege Escalation via Active Directory Account Sighting

Shand-De “John” Jiang
CyCraft Technology

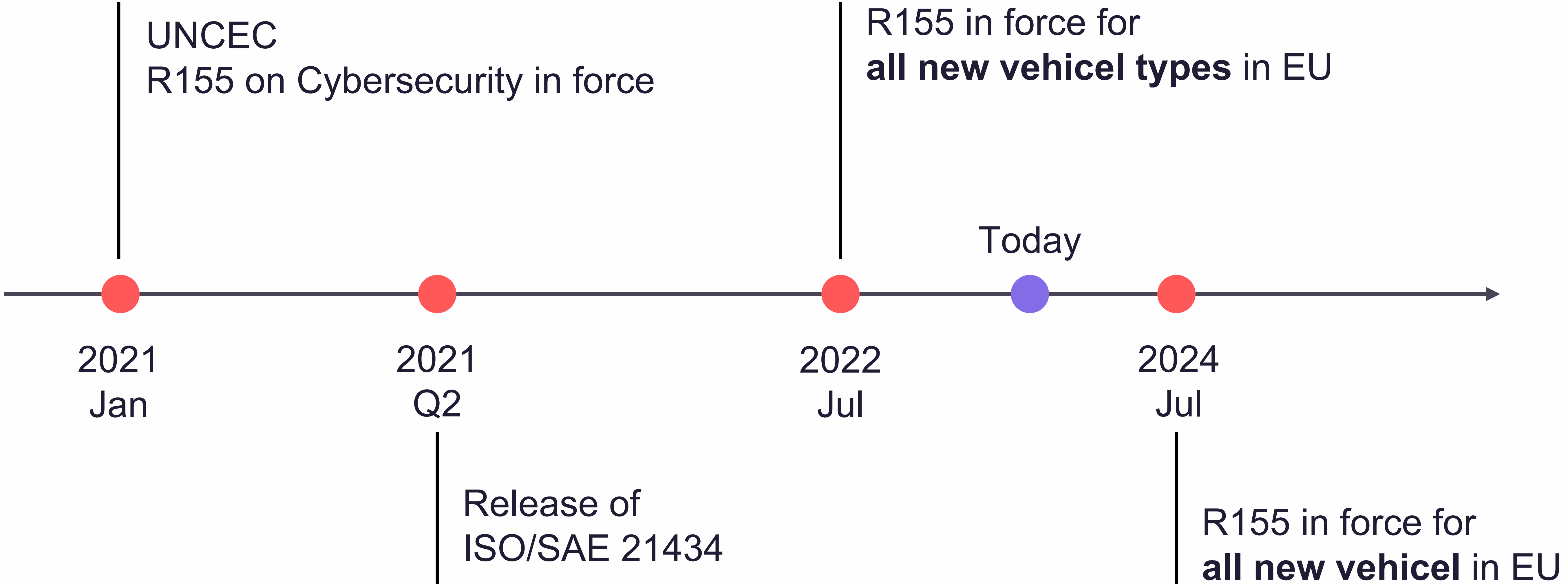
Gary Sun
CyCraft Technology

Identity base Attack Path Analysis

Outline

- Background: Regulation and Standard
- Challenges and Difficulties: Consulting Case Study
- ATHENA: Advanced THreat knowlEdge-base for Networked Automotive
- Case Studies: Integrate ATHENA with ISO/SAE 21434
- Conclusion

Background



UNCEC
R155 on Cybersecurity in force

2021
Jan

2021
Q2

Release of
ISO/SAE 21434

R155 in force for
all new vehicel types in EU

2022
Jul

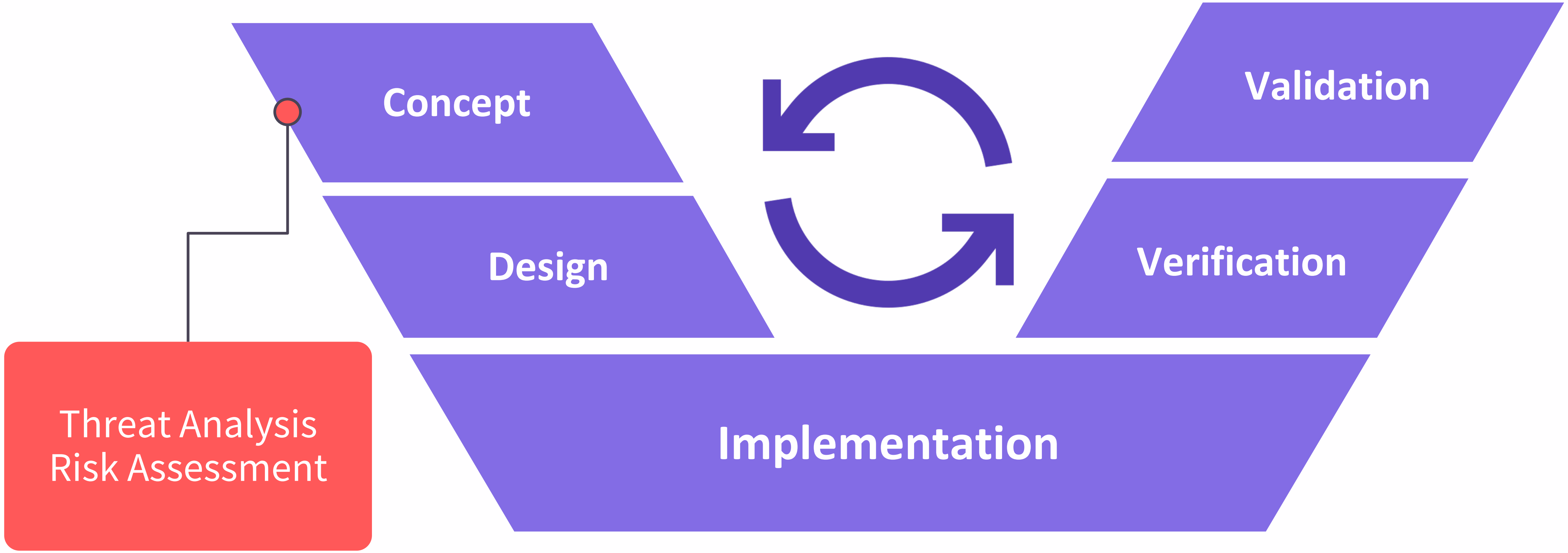
Today

2024
Jul

R155 in force for
all new vehicel in EU

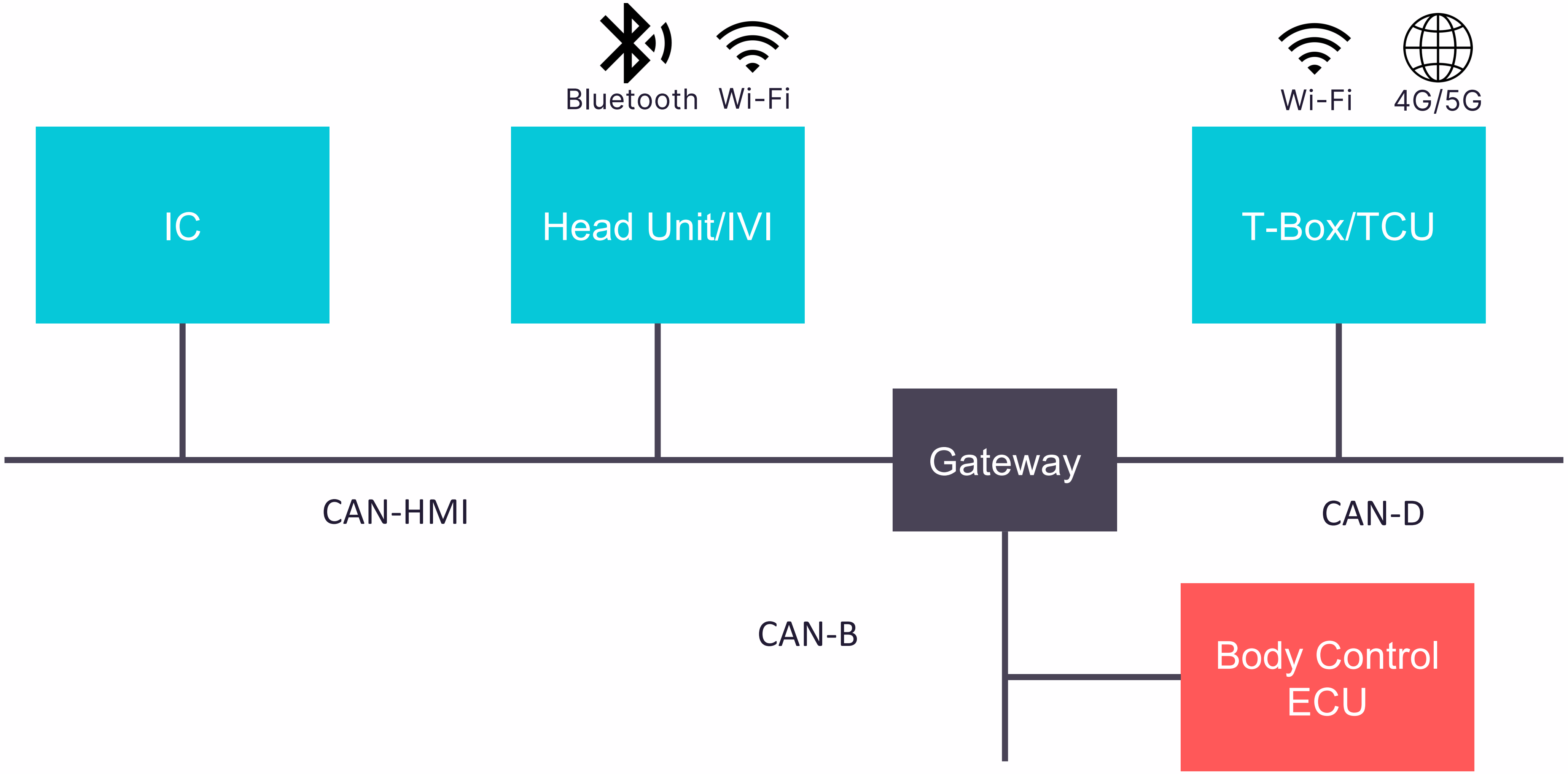
https://www.continental.com/en/press/fairs-events/continental-commercial-vehicle-days/cybersecurity/

