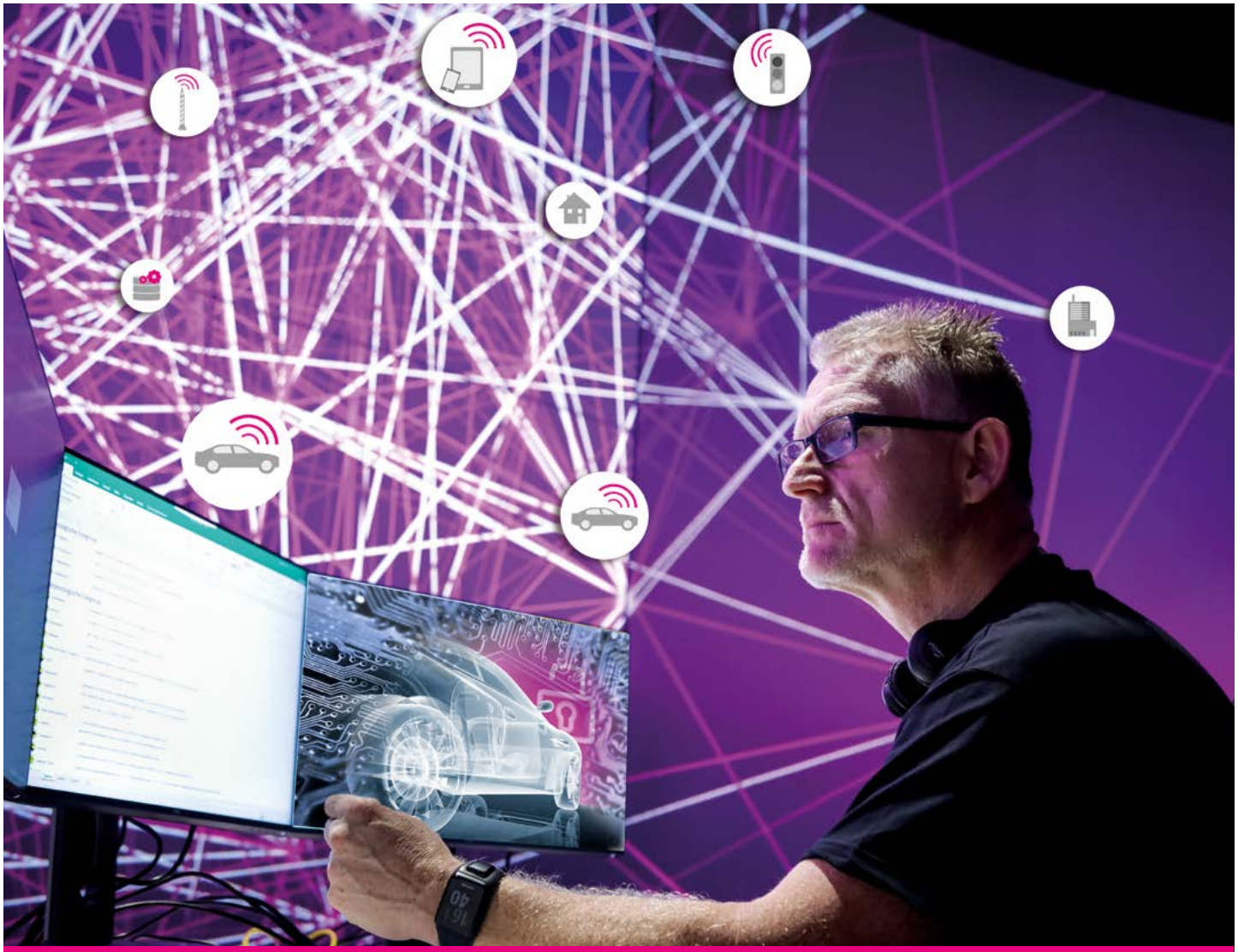
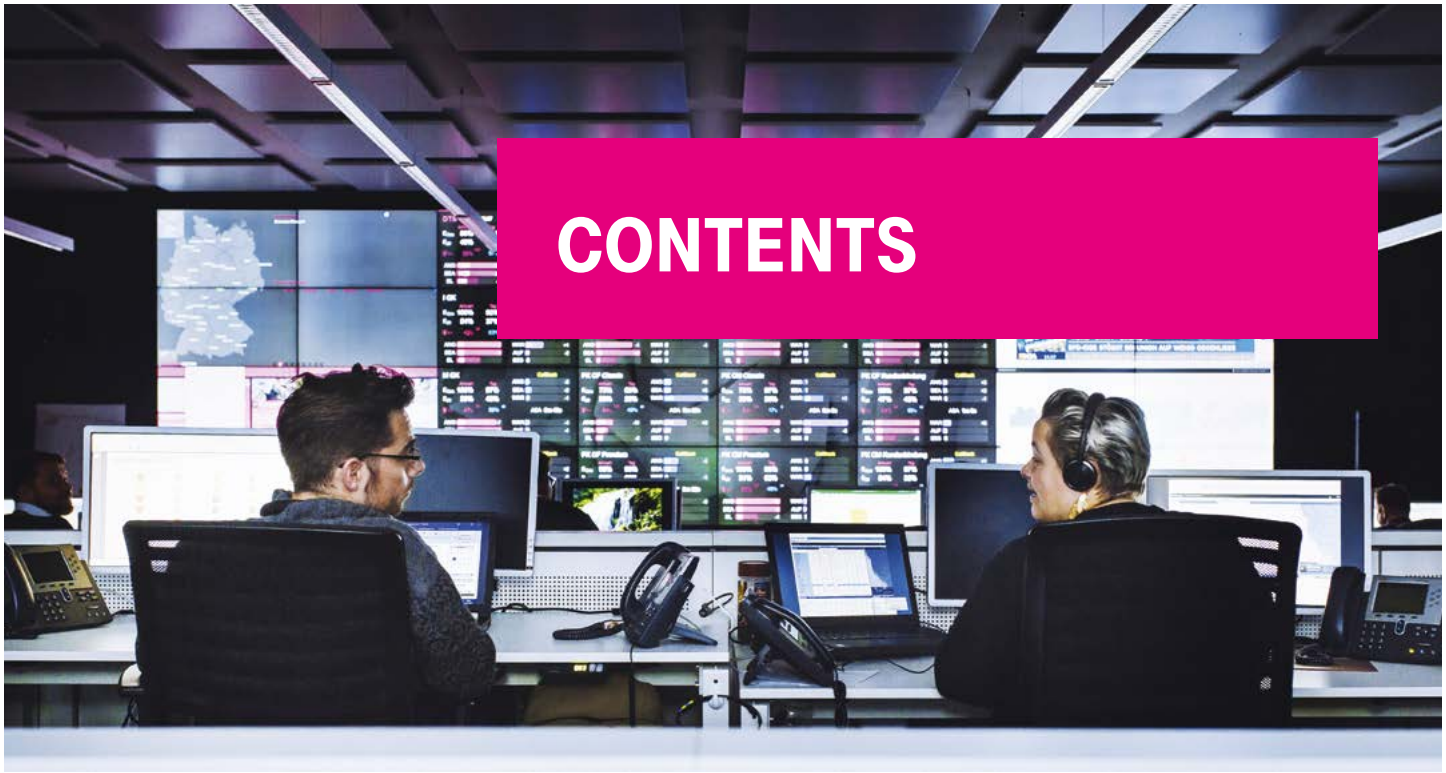


CYBERSECURITY FOR CONNECTED CARS

Pathways to a Security Operation Center for the Automotive Industry

T · · Systems ·



CONTENTS

1. INTRODUCTION
IT SECURITY MOVES OUT INTO THE STREETS

The cyberwars have reached the streets. Hackers are setting their sights on connected cars. Clearly, connected cars' IT systems need to be monitored constantly – at all times, and throughout the cars' service lifetimes. A Security Operation Center (SOC), staffed with a team of security experts, could provide just the kind of cybersecurity that connected cars need.

In the most-publicized auto-hacking incident to date, both the driver and the car wound up in a ditch. Prior to the incident, the result of a demonstration staged by the U.S. magazine Wired in 2015, editor Andy Greenberg had been forewarned that two security specialists would be using a special hacking technique to gain remote, wireless control over his Jeep Cherokee. With that hacking demonstration, the issue of hacker attacks against connected cars – and the dangers they could cause – burst into the public's perception. Since then, the automotive industry, policymakers and consumers have all become acutely aware of just how important the issue of cybersecurity for connected cars has become. The problems have by no means been solved. In August 2017, for example, security experts found a way to cripple the CAN bus – the heart of the on-board networks found on a great many different types of vehicles – via a denial-of-service (DOS) attack [Wired].

63 PERCENT OF ALL DRIVERS IN GERMANY, THE U.S. AND CHINA SAY THEY WOULD SWITCH TO A DIFFERENT CAR MANUFACTURER IF THEIR CURRENT VEHICLE FELL VICTIM TO A HACKER ATTACK.

