Driving Automotive Cybersecurity Forward

Simplifying Security Collaboration: VicOne and Block Harbor Unite to Bridge the Gap Between VSOC and PSIRT/Engineering Teams

Imagine a future where automakers and suppliers are collaborating at a high frequency to release updates to vehicles. A new cybersecurity event in production and operations means a new security fix must be rolled out — just like with smartphones and other IoT devices. How quickly can the monitoring team navigate the complex network of affected parties to deploy a security patch?

Driving Value by Rethinking Vehicle Security

In the automotive industry, ensuring the cybersecurity of vehicles and their associated systems has become paramount. To achieve this, automakers often employ a vehicle security operations center (VSOC) framework, drawing inspiration from traditional IT security practices for incident detection and response. However, vehicles present a significantly more intricate challenge than conventional digital systems. In this context, the concept of a VSOC takes on a different dimension, focusing on specific, value-added use cases aimed at safeguarding revenue streams, business reputation, and operations, rather than just purely detecting real-time cyberattacks against cars. We highlight a few of those:

- **Detecting vehicle tampering for financial gain, such as odometer rollback and unlocking of paid features.** In 2023, odometer fraud has emerged as a significant US$1 billion problem in the US. This form of deceit causes buyer losses and market trust issues. Additionally, with the rise of subscription services, the need to unlock premium features is likely to grow. Recently, researchers at the Technical University of Berlin successfully jailbroke a popular electric car company's in-vehicle infotainment (IVI) system. They demonstrated the ability to adjust a compromised vehicle's settings — including for the purpose of unlocking paid features — and gain access to stored credentials within the IVI system.

- **Detecting abuse of off-board APIs causing operational disruption.** In 2022, incidents involving a vulnerability in the remote vehicle management services of a telematics and infotainment service provider and an attack on a taxi hailing app raised public awareness about the potential for attackers to remotely unlock and start connected cars by abusing off-board APIs. In the taxi app's case, attackers sent dozens of cars to a specific location, leading to a massive traffic jam in Moscow that lasted for up to three hours.

- **Detecting software rollback or replacement on vehicles.** In an experimental case in 2020, researchers successfully injected malicious code that made the compromised IVI system automatically connect to a rogue Wi-Fi hotspot, enabling them to inject malicious CAN messages and make a car perform diagnosis without authentication.

- **Detecting design flaws leading to risk of car theft.** A popular challenge trend that had been making the rounds on TikTok since 2021 led to a settlement in 2023 that had the affected automakers paying an expected US$200 million. This compensation came as roughly 9 million primarily base trim vehicles were affected. Separately, a car theft incident in 2022 underscored the applicability of the "CAN injection" technique across numerous car models.
- **Detecting car owner personally identifiable information (PII) or privacy data leak affecting business reputation.** According to a recent study by the Mozilla Foundation, all 25 researched car brands received a "Privacy Not Included" warning; the foundation's findings label these vehicles a "privacy nightmare." This indicates concerns regarding extensive data collection in modern vehicles and the adequacy of security measures. In April 2023, Reuters reported that between 2019 and 2022, former employees of a prominent electric car company shared intimate footage of car owners, recorded by built-in cameras, through a private internal messaging system. This incident could lead to the public losing trust in their cars.

Analyzing Incidents: Collaborative Root Cause Investigation

Each automaker will have different use cases based on its own business priorities, and it will set up systems to monitor these use cases. However, the question always arises: *Once a use case is triggered, now what?* Many automakers set up a completely separate VSOC team that is focused purely on monitoring. But now that they're facing a cybersecurity incident, they're liable for it. We walk through the process of how it may be handled:

- **Detect:** When the VSOC platform identifies a persistent attack on the vehicle through its monitored use case, it collaborates with the on-board intrusion detection or prevention system (IDS/IPS) to gather detailed information and correlate vehicle telemetry data to trigger an alert and notify the VSOC team. The VSOC team then begins a quality assessment of the incident to determine if it is a real issue.
- **Analyze:** Once the VSOC team confirms the incident's severity, it escalates the incident to the product security incident response team (PSIRT) for root cause analysis. This involves engaging various stakeholders, including different feature teams, different engineering teams, and external module suppliers associated with the affected components. Each of the stakeholders then follows their cybersecurity engineering processes, often based on ISO/SAE 21434, to independently develop a solution, which may include a software update or security patch for the vehicle.
- **Respond:** The developed solution undergoes thorough testing to ensure its effectiveness and reliability before being released via over-the-air (OTA) update.
- **Recover:** Once the system has been patched, it is restored to its original condition. The VSOC team continues to monitor for any future use case anomalies.

