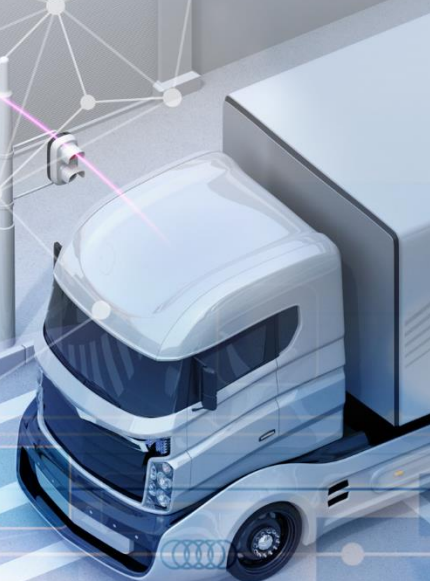
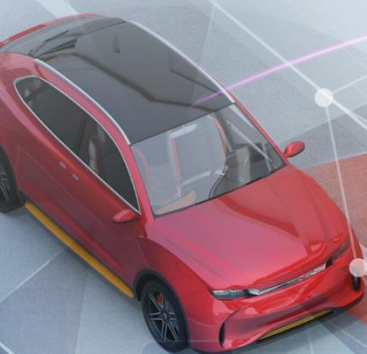


AUTO-ISAC
AUTOMOTIVE CYBERSECURITY BEST PRACTICES

THREAT DETECTION, MONITORING AND ANALYSIS

Best Practice Guide
Version 1.3



Traffic Light Protocol: WHITE.

This information may be shared in public forums.



THREAT DETECTION, MONITORING & ANALYSIS

Traffic Light Protocol: White (May be shared in public forums)

Version History

This is a living document, which will be periodically updated under the direction of the Auto-ISAC Best Practices Working Group. We will track any updates in the table below.

Version Notes:

Version	Revision Date	Notes
v1.0	24 September 2018	
v1.1	30 November 2018	Changed from TLP Amber to TLP Green for release to industry stakeholders via request on Auto-ISAC website
v1.2	01 July 2019	Performed periodic continuity and consistency refresh across all Best Practice documents
v1.3	19 August 2019	Changed from TLP Green to TLP White for release to the public via request on Auto-ISAC website

This Guide does not prescribe or require specific technical or organizational practices. These are voluntary and aspirational practices, which may evolve over time. Please see Section 1.2 for more information.

Contents

Version History	
1.0 Introduction	1
1.1 Best Practices Overview	1
1.2 Purpose	1
1.3 Scope	1
1.4 Audience	2
1.5 Authority and Guide Development	2
1.6 Governance and Maintenance	2
2.0 Best Practices	3
2.1 Framework for Threat Detection, Monitoring and Analysis in Vehicle Cybersecurity	3
2.2 Best Practices for Defining a Threat Detection and Analysis Process	4
2.2.1 Threat Team Structure and Operating Model	4
2.2.2 Stakeholder Roles and Responsibilities	5
2.2.3 Automotive Threat Environment	6
2.3 Best Practices for Threat Intelligence	7
2.3.1 Defining Threat Intelligence Requirements	8
2.3.2 Defining Threat Intelligence Sources	8
2.3.3 Threat Intelligence Collection	9
2.4 Best Practices for Threat Monitoring Processes	10
2.4.1 Defining Priorities for Monitoring	10
2.4.2 Threat Monitoring Techniques and Approaches	11
2.5 Best Practices for Threat Analysis	11
2.5.1 Threat Event Identification	11
2.5.2 Validation and Verification of Identified Threats	12
2.5.3 Taking Necessary Action	13
2.6 Best Practices for Information Organization, Storage, and Sharing	13
2.6.1 Key Considerations for Information Storage and Organization	14
2.6.2 Approaches for Internal and External Sharing	15
Appendix A: Glossary of Terms	16
Appendix B: Additional References and Resources	17
Appendix C: Acronyms	18

1.0 Introduction

1.1 BEST PRACTICES OVERVIEW

This Best Practice Guide is one in a series of seven Guides intended to provide the automotive industry with guidance on the Key Cybersecurity Functions defined in the [Automotive Cybersecurity Best Practices Executive Summary](#):

1. Incident Response
2. Collaboration and Engagement with Appropriate Third Parties
3. Governance
4. Risk Assessment and Management
5. Awareness and Training
- 6. Threat Detection, Monitoring and Analysis**
7. Security Development Lifecycle

Guides offer greater detail to complement the high-level Executive Summary. This Guide aligns with the “Threat Detection, Monitoring and Analysis” function and is made available for use by companies, as appropriate for their unique systems, processes, and risks.

1.2 PURPOSE

The purpose of this Guide is to assist automotive industry stakeholders with identifying, monitoring, and analyzing vehicle cybersecurity threats.

This Guide provides forward-looking guidance without being prescriptive or restrictive. These best practices are:

- **Not Required.** Organizations have the autonomy and ability to select and voluntarily adopt practices based on their respective risk landscapes and organizational structures.
- **Aspirational.** These practices are forward-looking and voluntarily implemented over time, as appropriate.
- **Living.** Auto-ISAC plans to periodically update this Guide to adapt to the evolving automotive cybersecurity landscape.

1.3 SCOPE

This Guide describes key considerations for companies around vehicle cybersecurity threat management efforts. It contains best practices and implementation guidance for companies to identify, monitor, and analyze vehicle cybersecurity threats.