TÜV Rheinland [TÜV]

ECALL INCREASES THE NEED FOR CYBER DEFENSE

The importance of vehicle security has increased still further since March 31, 2018. All vehicle models for which manufacturers want to obtain type approval in the EU must now be fitted with the eCall emergency assistance system. This means that the number of connected cars, and therefore the number of cars vulnerable to remote attacks, will increase enormously. Gartner is forecasting that 60 million new vehicles will be built with connectivity in 2020 and 220 million will be on the roads globally. [Gartner3]. Particularly in the case of fully or partially autonomous vehicles, IT security is vital for driving safety, and therefore for the lives and the physical protection of those in the vehicle. Users are well aware of this, too. At present, more than half of all drivers in the United States and Germany would not board a fully autonomous vehicle due to concerns of inadequate security or technical faults. [Gartner1].

SECURITY BY DESIGN IS JUST THE BEGINNING

Automakers have certainly come around to the cybersecurity issue. In a recent survey of automotive- and technology-industry decision-makers conducted by the law firm of Foley & Lardner, 63 percent of all respondents in the U.S. and Asia indicated that their developments in the area of connected and autonomous cars were taking account of the risks of cyberattacks [Foley]. The concept of making security a basic criterion in product development is referred to as "security by design." This concept is now playing an important role with regard to IT in the automotive sector, as a T-Systems white paper, "IT security for connected cars", illustrates [TSI1].

As important as it is, security by design cannot make connected cars immune to cyberattacks. Security also has to play a central role in production. And vehicles continue to require protection after they come off the production line – and throughout their service lifetimes of 15 to 20 years. The necessary measures include regular software updates and patches. And yet, all such efforts and measures notwithstanding, security vulnerabilities can go undiscovered – or suddenly emerge when hackers develop new attack strategies. Seemingly secure encryption can unexpectedly get defeated, for example. One answer to this problem are attack-detection systems – in vehicles (factory-installed), in mobile networks and in automakers' own back-end systems. When such systems are in place, the final line of defense for connected cars is an automotive security operation center (SOC) – a facility that brings together all security-relevant data in connected car "ecosystems" and that is staffed with a special cybersecurity team.

AUTOMOTIVE SOCS COMPLEMENT IT SOCS

Major corporations, including automotive-industry companies, already use security operation centers to protect their corporate IT systems. To protect growing numbers of connected cars, however, automakers need to build and install additional IT infrastructures and processes. This is because the security challenges for connected cars call for profound automotive expertise, in addition to basic IT and security know-how. The automotive industry is now working intensively on integrating attack-detection systems in vehicles. Putting an automotive SOC in place is the next necessary step in the process of making the best-possible use of the alerts and data such systems provide – and of establishing a complete cybersecurity environment for connected cars, throughout their entire service lives.

THE LAWS ARE BECOMING MORE DEMANDING

Laws and standards are now being updated in the area of vehicle security. ISO and SAE standardization initiatives, for example, are developing cybersecurity processes for vehicle development and utilization. The relevant standard, ISO-SAE AWI 21434, is to be in place in 2019. In addition, a UN task force is developing automotive cybersecurity guidelines that are to lead to mandatory criteria for type approvals in the 54 (current number) Member States of the United Nations Economic Commission for Europe (UNECE). The latest draft of the guidelines includes requirements pertaining to detection of cyberattacks against vehicles and to responses to such attacks [UN; BSI1]. In the EU, a new General Data Protection Regulation (GDPR), in force since May 2018, prescribes IT security measures for personal data and auto-position data (cf. p. 12). And in Germany, operators of critical infrastructures (KRITIS) already have to meet special IT security requirements.

2. SECURITY OPERATION CENTER (SOC)
A CENTER FOR VEHICLE SECURITY

The task of protecting connected cars while they are in operation includes continually monitoring and analyzing the data streams moving within cars and in their immediate environments. A Security Operation Center (SOC) reviews such data, for any indications of cyberattacks, and initiates defense measures whenever an attack is detected.

It is important to understand that hackers aiming at cars have a number of different interfaces to probe – including interfaces on vehicles themselves, interfaces within mobile networks and interfaces within automakers' back-end systems. For this reason, automakers need to monitor all vehicle-relevant IT and telecommunications systems, for any anomalies, throughout vehicles' entire service lifetimes. What's more, attacks can be detected only by drawing connections between anomalies in different systems and in multiple vehicles (cf. the box). This is a task that an automotive security operation center (automotive SOC) is especially equipped to carry out.

An automotive SOC is a facility that collects all security-critical data of relevance to connected cars and is staffed with highly qualified security teams that analyze data around the clock, minimize risks and detect, ward off and analyze attacks. In its role as a coordination center, an automotive SOC makes it possible to respond quickly to security incidents. This plays an indispensable role in the IT security of connected cars; after all, malware can spread throughout entire networks within just seconds or minutes.

EXPANDING FOR AN AUTOMOTIVE SOC

SOCs are found in many industries. Their primary purpose is to protect companies against cyberattacks. Currently, nearly half of all major corporations around the world have a security operation center in place [EY]. Most SOCs focus both on preventing and detecting cyberattacks and on responding to them. Such conventional-style IT-SOCs are also found throughout the automobile industry. To be able to protect connected cars, however, an automobile-industry SOC would need to add an automotive-SOC component that would combine know-how from the areas of both IT security and automotive IT. In any case, the IT-SOC component and the automotive-SOC component would need to collaborate closely to be able to detect interrelationships between any anomalies in vehicle systems and anomalies in back-office IT systems.

Automobile companies can either operate automotive SOCs themselves, as complements to their own IT-SOCs, or they can partly or completely outsource automotive-SOC tasks to a specialized service provider (cf. p. 18). National certifications of security operation centers can serve as guides for selection of an SOC service provider or for the establishment of a company's own SOC. Such certifications are relied on widely throughout the IT-security sector – for example, in selection of information-security-management systems, trust centers and security experts. No certification procedures have yet been established for security operation centers, however. In addition to the establishment of automotive SOCs, the key factors driving the IT security of connected cars will include close collaboration between the SOCs of automobile companies and those of other industries.

"FIELD OBSERVATIONS PLAY A FUNDAMENTAL ROLE. THIS INVOLVES IDENTIFYING AND ANALYZING ANY ATTACKS VIA BOTH TECHNICAL AND NON-TECHNICAL MEASURES."

German Association of the Automotive Industry (VDA) with regard to life-cycle management in the framework of automotive security [VDA2]

ROLES IN AN AUTOMOTIVE SOC WITH THREE-LEVEL ESCALATION

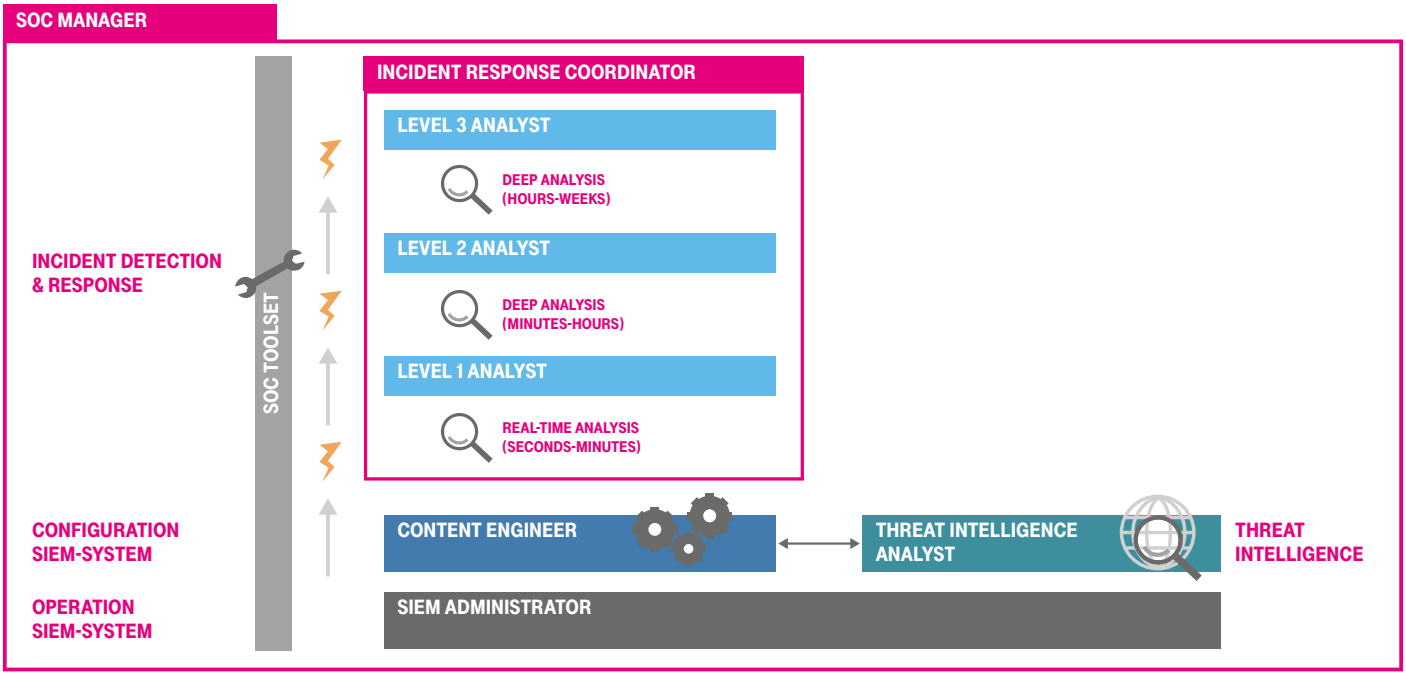


Fig. 1

FROM DATA COLLECTION TO CYBERSECURITY

An automotive SOC's basic approach can be roughly divided into four steps:

1. An SOC centrally collects security-relevant data from vehicles' operating environments (cf. p. 8).
2. The SOC structures the data – for example, by vehicle identification number (VIN) – and anonymizes or pseudonymizes the data prior to any sharing of the data (cf. p. 12).
3. Special systems within the SOC (such as security information and event management (SIEM) systems) scrutinize the data for any indications of hacker attacks (cf. p. 14).
4. If the SOC detects a potential security incident, it either initiates defined countermeasures or develops appropriate new response strategies (cf. p. 17).