ISO/SAE 21434 Lifecycle



Challenges and Difficulties

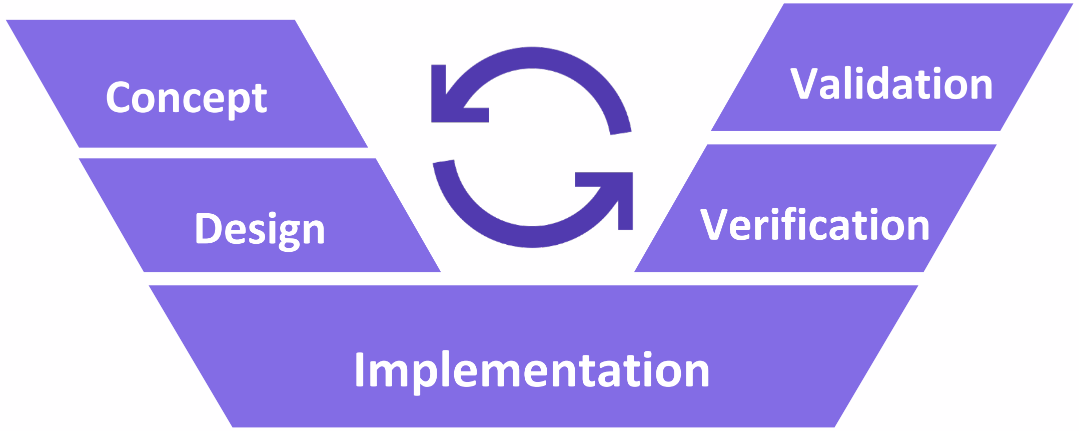
Consulting Case Study



Before Consulting

- Avoid Body Control ECU from being attacked.

Spoofing Attack: Forging Functional Signals



Concept

Design

Implementation

Verification

Validation

Implement ECU Protection Solution.

- Control Flow Integrity
- Exploit Protection

It detects abnormal program flows but not Spoofing Attacks.

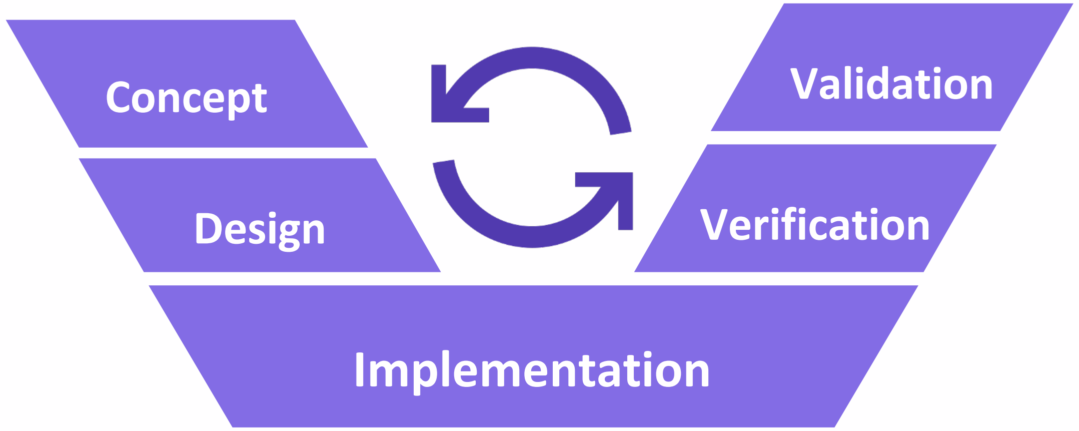
Intrusion from peripheral devices.

- T-Box
- Head Unit

- Full Vehicle Penetration Testing (Different Teams)

Difficulties: Information Inconsistence

- Lack of global view on attack techniques.
- Unknown the root cause of attack techniques.



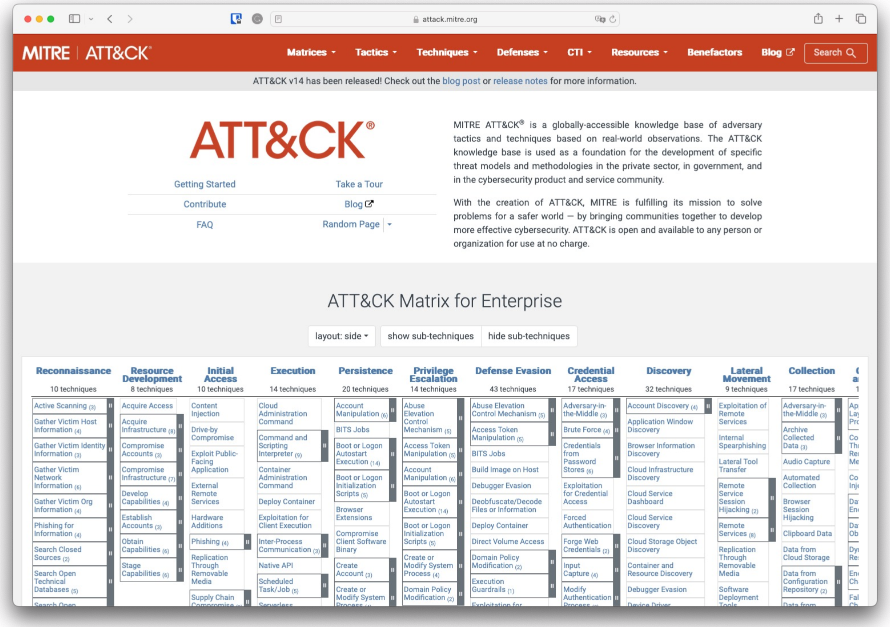
- Lack of systematic and comprehensive validation program

TARA results don't effectively transform to mitigation/detection solutions.

- Misunderstanding mitigate/detect coverage of solution.

TARA and implementation results don't effectively transform to validation program

ATHENA: Advanced THreat knowlEdge-base for Networked Automotive



attack.mitre.org

ATT&CK v14 has been released! Check out the blog post or release notes for more information.

ATT&CK®

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

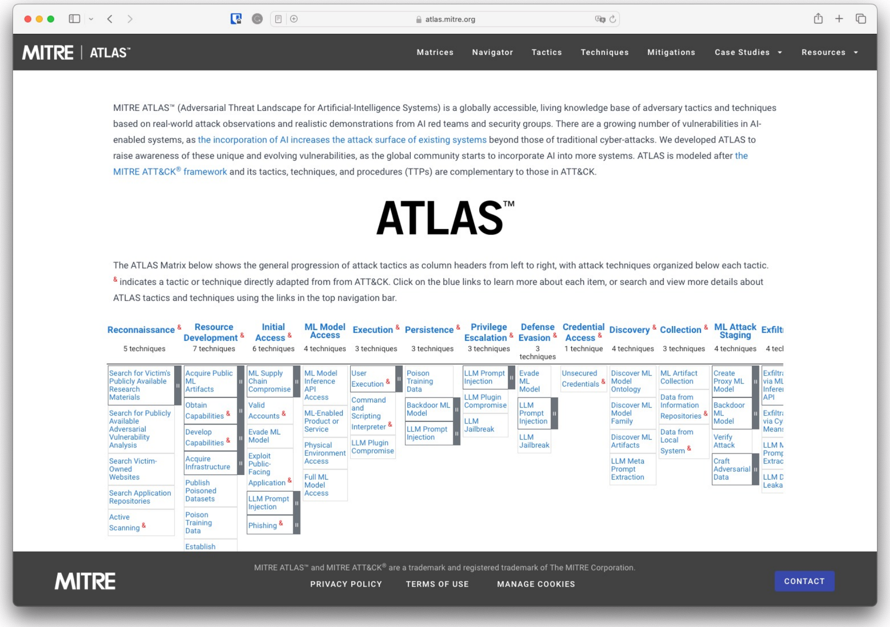
With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK Matrix for Enterprise

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise	Scheduled Task/Job (5)	Create or Modify System Process		Direct Volume Access	Modify Authentication Process	Container and Resource Discovery		Data from Configuration Repository (2)
						Domain Policy Modification (2)		Debugger Evasion		
						Execution Guardrails (1)				

Enterprise

https://attack.mitre.org



atlas.mitre.org

MITRE ATLAS™ (Adversarial Threat Landscape for Artificial-Intelligence Systems) is a globally accessible, living knowledge base of adversary tactics and techniques based on real-world attack observations and realistic demonstrations from AI red teams and security groups. There are a growing number of vulnerabilities in AI-enabled systems, as the incorporation of AI increases the attack surface of existing systems beyond those of traditional cyber-attacks. We developed ATLAS to raise awareness of these unique and evolving vulnerabilities, as the global community starts to incorporate AI into more systems. ATLAS is modeled after the MITRE ATT&CK® framework and its tactics, techniques, and procedures (TTPs) are complementary to those in ATT&CK.