Vehicle cybersecurity threats exist or emerge in all phases of the vehicle lifecycle, including design, development, and post-production. These phases are described in Figure 1 below.

THREAT DETECTION, MONITORING & ANALYSIS

Traffic Light Protocol: White (May be shared in public forums)

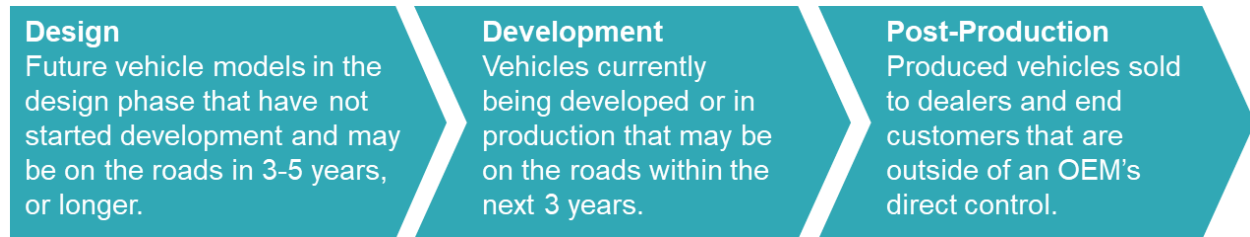


FIGURE 1: VEHICLE LIFECYCLE PHASES

Given the differences in these phases, it might be helpful for organizations to identify applicable factors that will aid in the identification and efficient monitoring of threats. Additionally, due to differences in each phase, threat detection approaches and analyses can differ across the vehicle lifecycle phases.

1.4 AUDIENCE

This Guide was written for use by light-duty and heavy-duty vehicle OEMs, light-duty and heavy-duty vehicle suppliers, and commercial vehicle companies (e.g. fleets, carriers). It may also provide insights for other stakeholders across the connected vehicle ecosystem.

Within these organizations, for the primary audience is vehicle cybersecurity managers, leaders, and senior executives responsible for identifying cyber threats.

1.5 AUTHORITY AND GUIDE DEVELOPMENT

The Auto-ISAC Best Practices Working Group wrote this Guide, with support from Booz Allen Hamilton vehicle cybersecurity Subject Matter Experts (SMEs) who facilitated the Guide's development. The Working Group is comprised of over 130 representatives from Auto-ISAC Members, including:

AT&T	FCA	Infineon	Nissan
Bosch	Ford	Kia	NXP
BMW	General Motors	Lear Corporation	Panasonic
Continental	Geotab	Magna	Subaru
Cooper Standard	Harman	Mazda	Toyota
Cummins	Honda	Mercedes-Benz	Volkswagen
Delphi	Honeywell	Mitsubishi Motors	Volvo
DENSO	Hyundai	Mobis	ZF
EHI			

The Working Group also coordinated with several external stakeholders while developing this Guide, including NHTSA, ISO/SAE, and DHS.

1.6 GOVERNANCE AND MAINTENANCE

The Auto-ISAC Best Practices Standing Committee is responsible for the maintenance of the Guide, which will undergo periodic refreshes to incorporate, as appropriate, lessons learned, new policies, updated or new engineering standards, and the like.

This Guide will be rolled out in phases and marked accordingly with the appropriate Traffic Light Protocol (TLP) classification:

- **First 3 months after publication:** **TLP Amber** - available exclusively to Auto-ISAC Members
- **3 to 9 months after publication:** **TLP Green** - released by request to industry stakeholders
- **9 months after publication:** **TLP White** - released to the public via the Auto-ISAC website (www.automotiveisac.com), subject to Board of Directors confirmation

This Guide was developed while the ISO and SAE were in the process of jointly developing the ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering Standard. After ISO/SAE 21434 is published, the Standing Committee plans to review and update this Guide, as appropriate.

2.0 Best Practices

This section identifies the primary elements of identifying, monitoring, and analyzing threats across the vehicle cybersecurity ecosystem. Companies should consider these Best Practices while also referring to the References and Resources listed in Appendix B, which informed the development of these Best Practices.

2.1 FRAMEWORK FOR THREAT DETECTION, MONITORING AND ANALYSIS IN VEHICLE CYBERSECURITY

A cybersecurity threat detection, monitoring, and analysis process is an organizational capability designed to reduce cybersecurity risk, ideally before an incident occurs (i.e. before a threat exploits a vulnerability). A framework for this Guide is provided in Figure 2, and each of the five functions is explained in more detail below. It should be noted that each of the five functions described below are iterative in nature.