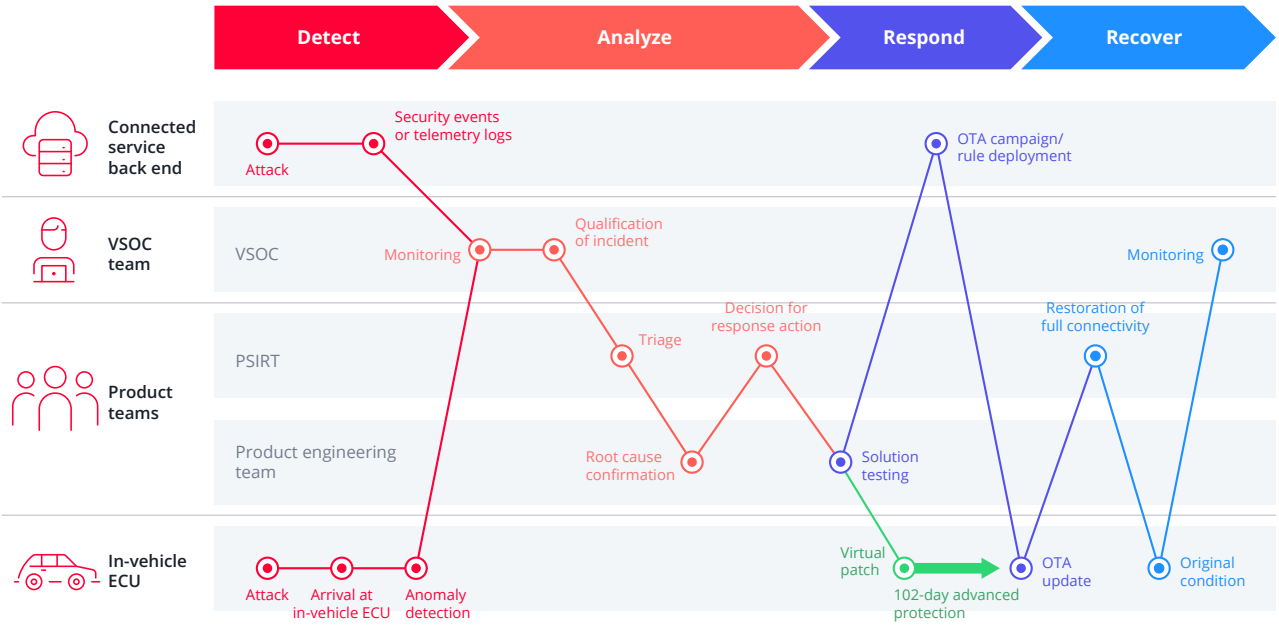

Figure 1. A process of handling a cybersecurity incident involving the VSOC and PSIRT/engineering teams

Challenges for VSOC and PSIRT/Engineering Teams

In the above process, we observe that the VSOC team and the product teams, such as the PSIRT and the product engineering team, have to work together to take action when incidents occur — even between different organizations, such as an automaker (OEM) and its suppliers. However, in reality, there are some challenges:

- **From the VSOC team's perspective**
  - **Alert overload:** Chasing false alarms distracts the VSOC team from more serious events. The team often receives a large volume of security alerts from various security tools and systems. The team might struggle to manage this influx, and many of the alerts might turn out to be false positives — especially since most detection tools in the market use only machine learning–based anomaly detection, leading to alert fatigue and potentially missing real threats. Given a scenario where the number of monitored vehicles exceeds one million, if each vehicle triggers a security alert, it means over a million alerts will come.
  - **Total impact measurement challenge:** In the fast-paced environment of the VSOC team, accurately measuring the total impact of an incident is a constant struggle. The team grapples with the question of whether a threat has the potential to affect multiple vehicles. Only after this determination can the team proceed with the proper escalation to engage the right parties.
  - **Evolving threat landscape:** The threat landscape is in a perpetual state of evolution, as attackers constantly employ new tools and techniques. The VSOC team must continuously adapt, learning and upgrading their skills to effectively combat emerging threats.