ATLAS™

The ATLAS Matrix below shows the general progression of attack tactics as column headers from left to right, with attack techniques organized below each tactic. & indicates a tactic or technique directly adapted from from ATT&CK. Click on the blue links to learn more about each item, or search and view more details about ATLAS tactics and techniques using the links in the top navigation bar.

Reconnaissance & 5 techniques	Resource Development & 7 techniques	Initial Access & 6 techniques	ML Model Access 4 techniques	Execution & 3 techniques	Persistence & 3 techniques	Privilege Escalation & 3 techniques	Defense Evasion & 3 techniques	Credential Access & 1 technique	Discovery & 4 techniques	Collection & 3 techniques	ML Attack Staging 4 techniques
Search for Victim's Publicly Available Research Materials	Acquire Public ML Artifacts	ML Supply Chain Compromise	ML Model Inference API Access	User Execution &	Poison Training Data	LLM Prompt Injection	Evade ML Model	Unsecured Credentials &	Discover ML Model Ontology	ML Artifact Collection	Create Proxy ML Model
Search for Publicly Available Adversarial Vulnerability Analysis	Obtain Capabilities &	Valid Accounts &	ML-Enabled Product or Service	Command and Scripting Interpreter &	Backdoor ML Model	LLM Plugin Compromise	LLM Prompt Injection		Discover ML Model Family	Data from Information Repositories &	Backdoor ML Model
Search Victim-Owned Websites	Develop Capabilities &	Evade ML Model	Physical Environment Access	LLM Plugin Compromise	LLM Prompt Injection	LLM Jailbreak	LLM Jailbreak		Discover ML Artifacts	Data from Local System &	Verify Attack
Search Application Repositories	Acquire Infrastructure	Exploit Public-Facing Application &	Full ML Model Access						LLM Meta Prompt Extraction		Craft Adversarial Data
Active Scanning &	Publish Poisoned Datasets	LLM Prompt Injection									
	Poison Training Data	Phishing &									
	Establish										

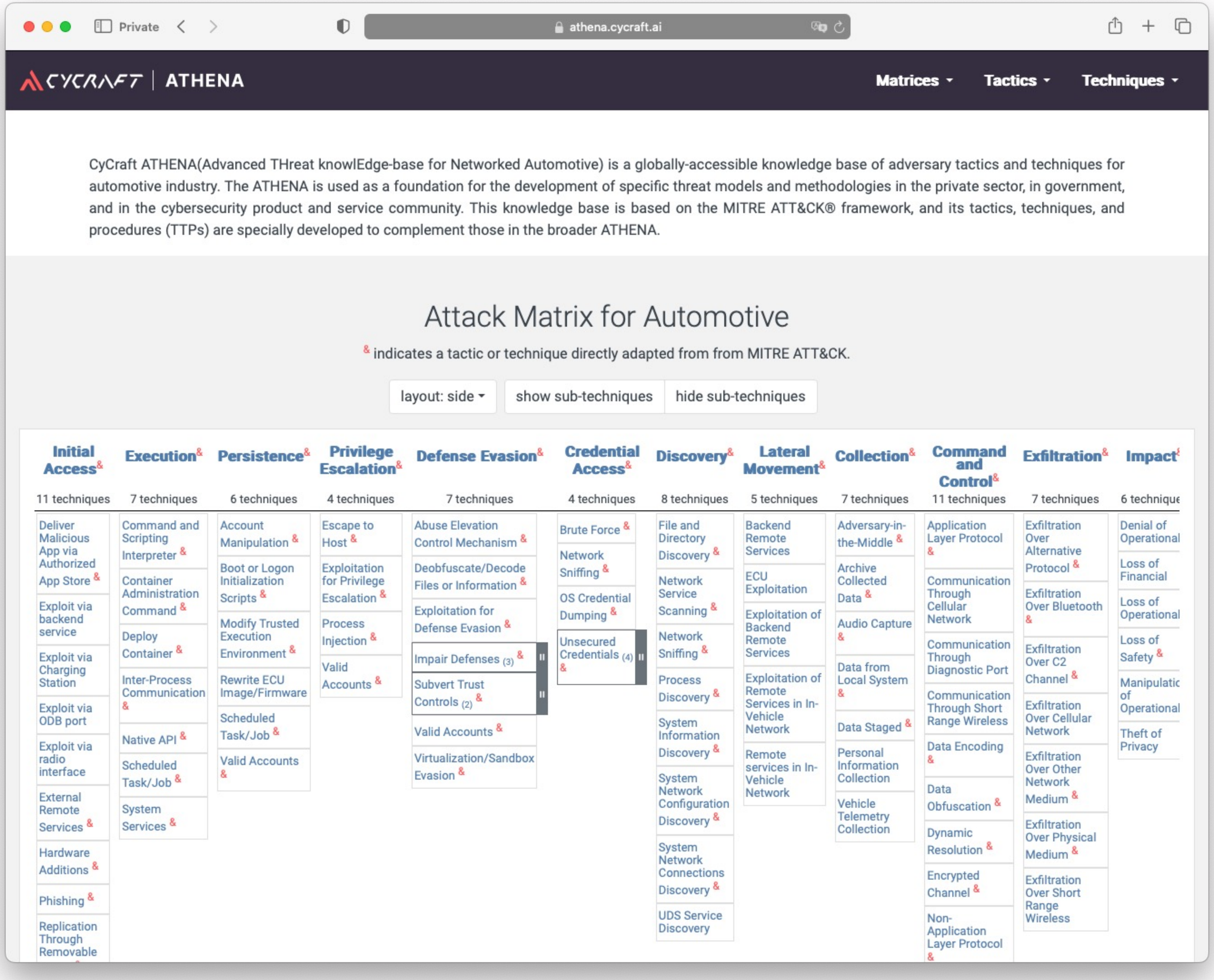
MITRE ATLAS™ and MITRE ATT&CK® are a trademark and registered trademark of The MITRE Corporation.

AI

https://atlas.mitre.org

?

Automotive



CyCraft ATHENA(Advanced THreat knowlEdge-base for Networked Automotive) is a globally-accessible knowledge base of adversary tactics and techniques for automotive industry. The ATHENA is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. This knowledge base is based on the MITRE ATT&CK® framework, and its tactics, techniques, and procedures (TTPs) are specially developed to complement those in the broader ATHENA.

Attack Matrix for Automotive

& indicates a tactic or technique directly adapted from from MITRE ATT&CK.