A SPECIALIST FOR EVERY TASK

Ideally, the team in an automotive SOC will consist of security specialists from various areas of expertise (cf. Fig. 1). A threat-intelligence analyst, for example, uses external sources such as social media in order to identify potential security vulnerabilities, and to learn about potential attackers' possible motives, methods and tools (cf. p. 8). A content engineer translates attack scenarios into rules for an analysis system (such as an SIEM system; cf. p. 14), to enable the system to be able to recognize the scenarios. A system administrator manages the operation and availability of an SIEM system. If the system registers any indications of an attack, it alerts a security analyst. Often the security analysts in an SOC will be grouped into various different expert levels. Each level forwards alerts to the next-higher level whenever a given incident takes longer than a defined period to process or simply requires more-complex analyses (cf. p. 15).

CENTRAL SOC WITH COUNTRY OFFICES

A total of 61 percent of organizations with global business rely on central SOCs instead of on distributed teams [SANS2]. A central SOC – i.e. an SOC for connected cars – also makes sense for automakers, because it can provide a comprehensive overview of the IT security of a global automotive infrastructure. If vehicles in France and Brazil are suddenly experiencing the same anomaly, for example, a central automotive SOC can detect the parallel occurrence. Such a central SOC can be usefully supported by local SOCs, however, that analyze security-relevant data locally and then forward the pertinent alerts to it, without the event data. Elimination of the need to forward event data significantly reduces the quantities of data that need to be transmitted. In any case, when an automotive SOC operates internationally, it has to ensure that its data-collection and data-processing procedures conform to local data protection laws in each case.

3. DATA COLLECTION
CYBERGUARDS IN ALL CORNERS

To be able to detect cyberattacks against vehicles, an Security Operation Center (SOC) has to collect extensive quantities of data. The data involved includes data from detection systems in vehicles and in their operating environments and data from sources that analyze security vulnerabilities and potential attack strategies and techniques.

In operation, a modern premium vehicle generates 25 gigabytes of data per hour, or enough to fill five DVDs. And autonomous vehicles will have even much higher data outputs [t3n]. Needless to say, a car itself is the best data source to use in looking for hacker attacks against the car. But vehicle-based detection may be unable to precisely differentiate between external interference and normal system functions. For example, unexpected diagnostic messages from a vehicle's Unified Diagnostic Services (UDS) system can be triggered by something other than cybercriminals. But if such messages occur very shortly after anomalies have occurred in the manufacturer's back-end systems, or in the pertinent mobile network, an attack becomes a more-likely explanation. This example illustrates why an automotive SOC requires security-relevant data from all domains of the automotive ecosystem, including vehicles, back-end systems, mobile networks and even drivers' computers and mobile devices. At the same time, for reasons of data protection (cf. p. 12), and to ensure that vehicles' mobile network connections are not overloaded, it has to be able to filter the data, so that it collects only the data it truly requires.

SELF-LEARNING ENTRIES

Detection systems within the various domains (such as within vehicles) supply a large portion of the data that an SOC collects. Such systems can operate according to defined rules and/or use machine learning techniques in order to detect anomalous behavior. Standards for detection systems' data transmissions to SOCs are still lacking, however, and this is proving to be a challenge for system designers. Every manufacturer uses different interfaces and data formats. This makes the task of integrating the different systems involved in each case all the more complex.

SEEING THROUGH ATTACKERS' STRATEGIES

To be able to proactively detect potential security vulnerabilities and new attack vectors – i.e. new attack strategies and techniques – an automotive SOC should also have external sources to rely on. Such sources can include both technical system sources, such as honeypots, and human sources, such as experts contacted in the security community (for example, in groups such as the "CERT-Verbund", an alliance of German security / IT emergency-response teams). The types of security vulnerabilities that such sources can reveal, for example, could include a weakness in a control unit that several different vehicle manufacturers are using. In addition, security experts can identify previously unknown attack methods and enable detection systems to detect them. This approach, referred to as "threat intelligence," is an obvious choice for vehicle security, given the success it has enjoyed in conventional IT security. It has not yet played a significant role in the automotive industry, however.

THREAT INTELLIGENCE IS A STRATEGY OF USING DIFFERENT SOURCES IN ORDER TO LEARN ABOUT THE THREATS IN A PARTICULAR ENVIRONMENT.

SANS Institute [SANS1]

OVERVIEW AUTOMOTIVE-SOC

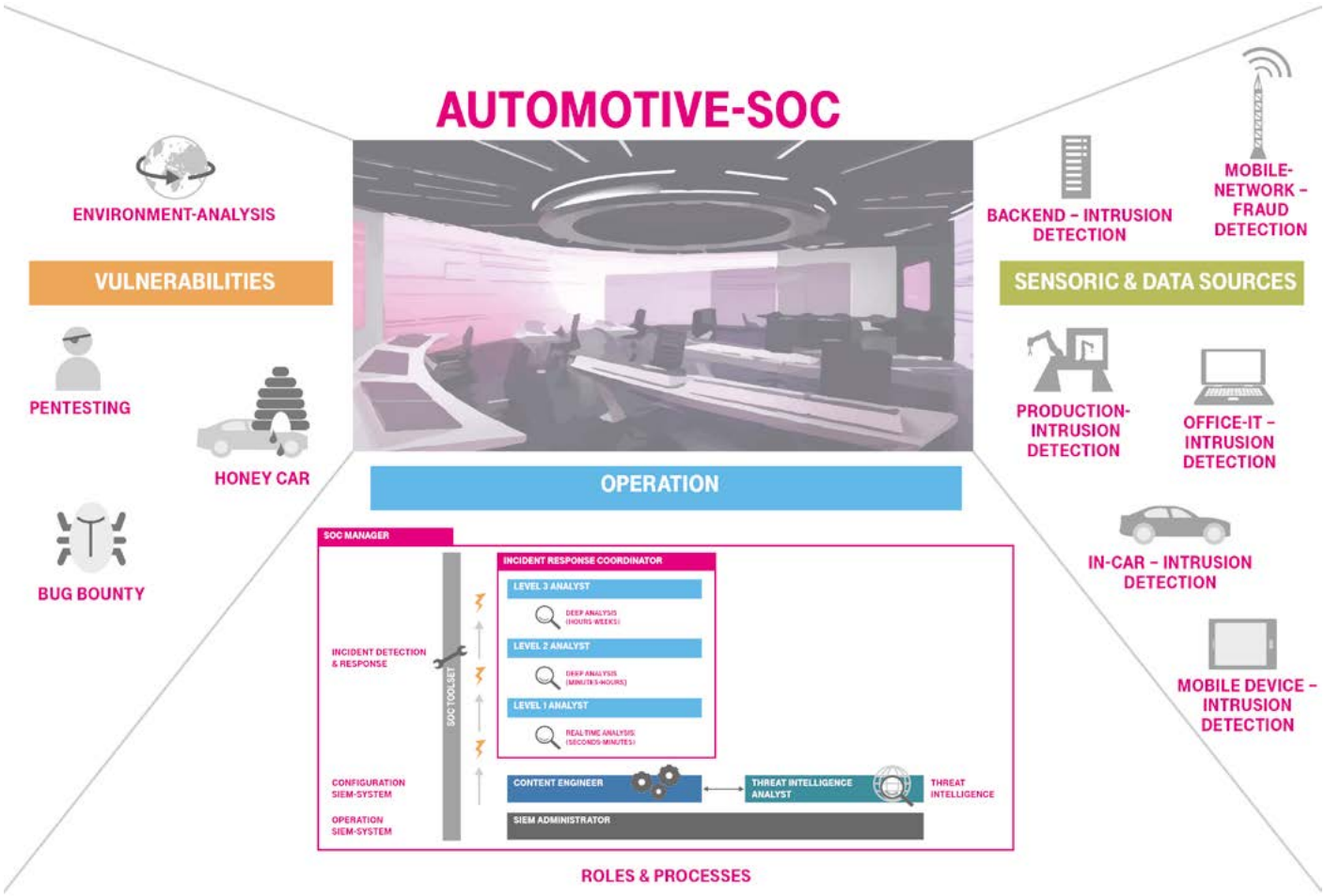


Fig. 2

DATA SOURCES FOR AN AUTOMOTIVE SOC

1. DETECTION SYSTEMS

IN VEHICLES

Three different types of vehicle data can be useful for an SOC:

- Unusual messages from vehicles' own networks,
- Information from control units (ECU) themselves, such as stored content and status information, and
- Specific alerts, or anomalies, from intrusion-detection systems (IDS) implemented within vehicles.

