IOActive®

Research-fueled Security Services

\ RESEARCH \

Commonalities in Vehicle Vulnerabilities

Samantha Isabelle Beaumont
Principal Security Consultant

2022 Decade Examination
September 2023

Table of Contents

EXECUTIVE SUMMARY 3
Technical Findings 3
The Research Analysis | Key Takeaways 4
INTRODUCTION 5
Foreword 5
THREAT SURFACE METHODOLOGY 6
Threat Vectors of a Connected Car 6
Modernizing Threat Vectors 7
Threat Assessment Practices 8
RISK CLASSIFICATION METHODOLOGY 9
Initial Ratings 9
Overall Severity (Risk) 10
Worked Example 11
COMMONALITIES AND TRENDS 12
Key Analysis Categories 12
Vulnerability Metrics 13
Attack Typecasting 22
Remediation Approaches 28
CONCLUSION 34
Technical Summary 34
Emerging Threats 34
Future Concerns 34
Final Considerations 35
FUTURE WORK 35
APPENDIX A: ADDITIONAL INFORMATION 36
About IOActive 36
About the Author 36
Table of Figures 37
Table of Tables 38
Table of Equations 38
APPENDIX B: GRAPHS 39
Impact 39
Likelihood 41
Risk 43
Attack Vectors 45
Vulnerability Types 48
Critical Impact Remediation 50
Ounce of Prevention 52
REFERENCES 55

Executive Summary

With the connected car now commonplace in the market, automotive cybersecurity has become the vanguard of importance for road user safety. At the forefront of cybersecurity research, IOActive has amassed over a decade of real-world vulnerability data about the cybersecurity threats today's vehicles face.

This paper collects the automotive-related data IOActive has discovered through thousands of testing hours and provides a wide-band analysis of the years 2012 to 2022 via data points such as the impact, likelihood, and overall risk of the vulnerabilities we discovered. Additional information regarding IOActive's test methodologies, as well as breakdowns of the attack vectors, vulnerability types, and prevention mechanisms we identified, is also included. IOActive originally published an analysis of vehicle vulnerabilities in 2016 and provided an update in 2018. The goal of this update is to deliver current data and discuss how the state of automotive cybersecurity has progressed over the course of 10 years, noting overall trends. The target audience is individuals seeking insights into automotive cybersecurity and how to better address common automotive vulnerabilities.

Technical Findings

The major technical findings from IOActive's analysis are the following:

- There was a significant drop in the proportion of critical-impact vulnerabilities from 2016 to 2018. Critical-impact vulnerabilities decreased by 15%, causing the distribution of medium- and low-impact vulnerabilities to increase.
- The industry saw significant growth in incorporating cybersecurity into the design of automotive systems from the start; for example, ensuring that processes that handle data run with limited privileges, which helps lower the impact of the most likely attacks in the event of a compromise.
- There was an early warning observed in 2018 that the industry appears to be focusing on severity of ease-of-exploitation over actual risk.
- A sharp decrease in physical attacks was reported, which was mainly due to industry attention focusing on remote-based attack vectors.
- There was an interesting variance in the newer classes of vulnerabilities discovered in modern systems. The largest increase has been in web-related vulnerabilities (+11%), followed by vendor-dependency vulnerabilities (+9%), and then information disclosure (+2%).
- There has been a definite overall increase in vulnerabilities related to web and vendor dependencies, an interim increase in information disclosure, and an overall decrease in issues caused by failure to follow the principle of least privilege and vendor backdoors.
- The trends observed between 2018 and 2022 are the complete opposite to what IOActive previously observed, which indicates a bounce-back effect. High-effort vulnerabilities have decreased by 6% and medium-effort have decreased by 11%, resulting in a major increase (17%) of low-hanging fruit issues.

In general, IOActive observed a net positive in risk-remediation strategies that have benefitted modern vehicles; however, while there is an overall decrease in the number of critical-impact and high-impact vulnerabilities, there is a net increase in the overall risk. Based on further investigation, these trends are largely the result of the new technologies in modern vehicles and supply-chain management. Although the automotive industry is "building better," there is an evident disparity in the maintenance and harmonization of new and existing systems.

Explicit emerging threats include managing the Software Bill of Materials (SBOMs) and third-party vendors and a subtle trend to hyper-focus on severe threats, potentially paving the way for attack chaining.

The Research Analysis | Key Takeaways

- New attacks techniques continue to emerge; therefore, it is unsustainable to maintain the cybersecurity of automotive components simply by chasing flaws in new technologies. Automotive vendors and manufacturers should consider developing risk-mitigation strategies that focus on building cybersecurity into the foundation of their vehicles—whether that be within the SBOM, hardware, or chosen cybersecurity requirement specifications *and their validation within targeted architectures.*
- Automotive manufacturers and vendors should not hyper-focus on critical-risk and high-risk vulnerabilities, and thus overlook vulnerabilities categorized as medium-risk and below. Attackers are inherently languid, and most exploits discovered in the wild follow the path of *least resistance.* Tolerating medium-risk vulnerabilities could lead to a rise in attack chains that achieve a critical compromise of an automotive component.
- The management of third-party vendors (e.g., after-market devices) and the influence of SBOMs on the overall cybersecurity of a vehicle is evident; therefore, risk-remediation strategies should include the hardening of supply-chain cybersecurity and verifying that the components integrated into existing automotive systems adhere to cybersecurity principles.

.

Introduction

This research provides a metadata analysis of the private automotive cybersecurity assessments IOActive has conducted. We have incorporated a rolling analysis of vulnerabilities in automotive components, including a discussion of the specific systems and attack vectors that are most often affected and the real-world significance of these vulnerabilities. This data is valuable for organizations considering cybersecurity strategy and planning for their automotive components. This paper is a follow-up to IOActive's 2016 and 2018 reports and revisits the topic of automotive vulnerabilities using data from the past four years (2018-2022) to analyze how the industry has progressed over the course of the last 10 years (2012-2022).

Automotive cybersecurity is a focused area of cybersecurity research for IOActive. IOActive has performed thousands of hours of specialized testing on transportation and automotive systems, accumulating thousands of metadata results relating to the cybersecurity postures of automotive systems.

Figure 1. Summary of IOActive's Work on Automotive Cybersecurity

IOActive's research uses hard data taken from real-world automotive systems. We have conducted enough assessments over the last 10 years to allow for proper data anonymization and normalization. Total vulnerability counts are not shared in this paper due to their statistical irrelevance in regards to the wider data distribution. Randomized groups for each category were selected throughout the analysis to continually validate that the trends we observed and conclusions we drew remained valid and representative of the total data set.

It is important to note that with few exceptions, this research does not include metadata sets related to supporting technologies, such as transportation-related backend systems, agnostic mobile applications, and agnostic web interfaces. Although such technologies are prevalent in the automotive industry, they are immaterial to the scope of this research—they are not explicitly related to automotive cybersecurity and thus any trends in these supporting technologies could cause unwanted skews in IOActive's automotive-specific control data sets.

This paper begins with a discussion of IOActive's threat surface methodologies, to explain how the vulnerabilities used in this research were discovered. IOActive's approach to the categorization of risks is then covered, including a worked example. Finally, we provide an in-depth analysis of commonalities and trends, including metrics, types, and approaches to remediation.

Foreword

The research described in this paper was initially presented at ESCAR USA 2022 in Dearborn, Michigan, USA by Samantha Isabelle Beaumont on behalf of IOActive. Since June 15th, 2022, no major changes have been noted between the finalized version of this paper and the presentation; the two should be considered complementary materials with the paper including a more detailed analysis and discussion of the information presented at ESCAR. Similar to the presentation, no photographs have been included in this paper to prevent material identification.

Threat Surface Methodology

Understanding the attack surface of connected cars is an important first step in analyzing common vulnerabilities in vehicles. This means enumerating the pathways to attack a target, from the entire vehicle to a single component. IOActive's threat methodology does not focus on attack *methods*, but rather, attack *vectors*—also known as threat vectors.

Threat Vectors of a Connected Car

Connected cars feature a wide array of interfaces that allow for user interaction, such as Bluetooth, cellular, WiFi, USB, and various manufacturer-specific interfaces. At IOActive we focus on practical threats, starting with exposed interfaces and identifying exploitable vulnerabilities in order to emulate the most realistic threat scenarios—we adopt an 'attacker's mindset.' Rather than digging through the entire codebase looking for every possible flaw, we determine where an attacker could get data into the system and look for the most likely attack vectors. In Figure 2, the most commonly attempted attack vectors are shown in red while those in grey are supplementary focuses which vary by target and threat scenario:

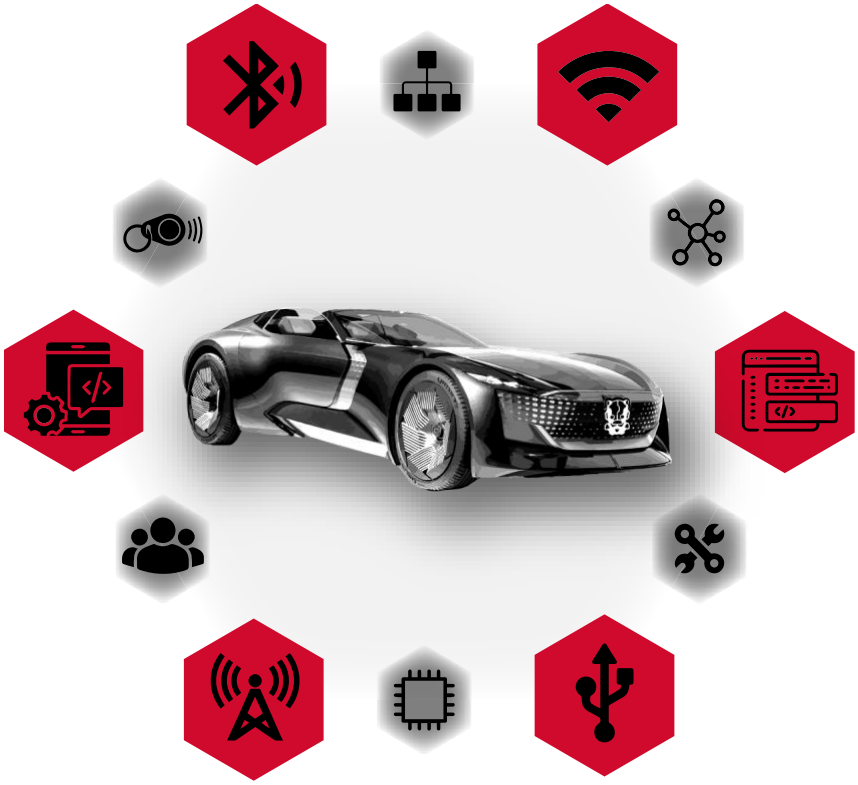


Figure 2. beginning from top centre, clockwise: Prototocol Bus (CAN/Serial), Wi-Fi, Backend Network, Software Bill of Materials/Onboard Firmware (SBOM), Manufacturer/Factory/Dealership Access, USB/Peripheral Devices, Hardware/ECU, Cellular, Physical, ECU/Mobile Applications, Remote Common Attack Vectors for the Connected Car (Audi Skysphere Concept - Design Sketch, 2021) (Remote Key Entry Systems (RKEs) and Bluetooth)

Modernizing Threat Vectors

One key difference between this paper and previous papers published by IOActive is the approach we used to categorize threats to the automotive industry. As automotive technology has evolved, so have the threat vectors and attempting to use a prescriptive model such as that illustrated in Figure 2 is not sustainable, nor entirely prescriptive to the entirety of the possibilities in automotive exploitation; it is evident that there are clear commonalities in the vectors which can be easily surmised. Furthermore, this method does not capture how the threats can be fixed. Therefore, IOActive has developed a new approach using categories that stakeholders can quickly digest; after all, a weakness in the firmware loaded onto a Telematics Control Unit (TCU) is different from a configuration flaw in the hardware components of a Battery Management Module (BMM).

IOActive's new approach organizes threat vectors into four categories based on how an attacker logically interfaces with a vulnerability and the main cause of the vulnerability within the vehicle ecosystem.

1. **Local**: Attacks that exploit vulnerabilities in the vehicle's software ecosystem.
   i.e., Filesystems, Firmware, Operating Systems, Binaries, Mobile Applications, ECU Applications, SBOMs
2. **Physical Hardware:** Attacks against the vehicle's physical hardware components that require the physical presence of the threat agent.
   i.e., Serial, USB, CAN, JTAG, Automotive Ethernet (100Base-T1/BroadR-Reach)
3. **Networked Connections:** Attacks that originate via the *far-field* RF spectrum.
   i.e., Wireless, Cellular, Backend Networks, V2X (802.11p)
4. **Peripheral RF:** Attacks that originate via the (approximate) *near-field* RF spectrum.
   i.e., NFC, RFID, Remote Key Entry (RKE), Bluetooth, On-board Telematics (TPMS, ADAS)

Figure 3 illustrates this updated approach to categorizing automotive attack vectors which allows for useful insights on the impact threat assessment practices have against a vehicle's presented attack vectors:

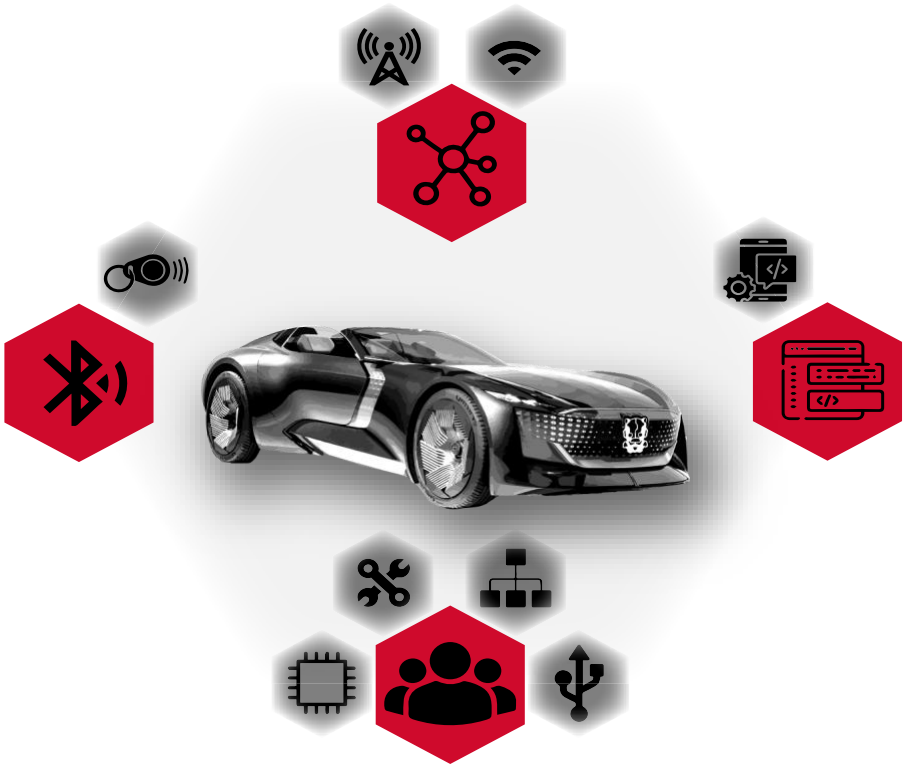


Figure 3. Major Cumulative Threat Vectors for the Connected Car (Audi Skysphere Concept - Design Sketch, 2021)

It should be noted that in some cases threat vectors cannot be accurately categorized without specific sources of information, such as the firmware or source code for the Device Under Test (DUT).

It should also be noted that some of the data used in this research (i.e., 2016 and 2018) used different categories. An in-depth discussion of aligning prior research with this work is discussed in Key Analysis Categories.

Threat Assessment Practices

IOActive uses a variety of test methodologies and threat assessment practices depending on the component being analyzed; however, most engagements take one of two approaches: black-box or white-box (grey-box can usually be considered as any combination of the two). Where IOActive predominantly specializes emulating real-world attack scenarios with an attacker's mindset, black-box and white-box testing can influence the types of vulnerabilities, threat vectors, and trends noted by an assessment team.

Black-box Approach

Black-box testing assumes no foreknowledge or insight into how the DUT operates. An IOActive cybersecurity consultant assumes the role of a zero-knowledge attacker who must evaluate the system, discover how it works, and attempt to find and exploit vulnerabilities while working within the scope and time-constraints of the engagement. Example black-box assessment activities include dynamic testing via protocol fuzzing, hardware analysis, chip desoldering, fault injection, serial bus line observation, and capturing firmware updates.

A usual motivation for taking this approach is to evaluate what a real-world attacker would see or do, but in reality, the assessment rarely plays out as intended as real-world attackers are not limited by scope or time when attacking a system. During black-box assessments, more time is dedicated to discovering how to use the DUT and developing the harnesses, tools, or methodologies required for testing. This limits the time available for the testing itself and is not indicative of a real-world scenario wherein an attacker would not have such limitations.

White-box Approach

White-box testing gives the IOActive cybersecurity consultant the opportunity to collaborate with key knowledgeable individuals, such as a product developer, to evaluate the system. Additional provisions may include providing the source code or a debug testing harness for the DUT.

In general, white-box testing provides the best return on investment (ROI) to customers and has produced the most useful data sets for this specific research. A white-box approach allows IOActive to establish true causality and perform in-depth root-cause analysis, which is valuable when analyzing trends and helps align associated risk with the specific business risk tolerance for the DUT.

Key advantages of white-box testing include:

- Less time figuring out how a system works and more time discovering vulnerabilities.
- Better able to evaluate the impact and likelihood levels of any discovered vulnerabilities.
- Better able to provide insights and assistance in areas of the system that may not be directly accessible to an attacker but might become accessible in the future via attack chaining or the presence of another vulnerability not presently known.

Risk Classification Methodology

Initial Ratings

Understanding how IOActive classifies risk—also termed severity—is a crucial step to understanding a substantial portion of this research's quantitative analysis. IOActive uses likelihood and impact scores when determining the total risk posed by a vulnerability:

- **Impact**: The business impact, influence or effect of successfully exploiting the vulnerability on the DUT and/or the associated vendor(s). *"What would happen if this vulnerability was exploited?"*
- **Likelihood**: The chances the vulnerability will be exploited by an attacker based on the skill set, tools, and knowledge required, as well as the associated attack vector required to locate and exploit the weakness. *"How easy is this vulnerability to find, access, and exploit?"*

Each area is assigned a rating of critical, high, medium, low, or informational with associated numeric scores ranging from 5 to 1, respectively.

Table 1 summarizes IOActive's rating methodology and specific considerations when evaluating a real-world threat scenario.

Table 1. Rating and score as applied to impact and likelihood

Rating (Score)	Impact	Likelihood
Critical (5)	Complete component compromise or definite ASIL safety concern if exploited.	Vulnerability can be exploited remotely and is easily discovered or already has publicly available information.
High (4)	May allow for partial component control, disclose sensitive personal information, disable functionality, or create a potential ASIL safety concern if exploited.	Vulnerability can be exploited from nearby or requires limited skills and information.
Medium (3)	May disclose sensitive technical details, compromise telematics communications, or disrupt driver and/or road user experience if exploited.	Vulnerability can be exploited with limited physical access or a skilled attacker can exploit the vulnerability.
Low (2)	Compromise is not sensitive or damaging on its own but could be useful in exploiting other vulnerabilities.	Vulnerability can be exploited with extensive physical access, by an attacker with limited insider knowledge, or significant skills and experience.
Informational (1)	Poor programming practice or design decisions that do not represent an immediate risk on its own but is considered 'bad practice.'	Exploitation requires an unreasonable amount of time, effort, or resources, or sensitive insider information.