- **From the PSIRT and engineering team's perspective**
  - **Complex system impact assessment challenge:** When the VSOC team has identified a threat, the next challenge for the PSIRT is to identify which vehicles, components, and suppliers are affected, and what the contractual provisions are for ongoing supplier cybersecurity support. The task of gathering necessary contacts alone is a formidable challenge. Assuming successful contact, both within the OEM's team and the involved suppliers, there is an urgent call to prioritize the fix.
  - **Fear of delays in taking action:** Every minute that passes after identifying the issue and recognizing its potential exploitability carries immense significance. The implications are wide-ranging, from potential safety risks for road users to potential revenue loss for the automaker if a feature becomes freely accessible. Failing to convey actionable information clearly and promptly from the VSOC team could lead to costly delays. This back-and-forth exchange often results in muddled or misunderstood details. Moreover, the failure to promptly triage and conduct a thorough root cause analysis opens the door for attackers to exploit further, potentially causing severe damage to systems.
  - **Navigation of stakeholder dynamics:** The pivotal issue at hand is establishing the timeline for implementing the necessary fix. Given the extensive involvement of multiple stakeholders, expeditiously deploying routine security updates becomes a daunting task. The urgency of generating and releasing a patch cannot be overstated; any delay in this process could leave vulnerabilities exposed, potentially inviting further breaches. It raises the question: Are there contingency measures in place that can temporarily thwart exploitation while the patch is being developed and serve as a stopgap before the patch is fully deployed?
  - **Data availability concerns:** After resolving the current issues, the VSOC team must now transition to a phase of proactive monitoring. This raises important questions: Does the team have the required data, based on past experiences, for timely detection? Are there any needs for acquiring new data feeds? This stage marks the initiation of planning for the next steps.

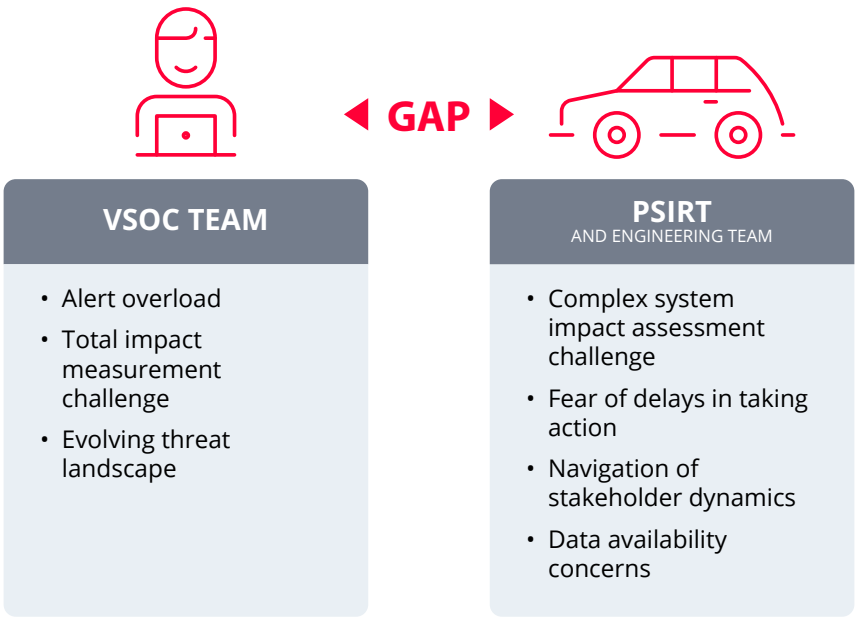

Figure 2. The VSOC–PSIRT/engineering teams gap

Enhancing Security Through VSOC–PSIRT/Engineering Teams Synergy

To assist OEMs in effectively tackling the aforementioned challenges, VicOne and Block Harbor have joined forces to offer an integrated solution for OEMs. This collaboration seeks to bridge the gap between the VSOC and product teams, ensuring timely response to threats by enhancing communication and bolstering trust through the provision of detailed information and facts:

1. **Accelerate incident qualification with actionable intelligence.**

   To accelerate the VSOC team's analysis and progress toward a solution, our VSOC platform filters out low-confidence alerts. This way, the VSOC team can concentrate its efforts on the most critical issues.