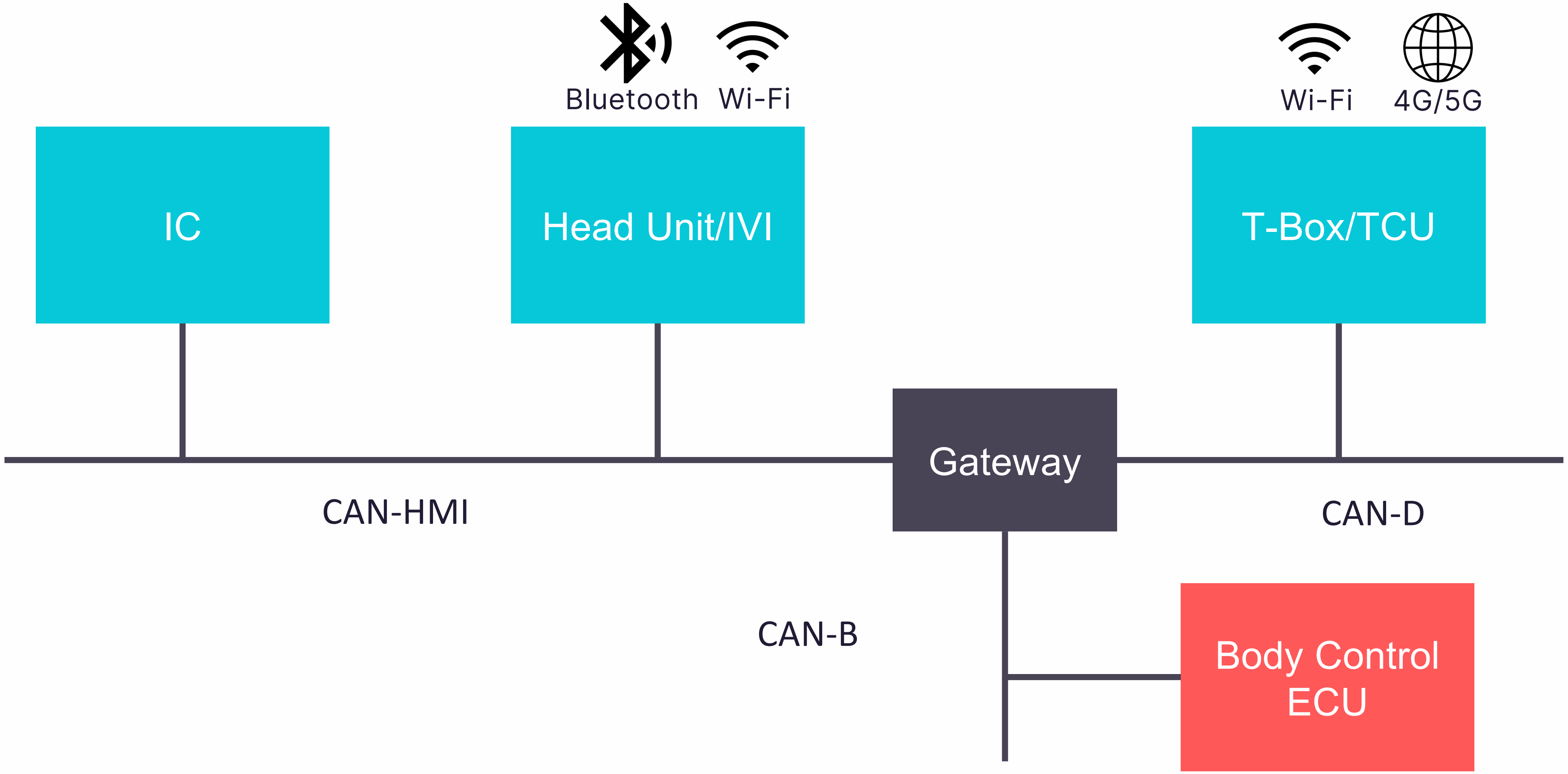
Initial Access&	Execution&	Persistence&	Privilege Escalation&	Defense Evasion&	Credential Access&	Discovery&	Lateral Movement&	Collection&	Command and Control&	Exfiltration&	Impact&
11 techniques	7 techniques	6 techniques	4 techniques	7 techniques	4 techniques	8 techniques	5 techniques	7 techniques	11 techniques	7 techniques	6 technique
Deliver Malicious App via Authorized App Store &	Command and Scripting Interpreter &	Account Manipulation &	Escape to Host &	Abuse Elevation Control Mechanism &	Brute Force &	File and Directory Discovery &	Backend Remote Services	Adversary-in-the-Middle &	Application Layer Protocol &	Exfiltration Over Alternative Protocol &	Denial of Operational
Exploit via backend service	Container Administration Command &	Boot or Logon Initialization Scripts &	Exploitation for Privilege Escalation &	Deobfuscate/Decode Files or Information &	Network Sniffing &	Network Service Scanning &	ECU Exploitation	Archive Collected Data &	Communication Through Cellular Network	Exfiltration Over Bluetooth &	Loss of Financial
Exploit via Charging Station	Deploy Container &	Modify Trusted Execution Environment &	Process Injection &	Exploitation for Defense Evasion &	OS Credential Dumping &	Network Sniffing &	Exploitation of Backend Remote Services	Audio Capture &	Communication Through Diagnostic Port	Exfiltration Over C2 Channel &	Loss of Operational
Exploit via ODB port	Inter-Process Communication &	Rewrite ECU Image/Firmware	Valid Accounts &	Impair Defenses (3) &	Unsecured Credentials (4) &	Process Discovery &	Exploitation of Remote Services in In-Vehicle Network	Data from Local System &	Communication Through Short Range Wireless	Exfiltration Over Cellular Network	Loss of Safety &
Exploit via radio interface	Native API &	Scheduled Task/Job &		Subvert Trust Controls (2) &		System Information Discovery &	Remote services in In-Vehicle Network	Data Staged &	Data Encoding &	Exfiltration Over Other Network Medium &	Manipulatic of Operational
External Remote Services &	Scheduled Task/Job &	Valid Accounts &		Valid Accounts &		System Network Configuration Discovery &		Personal Information Collection	Data Obfuscation &	Exfiltration Over Physical Medium &	Theft of Privacy
Hardware Additions &	System Services &			Virtualization/Sandbox Evasion &		System Network Connections Discovery &		Vehicle Telemetry Collection	Dynamic Resolution &	Exfiltration Over Short Range Wireless	
Phishing &						UDS Service Discovery			Encrypted Channel &		
Replication Through Removable									Non-Application Layer Protocol &		

Roadmap

- **Initial release**
  - Basic tactics and techniques
- Future update
  - Add real-world case study for each techniques
  - Add detection/mitigation for each techniques
  - Add UNCEC WP.29 R155 Annex 5 mapping
  - Add tactics related to autonomous and roadside unit

Case Studies: Integrate ATHENA with ISO/SAE 21434

Back to Consulting Case Study



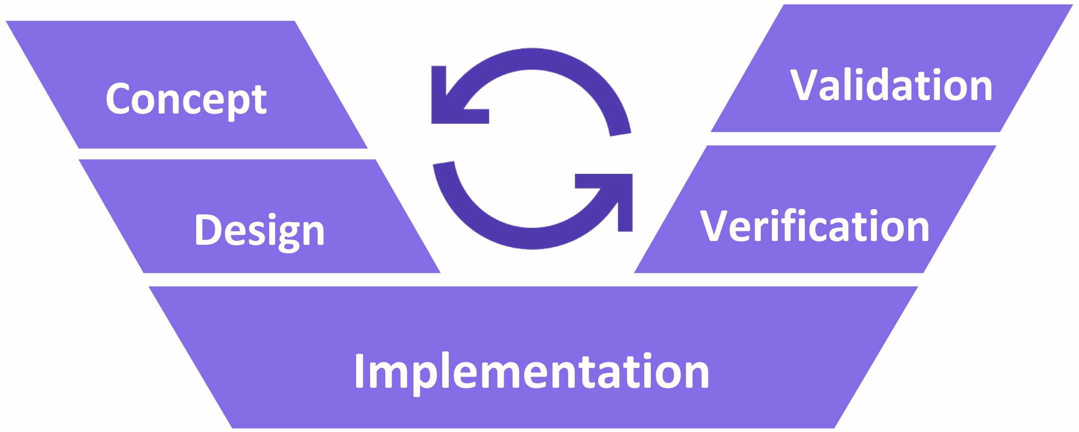
ISO/SAE 21434 Workflow

- TARA

Objectivity

Availability

The best practice solution offered by the **ATHENA**.



Concept

Design

Implementation

Verification

Validation

- V-SOC
- ECU Protection
- CAN/Ethernet IDPS
- Vulnerability Management

Quantification

Classification

- Functional Testing
- Vulnerability Scanning
- Fuzz Testing
- Penetration Testing

Effective Verification

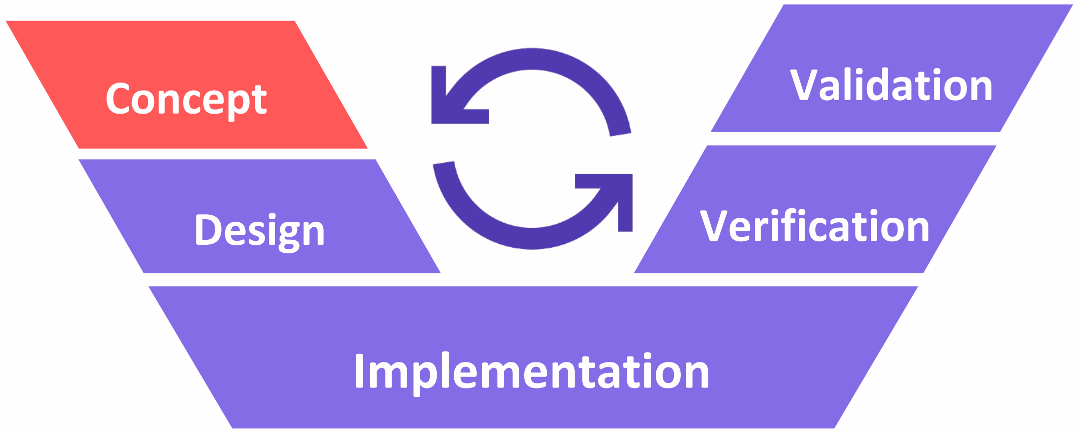
The verification program base on the TARA and implementation results offered by the **ATHENA**.