With regards to the automotive industry, IOActive's **impact** score is influenced by a vulnerability's effect on the vendor and their relationship with critical standards, such as ISO 26262 (International Organization for Standardization, 2018), SAE J3021 (SAE International, 2021), or, more recently, ISO 21434 (International Organization for Standardization, 2021) and UNECE R155 (United Nations, 2023).

Generally speaking, a vulnerability is considered a serious concern if its exploitation would meet a failure criterion for any functional safety requirements. More specifically, IOActive considers the impact of a vulnerability in relation to ISO 26262's Automotive Safety Integrity Levels (ASILs), which are based on three variables: severity, probability of exposure, and controllability by the driver.

Overall Severity (Risk)

Once impact and likelihood scores are determined, IOActive calculates an aggregate severity score using Equation 1.

Equation 1.

$$Impact \times Likelihood = Aggregate\ Severity\ (Risk)$$

For example, a vulnerability with 'high (4)' likelihood and 'low (2)' impact would have an aggregate risk score of eight (8), thus be classed as a "Medium". Now, in several instances, there will be cases where there will be multiple vulnerabilities under the same severity category. Thus, practically speaking, when performing vulnerability and risk assessments, a final question is posed:

"How does one determine levels of criticality within a severity category? i.e. How does one measure if a critical finding of Type A is 'more critical' than a critical finding of Type B?"

As such, when an aggregate risk score is calculated – which also determines a vulnerability's overall risk level - there are boundaries set which assist a more granular understanding of these risk levels and where a vulnerability sits within them, where necessary. These boundaries are as shown in Table 2.

Table 2. Overall risk levels and corresponding aggregate scores

Overall Risk Level	Aggregate Risk Score
Critical	20–25
High	12–19
Medium	6–11
Low	2–5
Informational	1

Therefore, in summary, in an example event where there are two critical-risk vulnerabilities – a vulnerability with an aggregate risk score of 20 would be deemed less-critical when compared to a vulnerability with an aggregate risk score of 25; allowing for an at-a-glance understanding of a DUT's threat surface.

Worked Example

The following is based on real vulnerabilities IOActive has discovered and is intended to provide a step-by-step example of IOActive's logic when evaluating critical elements of the vulnerability rating process. A short discussion of plausible remediation is also included.

The DUT in this case is an Automotive Head Unit (AHU) that allows users to load and play media files via USB. To emulate an attacker, the consultant would fuzz test (OWASP Foundation, Inc., 2022) the AHU's user-available interfaces (i.e., USB) with different media types looking for errors in the DUT's media parser. In this scenario, IOActive identified an issue within the parser, wherein a specially crafted malicious MP3 file would result in memory corruption and eventual code execution within the AHU on behalf of the media player user service.

Impact

This finding would not directly allow for total control of the vehicle or complete control of the DUT, as the media player user service has limited access and cannot directly access or influence any critical safety systems within the rest of the vehicle. While this vulnerability would be detrimental to the road user's experience and could be used as a foothold for further attacks, these would not be considered as severe to the safety of a road user. Therefore, the impact rating for this vulnerability would be medium (3).

Likelihood

Exploiting this vulnerability requires physical access to the device but does not require access for an extended period of time. Additionally, an attacker would need more than basic skills and expertise to find this vulnerability and develop an effective exploit. Furthermore, this flaw would be specifically limited to the AHU and firmware build, therefore limiting possible exploitation scenarios. Therefore, this likelihood rating for this vulnerability would be medium (3).

Overall Risk

With a medium impact and a medium likelihood, the aggregate risk rating would be calculated as follows:

Equation 2. $$Impact\ (3) \times\ Likelihood\ (3) = Aggregate\ Risk\ (9)$$

A score of 9 indicates that this vulnerability poses an overall medium risk on its own; however, a skilled attacker could develop an exploit that would allow someone with limited access to gain a foothold on the device, possibly utilizing this vulnerability for further exploration or exploitation of the DUT via newly discovered attack vectors.

Remediation

Remediating this issue would vary significantly based on its root cause. If it was the result of an outdated media library, the recommendation would be to update the media library. If the flaw is instead located within an open-source library, it may be feasible to suggest back-patching the codebase. The specific recommendations depend on how much context and insight IOActive has into the system at the time of assessment, as discussed in Threat Assessment Practices.

Commonalities and Trends

This section presents IOActive's methodology for analyzing commonalities and trends as well as the results.

Key Analysis Categories

Having described IOActive's threat surface and risk classification methodologies, it is possible to describe commonalities and trends within the raw vulnerability data sets. This research is organized into three main evaluation categories:

1. Vulnerability Metrics
    i. Impact
    ii. Likelihood
    iii. Overall Risk
2. Attack Typecasting
    i. Attack Vectors
    ii. Vulnerability Types
3. Remediation Approaches
    i. Level of Effort/Difficulty Ratings for Critical Impact Remediation
    ii. Ounce of Prevention Suggestions

The purpose of these categories is to definitively determine the cause of any skews noted within the raw data. Each category is further broken down into subsections that include a refresher of the insights from the 2016 and 2018 papers, as well as analysis results from 2022 and 10-year trends.

When considering the data sets covered in this research, it should be noted:

- The initial paper, published in 2016, covers data collected between 2012-2016 (Thuen, 2016).
- The updated paper, published in 2018, covers data collected between 2017-2018 (Hammond & Culiss, 2018).
- This major update covers data collected between 2019-2022 and includes an overall trend analysis of data collected between 2012-2022.

Note that a key for all of the graphs and charts is provided at the beginning of each subsection. All of the graphs and charts in this section are presented in a larger format in Appendix B.

Vulnerability Metrics

When considering the state of automotive cybersecurity, an obvious place to begin is to evaluate how the distribution of risk ratings has changed over time. The goals of this analysis were to determine if the severity of vulnerabilities was increasing or decreasing and the reasons behind these changes. A breakout of the vulnerability metrics is done at this stage to granularly understand causality in vulnerability trends: i.e., *"Are vulnerabilities becoming more or less critical? Are they requiring attackers to be more skillful?"*

Impact

Definition: "The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the cybersecurity state of the system" (National Institute of Standards and Technology, 2011).

Figure 4. Impact Key for Charts and Trends

2016 and 2018 Refresher

Looking at the data from 2016 to 2018 (Figure 5), most vulnerabilities were medium-impact. In general, these types of vulnerabilities would result in personal information disclosure or compromised network connections, but not persistent, privileged access to the system.

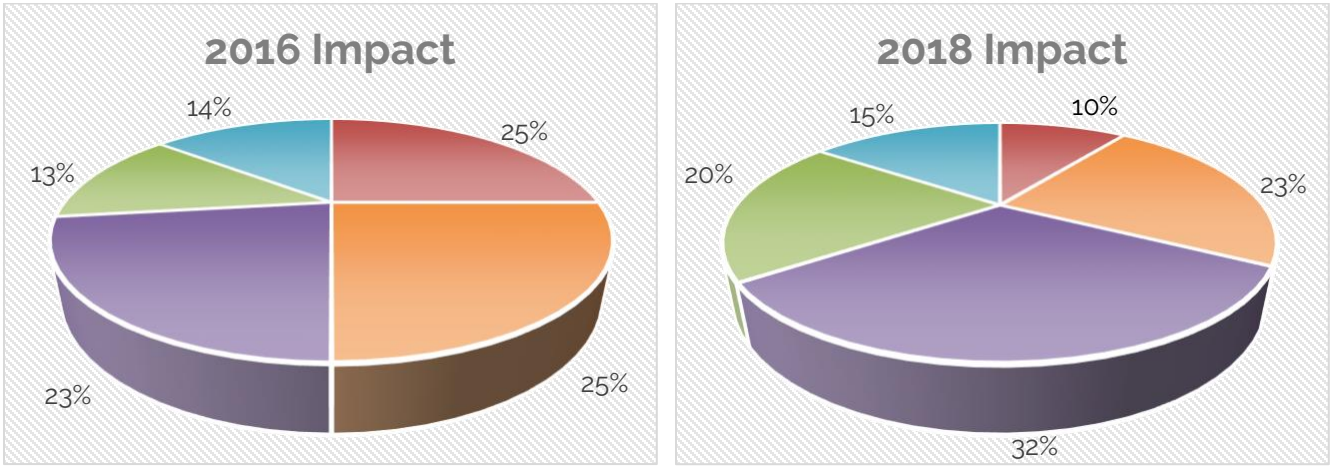


Figure 5. Impact Ratings 2016 (left) and 2018 (right)

There was a 15% drop in critical-impact vulnerabilities from 2016 to 2018, with a corresponding increase in medium-impact and low-impact vulnerabilities. Investigation into these years' vulnerabilities determined the trends were likely the result of better cybersecurity awareness and user separation due to the maturation of the automotive industry.

2022 Update and 10-year Trends

The impact distribution for automotive-related vulnerabilities discovered by IOActive from 2018 to 2022 (Figure 6) paint a slightly different picture. While high-impact vulnerabilities have decreased by 2%, critical-impact vulnerabilities have increased by 2%. Additional changes include a 2% increase in both medium-impact and low-impact vulnerabilities, and a 4% decrease in informational-impact vulnerabilities.

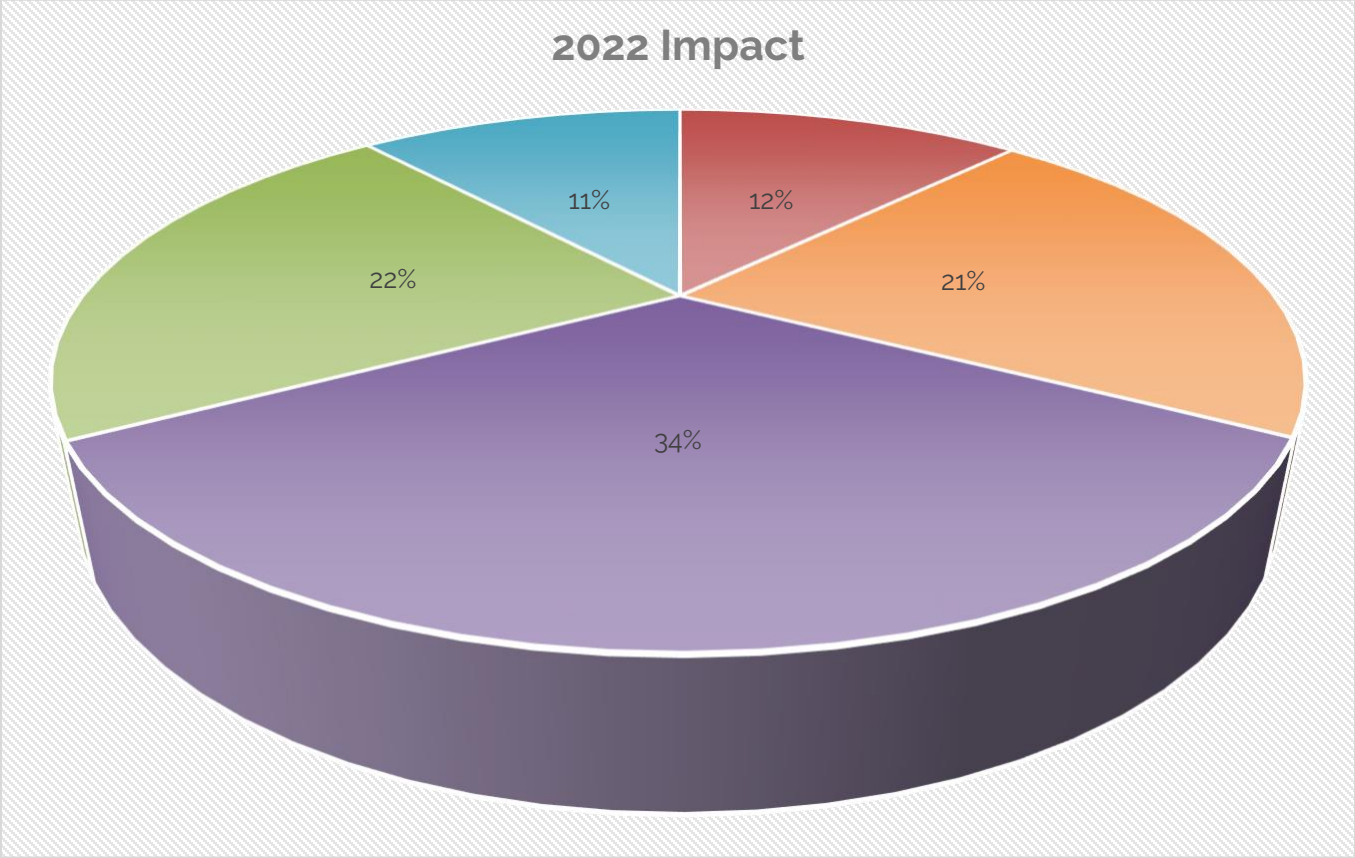


Figure 6. Impact Ratings 2022

Although this may appear to lead to unfavorable conclusions, it is important to note that during this same time period, the industry moved to incorporate cybersecurity in the design of automotive systems from the start. For example, designers began to ensure that processes that handle data run with limited privileges (covered in more detail in later sections), which helped lower the impact of the most likely attacks in the event of a compromise.

Nevertheless, with a negative distribution showing a distribution skew towards critical-impact vulnerabilities, breaking the 2016-2018 trend noted in previous years, this is where an overall big-picture analysis is highly effective in displaying the overall trends seen in automotive cybersecurity. Thus, Figure 7 displays the consideration of all 10 years of data, revealing the overall impact rating trends in automotive cybersecurity:

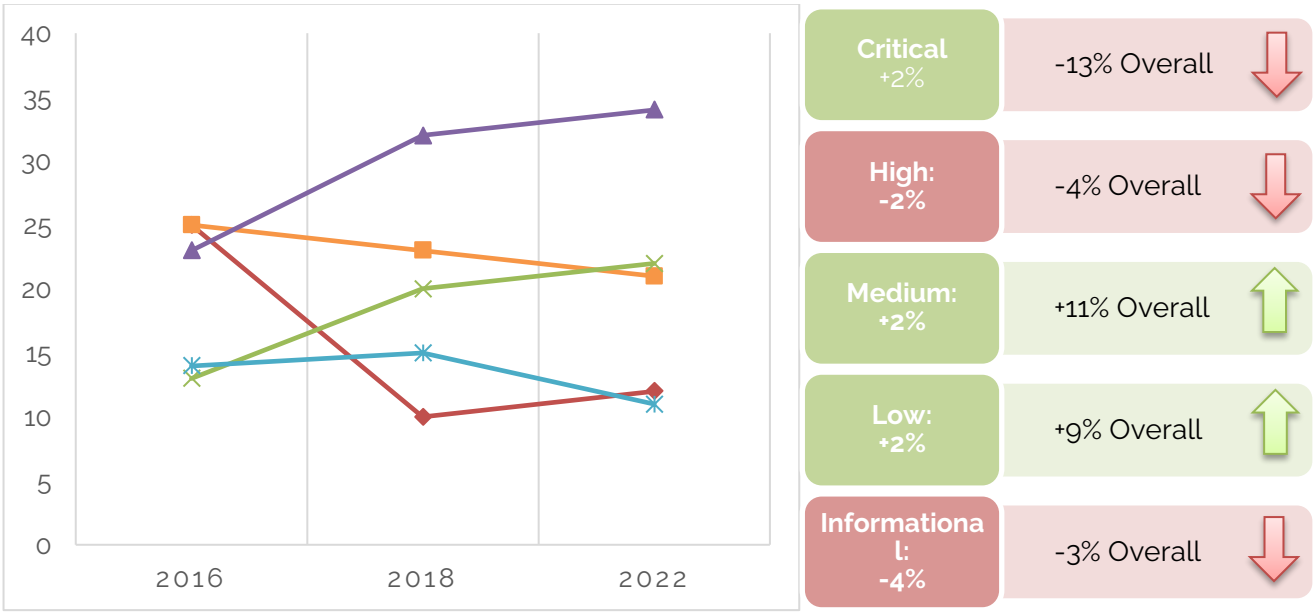


Figure 7. Impact Trends and Percentages 2018-2022 (left) and 10-year (right)

Figure 7 captures the fact that although critical-impact vulnerabilities have increased by 2% for the most recent analysis period, the 10-year trend is a 13% decrease. Furthermore, there is a positive distribution skew towards low-impact and medium-impact vulnerabilities. Based off the raw vulnerability data, this is largely due to the automotive industry building cybersecurity into earlier stages of the development process.

However, the interim increase in critical-impact vulnerabilities between 2018 and 2022 could be an early-warning sign of another trend present within the data; it is not enough to only look at one data set. To explore this hypothesis and determine if a similar trend is present elsewhere, further analysis into additional vulnerability metrics must be conducted, leading us to the analysis of Likelihood's and *"Are vulnerabilities more critical-impact due to vulnerabilities becoming easier to exploit?"*

Likelihood

Definition: "A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities" (National Institute of Standards and Technology, 2012).

Figure 8. Likelihood Key for Charts and Trends

2016 and 2018 Refresher

Data from 2016 and 2018 (Figure 9) indicated that a majority of findings were medium-likelihood or low-likelihood, meaning that most vulnerabilities were either only exploitable by highly skilled attackers or required the compromise of another vulnerable automotive system to be exploitable.

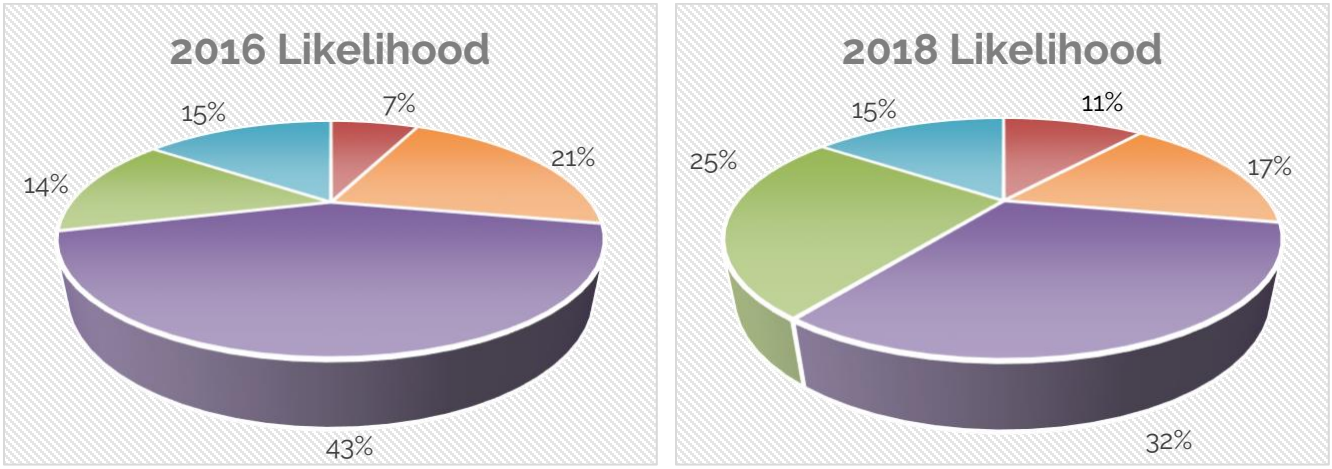


Figure 9. Likelihood Ratings 2016 (left) and 2018 (right)

Between 2016 and 2018, high-likelihood findings shifted towards critical-likelihood by 4% and medium-likelihood vulnerabilities skewed to low-likelihood by 11%. This complex interaction was likely the result of vulnerability type and attack vector changes caused by the introduction of new technologies into the automotive industry. During this time period, IOActive saw cybersecurity architecture improve significantly while also observing a significant increase in the number and scope of remote services which could easily be leveraged by a threat agent to attack the system.