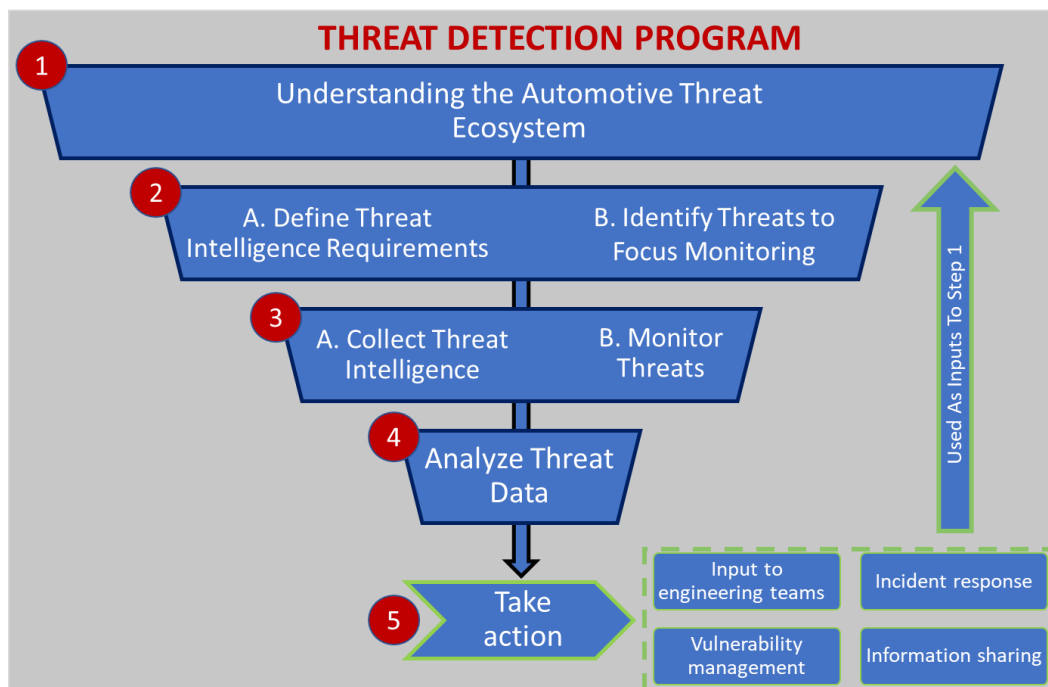


FIGURE 2: FRAMEWORK FOR THREAT DETECTION

1. This step focuses on understanding the automotive threat ecosystem which forms the basis of a threat detection, monitoring, and analysis program. This can involve understanding previously executed research and exploits, and threat agents across three environments, namely: customers, enterprise, and third parties. The customer environment can include deployed vehicles, vehicle components, workshop tools, software applications, or other connected services. The enterprise environment could include insider threats (e.g. disgruntled employees), manufacturing, IT, and other operational technologies (OT) relevant to the vehicle ecosystem. Finally, the third-party environment covers vendors, suppliers, delivery, and products (e.g. devices or services).
2. The second step is defining your organization's threat intelligence requirements across the ecosystem. The goal is to understand which type of information is of interest for a given organization. For example, understanding requirements for indicators of compromise, tactics, and anomalous events can help your organization identify threats to focus monitoring and better understand the threat landscape.
3. An appropriate knowledge base can help each organization filter down what threats are relevant or applicable based on their risk profile or tolerance. Once a company has identified relevant threats to monitor, appropriate techniques to monitor the threats can be refined.
4. With accurate threat information, companies can then develop relevant cyber forensic analysis processes where applicable. Results of such analysis serves as an input into the development of a comprehensive response strategy.
5. Threat information also enables companies to decide on the next course of action. Actions can range from providing input to engineering teams (e.g. design and security engineering), penetration testing teams, vulnerability management teams, incident response teams, and appropriate industry partners.

This Guide does not prescribe specific requirements for threat intelligence gathering, threat monitoring, threat analysis, or information organization and storage. Instead, it describes decision factors that companies may use to determine what is appropriate for their unique business environment and risk landscape. The above framework can help organizations at different levels of cybersecurity capabilities to apply a structured approach to build or refine their threat detection and analysis processes.

2.2 BEST PRACTICES FOR DEFINING A THREAT DETECTION AND ANALYSIS PROCESS

The scope of a threat detection and analysis process may encompass any relevant vehicle cybersecurity threats, including those that originate from both internal and external sources throughout design, development, and post-production processes. Choosing the appropriate threat scope (which can vary from organization to organization) is fundamental for effective threat detection and analysis.

2.2.1 Threat Team Structure and Operating Model

The threat team may draw upon a company's broader vehicle focused cybersecurity team or other appropriate stakeholders as it creates collection requirements, reviews intelligence, validates threats, and creates actionable intelligence analysis. The threat team can potentially benefit from the following:

- An executive level authority for the central team responsible for vehicle related threat detection and analysis
- Access to necessary information in the vehicle security ecosystem
- Pre-approved and documented actions that may be taken based on security events

The threat team may also be supported by a data science team to analyze data from various sources (e.g. diagnostic trouble codes, intrusion detection systems, telematics data, transactions, customer support – case analysis, text analysis, social media). This team can help design and maintain cross-functional design and test requirements for an in-vehicle network intrusion detection system. The data science team may also support anomaly detection of any data that supports the vehicle and provide the capability to monitor performance and correctness of vehicle network communications against design parameters.

Components of a successful operating model for threat detection and analysis programs may include effective data collection and management processes, testing the threat detection program, and other appropriate handoff processes. Regardless of the process or method chosen by the company, there may be a need to adapt threat detection and analysis processes based on the company's changing risk landscape.

For example, an effective data collection process can be based on risk. Typically, the data collected and stored is as detailed as required for event analysis and may include any identified threat vectors within the vehicle ecosystem. By collecting this data, actionable intelligence can be created, reviewed, and distributed to appropriate product cybersecurity engineering teams for structured analytic techniques including: anomaly analysis, trend analysis, signature analysis, heuristic/behavioral analysis, and elimination of false-positives and false-negatives. These actionable findings from the analysis of collected data may benefit incident response and vulnerability programs by: informing incident response processes, refining vulnerability severity ratings, and refining playbooks for possible incident types.