ISO/SAE 21434 Workflow

- TARA

Objectivity

Availability



- Functional Testing
- Vulnerability Scanning
- Fuzz Testing
- Penetration Testing

Effective Verification

The best practice solution offered by the **ATHENA**.

- V-SOC
- ECU Protection
- CAN/Ethernet IDPS
- Vulnerability Management

Quantification

Classification

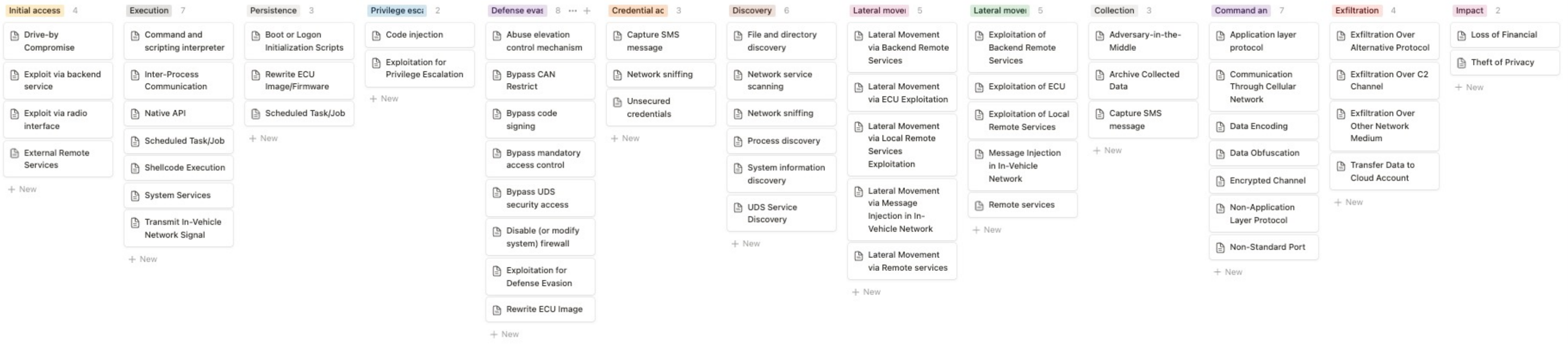
The verification program base on the TARA and implementation results offered by the **ATHENA**.

Potential Risk Matrix for each Component

Component | **Potential Risk Matrix**

T-Box

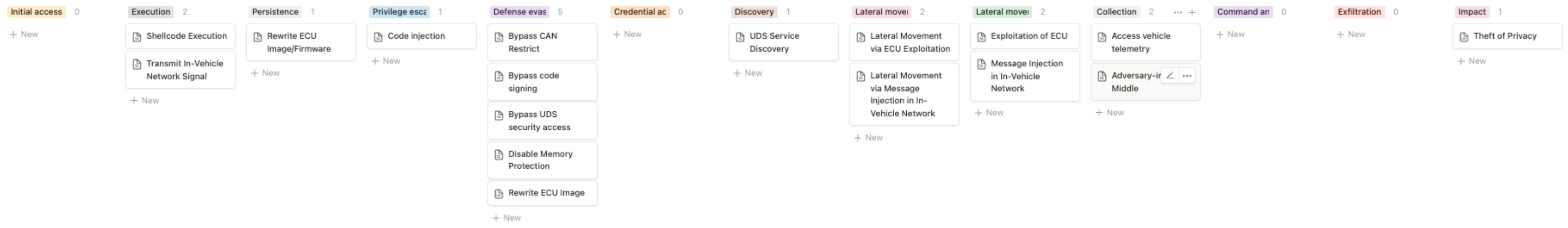
- Linux
- Remote Control
- Service
- CAN Bus



Initial access 4	Execution 7	Persistence 3	Privilege esca 2	Defense evas 8 ··· +	Credential ac 3	Discovery 6	Lateral movei 5	Lateral movei 5	Collection 3	Command an 7	Exfiltration 4	Impact 2
Drive-by Compromise	Command and scripting interpreter	Boot or Logon Initialization Scripts	Code injection	Abuse elevation control mechanism	Capture SMS message	File and directory discovery	Lateral Movement via Backend Remote Services	Exploitation of Backend Remote Services	Adversary-in-the-Middle	Application layer protocol	Exfiltration Over Alternative Protocol	Loss of Financial
Exploit via backend service	Inter-Process Communication	Rewrite ECU Image/Firmware	Exploitation for Privilege Escalation	Bypass CAN Restrict	Network sniffing	Network service scanning	Lateral Movement via ECU Exploitation	Exploitation of ECU	Archive Collected Data	Communication Through Cellular Network	Exfiltration Over C2 Channel	Theft of Privacy
Exploit via radio interface	Native API	Scheduled Task/Job	+ New	Bypass code signing	Unsecured credentials	Network sniffing	Lateral Movement via Local Remote Services Exploitation	Exploitation of Local Remote Services	Capture SMS message	Data Encoding	Exfiltration Over Other Network Medium	+ New
External Remote Services	Scheduled Task/Job	+ New		Bypass mandatory access control	+ New	Process discovery	Lateral Movement via Message Injection in In-Vehicle Network	Message Injection in In-Vehicle Network	+ New	Data Obfuscation	Transfer Data to Cloud Account	
+ New	Shellcode Execution			Bypass UDS security access		System information discovery	Lateral Movement via Remote services	Remote services		Encrypted Channel	+ New	
	System Services			Disable (or modify system) firewall		UDS Service Discovery	+ New	+ New		Non-Application Layer Protocol		
	Transmit In-Vehicle Network Signal			Exploitation for Defense Evasion		+ New				Non-Standard Port		
	+ New			Rewrite ECU Image						+ New		
				+ New								

IC

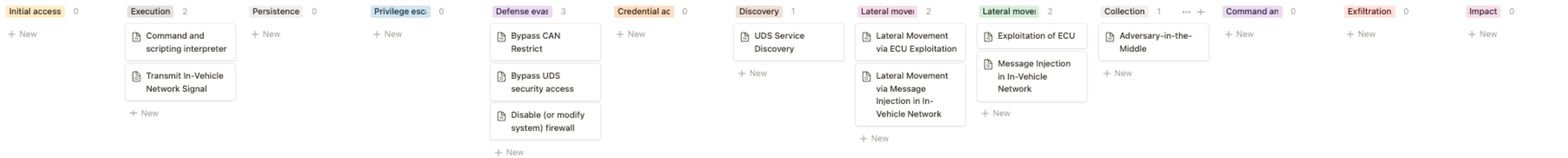
- RTOS
- CAN Bus



Initial access 0	Execution 2	Persistence 1	Privilege esca 1	Defense evas 5	Credential ac 0	Discovery 1	Lateral movei 2	Lateral movei 2	Collection 2 ··· +	Command an 0	Exfiltration 0	Impact 1
+ New	Shellcode Execution	Rewrite ECU Image/Firmware	Code injection	Bypass CAN Restrict	+ New	UDS Service Discovery	Lateral Movement via ECU Exploitation	Exploitation of ECU	Access vehicle telemetry	+ New	+ New	Theft of Privacy
	Transmit In-Vehicle Network Signal	+ New	+ New	Bypass code signing		+ New	Lateral Movement via Message Injection in In-Vehicle Network	Message Injection in In-Vehicle Network	Adversary-ir Middle			+ New
	+ New			Bypass UDS security access			+ New	+ New	+ New			
				Disable Memory Protection								
				Rewrite ECU Image								
				+ New								