2022 Update and 10-year Trends

Unlike the unfavorable skews of previous years, the analysis presented in Figure 10 shows just the opposite. Between 2018 and 2022, critical-likelihood vulnerabilities decreased by 10% and high-likelihood and medium-likelihood vulnerabilities decreased by 1%, leading to an overall increase in low-likelihood vulnerabilities of 4%.

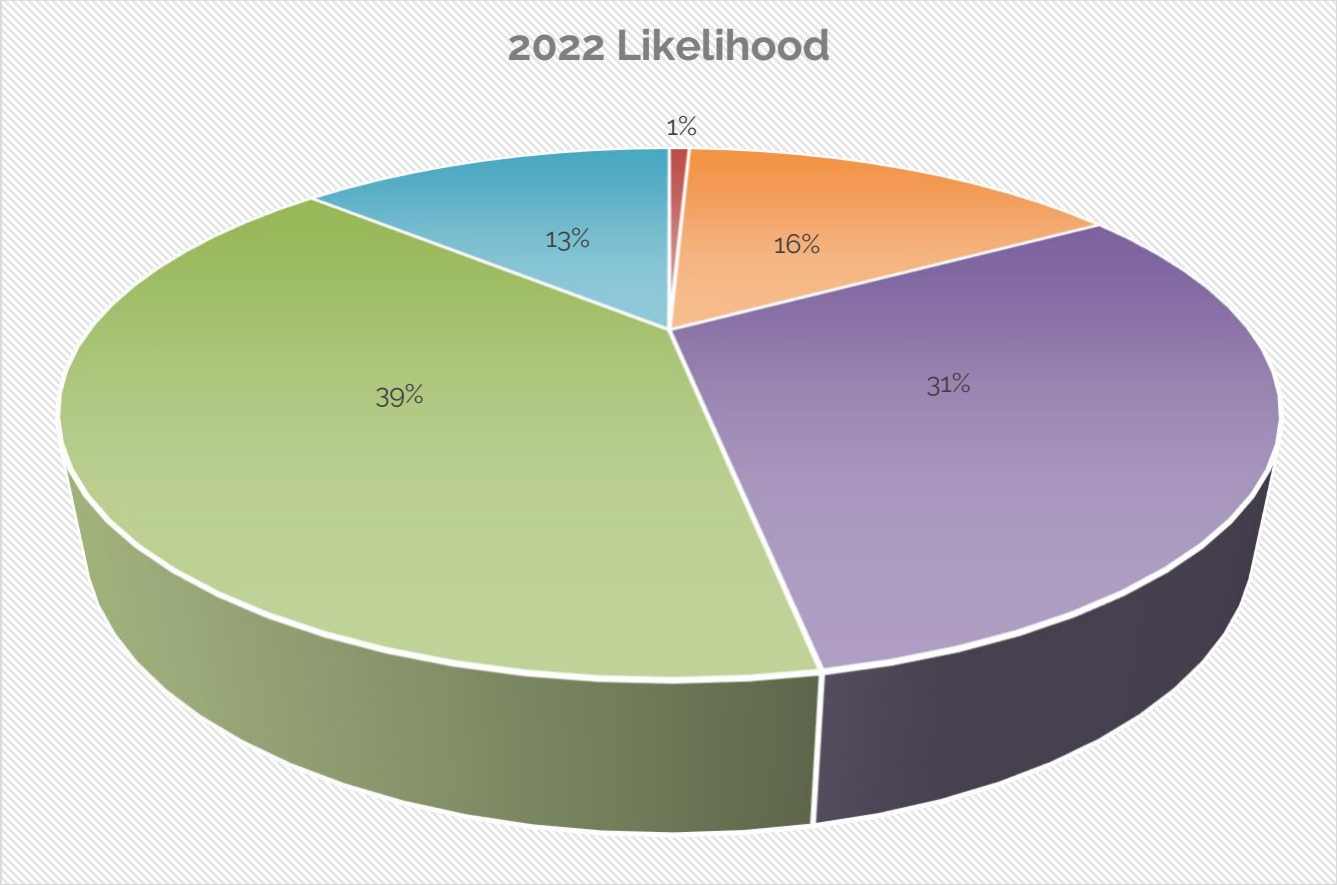


Figure 10. Likelihood Ratings 2022

Unlike impact, the likelihood displays a positive commonality hinting at the conclusion that either vulnerabilities are becoming harder to exploit (i.e., require higher skilled attackers to execute) or the vectors to discover vulnerabilities are becoming less remote. In cybersecurity parlance, there is less 'low-hanging fruit,' indicating that between 2018 and 2022, the automotive industry learned from its initial mistakes and is building better.

Figure 11 illustrates how the 10-year trends benefit from the bounce-back between 2018 and 2022.

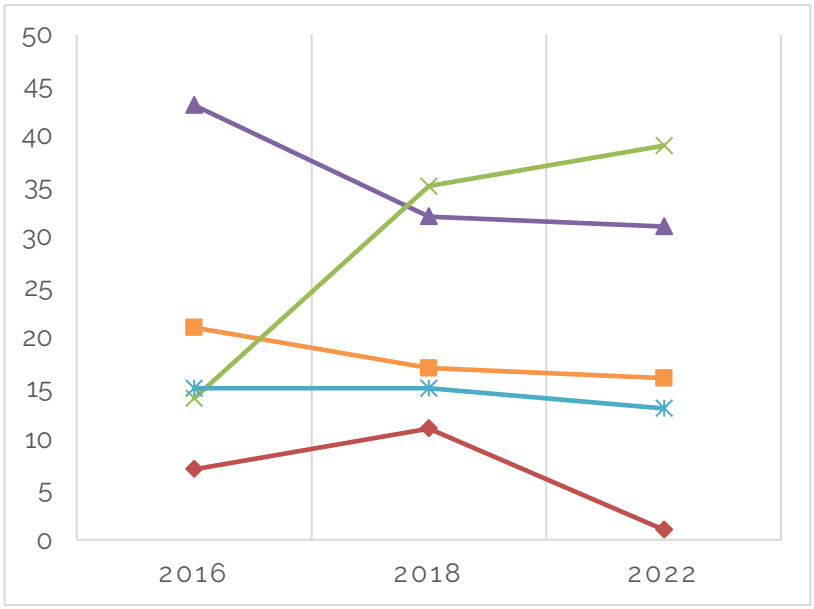


Figure 11. Likelihood Trends and Percentages 2018-2022 (left) and 10-year (right)

There is a positive skew of the entire data set resulting in low-likelihood vulnerabilities growing by 25%. Numerous factors could explain this trend, such as changes to the types of assessments and DUTs between these years; however, IOActive's observations of the raw vulnerability conclude that the automotive industry exposed fewer physical and network attack vectors, which are traditionally associated with easy-to-find vulnerabilities that only require low-skilled threat actors.

With a negative skew noted in impact, yet a strong positive skew observed in likelihood; the next stage of this analysis is to determine how these considerations translate to overall aggregate risk to a vehicular system. I.e., *"Although things are having a higher impact, with the ease-of-exploitation massively decreasing, does this directly translate into an overall decrease in risk?"*

Overall Risk

Definition: "The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or systems" (National Institute of Standards and Technology, 2012).

Figure 12. Risk Key for Charts and Trends

Note: This section does not include data related to informational-risk vulnerabilities wherein both impact and likelihood are informational. By definition, informational-risk vulnerabilities do not present a cybersecurity risk to an organization and thus are out of scope for this analysis.

2016 and 2018 Refresher

Figure 13 shows that the overall risk ratings for vulnerabilities were mostly medium and low for 2016 and 2018

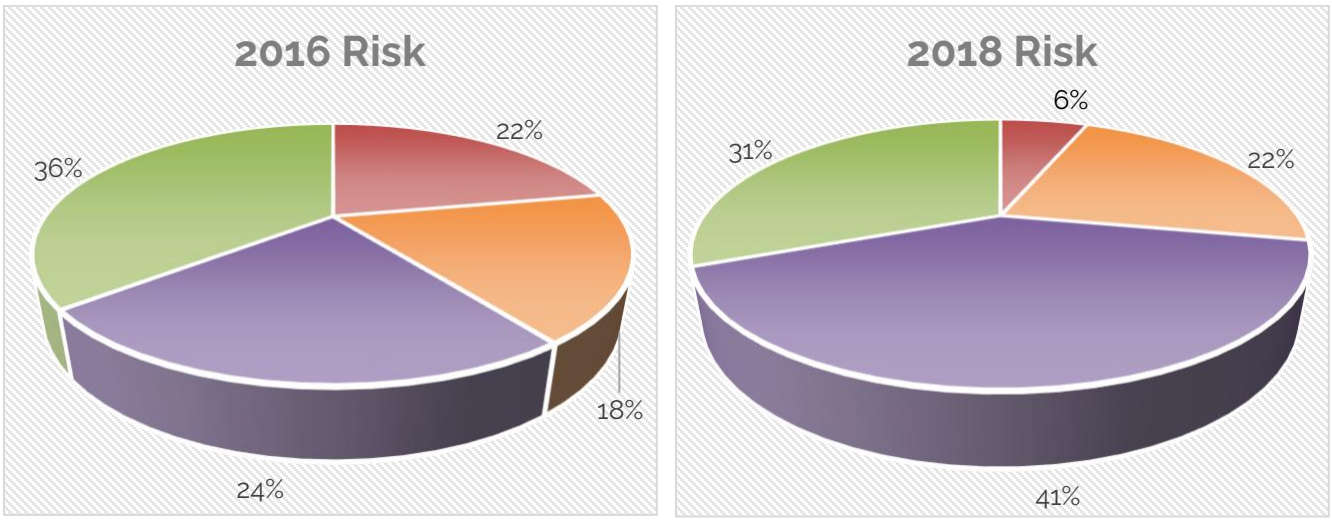


Figure 13. Overall Risk Ratings 2016 (left) and 2018 (right)

Critical-risk ratings underwent a major decrease (16%), indicative of the overall cybersecurity improvements IOActive detected in the automotive industry during this time. Notably, however, high-risk vulnerabilities increased by 6%, leading IOActive to warn that while this could be a natural movement of data normalization, since medium-risk vulnerabilities increased 17%, it could be a symptom that the automotive industry was choosing to only address critical-risk vulnerabilities; an observation IOActive had made in select instances.

2022 Update and 10-year Trends

As shown in Figure 14, critical-risk ratings continued to trend down, this time by 1%, and high-risk vulnerabilities also decreased by 1%, a positive change compared to prior years.

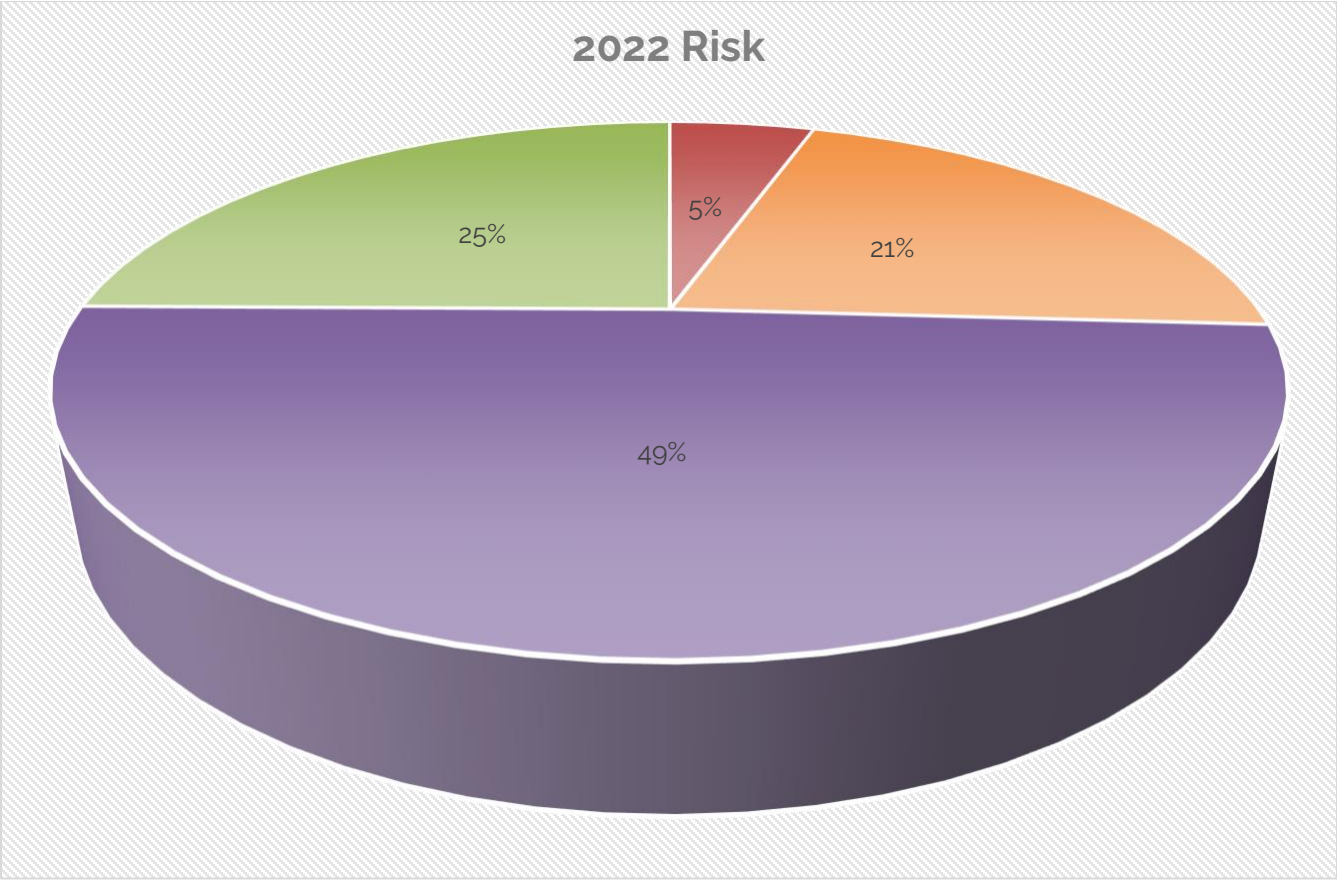


Figure 14. Overall Risk Ratings 2022

Medium-risk vulnerabilities increased by 8%, while there was a 6% decrease in low-severity findings; supporting the hypothesis made in earlier reports that the industry is tunnel-visioned on only fixing critical-risk findings.

The substantial number of medium-risk and low-risk vulnerabilities, however, does not necessarily equate to an overall reduction in risk to automotive cybersecurity. These vulnerabilities may not be as severe on their own; nonetheless they may still be harmful when exploited together in an attack-chain or leveraged as part of a larger attack-path if another, presently unknown, vulnerability is discovered.

Figure 15 explores the 10-year trends to determine the influence of an increased number of medium-risk vulnerabilities.

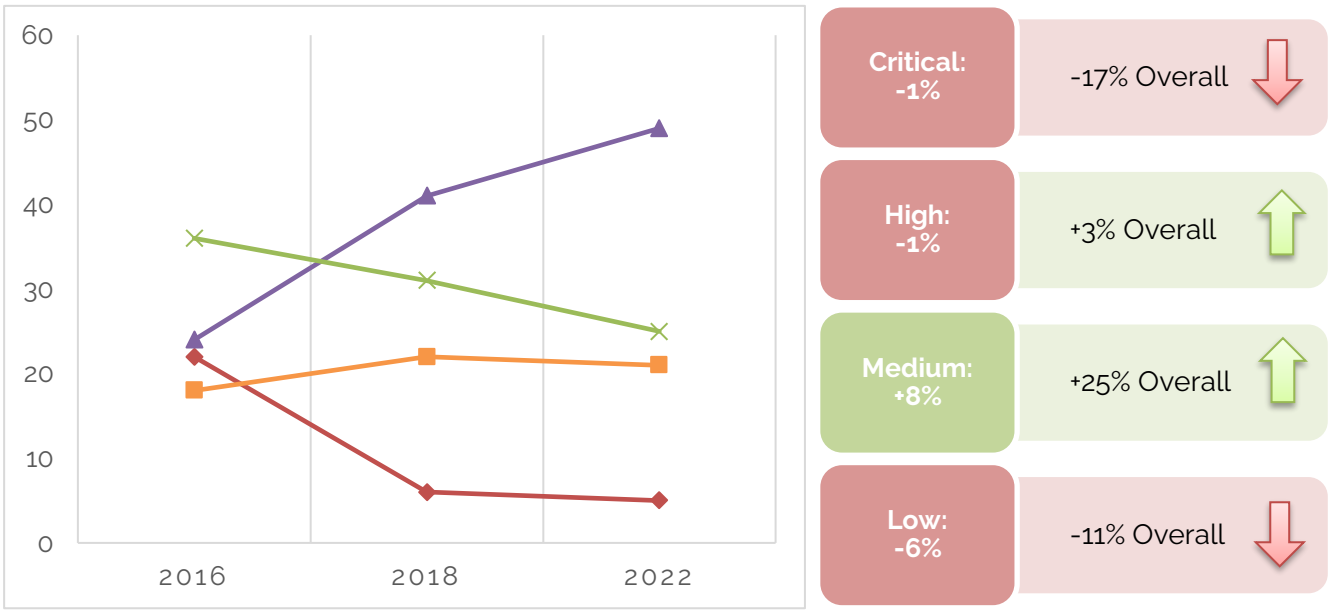


Figure 15. Overall Risk Trends and Percentages 2018-2022 (left) and 10-year (right)

As indicated, despite the positive trends shown between 2018 and 2022, there is an overall negative 10-year trend showing a net 3% increase in high-risk vulnerabilities.

In reviewing the raw data, IOActive noted that fixating of critical-risk issues may be the result of the standardization of risk across organizations. Customers tend to care more about critical-risk vulnerabilities simply because of time and financial constraints during manufacturing or testing.

This negative trend confirms IOActive's 2018 warning that the industry appears to be focusing on ease-of-exploitation over actual risk, resulting in overall severity beginning to favor high and medium.

Stepping back, it is not enough to focus on vulnerability risk, as several factors affect the industry's ability to change. Hence, we start by looking at attack vectors and vulnerability types in the next section "Attack Typecasting".

