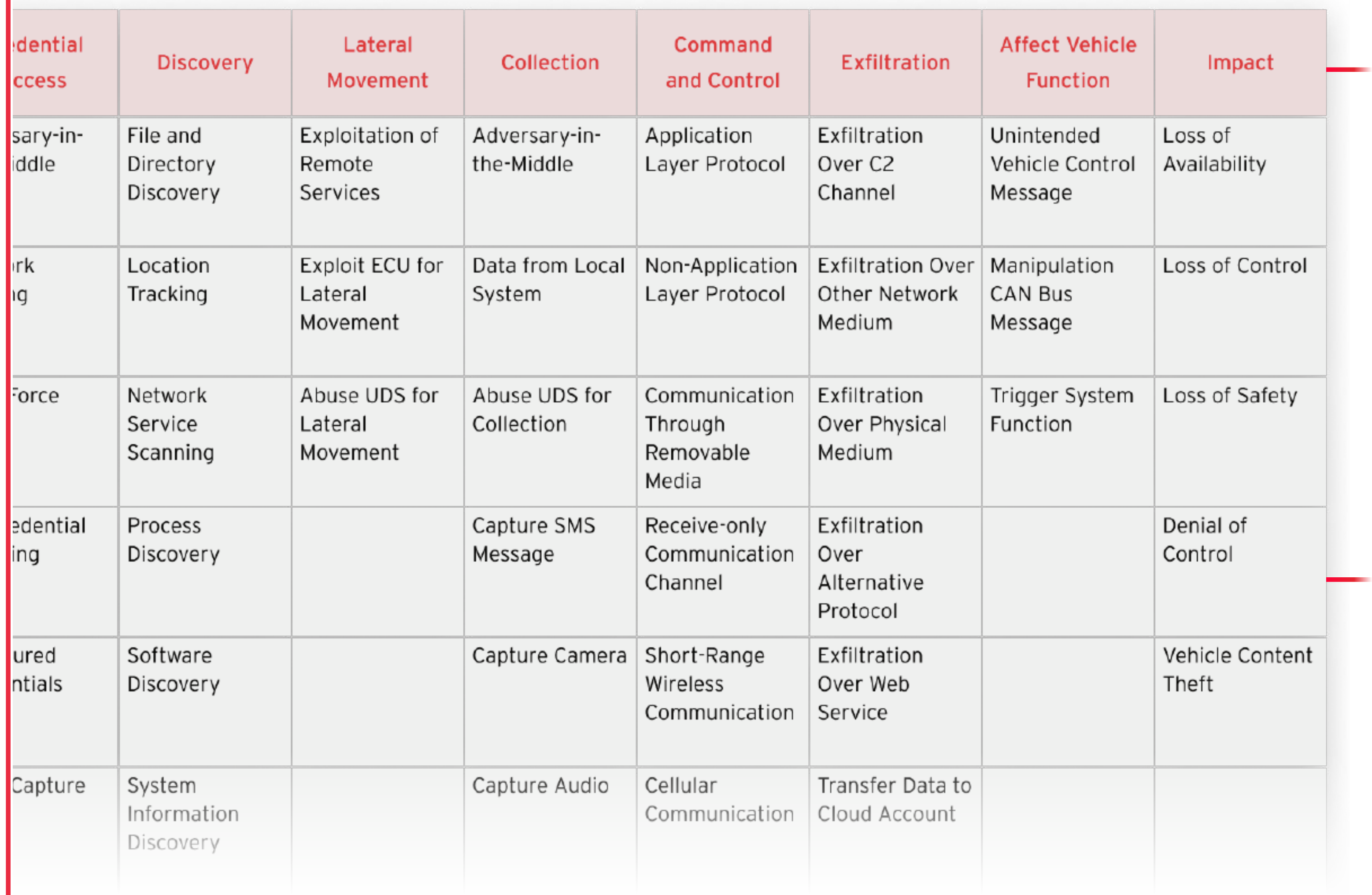
VicOne

USE CASE

Mapping Automotive Threats to Perform Threat Investigations

Mapping automotive threats

VicOne refers to MITRE ATT&CK®, a curated knowledge base of adversarial tactics, techniques, and procedures (TTPs) to highlight threats in the ATT&CK Matrix that could be used by threat actors to launch cyberattacks on connected cars. VicOne breaks down the life cycle of a cyberattack into its component stages and provides a simulation of an automotive cyberattack based on Trend Micro's global threat intelligence and automotive expertise. By understanding what attackers are trying to achieve and their attack methods, security analysts can gain a clear picture of the attack scope and implement necessary remediation and improvement plans.