Gateway

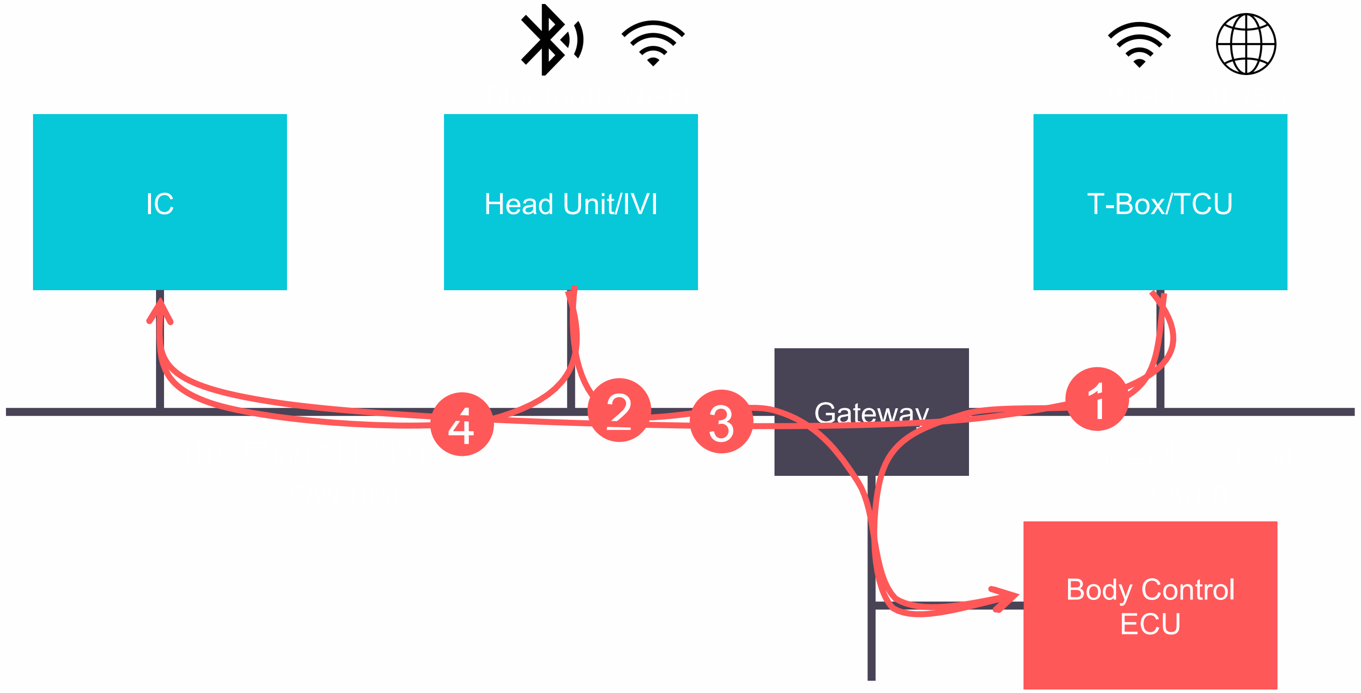
- CAN Bus
- Firewall
- AUTOSAR

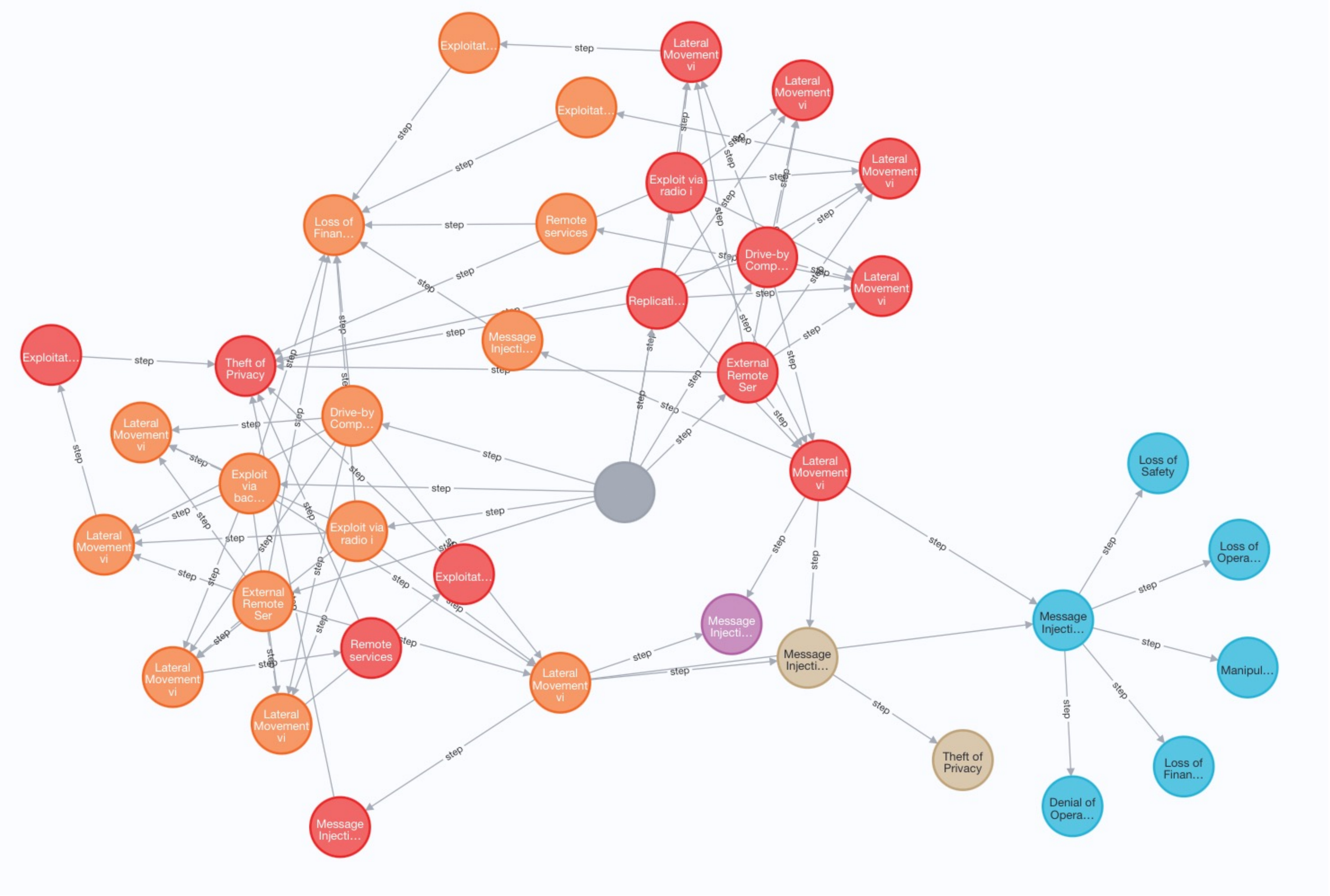


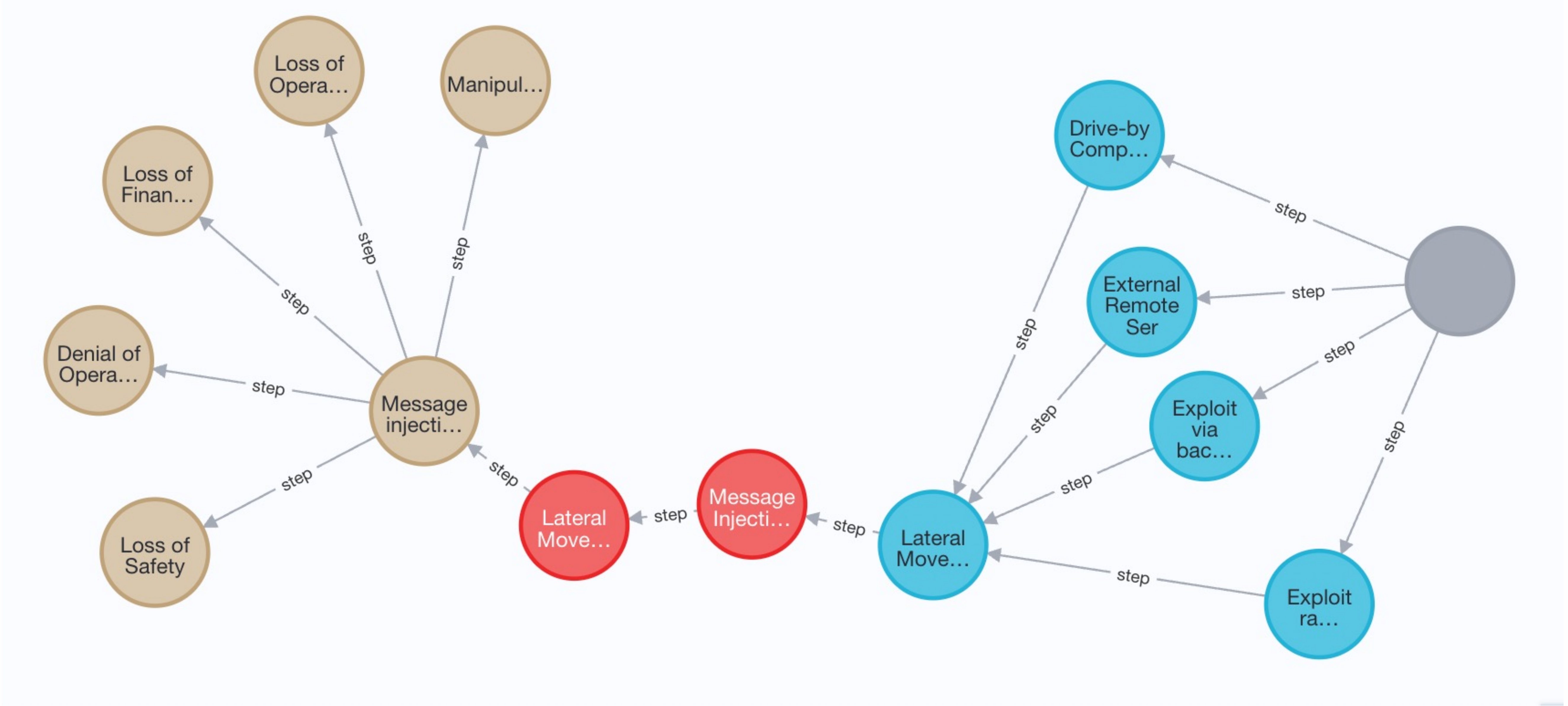
Initial access 0	Execution 2	Persistence 0	Privilege esca 0	Defense evas 3	Credential ac 0	Discovery 1	Lateral movei 2	Lateral movei 2	Collection 1 ··· +	Command an 0	Exfiltration 0	Impact 0
+ New	Command and scripting interpreter	+ New	+ New	Bypass CAN Restrict	+ New	UDS Service Discovery	Lateral Movement via ECU Exploitation	Exploitation of ECU	Adversary-in-the-Middle	+ New	+ New	+ New
	Transmit In-Vehicle Network Signal			Bypass UDS security access		+ New	Lateral Movement via Message Injection in In-Vehicle Network	Message Injection in In-Vehicle Network	+ New			
	+ New			Disable (or modify system) firewall			+ New	+ New				
				+ New								