Ideally, a vehicle will be equipped both with a central-gateway IDS that monitors communications within the on-board network and with local detection mechanisms in key control units such as engine-control units and electronic braking systems. In a case, for example, in which an attacker operates an obtained control unit (with a mobile communications module) externally, an IDS system would notice that communications that normally accompany such a unit's operation (with other control units, for example) were lacking. It would then pass on that information, in the form of an alert, to the SOC (see p. 16, fig. 4). The automobile industry is currently working on integrating a first generation of vehicle IDS systems.

IN MOBILE DEVICES OF DRIVERS AND PASSENGERS

In Germany, five to ten percent of all attempted malware attacks target mobile devices [Kasp]. When a driver or passenger connects a compromised device with a vehicle, via Wi-Fi, USB or Bluetooth, he/she may be enabling an attacker to hijack the vehicle manufacturer's remote app or to penetrate the vehicle's bus. For this reason, drivers and passengers in connected cars should have an additional protective app on their mobile devices that monitors the security status of their devices and the devices' interfaces and reports any anomalies to the SOC. Drivers can install such an protective app in order to provide additional protection for their mobile devices – and, therefore, their vehicles. It could also make sense to integrate such a protective app function within the vehicle manufacturer's remote app and/or in mobility-service providers' car-sharing apps. With such functionality in place, only non-compromised mobile devices would be able to activate such key functions as "open door."

IN THE MOBILE NETWORK

A fraud-detection system uses defined rules in order to detect abuse of mobile connections. It generates an alarm, for example, when a SIM card does not use the serial number of the pertinent control unit when it logs onto a network, or when it contacts phone numbers that are not on a predefined white list [TSI1]. Tampering is always involved when a vehicle calls unknown hotline numbers, and thus such calls can signal that an IT attack is about to take place. A detection system can detect such anomalies very quickly – even before the network is able to establish the connections involved. In some cases, therefore, such a system can give security experts valuable additional time to carry out analyses and countermeasures.

IN BACK-END SYSTEMS

A detection system in a vehicle manufacturer's back-end system can monitor, for example, how often a vehicle uses particular services. Is a vehicle trying to authenticate itself without a valid security certificate? Is someone trying to delete logs within the back-end system? Such actions could be indications of a cyberattack. As a rule, today's vehicle manufacturers already have central IT-SOCs and suitable SIEM systems in service. At the same time, they have to continually update such centers and systems with new scenario data and detection logic, in order to keep up with the continually changing threats.

IN TERMINAL DEVICES OF AUTOMAKERS

The computers, smartphones and tablets of vehicle manufacturers' employees can also be points of entry for attackers. For example, hackers can use spear-phishing attacks, or specially targeted social-engineering attacks, to compromise specialists' accounts and thereby become able to attack back-end or production systems. For this reason, any automotive SOC has to be supported with data from the automaker's IT-SOC, i.e. with data from the automaker's local infrastructures, and with data from protective apps installed on the mobile devices of certain groups of employees (such as administrators of back-end systems).

IN PRODUCTION

Where an automaker also uses a detection system in production, it is useful to add that system's data to the data analyzed by the SOC. If any security incidents occur in production, the vehicles produced during or after those incidents can exhibit operational anomalies even months later. Such a connection will normally be missed, unless the relevant data from vehicle production and operation can be suitably correlated.

2. THREAT INTELLIGENCE

TRAPS FOR HACKERS: "HONEY CARS"

"Honeypots" are proven security tools in the IT world. They are computers or network components that are specifically designed to lure hackers. The resulting attacks, which are harmless because the honeypots are decoys, then can be analyzed by security experts with regard to the methods used. What's more, honeypots can help lure attackers away from other, "real" targets. Deutsche Telekom, for example, operates 2,200 virtual honeypots, and 511 physical honeypots, within its network. The cyberattacks they register can be followed in real time at http://sicherheitstacho.eu/. Automakers could benefit by setting similar traps for vehicle hackers. A "honey car," for example, could simulate a vehicle that has vulnerable interfaces and can be attacked via the Internet. To keep the deception from being discovered too quickly, the simulation would have to emulate a real vehicle on the road. This means the "honey car" would have to present realistic movement profiles, along with appropriate speed and fuel-consumption data. Significantly, such virtual simulation will become considerably more complex when it presents not just a vehicle but also the vehicle's connected back-end systems and/or its entire digital environment (including any "smart" stoplights).

PRIZES FOR "GOOD-GUY" HACKERS

Many large corporations, including Apple, Google and Microsoft, and a number of vehicle manufacturers, such as Tesla, General Motors and Fiat Chrysler, operate prize programs ("bug bounties") for external security experts who report detected security vulnerabilities before publishing their findings. Such support gives automakers time to eliminate the vulnerabilities before they are discovered by cybercriminals. The informants receive rewards based on the criticality of the vulnerabilities they discover. Bug bounties can be established on a permanent basis or used temporarily – for example, for hacking events. Deutsche Telekom runs a bug-bounty program of its own that provides valuable information. To be effective, such programs need to operate on the basis of predefined rules for informants. In addition, the security vulnerabilities they report should be prioritized by security experts in an automotive SOC, to ensure that critical weaknesses are addressed before non-critical ones.

PENETRATION TESTS

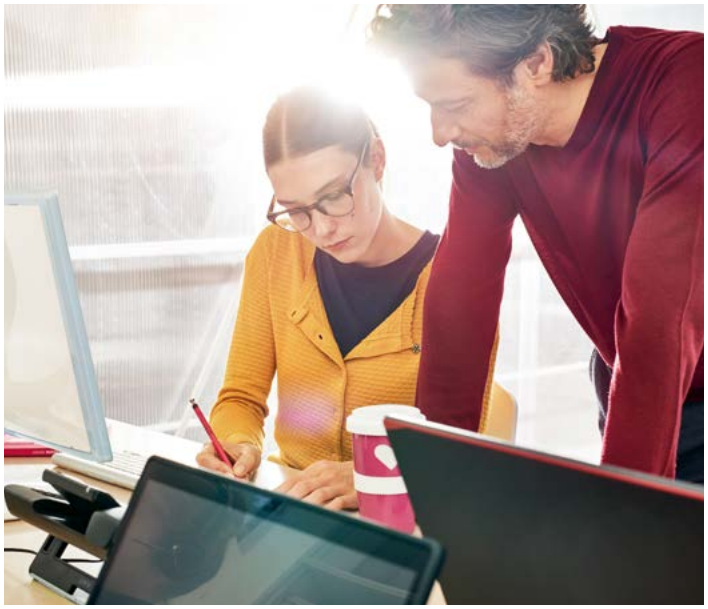
Vehicle manufacturers obtain additional information about potential security vulnerabilities and attack methods by commissioning penetration tests, or "pen tests." In a pen test, one or more security experts try to hack a car or back-end system (for example) with the same methods and techniques that a cybercriminal might use. There are three basic types of pen tests. In white-box tests, experts receive and make use of internal system data such as source code and passwords. In gray-box tests, they receive only limited quantities of system information, such as an IP address space. In black-box tests, they receive no information – i.e. no assistance – and thus have to proceed the way a real-world hacker would. In automotive development, pen tests are commonly used for such tasks as testing suppliers' components. They can also uncover security vulnerabilities while cars are in operation.

A LOOK AT THE WEB

With the help of special tools, security specialists scan various social media channels (such as Twitter and Facebook) and relevant forums. They look for key words in specific contexts. For example, they might look for a specific make of car in connection with terms such as "0-day," "pwned" or "exploit." On the basis of how often, and in which sources, such combinations occur, experts can prioritize their searches for indications of attacks that are either planned or in progress. On behalf of vehicle manufacturers, experts also monitor the darknet for any indications of trading of sensitive data such as activation codes, certain server IP addresses or other, similar information.

SHARING INFORMATION

Automotive security profits when automakers share their security-related findings with each other and with other security players such as IT companies, researchers and security authorities. This sharing principle also holds for automotive SOCs. Is the frequency of certain attack patterns growing in the industry? Has someone discovered a security vulnerability in an automotive CAN bus network? Many incident-response teams already share information in manufacturer-independent, cross-sector organizations such as the global Forum of Incident Response and Security Teams (FIRST) and the German "CERT-Verbund," an alliance of German security / IT emergency-response teams. In addition, the 15 automakers in the European Automobile Manufacturers Association (ACEA) have signaled their willingness to share and discuss information, with regard to new cybersecurity threats, with government agencies, industry stakeholders and relevant third parties [ACEA 2017].