2.2.2 Stakeholder Roles and Responsibilities

The stakeholder roles and responsibilities to maintain and mature an effective threat detection and analysis process represent a wide range of technical staff and partners across the business. Roles and responsibilities in this team may include:

- Intelligence analysts: To execute the collection requirements plan, gather and analyze intelligence, and create timely and actionable intelligence products for decision makers.
- Technical experts: To provide guidance on collection requirements and feedback on the value of intelligence products.
- Penetration testers: To understand the latest attack vectors and trends of the offensive cybersecurity community.
- Detection experts: To provide detection capabilities by gaining specialized knowledge of the vehicle security ecosystem along with the awareness of the data and tools available for analyzing security events.

Teams with roles and responsibilities within a threat detection and analysis program could potentially include:

- Information technology team: To identify threats to IT infrastructure that may be connected to the vehicle ecosystem.

- Data science team: To detect anomalies and provide the capability to monitor performance and correctness of vehicle network communications against design parameters.
- Connected vehicle operations team: To identify threats to the connected vehicle ecosystem by analyzing vehicle telematics which may include working with vendors to manage threats to cloud-connected environments.
- Security analysts' team: To identify threats and provide additional support such as research and communication with appropriate individuals or groups.
- Customer care and aftermarket teams: To detect fraud or abuse that affects the operation of vehicles.
- Engineering and support team: To bring knowledge of threat detection and domain specific vehicle systems. This engineering support team may provide and support tools for use by the threat detection team for vehicle security events and log monitoring.
- Internal legal team: To bring regulatory and compliance perspectives that will protect the organization.
- External teams: Such as law enforcement and other public authorities that can share threat intelligence information from their position as external third parties.

As appropriate, service level and support agreements apply to interactions among stakeholders and provide documented and agreed upon timeframes for providing information, feedback, data, and support related to the vehicle security ecosystem.

2.2.3 Automotive Threat Environment

The threat environment can generally be described by two concepts, threat actors and attack vectors. A person or thing (threat actor) uses different avenues (attack vectors) to execute a cybersecurity attack within the vehicle ecosystem. Threats can exploit points of data ingress and egress across the vehicle ecosystem and change throughout a vehicle or feature lifecycle. A common and effective way to identify, define, and categorize threats is by considering the impacts to confidentiality, integrity, and availability (CIA). Security attacks that threat actors to the vehicle ecosystem could carry out include:

- Theft or exposure of data
 - Theft or exposure of personally identifiable information (PII) or other sensitive data
 - Theft or exposure of vehicle-related data or software
- Physical theft or compromise
 - Unauthorized physical access to the interior or breaking door locks
 - Theft of vehicle parts
 - Theft of the entire vehicle
- Manipulating vehicle controls
 - Breaking a vehicle's immobilizer
 - Illegal manipulation of components and functions
 - Unauthorized activation or deactivation of functionality
 - Co-opting vehicle systems
 - Loss of vehicle control
- Threats to availability
 - Bricking vehicle systems
 - Denial of service attack
 - Ransomware attack

Threat Actor: A person or entity with motivation and capability to exploit a vulnerability in the vehicle ecosystem. Understanding of threat actors typically includes both capabilities and motivation. This information may be incorporated directly into both risk assessments and incident response processes. Threat actors who may affect the vehicle ecosystem include:

- Terrorist organizations
- Malicious insiders
- Cyber-criminals
- Organized crime groups
- Governmental organizations
- State sponsored attackers and intelligence agencies
- Vandals/pranksters/hacktivists

Attack Vectors: The avenues or paths on an attack surface used to attack the vehicle ecosystem. Attack vectors to the vehicle ecosystem may include:

- Remote to vehicle
 - Adjacent
 - Bluetooth
 - Wi-Fi
 - Tire Pressure Monitoring System (TPMS)
 - Distant
 - Via back office channels
 - Via remote capabilities
- Internal to vehicle
 - Standard user interface
 - Infotainment
 - USB
 - Standard programming/data interface
 - Non-standard interface
 - Accessing and modifying vehicle electrical systems

2.3 BEST PRACTICES FOR THREAT INTELLIGENCE

The purpose of threat intelligence is to know your adversary by understanding their motivation and how they would manifest themselves in your environment. Threat intelligence can go beyond the technical operational artifacts and can sometimes include the economic or ideological drivers that reveal the motivation and/or priority of your adversary. This can assist with the prioritization of processing, communicating, or sharing of that intelligence information both internally and externally. Components of a threat intelligence capability include:

- Threat intelligence requirements
- Threat intelligence sources
- Threats and intelligence collection and analysis
- Internal and external intelligence sharing standards and methods

2.3.1 Defining Threat Intelligence Requirements

Definition of threat intelligence requirements allows a company to appropriately scope the threat intelligence collection effort. To define vehicle threat intelligence requirements, organizations may identify the types of threats, threat actors, and attack vectors that will be subject to intelligence collection. This process benefits from collaboration with cross-functional teams to define and validate requirements.

To support this collaboration, the threat team can identify stakeholders from cross-functional teams (e.g. the domain architects and engineers, business partners, supply chain) and initiate activities to foster relationships with SMEs to build trust and drive information sharing. Organizations can also develop an understanding through regular discussions focused on what cybersecurity threat concerns are most important.