Attack Path Analysis

1. T-Box → Gateway → Body ECU
2. Head Unit → Gateway → Body ECU
3. T-Box → Gateway → IC
4. Head Unit → IC




Exploitat…
Lateral Movement vi
Exploitat…
Lateral Movement vi
Lateral Movement vi
Exploit via radio i
Loss of Finan…
Remote services
Drive-by Comp…
Lateral Movement vi
Replicati…
Message Injecti…
Exploitat…
Theft of Privacy
External Remote Ser
Drive-by Comp…
Lateral Movement vi
Lateral Movement vi
Loss of Safety
Exploit via bac…
Lateral Movement vi
Exploit via radio i
Loss of Opera…
Exploitat…
External Remote Ser
Message Injecti…
Message Injecti…
Remote services
Lateral Movement vi
Lateral Movement vi
Message Injecti…
Manipul…
Lateral Movement vi
Theft of Privacy
Loss of Finan…
Denial of Opera…
Message Injecti…
step



Body ECU

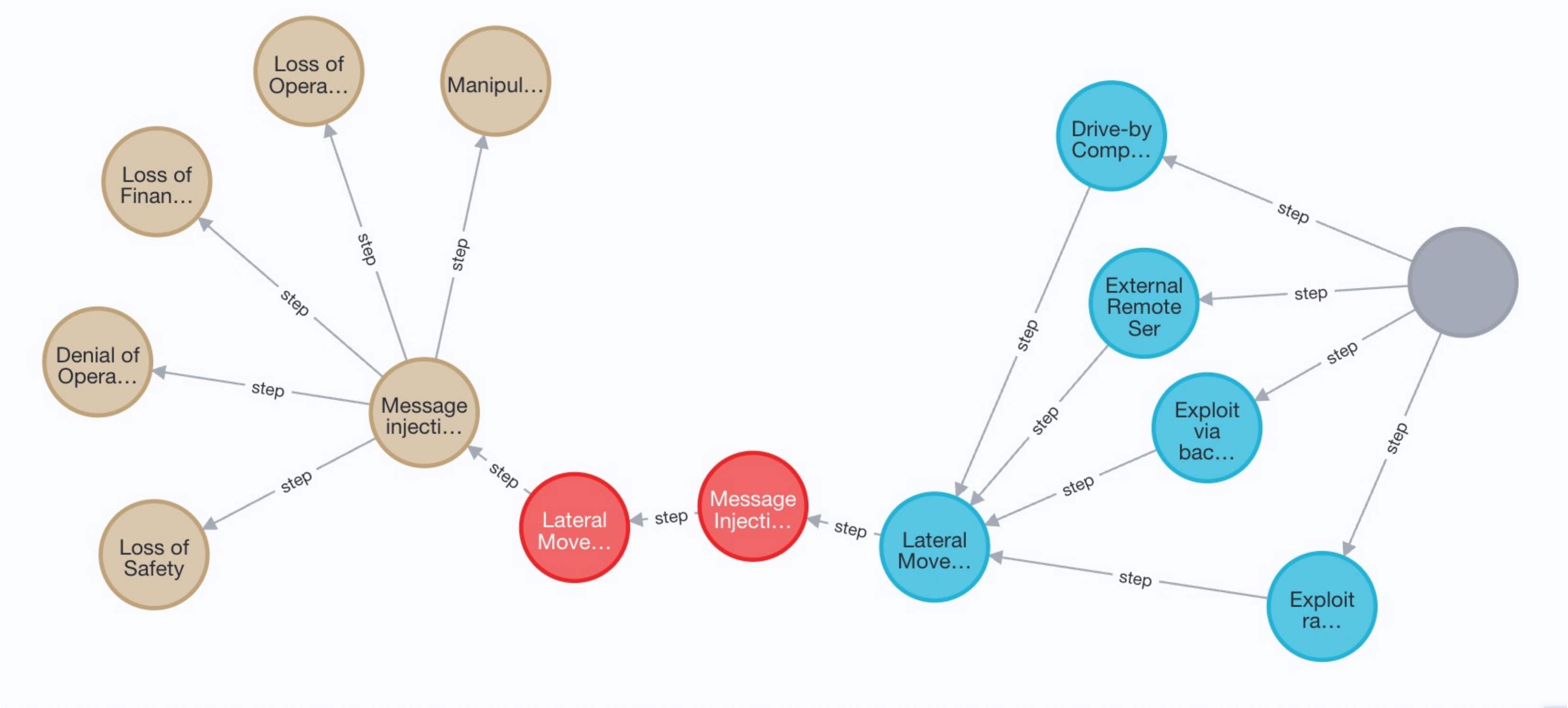
Gateway

T-Box

Root

Export Actionable Mitigation/Detection

- Network Segmentation
- V-SOC
- Security OTA
- Exploit Protection
- APP Sandbox

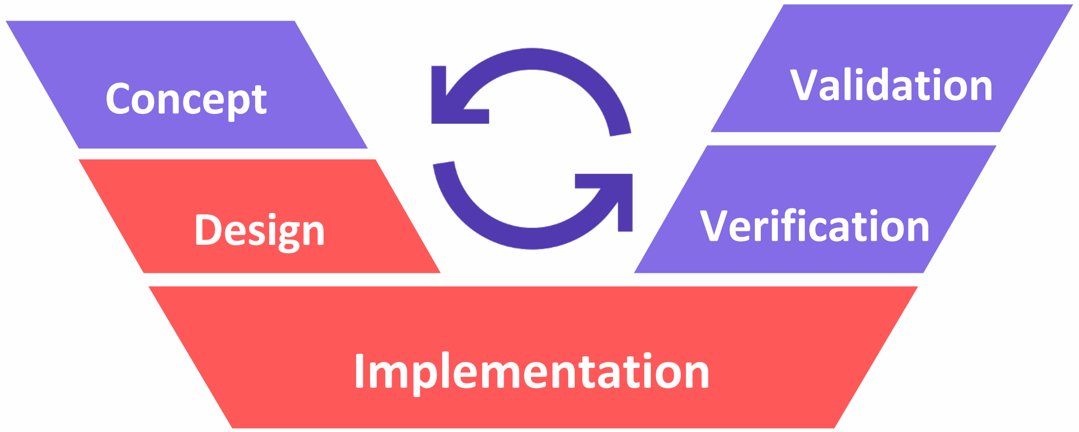


ISO/SAE 21434 Workflow

- TARA

Objectivity

Availability



Concept

Design

Implementation

Verification

Validation

- Functional Testing
- Vulnerability Scanning
- Fuzz Testing
- Penetration Testing

Effective Verification

The best practice solution offered by the **ATHENA**.

- V-SOC
- ECU Protection
- CAN/Ethernet IDPS
- Vulnerability Management

Quantification

Classification

The verification program base on the TARA and implementation results offered by the **ATHENA**.