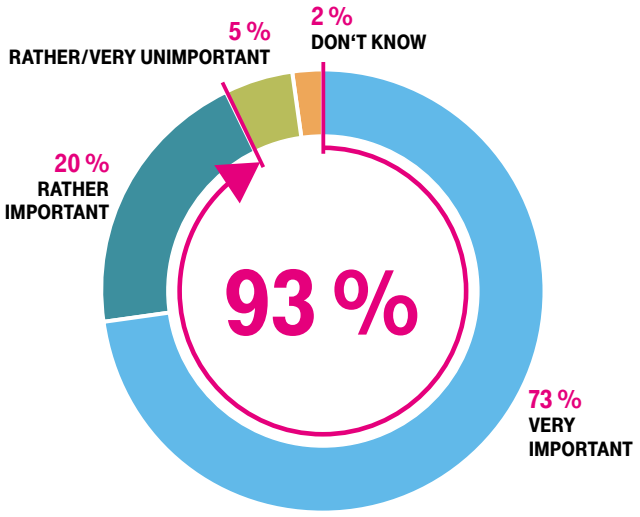
4. DATA PREPARATION AND DATA PROTECTION
BEING CAREFUL WITH PERSONAL DATA

When an car manufacturer collects, stores and processes data for an automotive SOC, it has to give particular attention to data privacy issues. The manufacturer has to ensure that data are pseudonymized before they are analyzed in the SOC.

Data on a car engine's speed can't be considered sensitive in terms of data privacy – or can it? When an automaker uses data from a connected car and its environment for security-monitoring purposes, it must ensure that its actions are conform to all data privacy laws. And such laws apply to all personal data, and personal data include all information connected with an identified or identifiable natural person. The German Association of the Automotive Industry (VDA) and the Conference of the independent data-protection authorities of the Federal Government and the State Governments consider data to be personal data if they are linked with a vehicle identification number (VIN) or a license plate number [VDA1]. With respect to a vehicle as a whole, therefore, "personal data" includes vehicle GPS data, vehicle-speed data and data on the engine's on/off state. "Personal data" in this context also includes data that can be correlated with a specific vehicle's smart key or SIM card (IMSI) – and, thus, at least with the vehicle's owner. As a precaution, therefore, it makes sense to consider all of the data that an automotive SOC uses to be personal data. After all, even engine-speed data, when combined with other data, could point to a particular driver, even in the absence of any direct personal correlation [Ritz].

The degree to which data used in an automotive-SOC context are sensitive in terms of data protection also depends on whether they refer directly to the driver himself/herself (data such as body weight or fatigue levels) or to only the vehicle (such as speed data), and on whether they are collected continuously or only in connection with certain events.

WHAT GERMAN CONSUMERS THINK ABOUT THEIR CARS' DATA



HOW IMPORTANT IS IT FOR YOU TO KNOW WHO IS USING THE DATA GENERATED FROM CONNECTED CARS?

Fig. 3, Bitkom association [Bitkom]

RIGHTS OF DATA OWNER IN THE EU

The EU General Data Protection Regulation (GDPR), which entered into force on May 25, 2018, accords data owner extensive rights with regard to their personal data [TSI2]. In the present context, for example, it implies that automakers may collect data only if the data serve a defined purpose. In addition, they have to ensure that data collection:

- is necessary for the performance of a relevant contract (this applies to position data in connection with carsharing, for example),
- is legally required (as is the case in connection with the eCall automated emergency response system),
- is in keeping with a specific business interest of the automaker (such as collection of data on causes of accidents, in the interest of product improvement)
- or has been consented to by the data subject.

Furthermore, pursuant to the GDPR, data subjects always have the right to obtain information about their collected data, as well as the right to have data rectified or erased. Such provisions also apply to data that, at some point, are analyzed in an automotive SOC.

HIDING IDENTITIES

After ensuring that data collection for an automotive SOC conforms to data protection laws and guidelines, an automaker can begin storing data. The first point of storage is his back-end system. Before he transmits stored data to the SOC, he has to anonymize or at least pseudonymize it. That way, the automaker fulfills the GDPR's principle of data minimization, whereby data processing should use only as much personal data as is absolutely necessary for the defined task in question. For the purposes of security analysis in an SOC, correlations with a specific vehicle or person are not necessary. A general ID number is retained, however, to ensure that a vehicle's mobile-communications and intrusion-detection data remain correlated.

ANONYMOUS OR PSEUDONYMOUS?

When data are anonymized, all correlations with specific persons are eliminated, and the data cannot, in principle, be restored to its original state. In pseudonymization, by contrast, identity characteristics such as a VIN, license plate number and SIM card ID are replaced with a pseudonym, and the data can, in general, be restored to its original state. Such restoration could become necessary, for example, if an automotive SOC found malware in a vehicle and the automaker then wished to notify the vehicle owner.

Various methods for anonymizing and pseudonymizing personal data are available. For example, identity data can be erased, or replaced with constant or changing pseudonyms. Alternatively, data can be encrypted – either with or without retention of the pertinent encryption key – or made illegible via a hash function. In the case of pseudonymization, it is important to ensure that only a small group of authorized persons can reverse the pseudonymization, and that no pseudonyms are ever reused.

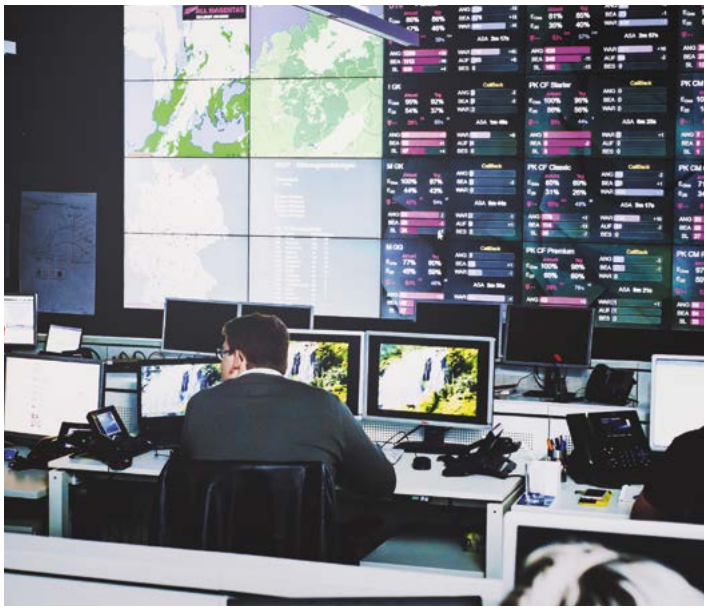
FINDING A BALANCE BETWEEN DATA PROTECTION AND SECURITY

In any case, regardless of which procedure – anonymization or pseudonymization – is used, the technique used to hide identity has to strike a balance between data protection and security. On the one hand, cyberattacks are easier to detect when more of the original data remains intact. On the other hand, increasing the amount of data that remains intact also increases the risk that other data, i.e. data without any specific identification, will allow correlations with specific persons, via profiling. For example, GPS data and other information – such as information about the vehicle owner's family and their places of work – could possibly be used to determine who was driving a particular vehicle at a particular time.

5. DATA ANALYSIS
NO MORE HIDING

A central analysis system (SIEM) scans data from connected cars' IT and TC infrastructures for any indications of cyberattacks. Precise descriptions of possible attack scenarios provide a basis for detection.

The heart of an automotive SOC is a Security Information and Event Management (SIEM) system. Its task is to identify and report any potential cyberattacks, and to facilitate real-time analyses and security reports. For this reason, an SIEM collects log files from a range of different input systems, such as vehicles' intrusion-detection systems and mobile networks' fraud-detection systems (cf. p. 9-10). The core of the system consists of rules for correlating data and for checking for any indicators that point to possible compromising of systems (indicators of compromise – IOC). In the context of an automotive SOC, IOCs are signs of activity, in the networks and systems in and around a vehicle, that are very likely tied to intrusion.



THINKING LIKE AN ATTACKER

An SIEM system's rules are based on concrete use cases (attack scenarios) that describe, in detail, how a cybercriminal would operate (see the sample scenarios on p. 16). A collection of use cases is referred to as a "threat library." The IT sector has already identified and described numerous attack scenarios, including the means by which they can be detected and the best ways of addressing them. Automakers need to develop such threat libraries for their relatively young (in IT terms) automotive sector, in cooperation with security experts. For automotive SOCs, the IT sector offers a proven model for structured description of cyberattacks: the "cyber kill chain," which describes attacks in terms of phases. Similarly, an "automotive kill chain" could describe attacks against connected cars in terms of phases – for example, the following seven phases [SANS3]. Depending on the way an attack is structured, it may be useful to combine some of the phases:

1. **Reconnaissance:** The attacker collects information about his target, such as IP addresses and software-version data.
2. **Weaponization:** The attacker prepares his attack – for example, by writing malware.
3. **Delivery:** The attack weapon is delivered to the victim. For example, the attacker distributes malware-containing USB flash drives in a parking area.
4. **Exploitation:** The attacker gains illegal access to the target system – for example, when a compromised USB flash drive is plugged into a vehicle's port.
5. **Installation:** If malware is to play a role in the attack, it is installed.
6. **Command and control:** The attacker acquires control – for example, by setting up a secret point of access (back door) to the vehicle's IT systems.
7. **Actions on objectives:** By being able to access the target system, the attacker is able to carry out actions that support his aims – for example, retrieving data from the vehicle's infotainment system, for the aim of spying on the vehicle owner.