Steps to make threat intelligence requirements beneficial typically include:

- Documenting intelligence requirements that can be used as an operating guideline
- Maintaining the threat intelligence requirements in an official repository
- Revising threat intelligence requirements and operating guidelines at regular intervals to capture changes

2.3.2 Defining Threat Intelligence Sources

An important step in building threat intelligence includes determining the best intelligence sources. These could include internal teams, information repositories, and public and private intelligence sources. Examples of threat intelligence sources could include:

- Cybersecurity conferences or summits (e.g. BlackHat, DEFCON, USENIX)
- Fleet and enterprise monitoring (e.g. remote diagnostic monitoring, service monitoring, and other anomaly detection initiatives)
- Information sharing organizations (e.g. Auto-ISAC, CISCIP)
- U.S. local, state, and federal government resources (e.g. NCICC, DHS ICS CERT, US-CERT)
- International government resources (e.g. CERTs, BSI)
- Coordinated disclosure program or bug bounty program
- Dark Web or Darknet
 - Darknet marketplaces for technology, vulnerabilities, and credentials
 - Dark Web forums
- Open source intelligence
 - Enthusiast, technical, and cybercriminal
 - Paste-and-code repository sites
 - News aggregators and feeds
 - Vendors
 - Data and credential breach forums
- Industry peers, suppliers, and partners
- Security event and incident data
- Reports from employees and social media
- Data from secondary extrapolation methods that could serve as impending threat indication

Teams can share information to enable a high-level understanding of those threats related to their work environment (e.g. trends in types of calls or inquiries about specific topics around safety or telematics systems). Additionally, working with technical staff can be beneficial in gaining intrinsic knowledge of digital communities, distribution lists, and other resources that can serve as early indicators of incidents, events, research, and other intelligence.

An organization may also choose to engage external partnerships with third-party vendors for intelligence research programs. For example, programs that have high priority collection requirements can benefit when the capability is unavailable internally, unique search capabilities are required, or an organization wants a layer of separation from the research. (See the Auto-ISAC's *Collaboration and Engagement with Appropriate Third Parties Best Practice Guide* for more information)

2.3.3 Threat Intelligence Collection

Intelligence on threats is collected from selected and prioritized intelligence sources that are pertinent to the organization. The volume of data might be large. Therefore, an agreed upon method can be applied to prioritize collection and analysis. The results are then used to differentiate the highest risk threats, as well as highlight any gaps in the intelligence collection.

Steps for analyzing and prioritizing intelligence typically include:

- Determining applicability of the threat to your environment (e.g. is the impacted software version in your ecosystem?)
- Identifying the date and time of the last known threat exploit within cyber landscape
- Determining whether the threat has been seen in the relevant environment
- Documenting potential impact of the cyber threat on vehicle ecosystem throughout the product lifecycle
- Identifying potential vectors for cyberattack. (e.g. physical access, Bluetooth, cellular)
- Evaluating the reliability of the data sources from which the search criteria would generate results (e.g. CAN log, diagnostic data, IDS)
- Considering the capabilities and limitations of each intelligence source (e.g. sources with limited capability, or restrictions to consumption or funding may influence prioritization)
- Using normalized nomenclature of technical systems to account for regional vernacular, colloquialisms, and acronyms; as well as foreign scripts
- Considering the input and contribution of technical SMEs and consumers to help ensure the most relevant coverage

The results of analysis and prioritization are typically documented in a threat intelligence repository. Using a common repository or documentation process enables ease of tool integration and intelligence sharing. Areas of focus for documenting intelligence into any repository include:

- Identify and enumerate assets: To have a heightened awareness of threats by characterizing for value and risk
- Tag entries: To enable integration and analytics across tools (examples include threat type, adversary attribution, associations to incidents or other threats, CVE).
- Describe reliability: To validate the threat information (examples include confirmed by independent sources, plausible, logical).

- Rate threat severity: To understand impact. Consider the capability of the threat/adversary, focus or persistence of the threat, and indicator relation to the attack cycle (i.e., beginning or end).

Organizations can leverage threat intelligence to detect and address attacks as well as enrich analysis during the incident response process. (See the Auto-ISAC's *Incident Response Best Practice Guide* for more information)

2.4 BEST PRACTICES FOR THREAT MONITORING PROCESSES

Appropriate processes support monitoring of sources and data for new threats. To effectively create intelligence monitoring processes, organizations may define the threat areas with the most significant risks to the business, and then focus processes and techniques on monitoring threat intelligence related to those areas. Processes to monitor sources and gather new information typically are flexible because vehicle cybersecurity risks are constantly evolving because of advancing vehicle technologies and an increase in sophistication among threat actors.

Since threat intelligence monitoring for vehicle cybersecurity shares many common practices with enterprise cybersecurity, it can be good practice to use existing enterprise processes as an initial guideline when developing vehicle threat monitoring techniques. There are, however, some differences between the skills and knowledge needed for vehicle threat intelligence monitoring and those needed for enterprise threat intelligence monitoring. Thus, it is also good practice to develop additional awareness and training content that is unique to each.

2.4.1 Defining Priorities for Monitoring

Defined and prioritized threats provide the foundation for monitoring new threat intelligence to protect the vehicle ecosystem. Once threats are prioritized, an organization can begin monitoring intelligence sources for new information on those defined and prioritized threats. This will help enable effective alignment of available, and often limited, resources.