Attack Typecasting

As vulnerability metrics can be influenced by the type of attack, IOActive's next step was to evaluate the effects of how vulnerabilities are being exploited. The goals of this analysis were to determine if the attack vectors and vulnerability types were the reason for the trends seen across severity. i.e., *"Are vulnerabilities more severe due to the technology and vectors being exploited within vehicles?"*

Attack Vectors

Definition: Also known as 'Threat Vector', "an attack vector is a specific path, method, or scenario that can be exploited to break into a system, thus compromising its security" (International Organization for Standardization, 2021).

2016 and 2018 Refresher

Figure 16. Attack Vectors Key for 2016 and 2018 Charts

Attack vector categories are useful when evaluating how attackers approach a system. The most common attack vectors for the vulnerabilities IOActive discovered in 2016 and 2018 were local and network. Local attacks require an attacker to already have a foothold on the system, thus lowering their likelihood but increasing their impact since they often enable an attacker to elevate privileges or otherwise manipulate the system. Network attacks tend to represent the highest exposure and are often a major focus of cybersecurity testing.

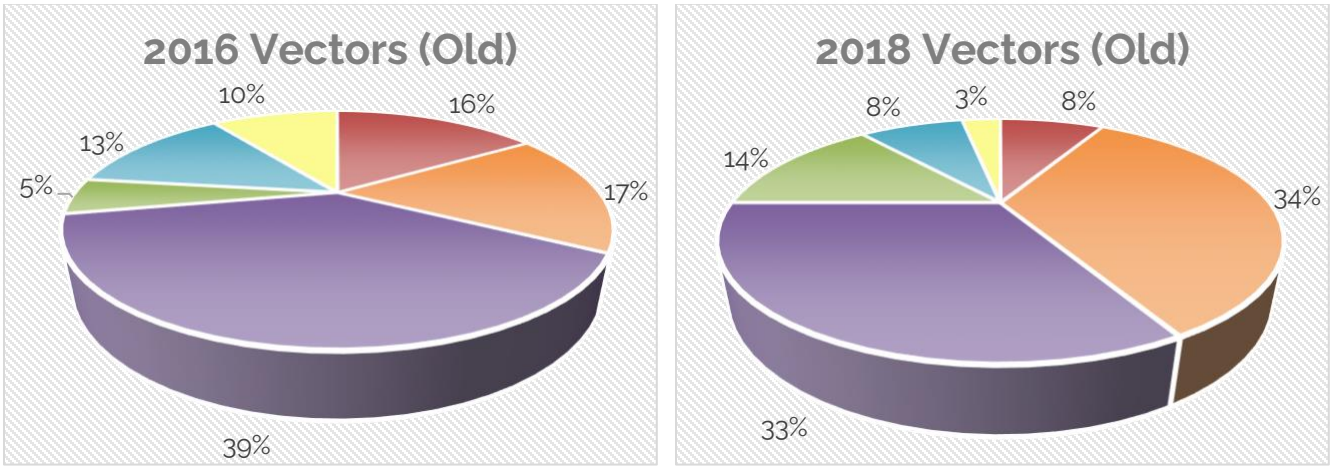


Figure 17. Original Attack Vectors 2016 (left) and 2018 (right)

As shown in Figure 17, there was a notable rise in local (17%) and serial attacks (9%) between 2016 and 2018. The attacks required physical access to the device and included the ability to read and modify firmware and discover data between components. They also often took advantage of debugging and test features left in the hardware.

Previous research attributed this increase to a shift from black-box to white-box testing. As the importance of cybersecurity increased between 2016 and 2018, IOActive noted that more companies provided documentation and debugging access to help identify vulnerabilities in their systems. The automotive industry also took more of an interest in lower-level cybersecurity features, like secure boot, which was reflected in the assessment areas.

2022 Update and 10-year Trends

Figure 18. Attack Vectors Key for 2022 Charts

As noted in Threat Surface Methodology, with the sharp rise in available technologies and attacks becoming increasingly specific, the 2022 update included a refactoring of the categories to more accurately reflect the types of attacks within the automotive industry. Figure 19 shows the 2016 and 2018 attack vector data translated to these new categories.

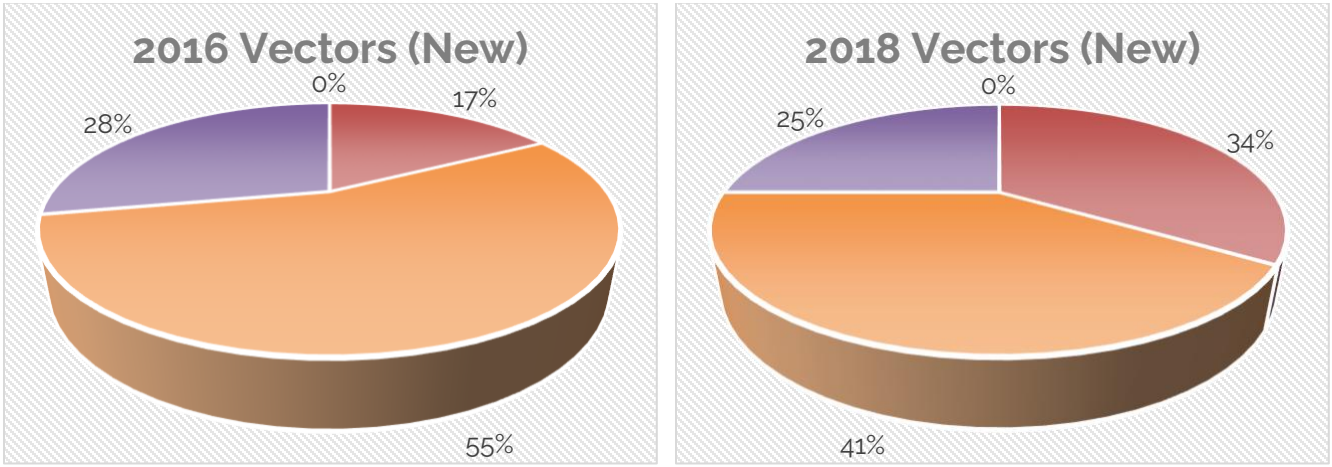


Figure 19. New Attack Vectors 2016 (left) and 2018 (right)

Similar to the previous work, there was a 17% rise in local attack vectors between 2016 and 2018, whereas there was a 14% decrease in networked connections attacks and a 3% decrease in physical hardware attacks. This is likely due to the more granular choice to define the boundaries between local, physical hardware, near-field (peripheral RF), and far-field (networked connections) vectors.

Carrying these observations forward and comparing them to the 2022 data sets is powerful. Figure 20 shows an increase in networked connections (8%) and local (6%) attack vectors and a sharp 15% decrease in physical hardware attack vectors. Most importantly, there is a new net increase in peripheral RF attack vectors of 1%, demonstrating how the modern technologies demanded by customers are beginning to have a clear and notable impact on automotive vulnerabilities.

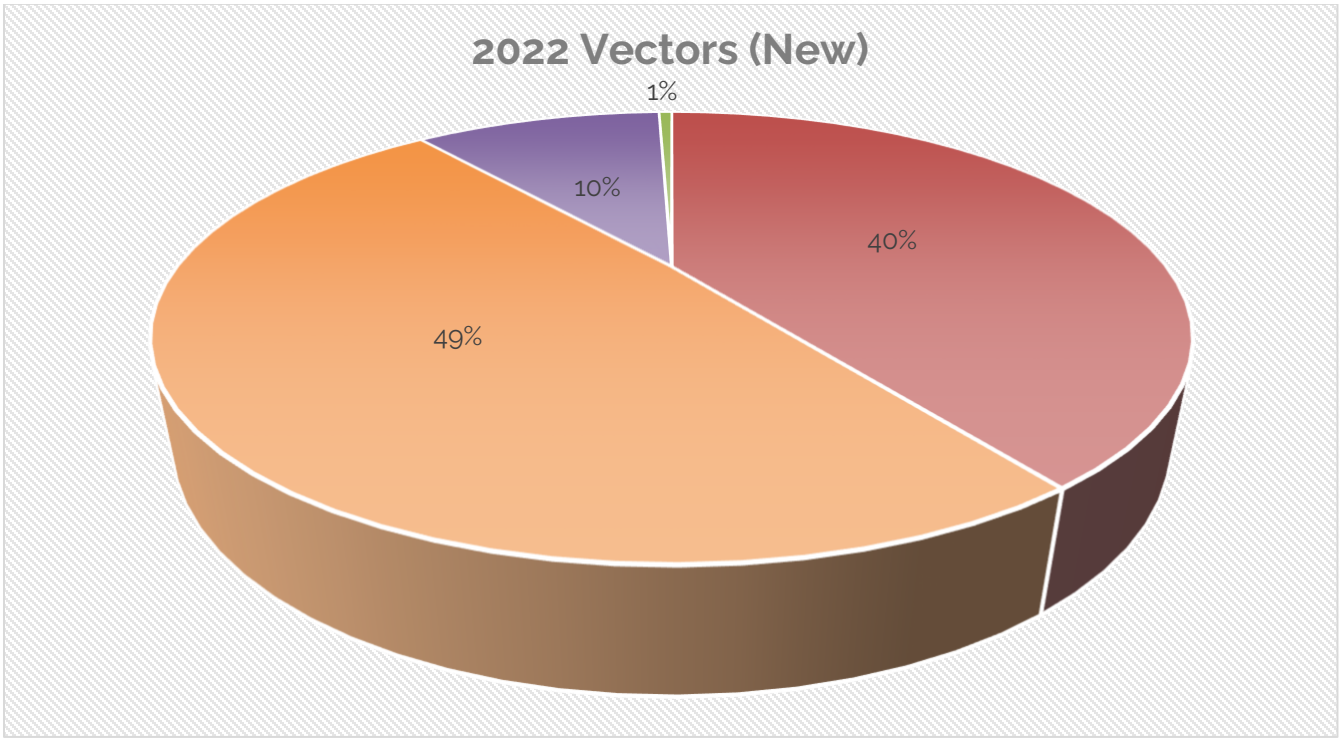


Figure 20. Attack Vectors 2022

IOActive's analysis found the 1% growth in peripheral RF attacks was largely due to RKE and Bluetooth-related vulnerabilities. The sharp decrease in physical hardware attacks was largely the result of the industry becoming more concerned with remote attack vectors (thus, those in the network category) at the expense of testing for physical cybersecurity.

The overall attack vector analysis shown in Figure 21 is positive with an 18% decrease in physical hardware attacks and 6% decrease in networked connections attacks. This positive skew is owed to the automotive industry's focus on reducing higher likelihood attack vectors, as indicated in Vulnerability Metrics.

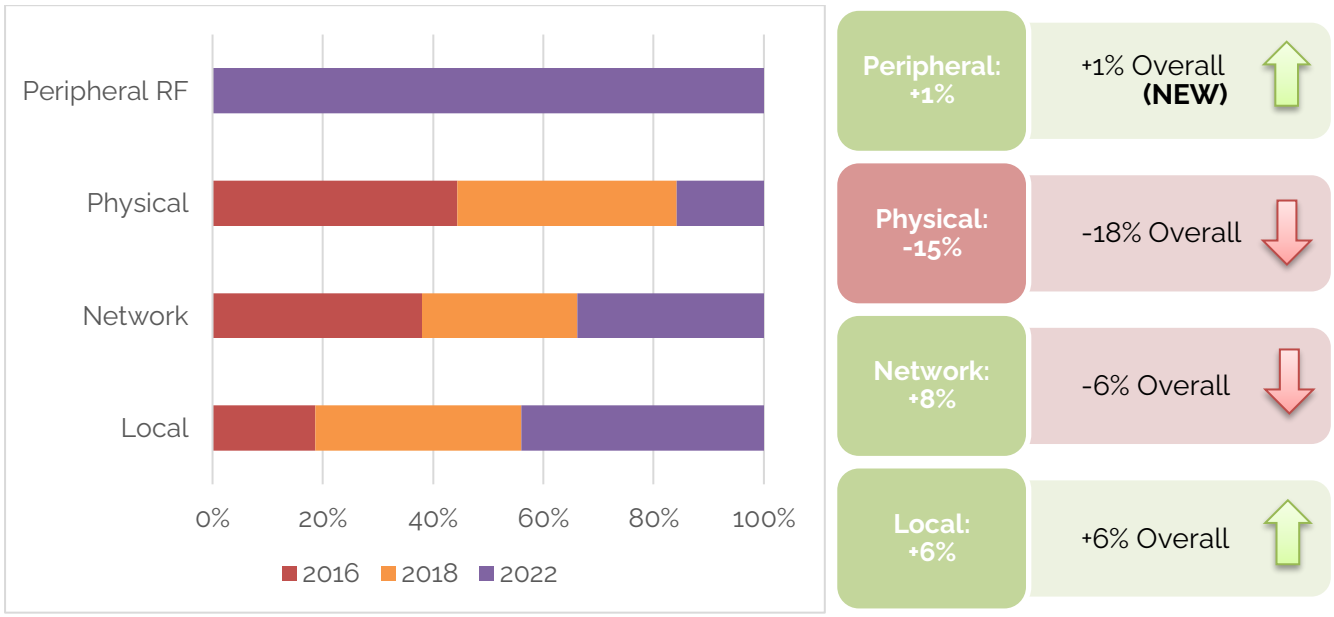


Figure 21. Attack Vector Trends and Percentages 2018-2022 (left) and 10-year (right)

One interesting trend is a year-over-year increase in local attacks, resulting in a 6% rise overall. This precludes a curious observation that the industry as a whole is struggling to keep up with attacks against vehicles' localized software stacks. Looking at the raw vulnerability data, this appears to be due to the exponential increase in software stacks within vehicles, where IOActive has noted larger codebases and firmware builds for similar components over time.

This leads perfectly to the next portion of this analysis which covers vulnerability types, i.e., *"Are the attack vector trends as a result of an increase in particular vulnerability types?"*

Vulnerability Types

Definition: "A weakness in an information system, system cybersecurity procedures, internal controls, or implementation that could be exploited or triggered by a threat source" (National Institute of Standards and Technology, 2006).

To help identify common issues and determine how these vulnerabilities come about in the first place, this research divides the collective vulnerability data into different types. Based on thousands of hours of testing, IOActive has determined that the majority of automotive-related vulnerabilities fall into three classes: system design, engineering, and deployment. These classes can be further divided into the following eight significantly weighted vulnerability types:

1. **Vendor-introduced Backdoors:** An undocumented way of gaining access to computer system (National Institute of Standards and Technology, 2017).
2. **Memory Corruption**: When a computer system's memory is altered without an explicit assignment. The contents of a memory location are modified due to programming errors that enable attackers to execute arbitrary code. Examples of such vulnerabilities include format strings, buffer overflows, and integer overflows.
3. **Coding Logic Errors**: Flaws in the design and implementation of logical code behavior that allow an attacker to elicit unintended behavior. This enables attackers to manipulate legitimate functionality to achieve a malicious goal. These errors come from bypassing the program logic rather than exploiting a technical flaw in how data is handled.
4. **Hardcoded Credentials:** The software contains information, like passwords or cryptographic keys, used for its own inbound authentication, outbound communication to external components, or encryption of internal data (The MITRE Corporation, 2010).
5. **Information Disclosure:** Sensitive information is exposed to an actor who is not explicitly authorized to have access to that information (The MITRE Corporation, 2006).
6. **Failure to Follow Principle of Least Privilege**: Secure architectures should be designed so that each entity is granted the minimum system resources and authorizations required to perform its function (National Institute of Standards and Technology, 2017).
7. **Vulnerable Dependency**: A vulnerability resulting from a flaw within a third-party dependency.
8. **Web**: A software code flaw, system misconfiguration, or some other weakness in an automotive-specific web application or its components and processes.

2016 and 2018 Refresher

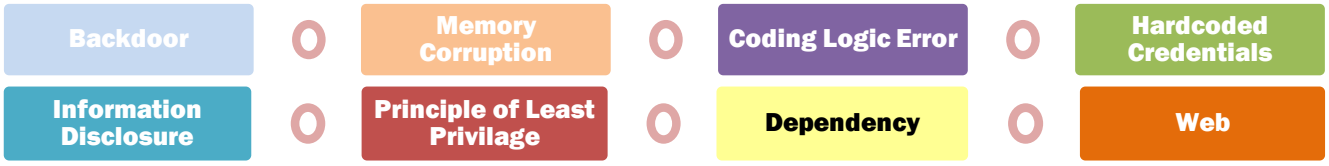


Figure 22. Vulnerability Types Key for Charts

Reviewing the data sets from 2016 and 2018, the most prevalent vulnerability type was coding logic errors, which, as indicated by Figure 23, also increased by 9%.

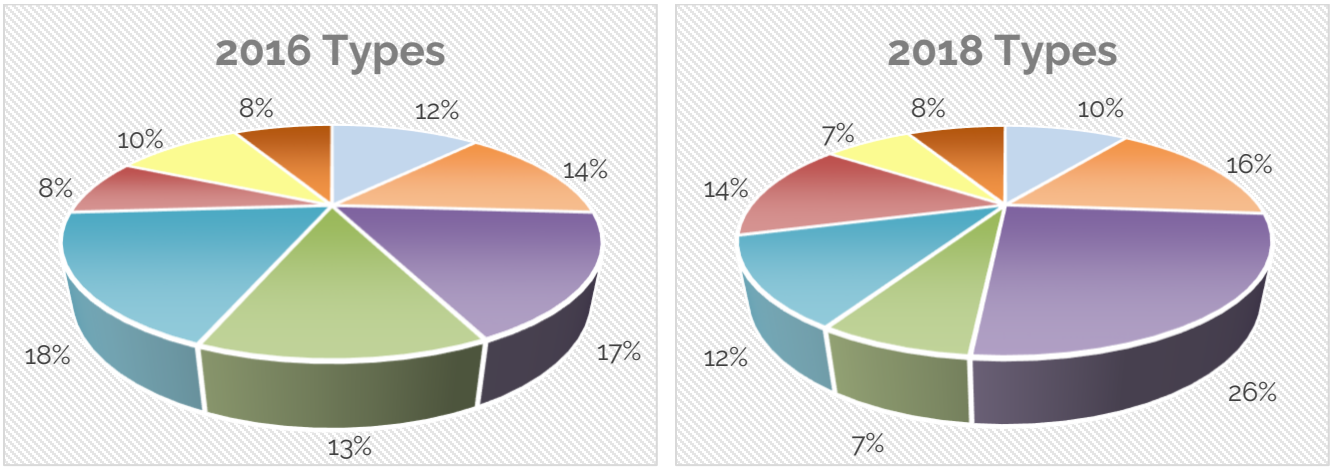


Figure 23. Vulnerability Types 2016 (left) and 2018 (right)

Previous analysis concluded that as architecture and development practices improved, coding logic flaws would represent an even larger portion of vulnerabilities, much like the trends seen in attack vectors—wherein an increase coding logic errors would directly result in an increase in local attack vectors. Similarly, memory corruption flaws also grew by 2%, further increasing the likelihood that the increase in local attack vectors was due to larger codebases and/or the increase in the related vulnerability type.

Additional notable trends included a 5% decrease in hardcoded credentials, which confirmed IOActive's observation that improved secure design processes had led to a decrease in the number of hardcoded secrets in automotive components.

2022 Update and 10-year Trends

Despite mostly positive trends in 2016 and 2018, Figure 24 shows a variance in the types of vulnerabilities discovered in recent systems. The largest increase, 11%, was in web-related vulnerabilities, followed by a 9% increase in dependency vulnerabilities and a 2% increase in information disclosure vulnerabilities.