edential ccess	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Affect Vehicle Function	Impact
sary-in-iddle	File and Directory Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Exfiltration Over C2 Channel	Unintended Vehicle Control Message	Loss of Availability
rk ng	Location Tracking	Exploit ECU for Lateral Movement	Data from Local System	Non-Application Layer Protocol	Exfiltration Over Other Network Medium	Manipulation CAN Bus Message	Loss of Control
Force	Network Service Scanning	Abuse UDS for Lateral Movement	Abuse UDS for Collection	Communication Through Removable Media	Exfiltration Over Physical Medium	Trigger System Function	Loss of Safety
edential ing	Process Discovery		Capture SMS Message	Receive-only Communication Channel	Exfiltration Over Alternative Protocol		Denial of Control
ured ntials	Software Discovery		Capture Camera	Short-Range Wireless Communication	Exfiltration Over Web Service		Vehicle Content Theft
Capture	System Information Discovery		Capture Audio	Cellular Communication	Transfer Data to Cloud Account		

Tactics

The objective behind an attack, which explains the reason for using a particular technique

Techniques

How a threat actor achieves their tactic

At the CanSecWest 2021 Conference, a German research team presented how it compromised Tesla and gained control of its in-vehicle infotainment (IVI) system. In the next section, we explore and map the hacking stages to the ATT&CK Matrix on the right-hand side of each hacking stage.

Dissecting the attack flow of an IVI system hack

1. **Establish connection with Tesla through a Wi-Fi network.**

   Most Tesla models automatically connect to a Wi-Fi network called "Tesla Service" when the vehicles park at a Tesla Service Center. The researchers built an unauthorized access point using the same name and leaked credentials.

2. **Attack zero-day vulnerabilities to access the IVI system.**

   Tesla uses ConnMan, an open-source network manager, to manage network connection for its IVI system. The researchers exploited two zero-day vulnerabilities in ConnMan to gain access to the IVI system.

3. **Obtain elevated privileges for the IVI system.**

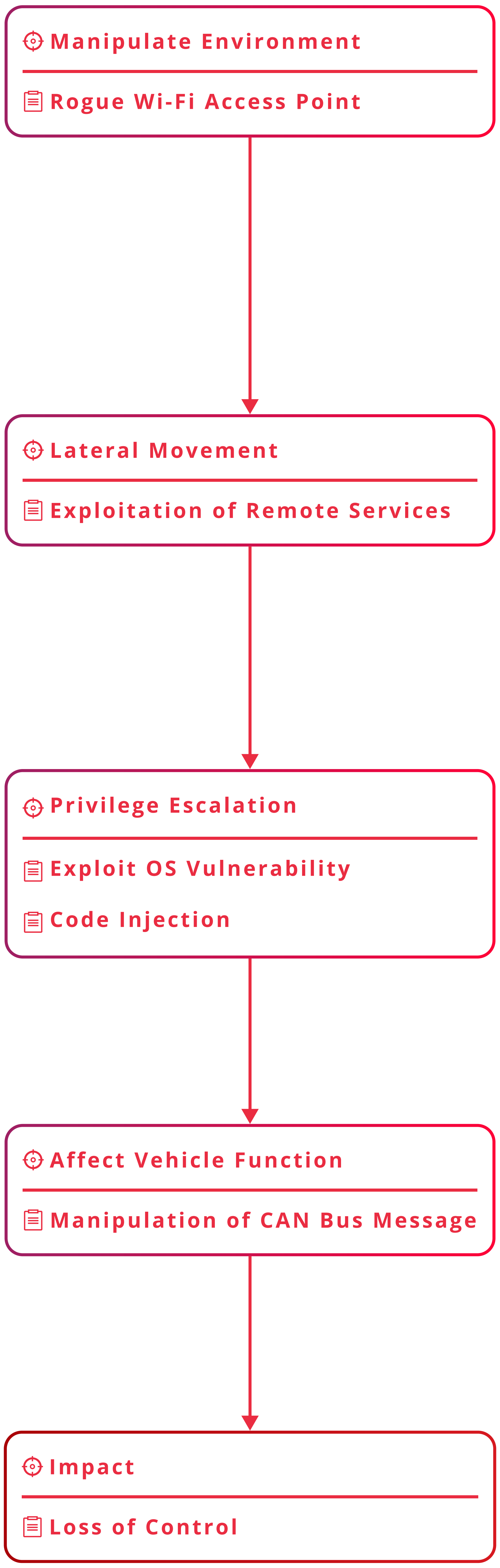
   The researchers took advantage of a bug in the Wi-Fi system on a chip (SoC) that has existed since 2017. They were able to insert unauthorized code to gain access to the IVI system with higher privileges.