   Our extended detection and response (XDR) platform, xNexus, goes the extra mile to reduce noise and deliver precise and explainable detection results. Unlike solutions in the market that rely solely on machine learning (ML) techniques, inundating VSOC teams with overwhelming and unexplainable anomaly events, xNexus connects various data points from vehicle on-board electronic control units (ECUs), telemetry sensors, and cloud services. It provides full, end-to-end visibility and actionable intelligence when managed fleets and their ecosystem are at risk of cyberattacks.

   With our up-to-date detection engines, we correlate scattered anomaly events to form an "attack story," surpassing our competitors. We transform this attack story into precise detection rules, allowing xNexus to achieve high detection engine accuracy. It also provides a comprehensive visual representation of the attack context across different ECUs, enabling rapid investigation and proactive threat mitigation. This means identifying potential threats even before the attack chain is completed.

   Thanks to the expertise of Block Harbor in designing vehicle cybersecurity architectures, white hat hacking, and penetration testing, in combination with VicOne's over 30 years of threat intelligence, we maintain continuous monitoring of threats and consistently improve the accuracy of our detection engines over time.

   Additionally, once malicious threats are detected, VicOne's xCarbon IDS/IPS solution transmits the detection logs and system telemetry back to xNexus. This allows for the identification of each observed attack tactic, technique, or procedure (TTP) and compromise event, showing attack timeline and attack path details for the VSOC team to perform early weakness and vulnerability assessments. To optimize bandwidth usage and save costs, xCarbon reports only high-confidence alerts to xNexus.

   In this manner, the VSOC team can correlate all the information and provide straightforward mitigation recommendations. Along with the ticket, the team will forward them to the PSIRT. Once a weakness or vulnerability has been confirmed due to an observed attack TTP or compromise event on xNexus, the VSOC team can generate a ticket, including mitigation recommendations from xNexus, to be sent to Block Harbor's Vehicle Security Engineering Cloud (VSEC).

2. **Accelerate root cause confirmation with VSEC.**

   After the vetted ticket arrives at VSEC with the appropriate information, the PSIRT or engineering team can assign it to potentially affected products or platforms. VSEC provides a repository for sharing component, system, and vehicle information, ensuring that the relevant parties, including the entire supply chain, can be promptly notified of any potential impact. It assists the user in effectively monitoring new and ongoing cybersecurity events, providing the necessary documentation in compliance with ISO/SAE 21434.

As an engineering platform, VSEC also provides access to tools necessary to design and verify updates quickly, including those used in organizing complex vehicle cybersecurity data, performing threat analysis and risk assessment, and automating cybersecurity testing. VSEC equips the PSIRT and engineering team with a singular platform to help address communication and engineering inefficiencies that might slow down the release.

By keeping track of VSOC incidents alongside other vehicle cybersecurity engineering data such as vehicle cybersecurity test results, culture metrics, and design risks, VSEC provides a complete picture of vehicle cybersecurity from an engineering perspective, allowing the VSOC team to focus on its core activities.

3. **Quickly mitigate the risk before vendor patch.**

The urgency of generating and releasing a patch is paramount. Delays in this process could leave vulnerabilities exposed, potentially inviting further breaches. To address this, the combination of the xNexus VSOC platform and the xCarbon IPS offers a solution that provides patent-pending virtual patches for effective postproduction mitigations. By leveraging virtual patching, xCarbon enforces attack signatures and security rules, allowing OEMs to protect their systems without making any changes. This approach provides an average of 102 days of protection while waiting for a vendor patch to become available. This capability helps block zero-day exploits and gives OEMs more time to develop mitigation plans and solutions.