Prioritizing threats for intelligence monitoring can be informed by analysis of an organization's threat tolerance to known and emerging threats within the automotive threat environment. When determining threat tolerance, organizations may use the following considerations to evaluate and prioritize intelligence topics for monitoring:

- The imminence of an attack by the threat (e.g. current attack, private disclosure)
- The severity of an attack by the threat (e.g. safety impact, privacy)
- The scope of an attack by the threat (e.g. single vehicle, few older vehicles, fleet)
- The ease of asset exploitation by the threat (e.g. few skills needed, exploit exists)
- The organizational risk the threat may pose due to an attack
- The financial risk the threat may pose due to an attack
- The practicability of an attack by the threat (e.g. remote attack vector versus physical attack vector)

Prioritizing threat intelligence areas and the resulting impact severity of an attack has multiple increasingly granular criteria, including:

- If an event related to the threat intelligence could pose safety risks to customers

- If an event related to the threat intelligence would have impacts onboard or offboard the vehicle
- If an event related to the threat intelligence may cause risk of PII data leaks
- If an event related to the threat intelligence would affect mobile or portal application features
- The resulting number of vehicles that would be affected by an event related to the threat intelligence
- The fix time associated with a threat event related to the threat intelligence
- The incident response effort associated with an event related to the threat intelligence
- The potential legal, regulatory, or disclosure requirements
- The resulting cost that would be associated with an event related to the threat intelligence
- The resulting negative publicity impact that an event related to the threat intelligence may cause

2.4.2 Threat Monitoring Techniques and Approaches

Organizations may use threat monitoring techniques and approaches based on their risk tolerance and existing capabilities. If an organization does not have the capabilities to meet their needs, they may also partner with another organization to collect and aggregate relevant threat data.

While collecting threat data and developing monitoring techniques, organizations may gather techniques and methods for how attackers are operating in the vehicle environment, as these discrete data points could have value. Knowledge of known techniques, in conjunction with data points available to an organization's unique environment, may allow the security teams to build detection models. Based on defined priorities for threat monitoring, organizations can implement threat monitoring techniques to maintain awareness of new threat information.

2.5 BEST PRACTICES FOR THREAT ANALYSIS

Teams leverage the collected data for threat analysis. Threat analysis allows for the identification, validation, and verification of threats. From validated threats, threat events can be detected, and response strategies to those events can be informed with threat intelligence.

2.5.1 Threat Event Identification

Organizations may implement techniques to detect the presence of threats within the vehicle ecosystem based on defined priorities for monitoring threats and gathered intelligence on associated threats to the vehicle ecosystem. Some techniques and approaches for threat identification in the vehicle ecosystem include:

- Monitoring diagnostic error codes
- Using intrusion/anomaly detection systems
- Monitoring back office/SYSOPS operations
- Monitoring connections to the vehicle

Similarly, techniques and approaches for threat identification within the vehicle fleet may include:

- Logging data collected by fleet monitoring systems to a centralized repository and maintaining the data in a useable format that is in accordance with a data retention plan

- Logging interactions between back office systems used for fleet monitoring activities and vehicle systems to a centralized system, with the logged data containing actions taken and timestamps
- Employing data analysis to monitor performance and compliance of in-vehicle network communications to design parameters
- Developing use cases that describe how collected data can be used to alert on identified threats

The use of these techniques may be facilitated by a cross functional team approach with monitoring techniques used by multiple teams and stakeholders. The overall efforts may be coordinated through a vehicle security operations center (VSOC). The VSOC is typically a centralized unit that deals with vehicle security issues on an organizational and technical level. The VSOC may monitor for high priority incident tickets raised automatically by the system or by an individual group using threat identification techniques, then escalate the incident tickets as necessary. The VSOC could assist in the escalation process (and event closures) for identified threats and security events within the vehicle ecosystem by:

- Triaging incident tickets for technical and business impact
- Assessing business impact to determine priority of an incident
- Driving incident process escalations and communications for high priority incidents
- Reviewing and accepting incident tickets and transferring wherever appropriate

A common challenge faced when defining an approach and appropriate techniques for threat identification is accounting for false positive threat identification and the overall effectiveness of the techniques against real world threats. Organizations can integrate considerations for false positive threat identification when designing threat monitoring techniques. The design considerations may include:

- Erring on the side of safety and privacy
- Being able to perform a controlled test to verify the systems and processes are working properly

One additional consideration when implementing threat identification techniques is how to classify and manage access to threat identification solutions and products within the organization. There are at least two options for managing access to threat identification information. One option is to create one access level for the engineering team, and a second access level for everyone else. Another option is to manage access based on user levels, and then use a “need to share” model, meaning the most information possible is shared. This “need to share” model may be used in contrast to a “need to know” sharing model, which involves withholding the most information possible.

2.5.2 Validation and Verification of Identified Threats

Organizations may validate and verify threats in different ways. Some companies may define a structured process to collect data points and analyze them to validate any threats in the vehicle ecosystem. Others may develop criteria for triaging security events with the relevant IT or engineering teams. Some companies may also consider providing escalation paths for the VSOC team to gather additional data if needed.

Some organizations may benefit from developing methods for generating security events with appropriate details for testing the full security event detection lifecycle. For example, organizations may want to have a way to trigger a system to cause the detection systems to believe a true security event has occurred. It is recommended that testing be continuous to help ensure that detection systems are operating as designed.