4. **Control the IVI system over Wi-Fi.**

   With root access to the IVI system, the researchers can send crafted Controller Area Network (CAN bus) messages to control the IVI system.

5. **Take control of the vehicle remotely.**

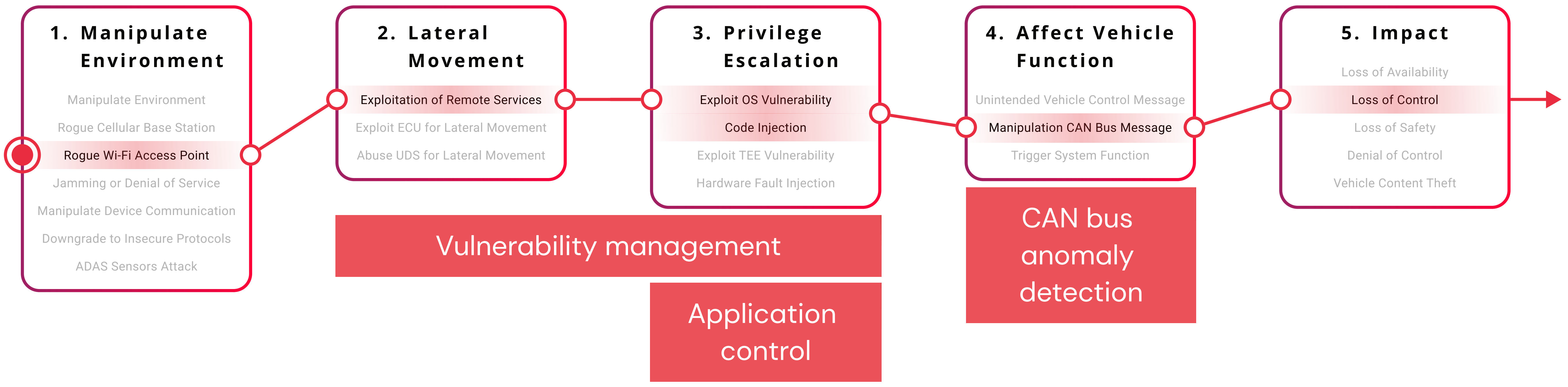
   The researchers could control actions available on the IVI console, such as unlocking the doors, changing seat positions, and modifying steering and acceleration modes.



How can VicOne help?

Mapping threats in automotive cyberattacks helps to understand the goal of threat actors and their reasons for using a particular technique in every hacking stage. This step-by-step breakdown helps car manufacturers outline an attack flow and evaluate the effectiveness of their defense tools. In this section, we discuss how VicOne can help manufacturers prevent attacks and secure their systems throughout a vehicle's life cycle.

xNexus, our vehicle security operation center (VSOC), has security features that allow manufacturers to monitor and analyze unusual vehicle events and maps threats to the ATT&CK Matrix. Based on what we learned from this hacking project, VicOne can help boost automotive cybersecurity in the following ways:


1. Manipulate Environment
Manipulate Environment
Rogue Cellular Base Station
Rogue Wi-Fi Access Point
Jamming or Denial of Service
Manipulate Device Communication
Downgrade to Insecure Protocols
ADAS Sensors Attack
2. Lateral Movement
Exploitation of Remote Services
Exploit ECU for Lateral Movement
Abuse UDS for Lateral Movement
3. Privilege Escalation
Exploit OS Vulnerability
Code Injection
Exploit TEE Vulnerability
Hardware Fault Injection
4. Affect Vehicle Function
Unintended Vehicle Control Message
Manipulation CAN Bus Message
Trigger System Function
5. Impact
Loss of Availability
Loss of Control
Loss of Safety
Denial of Control
Vehicle Content Theft
Vulnerability management
Application control
CAN bus anomaly detection

- **Discover vulnerabilities and mitigate risks at an early stage.**

  xZETA can identify software vulnerabilities in electronic control units (ECUs), while xCarbon can provide virtual patching for manufacturers to mitigate risks before an official patch becomes available.