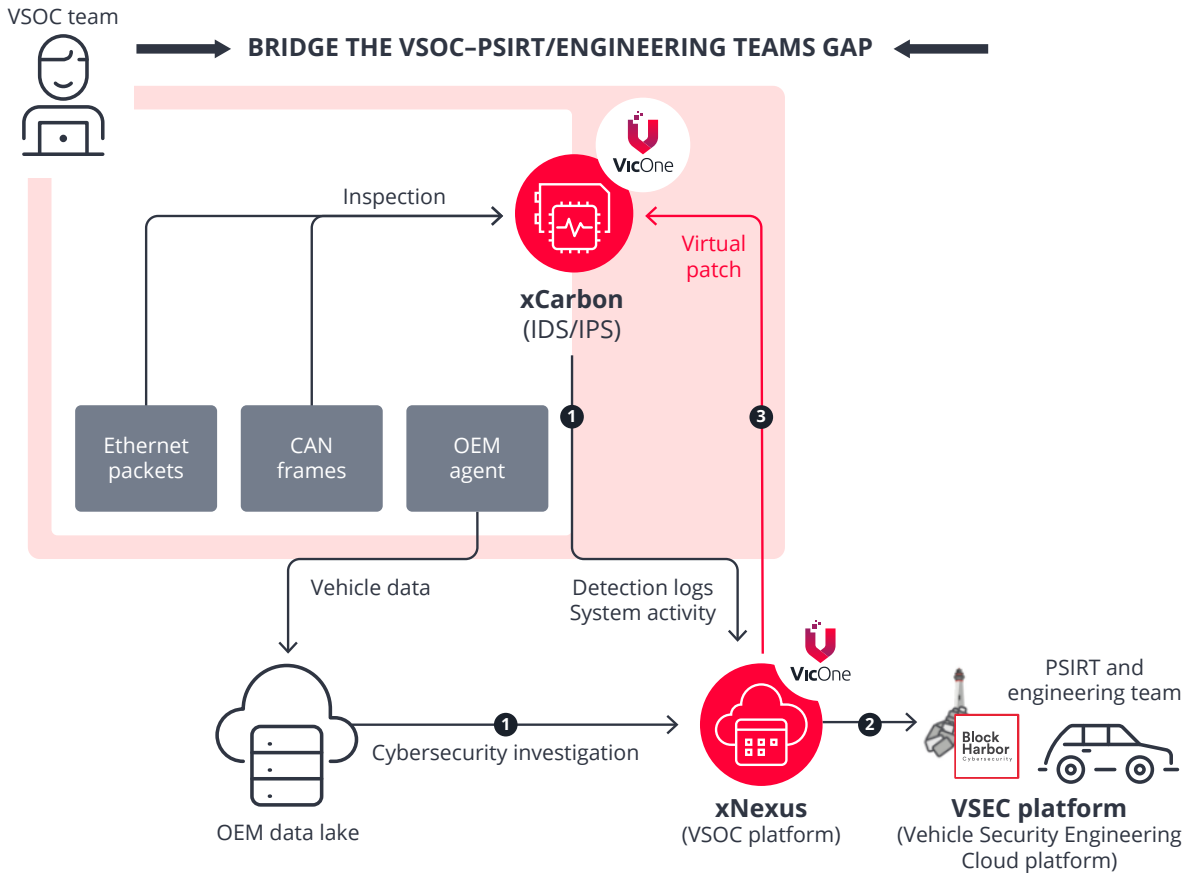

Figure 3. Bridging the VSOC–PSIRT/engineering teams gap with VicOne and Block Harbor

Use Case: Continuous Monitoring in Peacetime

In peacetime, xNexus serves as an informative threat intelligence knowledge base, consolidating diverse sources along with the dedicated insights of VicOne's threat researchers. This encompasses detailed information on attack vectors, attack paths, TTPs, and more. It provides security analysts and relevant users with a streamlined approach to monitor global cybersecurity events pertaining to vehicles.