Decision

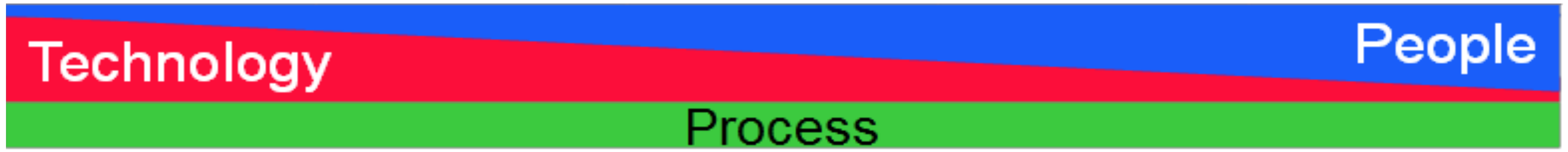
	Identify	Protect	Detect	Respond	Recover
Devices	Security OTA * 26 Vuln Scanning * 4	ECU Protection * 26 Anti-Virus * 4	V-SOC * 42 Threat Init * 8		
Applications	Security OTA * 26 Vuln Scanning * 4	PAM * 26 App sandbox * 12	Threat Init * 8		
Networks		Segment * 49 CAN IDPS * 35	CAN IDPS * 35 Threat Init * 8		
Data		PAM * 26 TPM * 11			
Users		PAM * 26 MFA * 4			

🟥 30 < Count

🟪 10< Count <30

🟦 Count < 10

Degree of Dependency



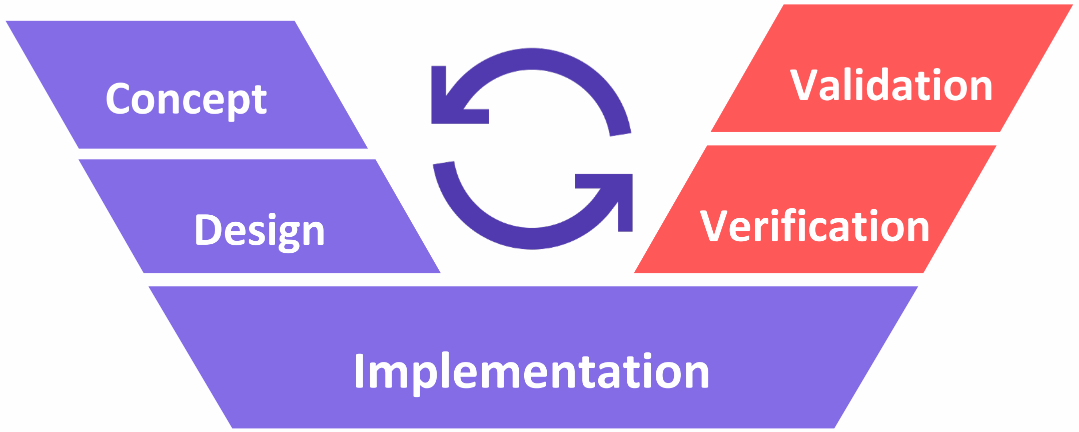
https://cyberdefensematrix.com

ISO/SAE 21434 Workflow

- TARA

Objectivity

Availability



- Functional Testing
- Vulnerability Scanning
- Fuzz Testing
- Penetration Testing

Effective Verification

The best practice solution offered by the **ATHENA**.

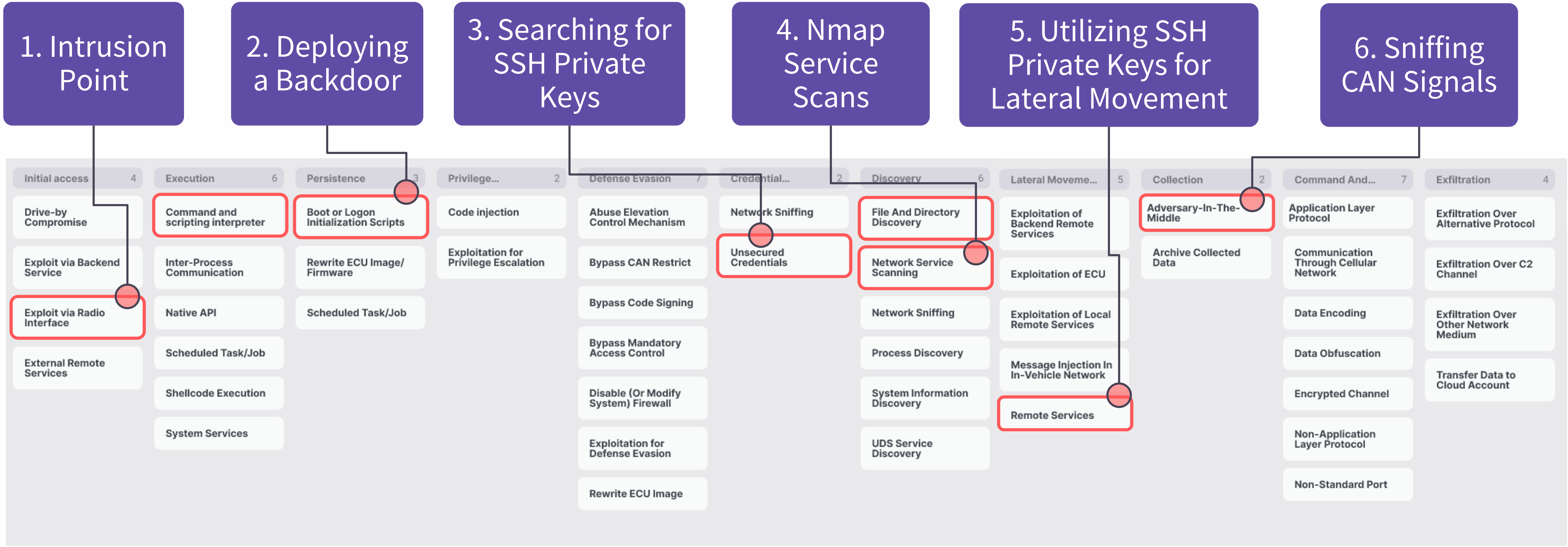
- V-SOC
- ECU Protection
- CAN/Ethernet IDPS
- Vulnerability Management

Quantification

Classification

The verification program base on the TARA and implementation results offered by the **ATHENA**.

Planning Penetration Testing with ATHENA



1. Intrusion Point

2. Deploying a Backdoor

3. Searching for SSH Private Keys

4. Nmap Service Scans

5. Utilizing SSH Private Keys for Lateral Movement

6. Sniffing CAN Signals

Initial access 4	Execution 6	Persistence 3	Privilege... 2	Defense Evasion 7	Credential... 2	Discovery 6	Lateral Moveme... 5	Collection 2	Command And... 7	Exfiltration 4
Drive-by Compromise	Command and scripting interpreter	Boot or Logon Initialization Scripts	Code injection	Abuse Elevation Control Mechanism	Network Sniffing	File And Directory Discovery	Exploitation of Backend Remote Services	Adversary-In-The-Middle	Application Layer Protocol	Exfiltration Over Alternative Protocol
Exploit via Backend Service	Inter-Process Communication	Rewrite ECU Image/ Firmware	Exploitation for Privilege Escalation	Bypass CAN Restrict	Unsecured Credentials	Network Service Scanning	Exploitation of ECU	Archive Collected Data	Communication Through Cellular Network	Exfiltration Over C2 Channel
Exploit via Radio Interface	Native API	Scheduled Task/Job		Bypass Code Signing		Network Sniffing	Exploitation of Local Remote Services		Data Encoding	Exfiltration Over Other Network Medium
External Remote Services	Scheduled Task/Job			Bypass Mandatory Access Control		Process Discovery	Message Injection In In-Vehicle Network		Data Obfuscation	Transfer Data to Cloud Account
	Shellcode Execution			Disable (Or Modify System) Firewall		System Information Discovery	Remote Services		Encrypted Channel	
	System Services			Exploitation for Defense Evasion		UDS Service Discovery			Non-Application Layer Protocol	
				Rewrite ECU Image					Non-Standard Port	

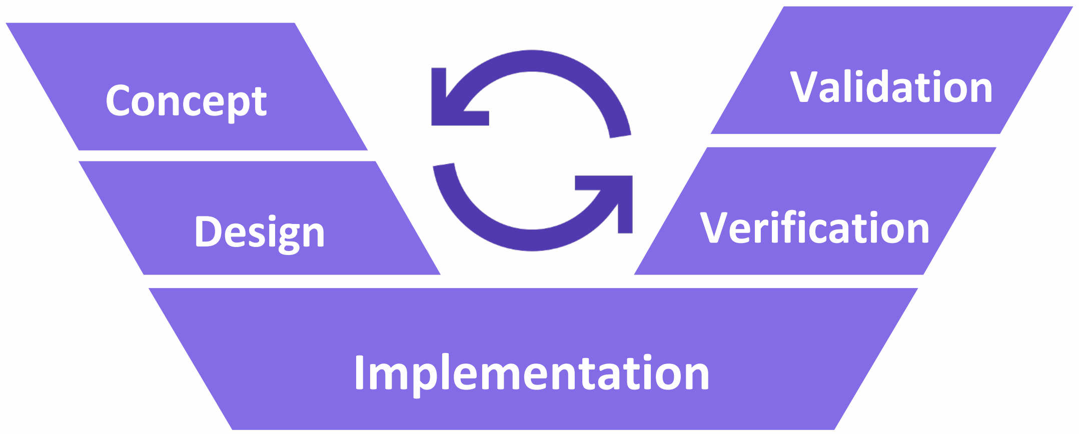
Conclusion

Overview

- TARA

Objectivity

Availability



Concept

Design

Implementation

Verification

Validation

- Functional Testing
- Vulnerability Scanning
- Fuzz Testing
- Penetration Testing

Effective Verification

The best practice solution offered by the **ATHENA**.

- V-SOC
- ECU Protection
- CAN/Ethernet IDPS
- Vulnerability Management

Quantification

Classification

The verification program base on the TARA and implementation results offered by the **ATHENA**.

Contact Us & Contribution

- dange.lin@cycarrier.com

ATHENA is avalible now!

- https://athena.cycraft.ai
- dange.lin@cycarrier.com