- **Prevent privilege escalation with application control.**

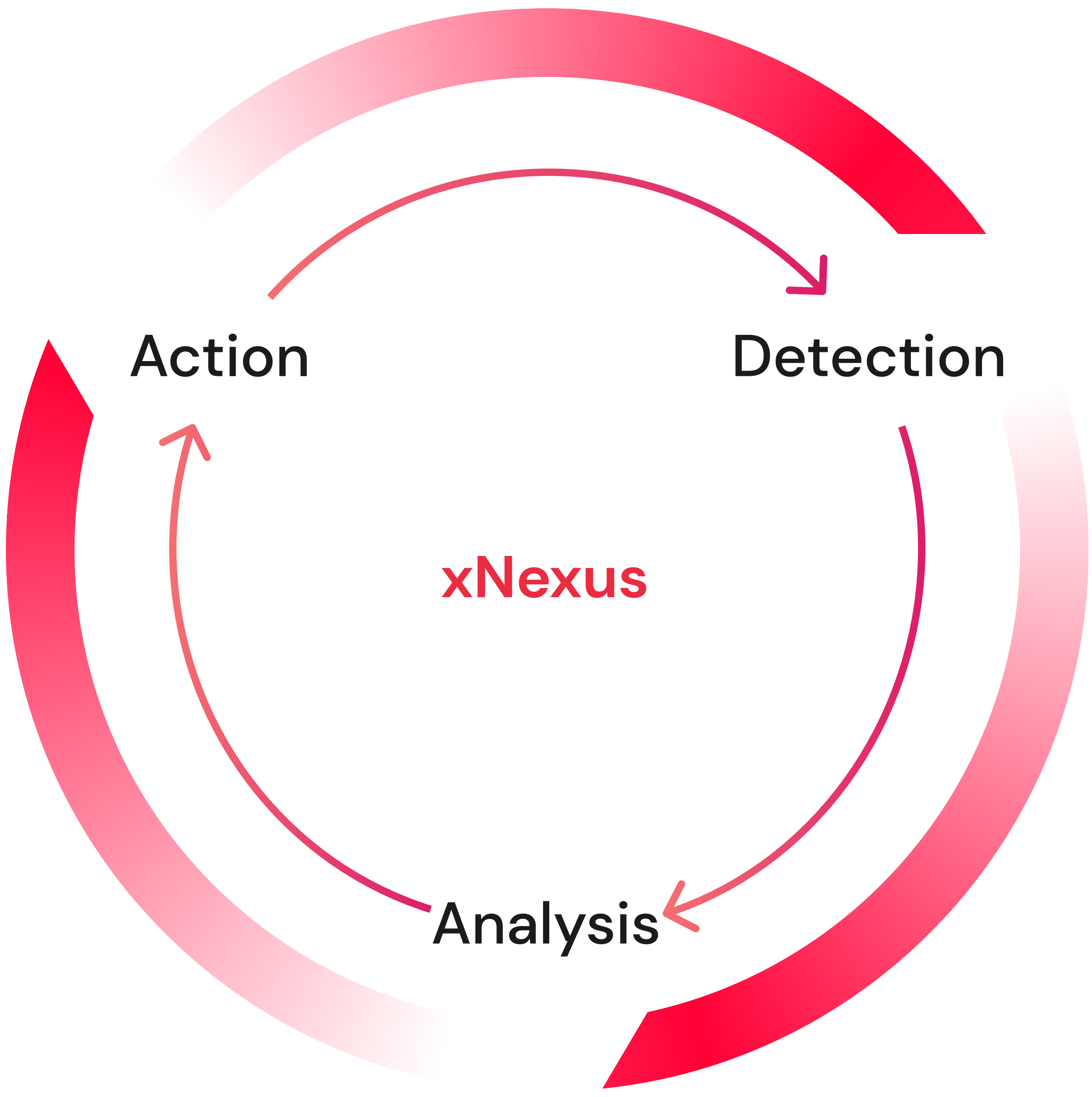
  xCarbon also provides application control to restrict the applications that can run in vehicles. This helps prevent privilege escalation attacks or unauthorized application execution.

- **Identify malicious CAN bus messages to protect vehicle function.**

  By comparing and analyzing vehicle telematics and profile, xNexus can identify anomalous vehicle events, such as unusual on-board diagnostics (OBD-II) connection, unauthorized updates, and malicious CAN bus messages.

About VicOne Automotive Security

Our Automotive Security team offers comprehensive protection against cyberattacks targeting connected vehicles through xNexus, a cloud-based vehicle security operation center (VSOC). By leveraging extended detection and response (XDR) capabilities, automotive threat intelligence, OEM data, and xCarbon in-vehicle sensors, xNexus ensures compliance with UN Regulation No. 155 (UN R155), maps threats to the ATT&CK Matrix, highlights threats applicable to automotive cyberattacks, and keeps up with the latest automotive cybersecurity incidents.



Detection

Receives data or security notifications from various sources

Analysis

Conducts broad-spectrum correlation analysis of threats

Action

Visualizes analysis results in a unified view to assist in further investigations or mitigation

For more information:

Website:
https://www.vicone.com/

Contact:
https://www.vicone.com/contact-us