IF-THEN RULES FOR DETECTION

Additional attack scenarios can emerge from analyses in the context of threat intelligence (for example, using a "honey car") and from ongoing exchanges with other automotive security experts (such as experts working for manufacturers and suppliers) (cf. p. 10-11). From such scenario information, and applying the "if-then" principle, a content engineer will develop analysis rules for his/her organization's SIEM system. With such rules, the system is able to detect suspicious incidents, provide alerts and prioritize alerts by criticality. Here is a simplified example: "If a vehicle's telecommunications module (TCU) attempts to log into the back-end system without showing a valid security certificate, then issue an alert. If, shortly thereafter, the back-end system attempts to establish a connection to an unknown IP address, increase the priority of the alert."

Ideally, the content engineer will improve the SIEM rules on a regular basis – on the basis of security analysts' feedback regarding false alerts (false positives), findings from threat intelligence or integration of additional log-file sources. In the future, SIEM systems will increasingly also rely on machine learning. That will enable them to detect anomalies even without the help of previously defined rules. Findings from machine-learning-based detection should always be checked by human specialists, however, and detected security incidents should always be translated into specific SIEM rules.

RESPONSIBILITY DEPENDS ON LEVEL COMPLEXITY

An SIEM system issues its alerts via a dashboard that security analysts (in the automotive SOC) use to process incidents in accordance with their priority. Ideally, analysts will be grouped into different escalation levels. SIEM-system alerts go first to a level-1 analyst. He/she filters out any false alerts and then processes the remaining alerts in keeping with their priority and a predefined set of rules (runbook). For such processing, it is useful to define a maximum period of time that the level-1 analyst should spend on any single alert. If analysis of an incident takes longer than just a few minutes (for example, because it requires additional research), or if no runbook is available for the specific case involved, the level-1 analyst terminates his/her processing and escalates the incident to a higher level.

THE "SHERLOCK HOLMES" OF VEHICLE IT

In cases that are especially complicated or critical – such as cases involving cyberattacks that could affect driving safety – an IT forensic analyst can become involved. The forensic analyst's task is to learn how the perpetrator proceeded, and to identify any systems and components that he/she has succeeded in hacking into. To that end, he/she thoroughly examines compromised systems. To ensure that all traces and records are saved, prior to his/her analysis, he/she makes copies of all the data storage media involved. For that process, he/she may even have to drive to the data center, remove the pertinent disk drives and copy the drives. In the case of a compromised vehicle, it also makes sense to copy all of the data involved (such as the fault log) – on location.

The disadvantage of such forensic duplication is that it can involve copying very large quantities of data. This is why "live forensics," a tool that was rarely used in the past but that is now being relied on increasingly, is used. Live forensics uses software agents, on the live system, that are able to rapidly identify affected areas in cases of attack and support fast response. Theoretically, a similar approach, with read-only remote access, could also be used in vehicles. With preselection of potentially affected system areas, only a few, small parts of a system – such as metadata – have to be copied for analysis in each case.

Forensic analysis in a conventional IT context can take days, weeks or even months. The chances of success vary, and depend on how many resources attackers have invested. In general, the later an attack is detected, the lower the chances of reconstructing the individual steps that went into the attack will be. Unfortunately, late detection is often what happens: In 2017, cyberattacks against conventional IT infrastructures went undetected for an average of 101 days [Mand].

ATTACK SCENARIO: THE SCRAP-YARD HACKER

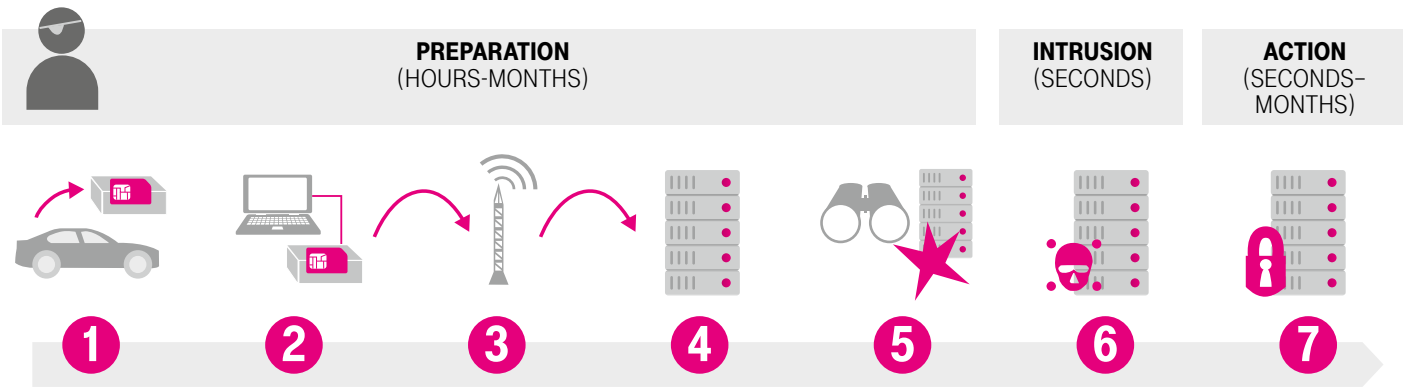


Fig. 4

1. The perpetrator obtains a control unit, with an activated SIM card, from a vehicle – such as a vehicle he finds at a scrap yard.
2. The perpetrator then activates the control unit by connecting it to a PC.
3. The vehicle's SIM card logs onto the relevant mobile network.
4. The stolen control unit then logs on, wirelessly, to the vehicle manufacturer's back-end system.
5. Once he is in the back-end system, the perpetrator searches for attack opportunities.
6. If he finds a vulnerability, he exploits it to gain access.
7. He then carries out an action such as inserting ransomware into the back-end system, in order to extort a ransom.

6. COUNTERMEASURES
FOR EFFECTIVE DEFENSE, YOU NEED A PLAN

When a cyberattack occurs, an automotive Security Operation Center (SOC) coordinates a response. Its security experts either execute a predefined incident-response plan or develop a new approach, if one is needed.

In an automotive SOC, both data analysis and responses to cyberattacks should be based on clearly defined rules. The instructions (runbooks) used by security analysts on lower levels should thus precisely specify what measures are to be used for which alert. The more efficient defense processes are, the less time a potential attacker will have to cause damage. To date, the automotive industry still has only a few best practices for such incident-response plans (just as it has only a few for attack scenarios). In the early phases of an automotive SOC's operations, therefore, the SOC will be unable to address every security incident within seconds or minutes. Automotive SOCs' development of standardized procedures for addressing alerts will have to be a gradual process.

BETWEEN SECURITY AND SERVICE QUALITY

In such procedures, it is important to define what roles, on the part of the vehicle manufacturer, are to become involved in any given type of incident. The more critical an alert is, the higher within the company's hierarchy the responsibility for addressing it should be. For example, the Chief Information Security Officer (CISO) is a suitable role for coordinating security-incident responses on the part of the vehicle manufacturer. Coordination can also be required in cases in which the planned countermeasures impinge on the driver's or passengers' user experience. An example: A vehicle's SIM card can generate considerable financial damages for the vehicle manufacturer by continually calling expensive added-value service numbers. One countermeasure could involve deactivating the vehicle's mobile communications module. That also takes away the driver's mobile access, however, and he/she will be unable to use network services such as real-time navigation or the vehicle's interior hotspot. The customer may well become disgruntled as a result.

How an Automotive-SOC exactly solves a security incident depends on the particular type of alert that is involved. In the future, it is likely that automatic defense responses will also come into play, in addition to the manual security measures now used. That said, it must be remembered that perpetrators could try to exploit automated protective measures and even turn them against drivers or vehicle manufacturers.

7. CAR SECURITY AT DEUTSCHE TELEKOM
TWO KEY INGREDIENTS FOR AN AUTOMOTIVE SECURITY OPERATION CENTER (SOC)

Cybersecurity for connected cars calls for special know-how with regard to both security and automotive technology. Deutsche Telekom, including T-Systems, its arm for corporate customers, has years of experience in both of these areas, and operates one of Europe's largest and most-advanced security operation centers.