Interestingly, there are some reversals in vulnerabilities. There was a modest 2% decrease in backdoors and memory corruption flaws and a substantial 9% decrease in both coding logic errors and failure to follow the principal of least privilege.

Looking at this data holistically, these trends could be an implicit bias in the type of assessment conducted; a white-box assessment will find more memory and logic flaws than a black-box assessment that does not allow for physical testing. This observation was supported by the raw metadata, where IOActive noted a substantial decrease in the industry choosing these assessment types due to factors such as cost, time, and preference to focus on newer vulnerability classes.

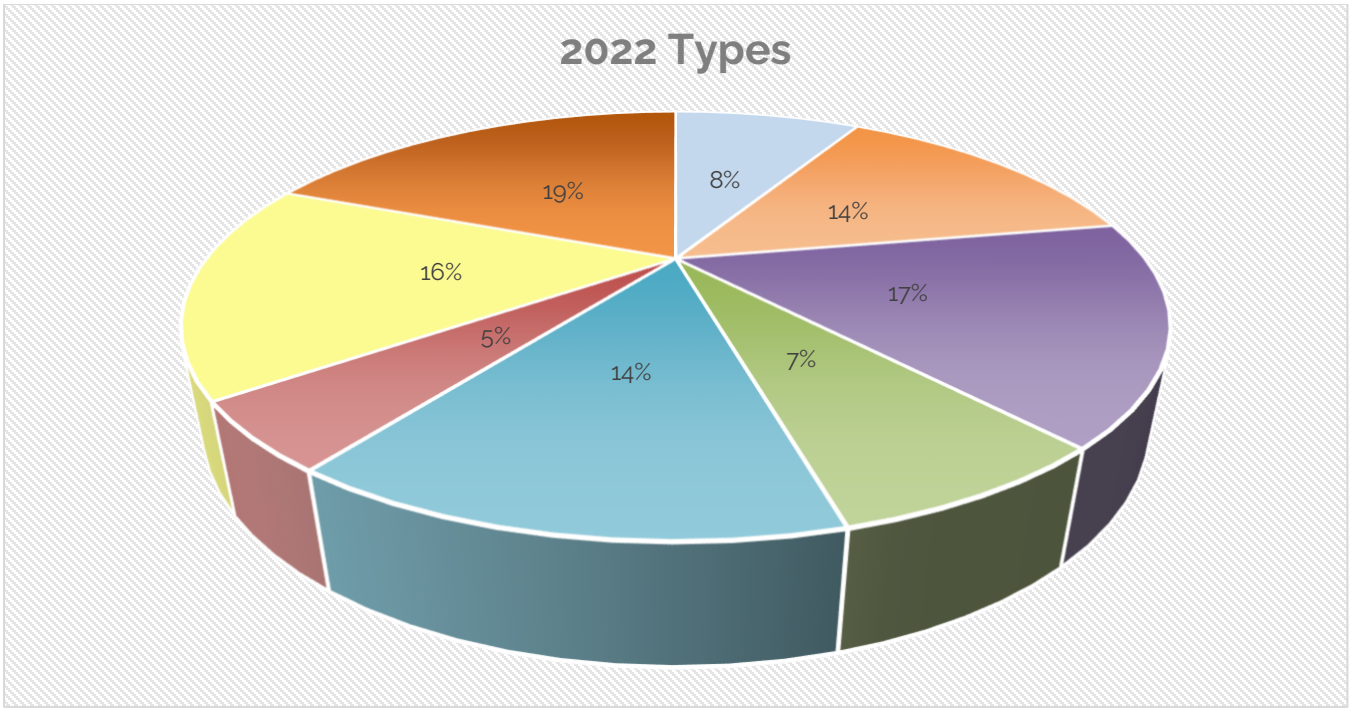


Figure 24. Vulnerability Types 2022

Plotting the data trends across 10 years shows a definite overall increase in web and dependency types, an interim increase in information disclosure types, and an overall decrease in backdoors and failure to follow principle of least privilege.

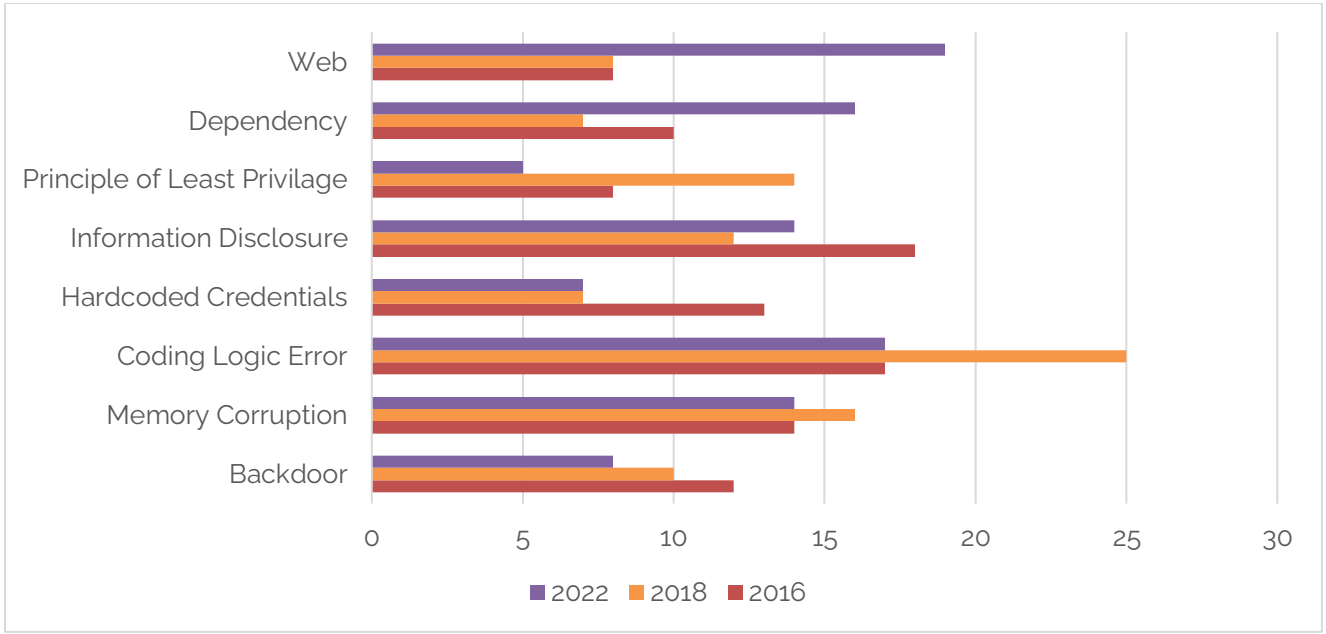


Figure 25. Vulnerability Type 10-year Trends

Vulnerabilities in the application stack as well as those in third-party vendors are on the rise as a result of newer technologies in automotive components and growing systems that require larger SBOMs and streamlined development practices. On the other hand, IOActive noted that the industry as a whole appears to be building systems better—as evidenced by fewer flaws being discovered in codebases.

Remediation Approaches

An important aspect of this research was to determine if the remediation approaches the industry has implemented (and those suggested by IOActive) are causal to the overall trends. The goal of this section is to explore if vulnerabilities are becoming easier or harder to fix, and if remediation strategies are improving or deteriorating overall automotive cybersecurity, i.e., *"Are vulnerabilities reducing in number under specific categories as a result of remediation implemented by the responsible parties?"*

Critical Impact Remediation

Definition: Vulnerabilities marked specifically as weaknesses within automotive systems that, if exploited, would result in the complete compromise of the component or a definite ASIL safety concern.

Figure 26. Critical Impact Remediation (Effort to Fix) Key for Charts and Trends

Part of IOActive's rating methodology includes providing an estimated level of effort to remediate a flaw. For example, low-effort fixes may involve patching a buffer overflow or enabling a feature in the DUT's configuration, whereas high-effort changes may require substantial modifications to the design of the vehicle's communication systems. It is important to note that the level of effort is based on how difficult IOActive believes it would be to develop and deploy a fix. This does not account for specific issues in the automotive industry, such as the effort required to push an update, especially for vehicles without remote firmware updates. In the interests of being concise, we have chosen to focus on critical-impact vulnerabilities for this research as these were classed as the ones the automotive industry would be most likely to fix.

2016 and 2018 Refresher

As indicated by Figure 27, the share of high-effort and medium-effort fixes increased by 4% and 14% respectively. Whereas low-effort fixes accounted for 77% of critical-impact vulnerabilities in 2016, they only accounted for 59% in 2018. Most issues were still relatively easy to fix, and IOActive's earlier research found that this trend was likely due to stronger cybersecurity practices, resulting in fewer low-hanging vulnerabilities.

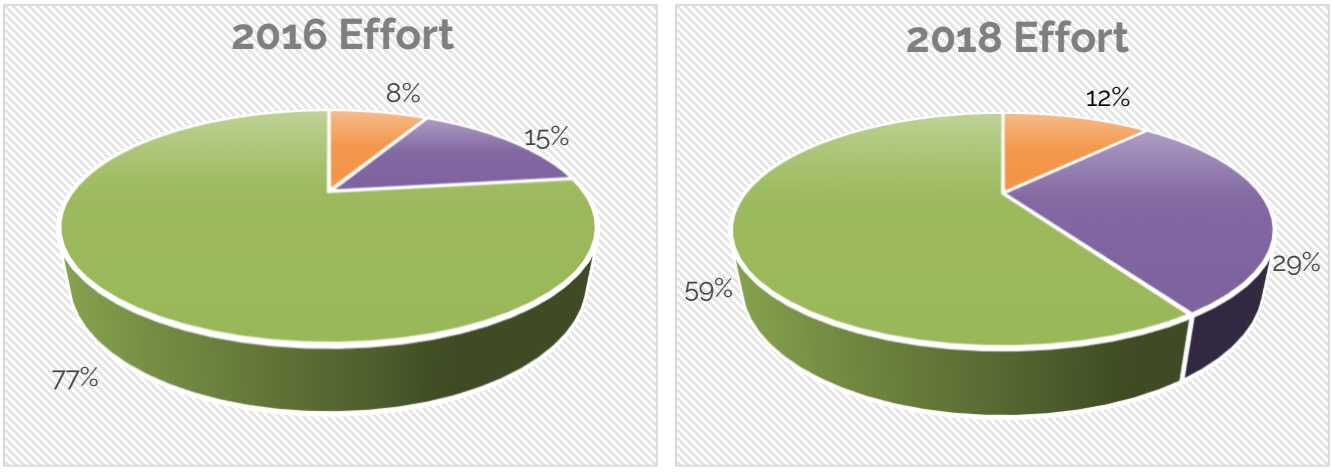


Figure 27. Effort to Fix 2016 (left) and 2018 (right)

2022 Update and 10-year Trends

Intriguingly, the trends observed between 2018 and 2022 are completely opposite, indicating a bounce-back effect. High-effort fixes decreased by 6% and medium-effort fixes decreased by 11%, resulting in a major increase in low-effort fixes (17%).

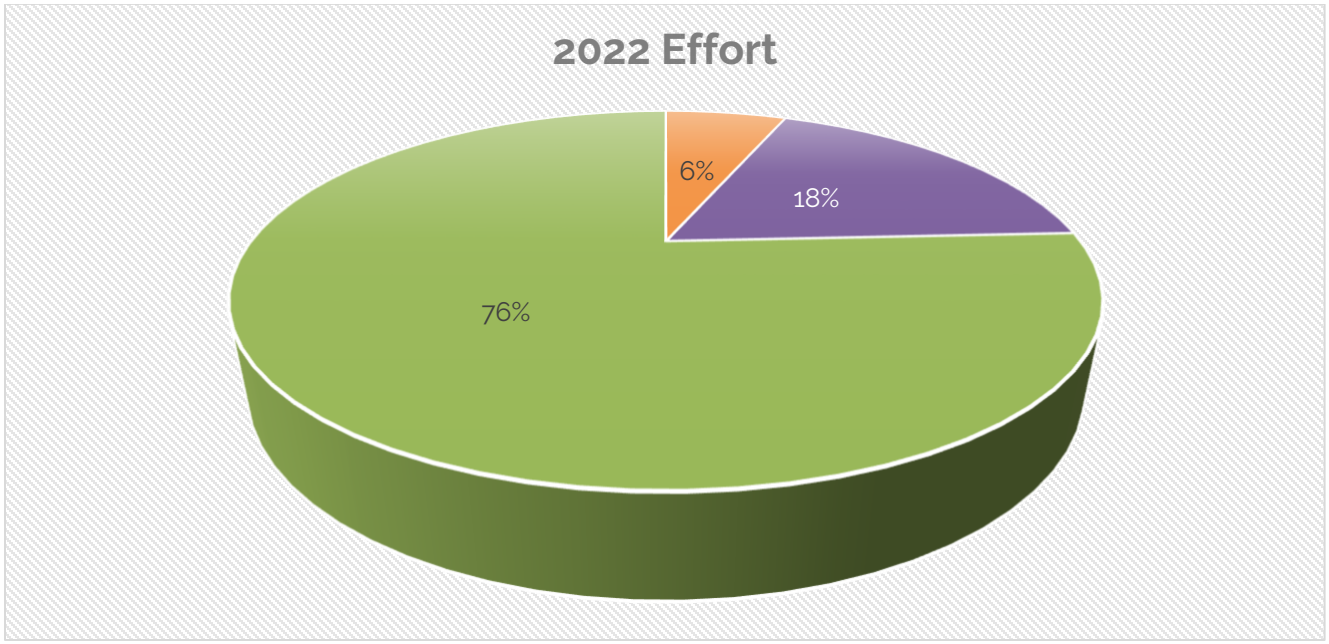


Figure 28. Effort to Fix 2022

When plotting the data to analyze the overall 10-year effect (Figure 29) this bounce-back observation is evident; however, there is an overall 3% increase in medium-effort fixes.

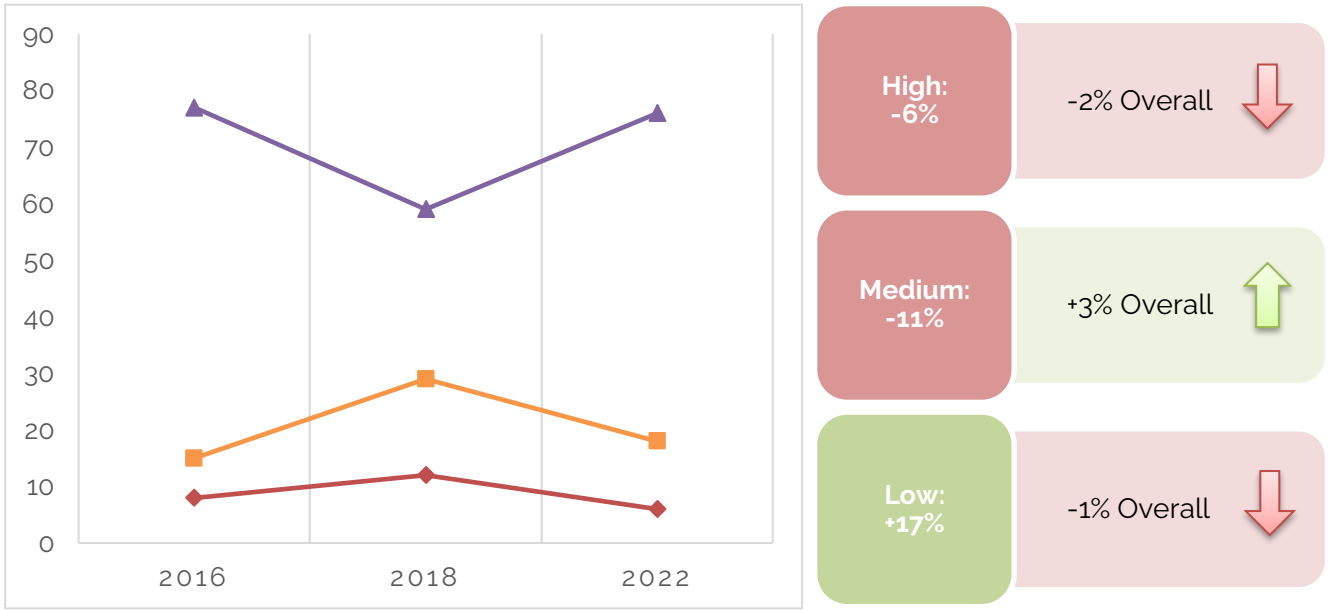


Figure 29. Effort to Fix Trends and Percentages 2018-2022 (left) and 10-year (right)

Despite previous research observations, the current trend information suggests that vulnerability types may be the direct result of the sharp rise in low-effort fixes. IOActive's raw data observations include several vendor-specific flaws that could have been caught via basic cybersecurity practices but were overlooked due to the incorrect assumption that cybersecurity architecture documentation had been followed. A lack of verification and secure onboarding for third-party vendors was also a factor in several critical-impact vulnerabilities which were considered easy fixes.

For this reason, the final stage of this analysis determines if the impact of prevention suggestions is a result of these skews between critical impact remediation and attack typecasting, leading to 'Ounce of Prevention.'

Ounce of Prevention

Definition: A measure to determine the techniques, policies, and methodologies that might have prevented a vulnerability from existing in the first place.

As part of every assessment, IOActive provides recommendations for how best to fix or mitigate each reported issue. Part of this research was broadly categorizing those recommendations to give a general sense of where vulnerabilities stem from and how they could be prevented in future devices.

2016 and 2018 Refresher

Figure 30. Ounce of Prevention Key for 2016 and 2018 Charts

Back in 2016 and 2018 the most prevalent suggested remediation by far was industry best practices. These were issues that could have been solved by following common guidance from groups such as Auto-ISAC and OWASP. These tended to be issues like not authenticating data, not encrypting or authenticating network traffic, and not filtering user inputs.

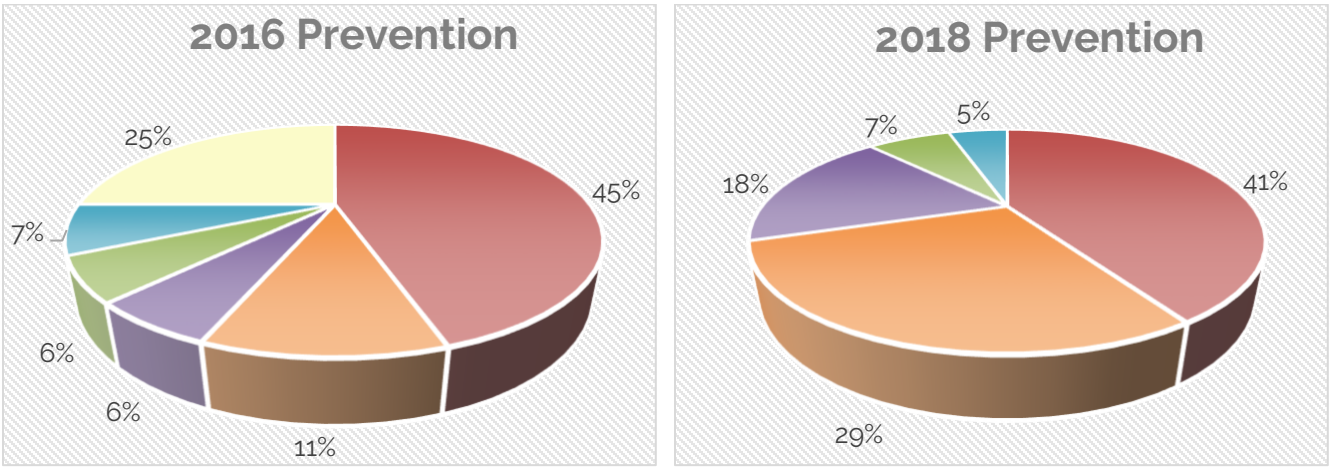


Figure 31. Ounce of Prevention 2016 (left) and 2018 (right)

The next largest category was secure coding practices, such as the use of insecure functions and not checking return values. These could be fixed with strong implementation guidelines and enforcing banned functions.