Unlike other solutions that provide only incident news with no actionable insights, our solution can provide impact assessment. This is important since when an incident occurs, users crave immediate answers to questions such as "What happened?" and "How does it affect me?" Our solution satisfies these inquiries by delivering the latest cyber incident information and comprehensive automotive attack mapping, inspired by the MITRE ATT&CK® framework. With just one click, users can gain immediate actionable insights on "How close are we to a severe attack?" Our solution empowers users to assess risks associated with incidents across the entire connected car ecosystem and identify vulnerable car models. Combined with the advanced knowledge stored within Vehicle Breakdowns in VSEC, such as firmware versions, system names, component names, and other key elements relevant to a vehicle platform, xNexus' threat detection can be tuned in real time to ensure both more accurate and more detailed threat information.

Use Case: Empowering Tier 1 Suppliers

Our integrated solution can also benefit Tier 1 suppliers as xNexus can be used more as a "product SOC" than as a VSOC. Tier 1 suppliers do not monitor live systems, but they may monitor their "product-level" units for threats. The goal is to help Tier 1 suppliers improve product quality and help them respond to OEMs when a weakness or incident is reported, because we know that they want to find issues *before their customers do*.

For example, if an OEM learns of a vulnerability in a Tier 1 supplier's module, the OEM will categorize this as a quality/warranty event and likely demand that the supplier provide a fix within a certain time frame. If the supplier learns of the issue ahead of the OEM, it can plan accordingly and present a complete action plan to the OEM, resulting in less friction and the OEM's being more likely to adopt the supplier's suggestion. Here is how our integrated solution can help the Tier 1 supplier shift its approach from reactive to proactive:

- The Tier 1 supplier can use VSEC vehicle breakdown information to automatically match relevant threat intelligence information from xNexus. When a threat event is matched, xNexus will push the threat intelligence to VSEC, allowing the supplier to intelligently filter and focus on potentially affected components from its portfolio based on known information about the threat, such as the vehicle model and year, the affected component or supplier information, the TTPs used in the attack, and the exploited vulnerabilities.
- VSEC enables the users to perform many of the activities and generate work products required by ISO/SAE 21434. With this threat intelligence feed, the supplier now has an all-in-one place for various activities, including ongoing monitoring. A single, central spot for maintaining the cybersecurity life cycle of the module gives the supplier an elegant and simple solution — from engineering to production.

Conclusion: Bridging the VSOC–PSIRT/Engineering Teams Gap

This collaboration highlights these major advantages:

- **Actionable intelligence sharing for both the VSOC team and the PSIRT:** Swift analysis and coordination within the VSOC team accelerates the resolution process. Clear and concise information from the VSOC team ensures prompt and effective action from the PSIRT and the rest of the cybersecurity organization. This reduces delays, preventing further exploitation and minimizing potential damage.
- **Proactive issuance of potential threat alerts *before* the completion of the attack path:** Our solution enables rapid investigation and response by visualizing the attack path across multiple layers and ECUs. This perspective empowers users to swiftly comprehend the attack context, uncover relationships, and assess the potential scope of impact. Through correlation visualization, users can seamlessly transition from identifying the source of abnormal activities to understanding the motives behind them.
- I**mproved incident qualification and impact assessment:** Having metrics, clear criteria for event priority and impact assessment, and most importantly, visibility into all affected components on a platform or in a product portfolio helps the PSIRT quickly assess the severity of the situation, connect with stakeholders, and initiate necessary action to create a fix. The visibility into all available information streamlines root cause analysis and prevents misdirected efforts.
- **Adaptive expertise:** Continuous learning and skill upgrading in response to an ever-evolving threat landscape enhances the VSOC team's effectiveness in countering emerging security challenges.
- **102-day advanced protection:** By utilizing our in-vehicle IDS/IPS, automakers can leverage our patent-pending virtual patching technology to provide distributed virtual patch protection for vehicle vulnerabilities within 14 days. This grants them an average of 102 days of protection and ensures issue resolution with minimal system changes.

To learn more about VicOne's solutions and partnerships, contact our experts and schedule a demo at vicone.com/contact-us.

To learn more about Block Harbor's solutions, reach out at blockharbor.io/contact-us.