After security events are detected and escalated, it is generally a good practice to track the lifecycle of these events. This process may allow for the tracking of documentation, information of interest, and any communications that occur as part of the security event lifecycle.

2.5.3 Taking Necessary Action

Threat identification, validation, and verification allows an organization to appropriately target and prioritize threats that may warrant development of response strategies. Threat response strategies typically leverage internal product inventories, third-party support, and internal teams responsible for coordination and strategy.

Cross referencing threat intelligence with internal inventories of internal assets, such as hardware bill of materials, software bill of materials, and VINs allow organizations to quickly identify vehicles affected by validated threats. A best practice is for organizations to have a thorough asset inventory list that can be used to speed up processes to identify the root cause of potential cyber events and contact appropriate supply chain partners as necessary. Additionally, thorough lists provide organizations confidence that the potential impacts of identified and validated threats are reasonably understood.

In addition to development of a thorough inventory list, maintaining the list is also important. Over time, inventory lists often become fragmented when project managers leave companies, resulting in legacy hardware and software inventories existing only on isolated spreadsheets. Organizations that do not have a methodology to track this information may leverage partnerships to obtain strategies that have worked well for other firms.

2.6 BEST PRACTICES FOR INFORMATION ORGANIZATION, STORAGE, AND SHARING

Much of the information generated as a byproduct of program requirements such as definitions, intelligence gathering, threat monitoring, and threat analysis is valuable to the organization, as well as its threat detection and response programs. Information can be organized, stored, and shared appropriately to inform future decisions in the threat detection and response program by using historical trends and results. Types of information to organize and store include:

- Threat actors
 - Name or identifier
 - Threat actor description
 - Source of primary threat actor intelligence (i.e., point of contact to help refresh data periodically)
 - Observed tactics, techniques, and procedures (TTPs)
 - Associated internet protocol (IP) addresses and assets
 - Threat events each actor is associated with
- Threat events
 - Affected systems
 - Affected system suppliers and product owners

This Guide does not prescribe or require specific technical or organizational practices. These are voluntary and aspirational practices, which may evolve over time. Please see Section 1.2 for more information.

- Threat event risk assessments
 - Associated references to vulnerability management systems
- Threat intelligence requirements
 - Source of collection requirements
 - Reference to risk or threat that each requirement is intended to address
- Threat monitoring
 - Data associated with monitoring requirements
 - Data associated with monitoring performance (false positives/negatives)
 - Data associated with performance of threat intelligence sources
- Any associated timestamps, coordinated in a way that events from disparate systems can be correlated to each other (e.g. universal time code)

2.6.1 Key Considerations for Information Storage and Organization

When defining steps to store threat detection and analysis information, organizations might want to consider several factors such as types of data, storage methodology, and length of period for storage.

The first decision organizations could make is how to securely store and manage access control to threat detection and analysis information. Steps for securely storing sensitive data and managing access control include:

- Developing a process for vetting and authorizing new access requests to the data
- Periodically auditing the authorized individuals to help ensure their access is still required
- Limiting access to the data to only those individuals that are providing updated data or need to query the data
- Limiting data modification capabilities to only those that require the need to modify the data
- Maintaining logs of data queries and modifications
- Ensuring high availability and disaster recovery
- Implementing encryption protocols
- Using an information classification system
- Giving more recent events priority over older events prior to overwriting or rollover
- Summarizing events (e.g. counts) prior to overwriting or rollover
- Implementing controls (e.g. digital signatures) to protect the integrity of event data while stored onboard and offboard
- Using a store-and-forward approach to cope with network availability issues
- Defining retention and backup requirements

Following storage, information can be organized to allow organizations and teams to effectively use it. A best practice for information organization is to define key process indicators using available information, and then create dashboards and reports to enable future analysis of stored information. Organizations may consider integrating this information into their vulnerability management and incident response processes. This will enable more rapid and accurate data access during an incident. It also makes the collating of information more efficient if all systems are using the same terminology and object models.

2.6.2 Approaches for Internal and External Sharing

Threat detection and analysis information may be shared and used across the organization to help ensure thorough analysis. Intelligence adds value when shared to assist with operational or strategic decisions. Actionable intelligence is especially useful if a threat is active. (See the Auto-ISAC's *Risk Assessment and Management Best Practice Guide* for more information). Some considerations for organizations when defining how and what information to share are:

- How to determine if information can or should be shared
- Approval process (if applicable) to share information internally and/or externally that could include: legal, safety, communications, and in-vehicle Subject Matter Experts (SME)
- Audiences for the type of information to be shared
- Mechanisms for distribution of information to approved parties
- Negotiating a common format for sharing information in advance of sharing (e.g. tagging or prioritization) (See Section 2.3.3)

Possible mechanisms for internal and external sharing of information include:

- Newsletter summaries with appropriate email distribution published daily or weekly with special alerts as needed
- Reoccurring staff meetings for cybersecurity stakeholders or cross functional staff to update and exchange information
- Dedicated internal website or portal
- Auto-ISAC portal
- Chat room alerts
- Providing feedback to intelligence sources related to quality of intelligence received
- Utilizing existing corporate/organizational communication platforms for sharing updates
- Incorporating information into training and awareness materials
- Sending information out to appropriate organization members on a regular cadence (e.g. monthly, quarterly) providing awareness information, industry updates around threats, information location, and communication contact points.