Authentication design recommendations may be the most difficult category to implement, as they are the result of a lack of strong controls in the system's architecture. As determined in previous research, fixing these may involve significant changes to how services communicate and the system is accessed. Less common in previous years were recommendation for deployment procedures, which mostly involved not disabling debugging features before releasing a product.

Finally, IOActive concluded that patch management remediation was the least common category because multiple instances of unpatched software were often grouped into one finding—resulting in an incidental bias by reducing the number of individual findings in the data set.

2022 Update and 10-year Trends

Note that between 2016 and 2018, 'Code Review and Testing' is absent in the analysis; this is due to the harmonization of remediation guidance's wherein Code Review and Testing suggestions were absorbed by 'Secure Coding Practices'.

Figure 32. Ounce of Prevention Key for 2018 and 2022 Charts

Figure 33 displays the 2018 to 2022 trends in prevention suggestions. Even with the absorption of code review and testing, secure coding practices remained steady between 2018 and 2022, while authentication design decreased by 8%.

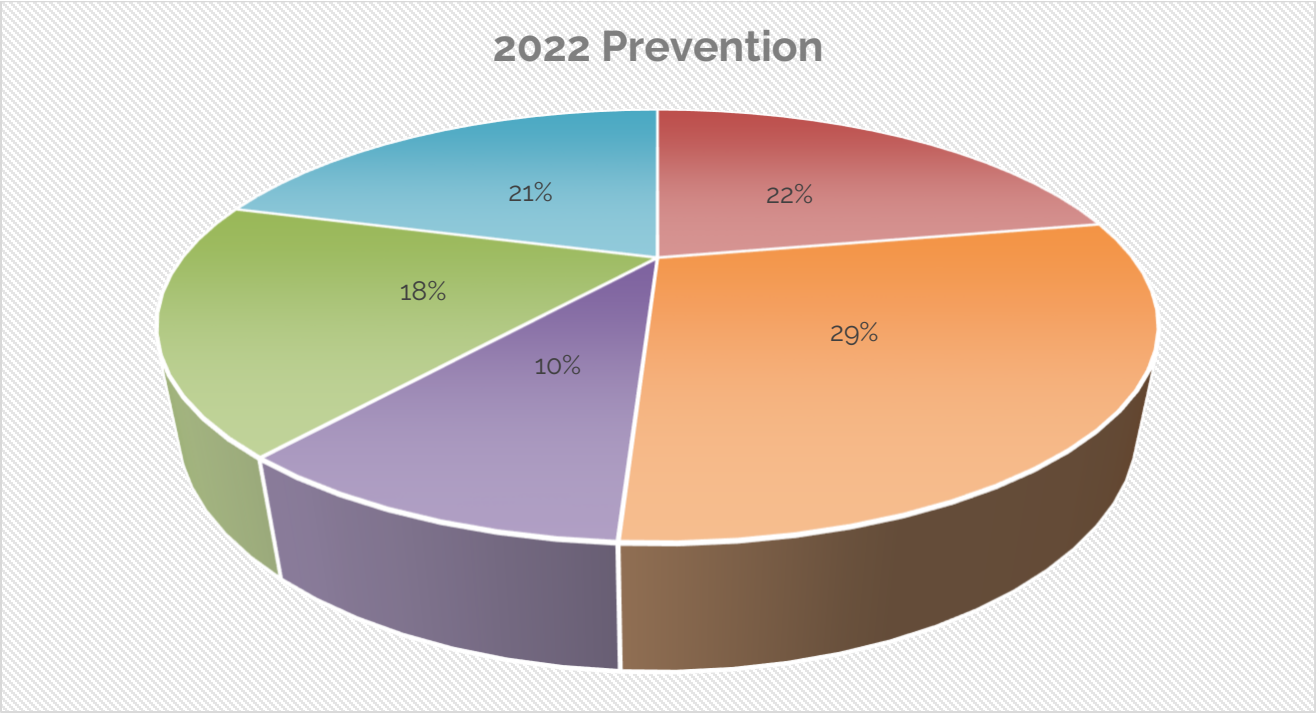


Figure 33. Ounce of Prevention 2022

However, there was a sharp increase in patch management (16%) and deployment procedures (11%). This points to the fact that devices within vehicles are suffering from poor SBOM maintenance and outdated libraries—likely due to the sheer increase in codebase size and an increased dependency on third-party components. Additionally, the rise in deployment procedures recommendations follows IOActive's observation that the industry is struggling to retrofit functionality or fixes into systems released early in the development cycle.

Nonetheless, when plotting the data trends across 10 years, Figure 34 at-a-glance shows a definite overall increase in Patch Management and Deployment Procedures, and an overall decrease or maintenance in all other categories.

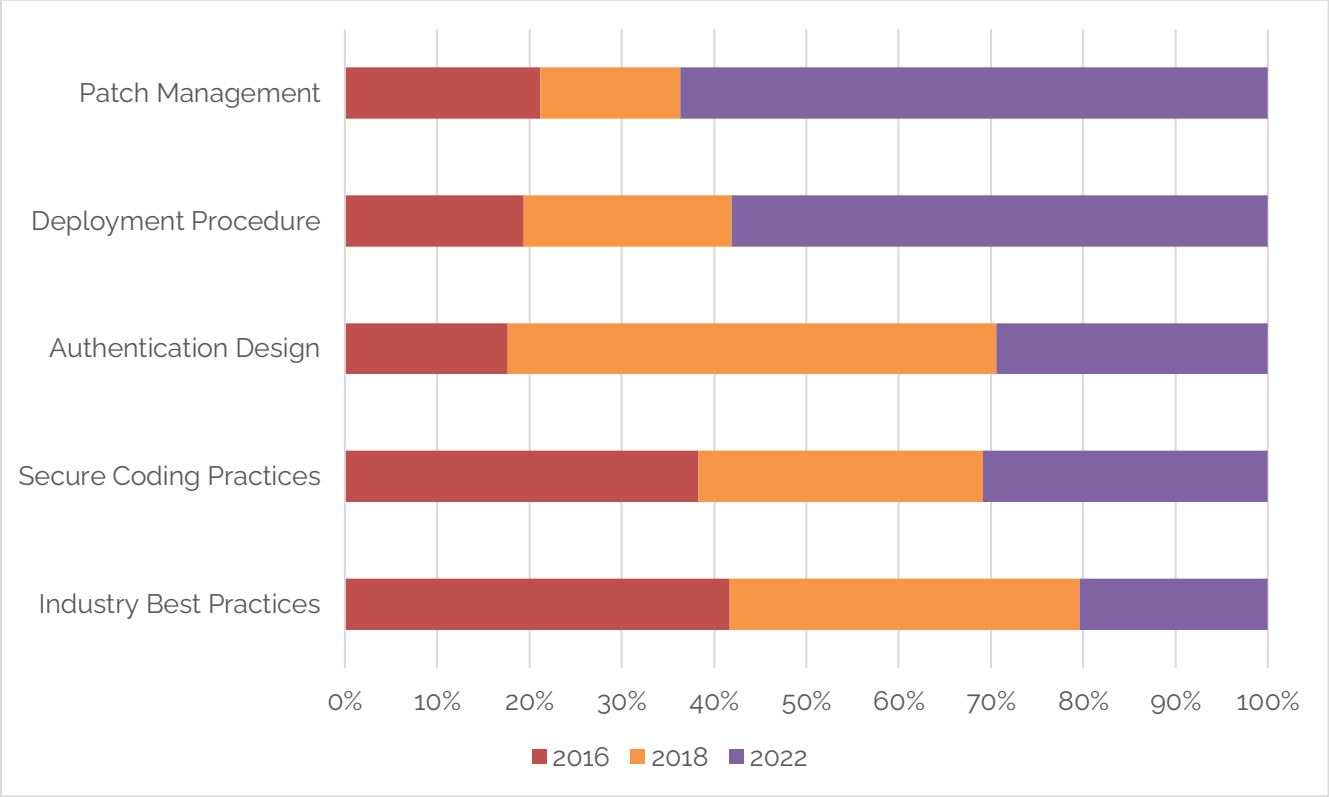


Figure 34. Ounce of Prevention 10-year Trends

As a final note, it should be emphasized that Figure 34 represents a positive industry trend in reducing authentication design issues. This is likely due to the hyper-focus on reducing the chances that remote threat actors can compromise the DUT.

While hyper-focusing on specific vulnerabilities or types of vulnerabilities can cause unfavorable trends, the positive effect of this particular effort should not be overlooked. The data since 2016, shows that the automotive industry has significantly matured in deploying cybersecurity practices. Cybersecurity is a fast-growing focus for the overall industry, and improvements in any category should be maintained to ensure future trends remain on track.

Conclusion

Technical Summary

IOActive's vulnerability metrics, attack typecasting, and remediation approaches work together to describe automotive cybersecurity as the industry has progressed over the last 10 years.

Between 2012 and 2018, IOActive's research and experience revealed several trends:

- Vulnerabilities generally decreased in both impact and likelihood.
- The most common attack vectors were via internal software components and network-connected applications.
- The hardening of local interfaces appeared to be improving.
- The most common vulnerability types were logic errors, whereas traditional memory corruption attacks were becoming less common.

Based on these conclusions, IOActive recommended diligently applying industry best practices and secure design and enforcing strong secure coding practices to help prevent easy-to-fix bugs in the first place.

Current trends, between 2018 and 2022, reflect the following:

- The risk-remediation strategies being deployed in modern automotive systems are beginning to pay off.
- The automotive industry is improving and building better; however, there is an evident struggle in the harmonization and maintenance of present systems.

Emerging Threats

Performing a big-picture, wide-band analysis of the 10-year trends for automotive cybersecurity reveals emerging trends which otherwise would have been lost in a more narrow-field analysis. This analysis has given rise to interesting observations and uncovered emerging threats that should garner the attention of automotive cybersecurity experts and policy makers:

- Management of SBOMs and third-party vendors are quickly becoming the primary reason for weaknesses in the vehicle ecosystem.
- Application cybersecurity in cyber physical systems is a main causality for easy-to-find and easy-to-exploit flaws, as the vehicle stack is increasingly reliant on newer technologies that include modern applications.

Future Concerns

The following future concerns are the result of combining this research with the expert opinions of key stakeholders and experienced IOActive consultants:

- The net decrease in the impact of vulnerabilities while the severity is increasing could be the result of the industry moving towards an undesirable state where most vulnerabilities are medium. This could lead to an incidental increased risk of attack chaining by threat actors.
- The industry must be careful of the observer effect where cybersecurity is more reactive than proactive, ultimately resulting in an increase in once-solved problems via a hyper-focus on new trends in automotive cybersecurity (Baclawski, 2018).

Final Considerations

The final considerations from this research are the following:

- It is unsustainable to maintain the cybersecurity of something as complex as a vehicle by only chasing new technologies and their flaws. Automotive vendors and manufacturers should consider adopting risk-mitigation strategies that focus on building cybersecurity into the foundation of their vehicles, whether that be in the SBOM, hardware, or specifications, *and validating cybersecurity within targeted architectures.*
- Automotive manufacturers and vendors should not strictly hyper-focus on critical-risk and high-risk vulnerabilities to the exclusion of medium-risk and low-risk. Attackers are inherently languid, and most exploits discovered in the wild use attack vectors that follow the path of *least resistance.* The industry must decide if the acceptable marketed median should be medium-risk, or if the industry should strive towards an overall positive skew to low-risk. Remaining at medium could pave the way for the rise of attack chains that exploit medium findings to achieve a critical compromise of an automotive component. This trend is also noted in the analysis section of this paper.
- The management of third-party vendors and the influence of SBOMs on the overall cybersecurity posture of a vehicle is evident. Therefore, new risk remediation strategies should consider hardening supply-chain cybersecurity and verifying secure practices are followed for components integrated into automotive systems. Expecting adherence without verification is not beneficial to automotive cybersecurity and should be addressed.

Future Work

As automotive technologies related to the use of Artificial Intelligence (AI), Machine Learning (ML), autonomous driving and Advanced Driver Assistance Systems (ADAS), and electrification in the form of Electric Vehicles (EVs) and Electric Vehicle Supply Equipment (EVSE) emerge, it will be interesting to see their impact on the industry. At the time of this publication, there are few if any standards that cover the cybersecurity of such systems in detail. Already, IOActive has seen how electrification significantly influences dependency-related issues due to the staggering increase in the number of Electronic Control Units (ECUs) and their associated software and hardware components.

Simultaneously, vehicles are becoming further integrated into human environments. The merging of critical infrastructure and transportation sectors demands further research to determine if these industries and their maturity are positively influencing automotive cybersecurity.

Appendix A: Additional Information

About IOActive

IOActive, a trusted partner for Global 1000 enterprises, provides research-fueled security services across all industries. Our cutting-edge security teams provide highly specialized technical and programmatic services including full-stack penetration testing, program efficacy assessments, and hardware hacking. IOActive brings a unique attacker's perspective to every engagement to maximize security investments and improve the security posture and operational resiliency of our clients. Founded in 1998, IOActive is headquartered in Seattle with global operations.

About the Author

Samantha (Sam) Beaumont is a Principal Security Consultant with IOActive, Inc., and has specializations and broad experiences in covering cyber-physical technologies including Automotive, Industrial Control Systems (ICS), Internet of Things (IoT), Biometrics, Medical and Financial and Electronic Point of Sale (POS) systems.

Her work with automotive systems includes raw Radio Frequency (RF) analysis of Remote Key Entry (RKE) solutions, critical testing of telematic control systems, and advanced testing of multitudes of ECUs including automotive infotainment systems, battery controller systems and centralized gateway systems for internal automotive networks.

Sam leads a variety of cybersecurity research projects for automotive OEMs and suppliers and has built specialized cybersecurity frameworks and developed training materials for diverse client bases within transportation and cyber-physical systems.

Table of Figures

FIGURE 1. SUMMARY OF IOACTIVE'S WORK ON AUTOMOTIVE CYBERSECURITY 5
FIGURE 2. BEGINNING FROM TOP CENTRE, CLOCKWISE: PROTOTOCOL BUS (CAN/SERIAL), WI-FI, BACKEND NETWORK, SOFTWARE BILL OF MATERIALS/ONBOARD FIRMWARE (SBOM), MANUFACTURER/FACTORY/DEALERSHIP ACCESS, USB/PERIPHERAL DEVICES, HARDWARE/ECU, CELLULAR, PHYSICAL, ECU/MOBILE APPLICATIONS, REMOTE COMMON ATTACK VECTORS FOR THE CONNECTED CAR (AUDI SKYSPHERE CONCEPT - DESIGN SKETCH, 2021) (REMOTE KEY ENTRY SYSTEMS (RKES) AND BLUETOOTH) 6
FIGURE 3. MAJOR CUMULATIVE THREAT VECTORS FOR THE CONNECTED CAR (AUDI SKYSPHERE CONCEPT - DESIGN SKETCH, 2021) 7
FIGURE 4. IMPACT KEY FOR CHARTS AND TRENDS 13
FIGURE 5. IMPACT RATINGS 2016 (LEFT) AND 2018 (RIGHT) 13
FIGURE 6. IMPACT RATINGS 2022 14
FIGURE 7. IMPACT TRENDS AND PERCENTAGES 2018-2022 (LEFT) AND 10-YEAR (RIGHT) 15
FIGURE 8. LIKELIHOOD KEY FOR CHARTS AND TRENDS 16
FIGURE 9. LIKELIHOOD RATINGS 2016 (LEFT) AND 2018 (RIGHT) 16
FIGURE 10. LIKELIHOOD RATINGS 2022 17
FIGURE 11. LIKELIHOOD TRENDS AND PERCENTAGES 2018-2022 (LEFT) AND 10-YEAR (RIGHT) 18
FIGURE 12. RISK KEY FOR CHARTS AND TRENDS 19
FIGURE 13. OVERALL RISK RATINGS 2016 (LEFT) AND 2018 (RIGHT) 19
FIGURE 14. OVERALL RISK RATINGS 2022 20
FIGURE 15. OVERALL RISK TRENDS AND PERCENTAGES 2018-2022 (LEFT) AND 10-YEAR (RIGHT) 21
FIGURE 16. ATTACK VECTORS KEY FOR 2016 AND 2018 CHARTS 22
FIGURE 17. ORIGINAL ATTACK VECTORS 2016 (LEFT) AND 2018 (RIGHT) 22
FIGURE 18. ATTACK VECTORS KEY FOR 2022 CHARTS 23
FIGURE 19. NEW ATTACK VECTORS 2016 (LEFT) AND 2018 (RIGHT) 23
FIGURE 20. ATTACK VECTORS 2022 24
FIGURE 21. ATTACK VECTOR TRENDS AND PERCENTAGES 2018-2022 (LEFT) AND 10-YEAR (RIGHT) 24
FIGURE 22. VULNERABILITY TYPES KEY FOR CHARTS 26
FIGURE 23. VULNERABILITY TYPES 2016 (LEFT) AND 2018 (RIGHT) 26
FIGURE 24. VULNERABILITY TYPES 2022 27
FIGURE 25. VULNERABILITY TYPE 10-YEAR TRENDS 27
FIGURE 26. CRITICAL IMPACT REMEDIATION (EFFORT TO FIX) KEY FOR CHARTS AND TRENDS 28
FIGURE 27. EFFORT TO FIX 2016 (LEFT) AND 2018 (RIGHT) 28
FIGURE 28. EFFORT TO FIX 2022 29
FIGURE 29. EFFORT TO FIX TRENDS AND PERCENTAGES 2018-2022 (LEFT) AND 10-YEAR (RIGHT) 29
FIGURE 30. OUNCE OF PREVENTION KEY FOR 2016 AND 2018 CHARTS 31
FIGURE 31. OUNCE OF PREVENTION 2016 (LEFT) AND 2018 (RIGHT) 31
FIGURE 32. OUNCE OF PREVENTION KEY FOR 2018 AND 2022 CHARTS 32
FIGURE 33. OUNCE OF PREVENTION 2022 32
FIGURE 34. OUNCE OF PREVENTION 10-YEAR TRENDS 33

Table of Tables

TABLE 1. RATING AND SCORE AS APPLIED TO IMPACT AND LIKELIHOOD 9
TABLE 2. OVERALL RISK LEVELS AND CORRESPONDING AGGREGATE SCORES 10