At Deutsche Telekom's Cyber Defense and Security Operation Center (SOC) in Bonn, and at connected national and international locations, a total of 200 experts monitor the systems of Deutsche Telekom – and of its customers – around the clock. Some 30 German DAX corporations and medium-sized companies now rely on Deutsche Telekom's SOC for their cybersecurity needs. In order to study the procedures used by cybercriminals, Deutsche Telekom operates a total of 2,200 virtual hacker traps – "honeypots" – worldwide. It streams attack records live at sicherheitstacho.eu. The company opened its new Cyber Defense and Security Operation Center in the fall of 2017.

Security services for the automotive industry play an important role at both the SOC and Telekom Security, Deutsche Telekom's security unit. In addition, automotive experts at T-Systems support 13 of the world's 20 largest automakers, along with international suppliers and over 3,000 car dealerships, in tasks such as development of connected and autonomous cars. The IT security of connected systems plays a key role in such support – throughout systems' entire life cycles. Protecting connected cars against hackers, throughout their entire service lives, means protecting them around the clock. This is why Deutsche Telekom is supporting the automotive industry in establishing and operating automotive security operation centers. In the process, automakers are profiting from Deutsche Telekom's own SOC group, which provides information on the general IT security situation, and on new threats, on a daily basis (see p. 19).

MADE-TO-ORDER SOC OPERATIONS

Deutsche Telekom sees three main options for operation of an automotive SOC:

- **Own operation:** The automaker puts the necessary competencies, processes and tools for an automotive SOC in place himself – including everything from the SIEM system to the necessary rules and to event analysis and response.

- **Hybrid operation:** The automaker assumes selected roles and tasks within the automotive SOC. A selected partner then provides certain resources and assumes certain responsibilities, such as creating the required rules and carrying out level-1 and level-2 analysis. The SOC team then coordinates closely, in accordance with defined processes, with the automaker and with his IT-SOC. (cf. Fig. 5).

- **Outsourced operation:** A partner operates the automotive SOC on behalf of the automaker. The partner provides the SIEM system, along with security and automotive specialists for the entire spectrum of tasks, from rule preparation to incident response.

Deutsche Telekom is a trusted partner in the automotive industry. It favors a hybrid approach that can be customized to the automaker's specific requirements in each case. Deutsche Telekom has extensive expertise and advanced tools in this area, also thanks to its decades of experience in protecting its own networks and infrastructures.

HYBRID OPERATION MODEL FOR AUTOMOTIVE-SOC

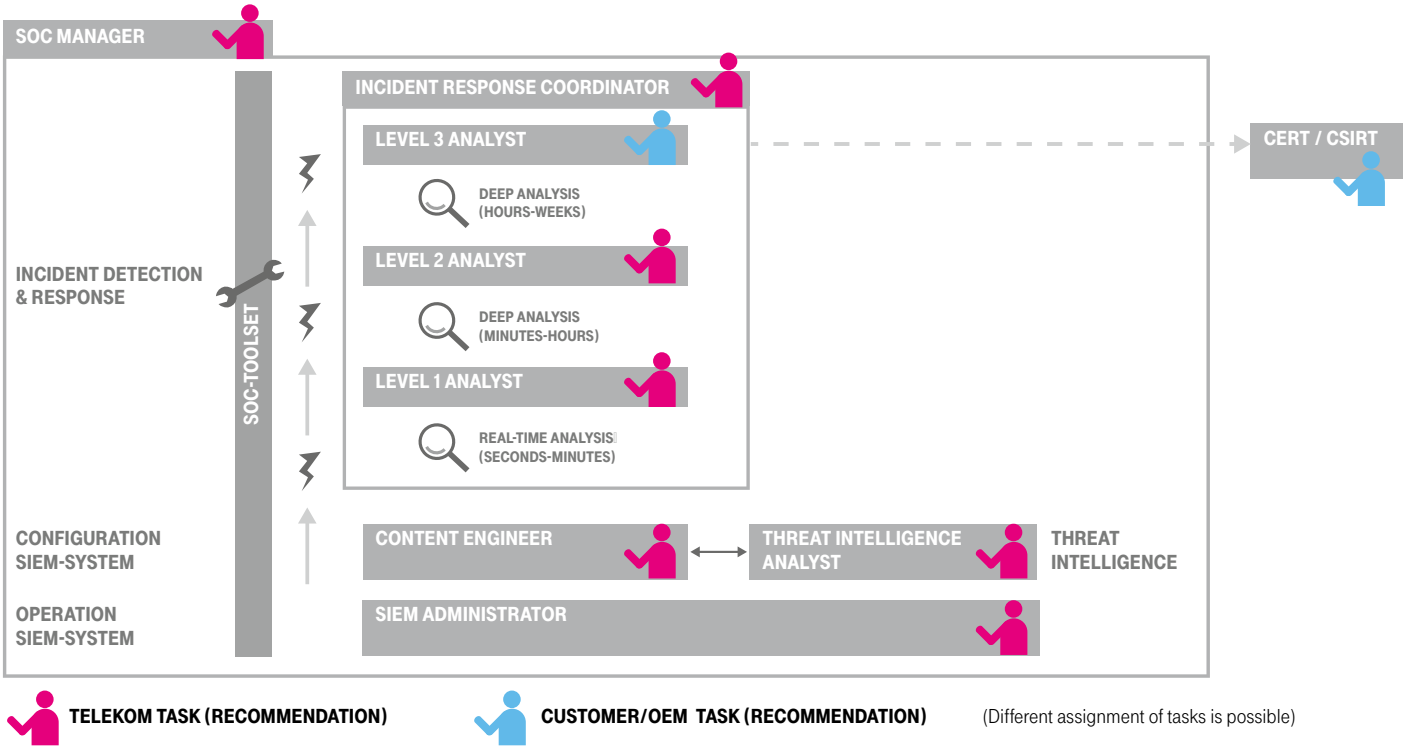


Fig. 5

Deutsche Telekom also supports the automobile industry in establishing data sources for automotive SOCs. For detection of hacker attacks against vehicles, the company has developed the ESLOCKS intrusion-detection system. The system detects anomalies within vehicles' CAN buses and analyzes them, with the help of machine-learning algorithms, in back-end systems – taking account of entire fleets. Deutsche Telekom also supports automobile companies in fraud detection – i.e. detection of SIM-card abuse. It supports companies in carrying out pertinent risk analysis and in developing suitable protective measures for mobile networks. Deutsche Telekom's range of automotive-SOC services thus links all kinds of individual measures to form a comprehensive automotive security architecture – and to ensure that vehicles on the road are protected against the dangers in cyberspace.

A DAY AT THE DEUTSCHE TELEKOM SOC, IN FIGURES

- **3,300 data sources** provide data for Deutsche Telekom's SOC.
- The SOC analyzes **1.5 billion security-relevant events**.
- Deutsche Telekom's honeypot sensors register **12 million attacks**.
- A total of **6 billion data records** on Deutsche Telekom's DNS servers are monitored for cyberattacks.
- The SOC filters out some **5,000 viruses and other malware** from the incoming data stream.
- The center's security specialists have created **21 security vulnerability advisories**.
- Deutsche Telekom's malware library already contains **20 million samples of malware code**.

8. SUMMARY
CARS NEED A DIGITAL "GUARDIAN ANGEL"

In its battle against car hackers, the automotive industry needs cybersecurity centers that focus especially on protecting connected cars. In such centers, car-security experts monitor vehicles' IT security throughout vehicles entire service lifetimes, and they take immediate action in the case of any attacks.

Roland Berger, the business consultancy, estimates that by 2020 nearly half of all cars on the road will be connected cars [RB]. In addition to opening up a world of new possibilities such as autonomous driving, wireless connections for automobiles also present an array of new challenges. This is because vehicles, like computers and smartphones, now need to be protected against cyberattacks. IT security, covering all aspects of automobile use, now plays a key role in automotive development and production. Security systems in vehicles and their operating environments have to be kept up to date, throughout cars' entire service lifetimes – and hacker attacks have to be quickly detected and blocked. In the future, automotive security operation centers (automotive SOCs) will provide cybersecurity for connected cars.

An automotive SOC is a central facility at which a team of security experts with both automotive and IT know-how analyze all security-critical data relative to connected cars – and detect and ward off cyberattacks. The data that enter into their analyses come from a range of different sources:

- detection systems – in vehicles, back-end systems and mobile networks,
- threat intelligence systems, which obtain information about hackers and their methods via digital traps (honeypots) and consultation with third parties, and
- vehicle data, such as telematics data.

When automakers collect, store and process data for an automotive SOC, they have to ensure they are remaining compliant with data protection laws and regulations. The required measures in this regard include pseudonymization of personal data before the data are transmitted to an automotive SOC.

WIDE USE OF SOC-OUTSOURCING

For its data analysis, an automotive SOC uses a Security Information and Event Management (SIEM) system. On the basis of preconfigured rules, an SIEM system scans data for indications of cyberattacks, and it automatically alerts the SOC's security analysts whenever it detects any suspicious activities. Analysts within an SOC are grouped into different "expert levels". Depending on their level, they process alerts on the basis of established guides, or carry out expanded and/or complex research. Their tasks include coordinating protective measures, such as blocking SIM cards.