Some internal stakeholders that may find intelligence valuable when shared include:

- Customer care and aftermarket teams: Data may allow analysis of user behavior, consistent with privacy policies, to prevent fraud, abuse, or exploit.
- Joint ventures and subsidiaries: May benefit from appropriate collection requirements and compartmentalization in each environment or region.
- Legal and public relations: May benefit from compliance requirements in each environment or region.
- Other internal teams: Share awareness and knowledge (e.g. threats, suspicious chatter, inquiries from researchers, reverse engineering that might result

In addition to defining how an organization is going to share information, they may define how to properly handle such information. An organization may define the specific data handling procedures that accompany certain types of data labels. Distributors of the sensitive information should take steps to help ensure that those receiving any information are aware of their duty to protect the sensitive information.

Appendix A: Glossary of Terms

Relevant terms used in this Guide are defined below.

TERM	DEFINITION
Attacker	Individual, group, organization, or government that conducts / has the intent to conduct an attack.
Attack Vector	A path or means by which a threat actor can gain access to the networks or assets to deliver a malicious outcome.
Attack Path	A possible way in which a threat could reach the asset
Bill of Materials (BOM)	A list of the raw materials, sub-assemblies, intermediate assemblies, sub-components, and the quantities of each needed to manufacture an end-product.
Future Vehicle Designs	Future vehicle models that are in the design phase and have not started development. These may be on the roads in the next 3-5 years, or longer.
Impact	Estimate of magnitude of harm to stakeholders originating from a threat and/or attack
Penetration Testing	The practice of testing a system, network or application to find vulnerabilities that a threat actor could exploit.
Post-Production Vehicle	Vehicles that have been produced and sold to a dealer or end customer and are outside the OEM's ownership.
Risk Profile	An evaluation of a company's risks, including the number of risks, type of risk, and potential effects of risks.
Risk Tolerance	The threshold of risk that an organization or individual is willing to accept without some form of response.
Threat	Any circumstance or event with the potential to adversely impact the vehicle ecosystem through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.
Threat Actor	A person or entity posing a threat to the vehicle ecosystem.
Threat Event	An event or circumstance, perpetrated by a threat actor, that has the potential to cause a negative impact to the vehicle ecosystem.
Threat Event and Actor Analysis	A method used in the risk assessment process in which a company identifies, analyzes, assesses, and prioritizes potential threat events to a system, including an analysis of the threat actors and attack vectors.
Vehicle Cybersecurity Risk	The likelihood of and potential impact from the exploitation of a vehicle ecosystem cybersecurity vulnerability in a threat event.
Vehicle Ecosystem	The components and infrastructure on or connected to the vehicle (e.g. hardware and software, intellectual property, mobile applications, customer data, vehicle data, supplier/manufacturing networks, applications, processes and organizations that directly or indirectly touch the vehicle and may play a role in vehicle cybersecurity).
Vehicle in Development	Vehicles currently being developed or in production that may be on the roads within the next 3 years.
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats.

Appendix B: Additional References and Resources

The following References and Resources provide additional content and expertise for companies to consider in conjunction with the Best Practices discussed in this Guide.

REFERENCES – DOCUMENTS THAT MAY OFFER ADDITIONAL IMPLEMENTATION GUIDANCE
ISO/SAE 21434 - Road Vehicle Cybersecurity Engineering Standard (under development) < link >
NIST SP 800-30 - Guide for Conducting Risk Assessments < link >
SAE J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems < link >
NIST Cybersecurity Framework < link >
ISO/IEC 15408 – Information Technology - Security Techniques < link >
ISO/IEC 17799 – Code of Practice for Information Security Management < link >
ISO/IEC 27001 – Information Security Management Systems - Requirements < link >
ETSI Cyber Security Technical Committee (TC CYBER) ETSI TR 103 456 – Implementation of the Network and Information Security (NIS) Directive < link >
ISO 31000:2009 – Principles and Guidelines on Implementation < link >
DOT HS 812 073 – NIST Cybersecurity Risk Framework Applied to Modern Vehicles < link >

RESOURCES – ORGANIZATIONS THAT MAY OFFER ADDITIONAL INSIGHTS
International Organization for Standardization (ISO) < link >
National Institute of Standards and Technology (NIST) < link >
National Highway Traffic Safety Administration (NHTSA) < link >
PMI PMBOK Guide < link >
SAE International < link >
Institute of Risk Management (IRM) < link >
ISA/IEC 62443 Cybersecurity Certificate Programs < link >

Appendix C: Acronyms

Auto-ISAC	Automotive Information Sharing and Analysis Center
CIA	Confidentiality, Integrity, and Availability
CERT	Computer Emergency Readiness Team
CISCP	Cyber Information Sharing and Collaboration Program
CVE	Common Vulnerabilities and Exposures
DHS	Department of Homeland Security
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IRM	Institute of Risk Management
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
NCICC	National Cybersecurity and Communications Integration Center
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OT	Operational Technologies
PII	Personally Identifiable Information
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
SAE	Society of Automotive Engineers
SME	Subject Matter Expert
TLP	Traffic Light Protocol
TTP	Tactics, Techniques and Procedures
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team



THREAT DETECTION, MONITORING & ANALYSIS

Traffic Light Protocol: White (May be shared in public forums)

VSOC

Vehicle Security Operations Center