Table of Equations

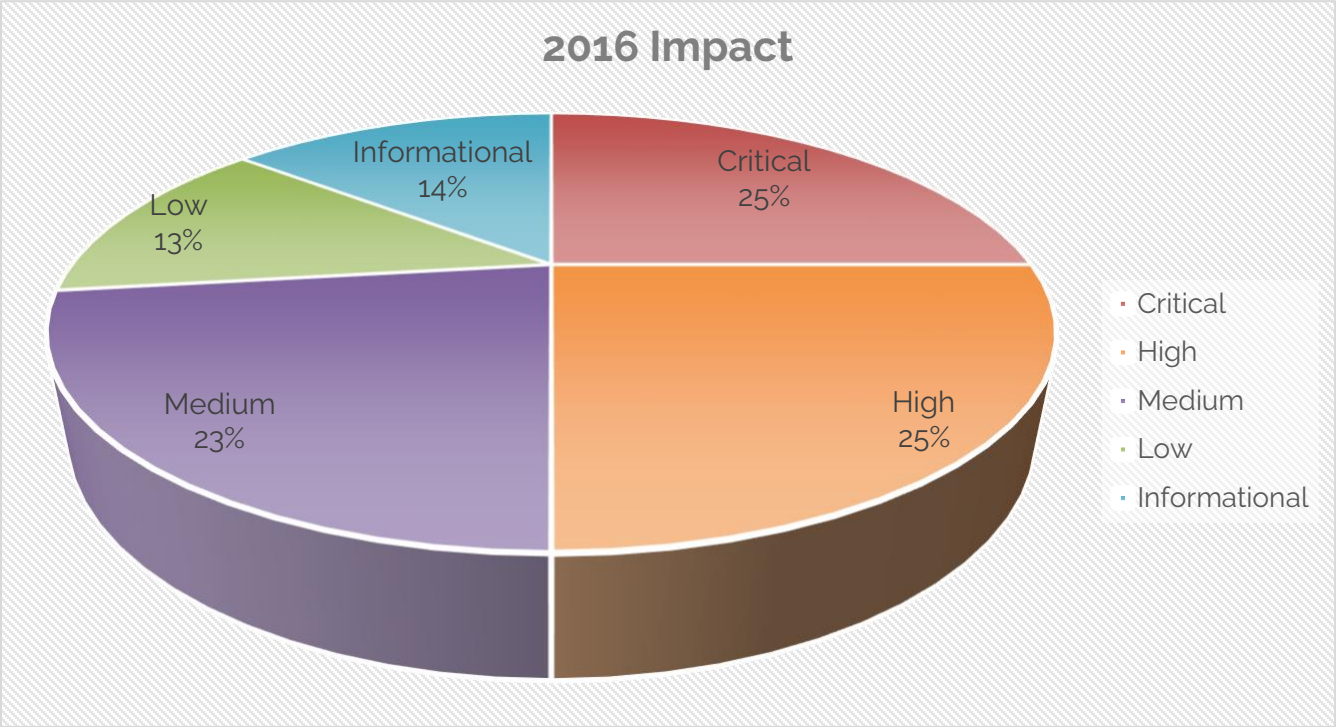
EQUATION 1. $\text{IMPACT} \times \text{LIKELIHOOD} = \text{AGGREGATE SEVERITY (RISK)}$ 10
EQUATION 2. $\text{IMPACT } 3 \times \text{ LIKELIHOOD } 3 = \text{AGGREGATE RISK } (9)$ 11

Appendix B: Graphs

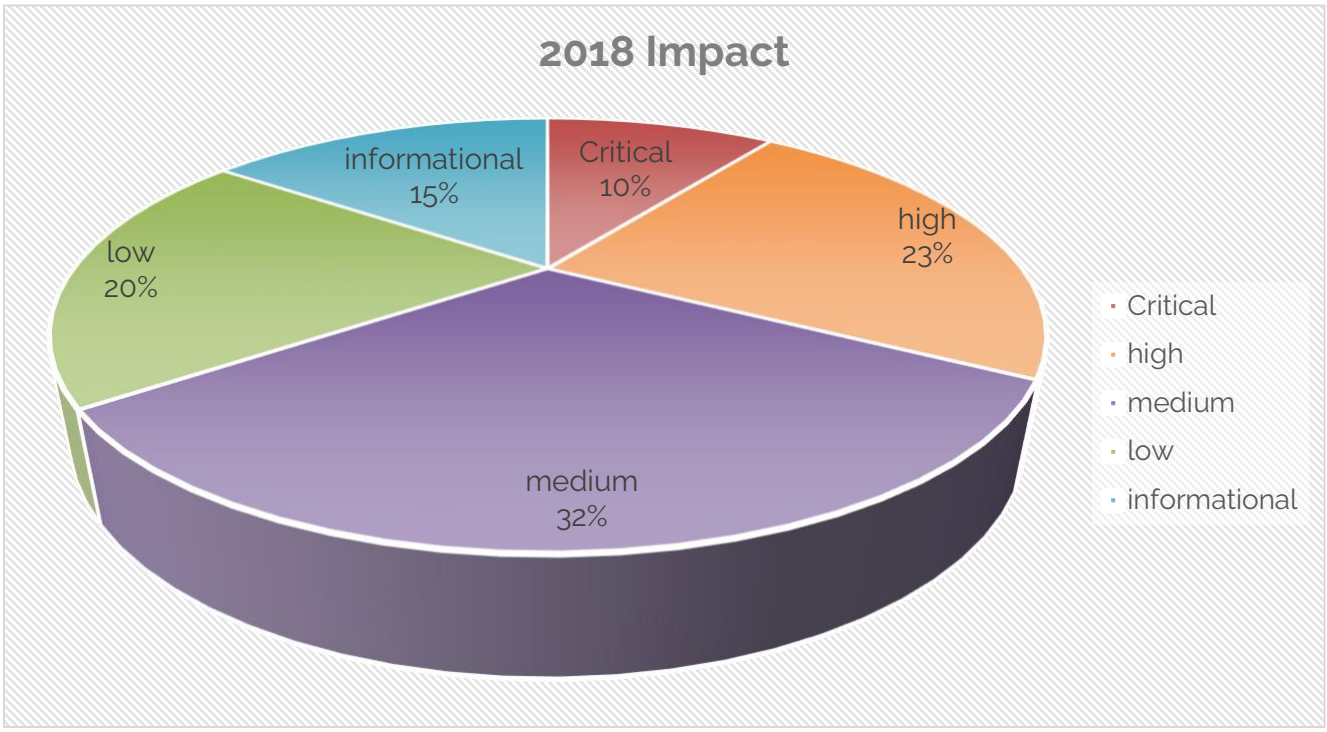
This appendix collects all of the data graphs included in this paper and presents them in larger format. The purpose of this Appendix is to provide the raw graphs used in this paper in larger format for analysis clarity. Note that not all colors for the graphs have been normalized to the colors found within this paper; **readers should use the key provided on the graph legends.**