Automobile companies can either operate automotive SOCs themselves, as complements to their own IT-SOCs, or they can partly or completely outsource automotive-SOC tasks to a specialized service provider such as Deutsche Telekom. "Building a SOC (...) is a costly and time-consuming effort that requires ongoing attention in order to be effective," stated Gartner Analyst Siddharth Deshpande in 2017, on the occasion of a security summit in Dubai [Gartner2]. In the same year, a study of the SANS Institute concluded that many organizations worldwide have been shifting part of their SOC tasks – especially threat intelligence, IT forensics and attack detection – to managed-service providers [SANS2].

9. GLOSSARY

0-Day	"Zero Day"; an attack that exploits a security vulnerability on the same day on which it is discovered.
Anonymization	The process of irreversibly removing any traceable personal references in data.
Blacklist	A list of blocked communication partners, such as SIM cards or IP addresses
CAN	Controller Area Network; a field bus
CERT	Computer Emergency Response Team; a team that responds to IT-security incidents
Cyber kill chain	A multi-stage model for description of cybercriminals' attack strategies
DNS	Domain Name System; a database that translates domains into in IP addresses
GDPR	The EU's General Data Protection Regulation; entered into force on May 25, 2018
eCall	An automated emergency response system; since April 2018, eCall equipment has been mandatory in the EU for all new models of cars
ECU	Electronic Control Unit; on-board control unit in vehicles
VIN	Vehicle identification number; each vehicle has its own unique VIN
False positive	False alert
Fraud detection	Detection of SIM-card abuse
Honeypot	A system that simulates computers or networks, in order to serve – for purposes of analysis – as a lure for cyberattacks
Incident response	Management of IT-security incidents
IoC	Indicators of compromise; events that give indications of cyberattacks
IDS	Intrusion detection system; a system for anomaly detection
ISO	International Standards Organization
IT forensics	Methodical data analysis for clarification of IT-security incidents
KRITIS	Critical infrastructures; organizations and institutions of particular importance for the public sphere [BSI2]
Logs	Files that record processes in computers and networks
Machine learning	Area of artificial intelligence; autonomous system learning via recognition of patterns in sample data
Malware	Malicious software such as viruses, trojan-horse programs and spyware
OBD2	An interface standard for On Board Diagnostic systems for vehicles
Penetration tests	IT-security checks that use the same methods that cybercriminals use
Pwned	From the world of gaming. To be "pwned" means to be "owned," i.e. be completely dominated; used to refer to victims of successful cyberattacks
Pseudonymization	Reversible removal of personal references in data
Runbook	Guide for handling of security incidents
SAE	Global association of engineers and technology experts in the areas of aviation and automotive technology (including trucks)
Safety	In this context, refers to the functional safety of vehicles
Security	In this context, IT security; the protection of electronically stored data and the processing of such data [BSI2]
SIEM system	Security Information and Event Management system
SOC	Security Operation Center, a type of cyber-defense center
Threat intelligence	Procedures for studying the motives and strategies of cybercriminals
Trust center	A trustworthy agency that issues digital certificates for authentication or encryption
UNECE	United Nations Economic Commission for Europe
UDS	Unified Diagnostic Services; diagnosis-communication protocol for control units in vehicles

10. REFERENCES

[ACEA]
„ACEA Principles of Automobile Cybersecurity“, ACEA, 2017, https://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf

[Bitkom]
„Autonome Autos: Hoffnung auf mehr Sicherheit und Umweltschutz“, Bitkom, 2018, https://www.bitkom.org/Presse/Presseinformation/Autonome-Autos-Hoffnung-auf-mehr-Sicherheit-und-Umweltschutz.html

[BSI1]
„Cyber-sicher fahren“, BSI-Magazin 2018/01, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2018_01.pdf;jsessionid=622DF61185298C982E4493138CB259F3.2_cid360?__blob=publicationFile&v=8

[BSI2]
Website des Bundesamts für Sicherheit in der Informationstechnik, last checked in 2018, https://www.bsi.bund.de

[Cap]
„Cybersecurity Talent: The Big Gap in Cyber Protection“, Capgemini Digital Transformation Institute, 2017, https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2018/02/the-cybersecurity-talent-gap-v8_web-2.pdf

[EY]
„20th Global Information Security Survey 2017-18“, EY, 2018, https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf

[Foley]
2017 Connected Cars & Autonomous Vehicles Survey, Foles & Lardner LLP, 2017, https://www.foley.com/files/uploads/2017-Connected-Cars-Survey-Report.pdf

[Gartner1]
Online-Study „Consumer Trends in Automotive“, Gartner, 2017, https://www.gartner.com/newsroom/id/3790963

[Gartner2]
„Security Operations Centers and Their Role in Cybersecurity“, Gartner, 2017, https://www.gartner.com/newsroom/id/3815169

[Gartner3]
„Best Practices for Direct Monetization of Connected Vehicles“, Gartner, 13. August 2018

[Heise]
„IT-Sicherheitsgesetz: Wer was wann zu melden hat“, heise.de, 2016, https://www.heise.de/newsticker/meldung/IT-Sicherheitsgesetz-Wer-was-wann-zu-melden-hat-3096885.html

[Kasp]
„IT threat evolution Q2 2017. Statistics“, Kaspersky, 2017, https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/

[Mand]
„M-Trends 2018“, Mandiant, 2017, https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf

[RB]
„Connected car: App based dongle solution as shortcut to connectivity“, 2016, Roland Berger, https://www.rolandberger.com/de/Publications/pub_connected_car.html

[Ritz]
„Mobilitätswende – autonome Autos erobern unsere Straßen“, Johannes Ritz, Springer Verlag, 2018, S. 178

[SANS1]
„Threat Intelligence: What It Is, and How to Use It Effectively“, Sans Institute, 2016, https://www.sans.org/reading-room/whitepapers/analyst/threat-intelligence-is-effectively-37282

[SANS2]
„SANS2 Security Operations Center Survey“, SANS Institute, 2017, https://www.sans.org/reading-room/whitepapers/incident/future-soc-2017-security-operations-center-survey-37785

[SANS3]
„Applying Security Awareness to the Cyber Kill Chain“, SANS Institute, 2018, https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain

[t3n]
„Wem gehören die Daten im Connected Car?“, Wolfgang Gründinger auf t3n.de, 2018, https://t3n.de/news/wem-gehoeren-daten-connected-car-1074195/

[TSI1]
„IT-Sicherheit für das vernetzte Fahrzeug“, T-Systems, 2016, https://www.t-systems.com/de/de/ueber-uns/unternehmen/newsroom/news/news/white-paper-car-security-459382

[TSI2]
„Europäische Datenschutzgrundverordnung“, T-Systems, last checked in 2018, https://www.t-systems.com/de/de/loesungen/digitalisierung/digitialisierung-themen/dsgvo/datenschutzgrundverordnung-753690

[TÜV]
Studie „Sicherheit autonomer Fahrzeuge“, TÜV Rheinland, 2017, https://www.tuv.com/germany/de/newsletter/mobilit%C3%A4t/2017-4/studie-autonomes-fahren.html

[UN]
Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 IWG ITS/AD, 26.04.2017, https://wiki.unece.org/pages/viewpage.action?pageId=56591540

[VDA1]
„Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA)“, VDA, 2016, https://www.vda.de/de/themen/innovation-und-technik/vernetzung/gemeinsame-erklaerung-vda-und-datenschutzbehoerden-2016.html

[VDA2]
Position zur Automotive Security, VDA, 2017, https://www.vda.de/de/themen/innovation-und-technik/datensicherheit/automotive-security.html

[Wired]
„A Deep Flaw in Your Car Lets Hackers Shut Down Safety Features“, Wired, 2017, https://www.wired.com/story/car-hack-shut-down-safety-features/

AUTHORS

Christian Olt, Senior Security Manager – Automotive & MI, T-Systems
Eva Saar, Senior Security Consultant – Telekom Security, T-Systems
Dr. Friedrich Tönsing, Head of Technology & Asset Management, T-Systems
Dr. Jan Göbel, Senior Security Analyst – Cyber-Defence-Center, T-Systems
Jens Scholz, Senior Consultant – Automotive Security, T-Systems
Klaus-Peter Hofmann, Senior Security Consultant, T-Systems
Mario Schneidereit, Principal Solution Sales Manager – Automotive Security, T-Systems
Mark Großer, Associate Partner (Risk, Security & Compliance) – Detecon (T-Systems)
Mirko Funk, Head of IoT Analytics Services, T-Systems
Stephanie Görges, Senior Cyber Security Consultant – T-Systems
Stefan Lück, Security Consultant, T-Systems
Thomas Fischer, Head of Embedded Digital Solutions – T-Systems
Yvonne Nestler, Technical Journalist – Palmer Hargreaves

CONTACT

T-Systems International GmbH
Christian Olt
Sales Automotive & Manufacturing Industries
Email: christian.olt@telekom.de

EDITOR

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Germany
www.t-systems.com

T · · Systems ·