Impact

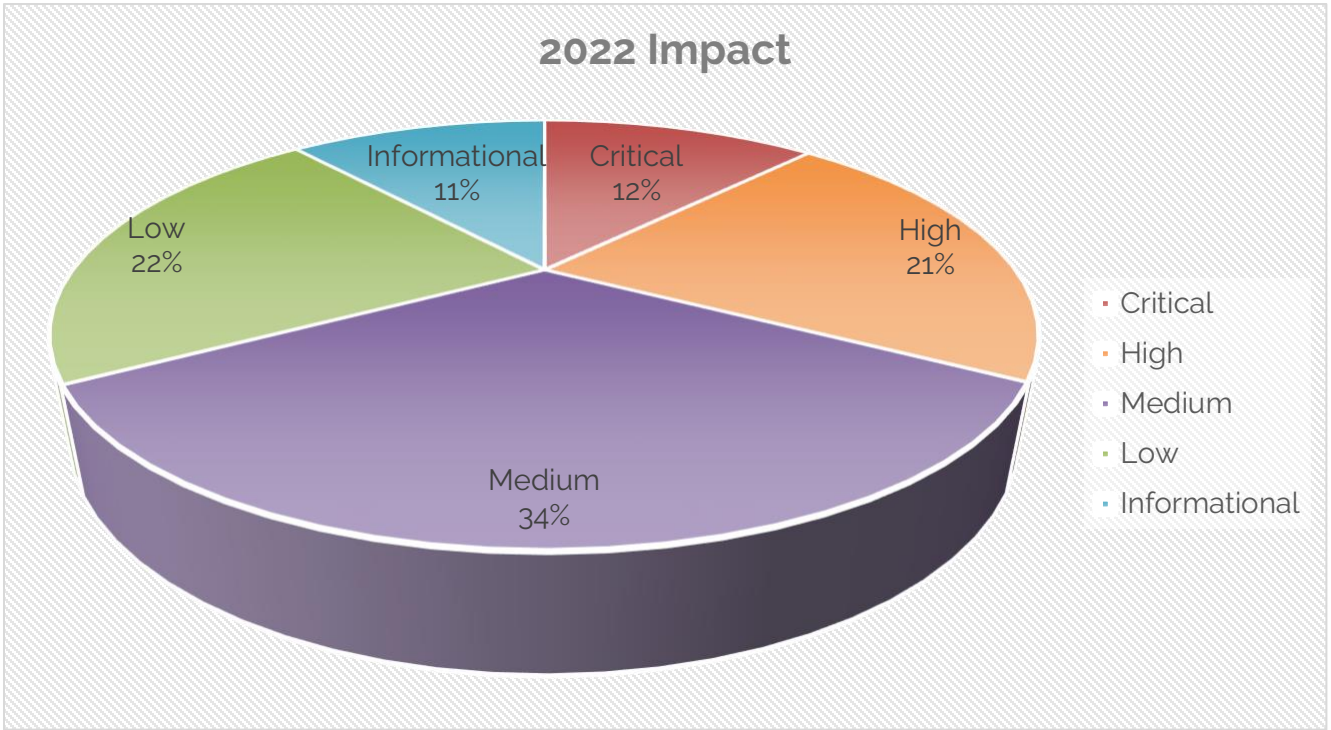
2016



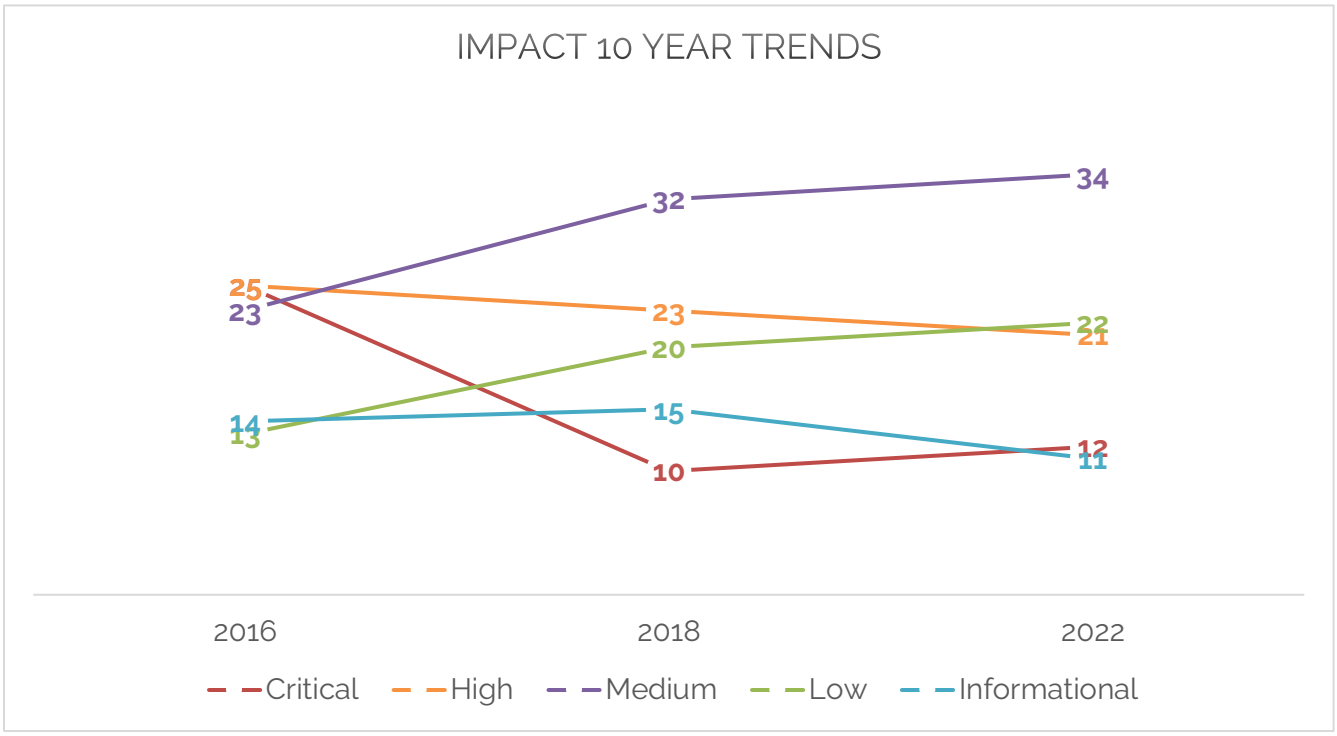
2018



2022

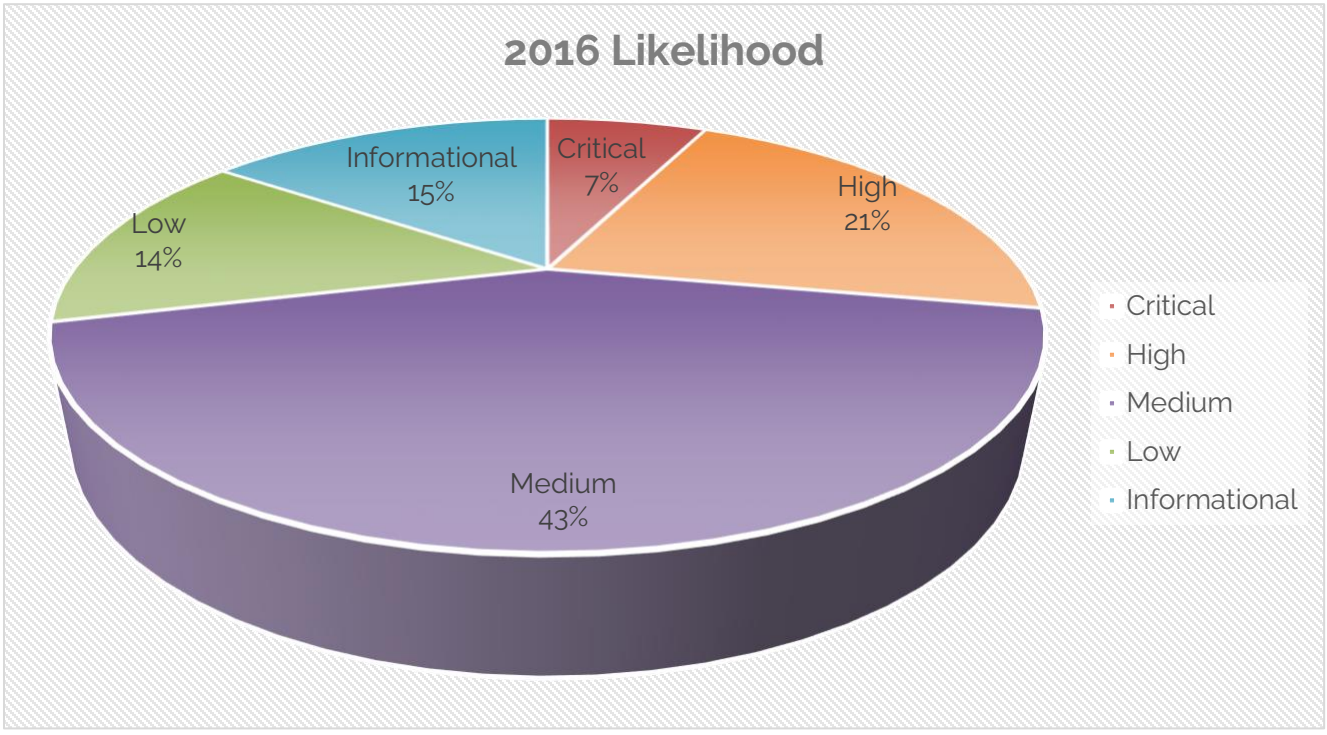


10-year Trend

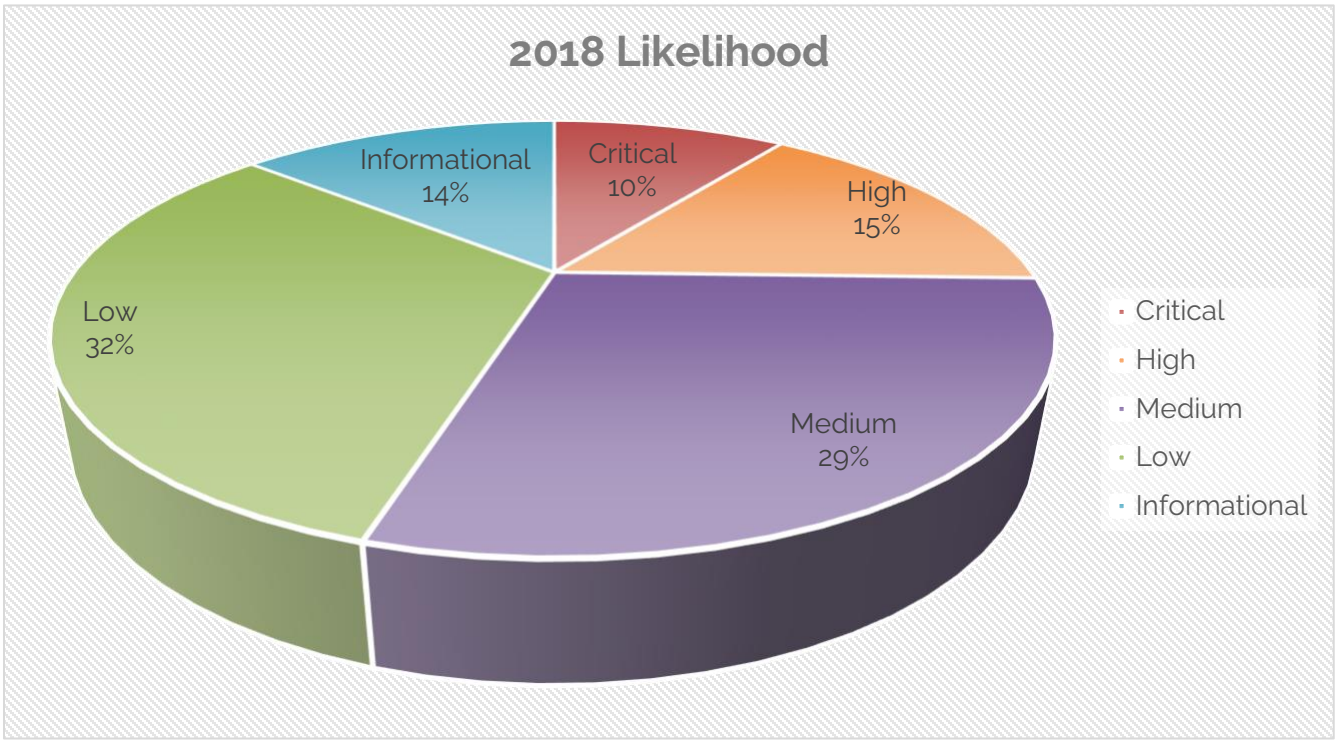


Likelihood

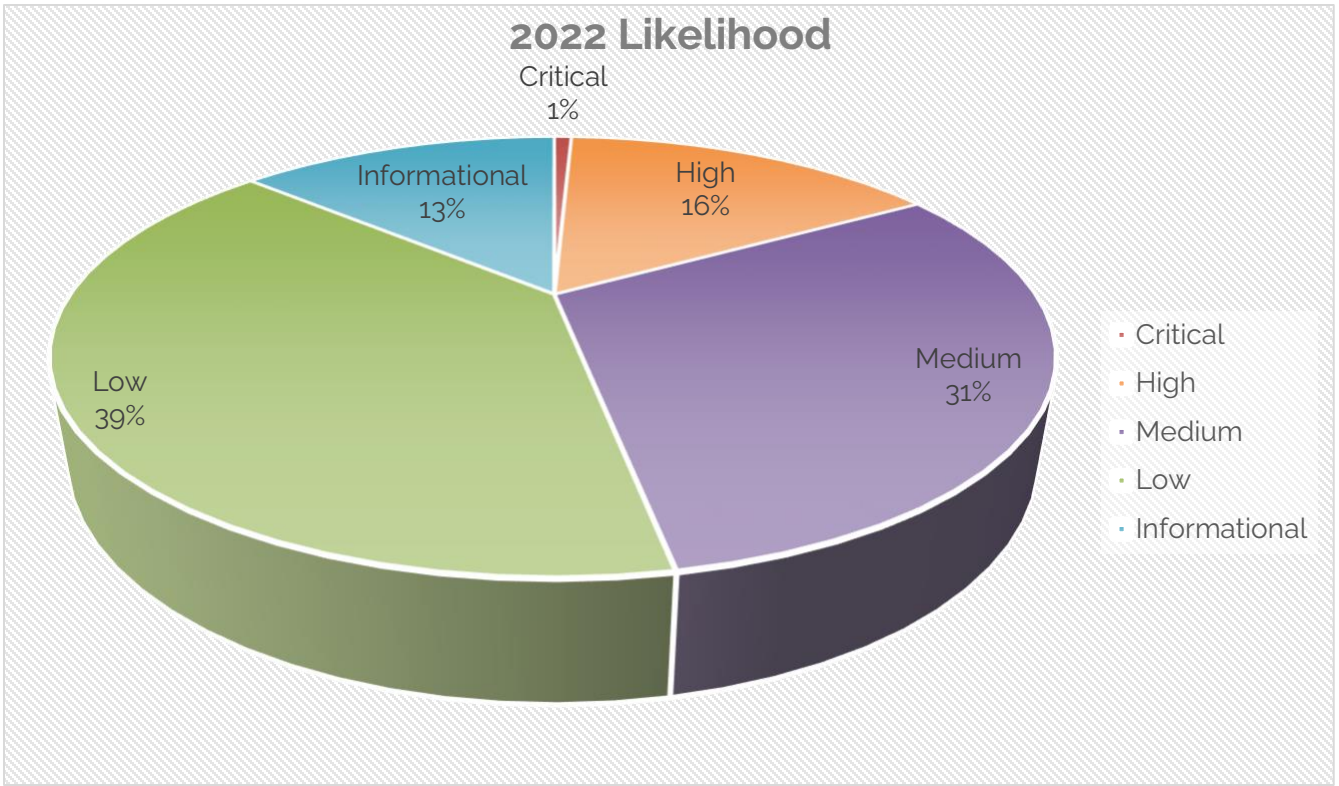
2016



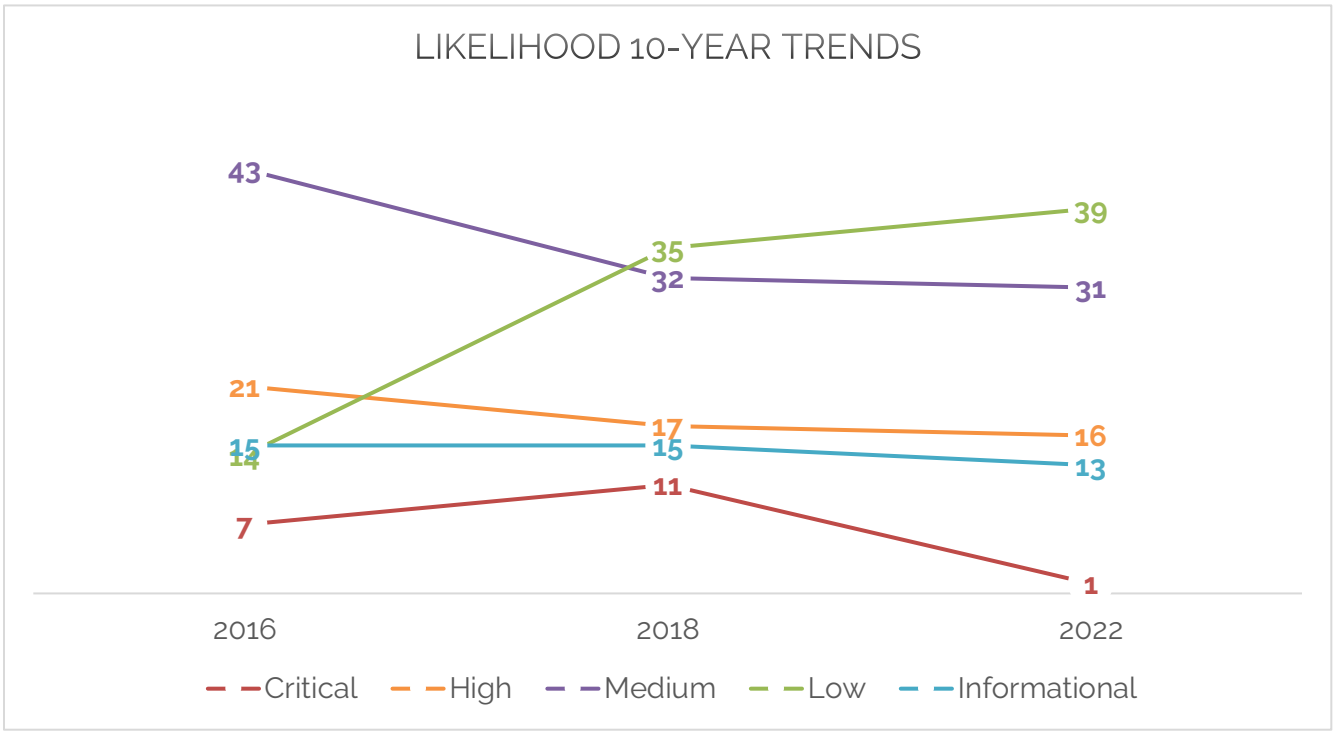
2018



2022

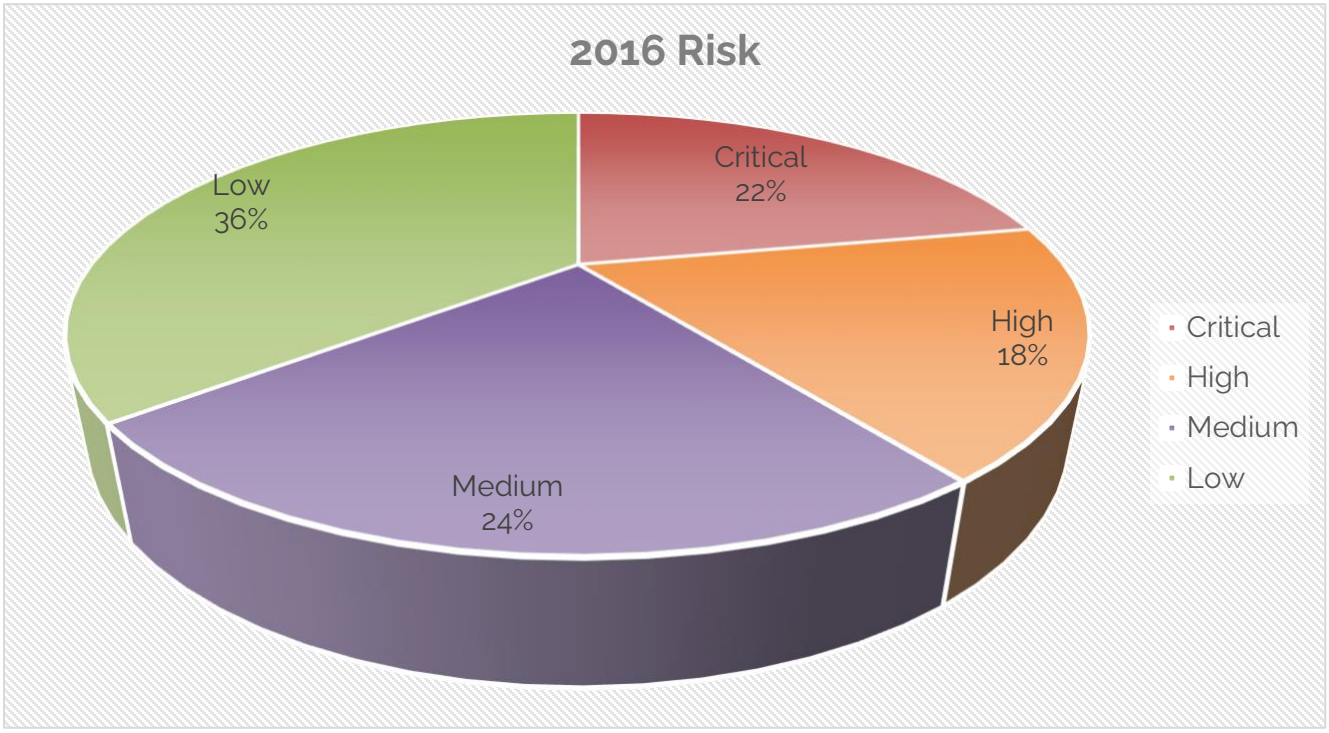


10-year Trend

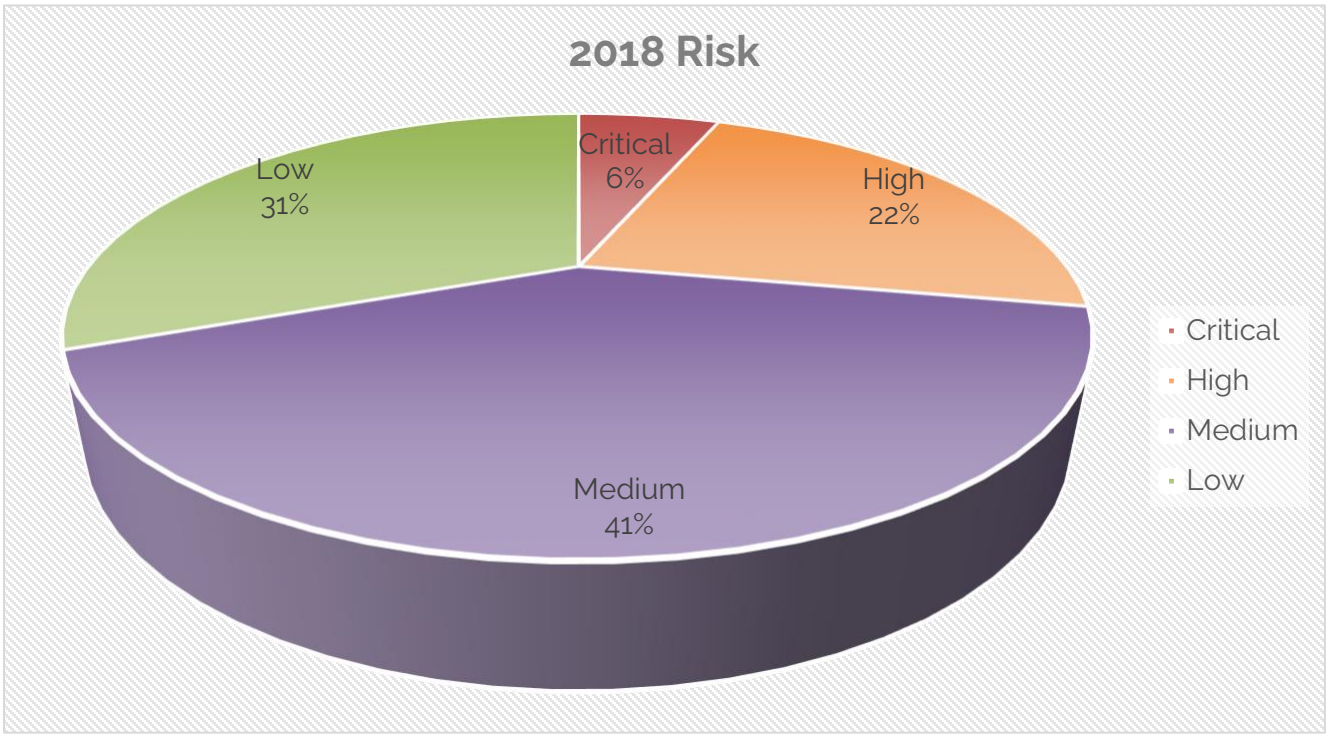


Risk

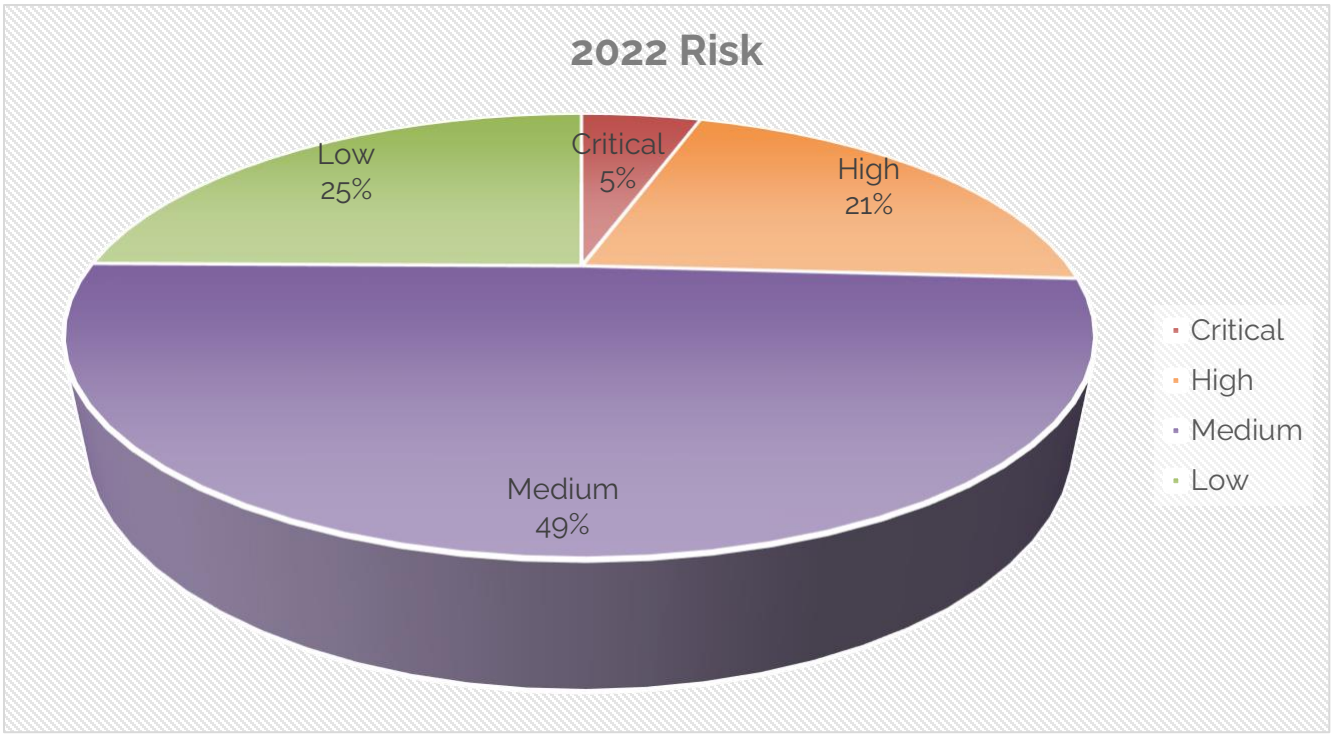
2016



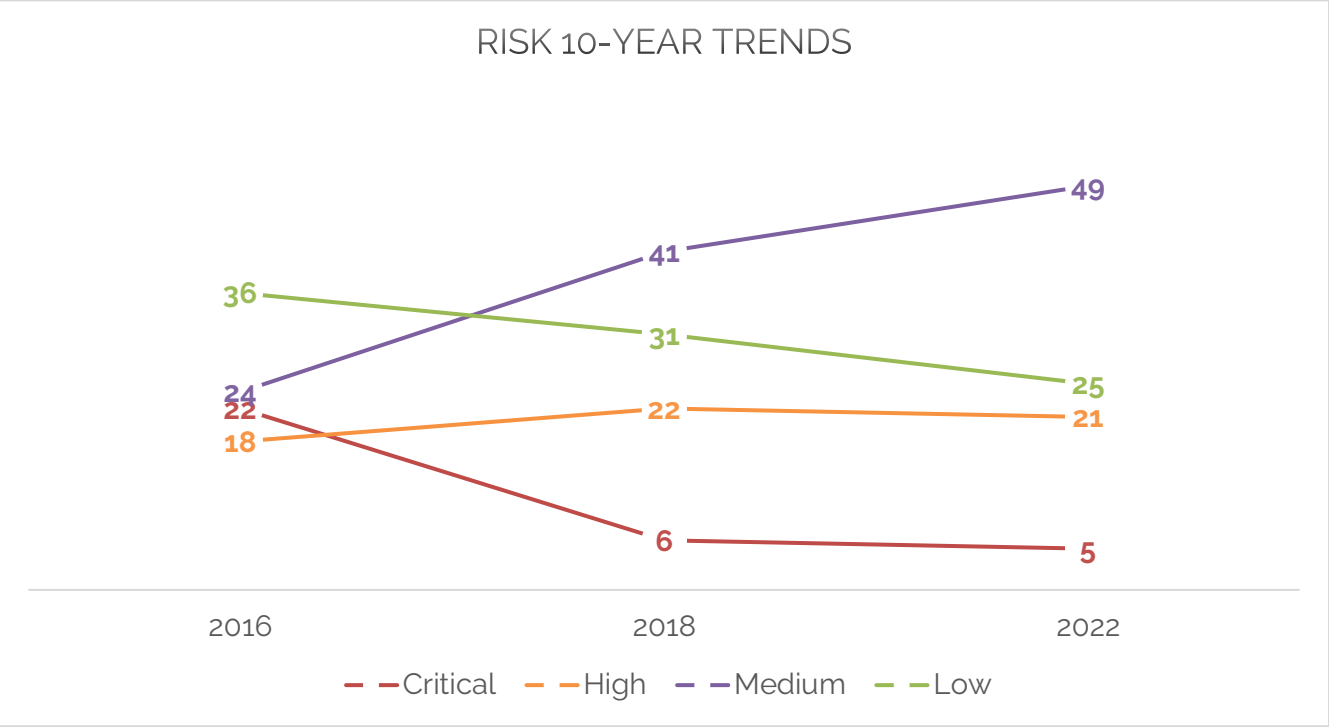
2018



2022

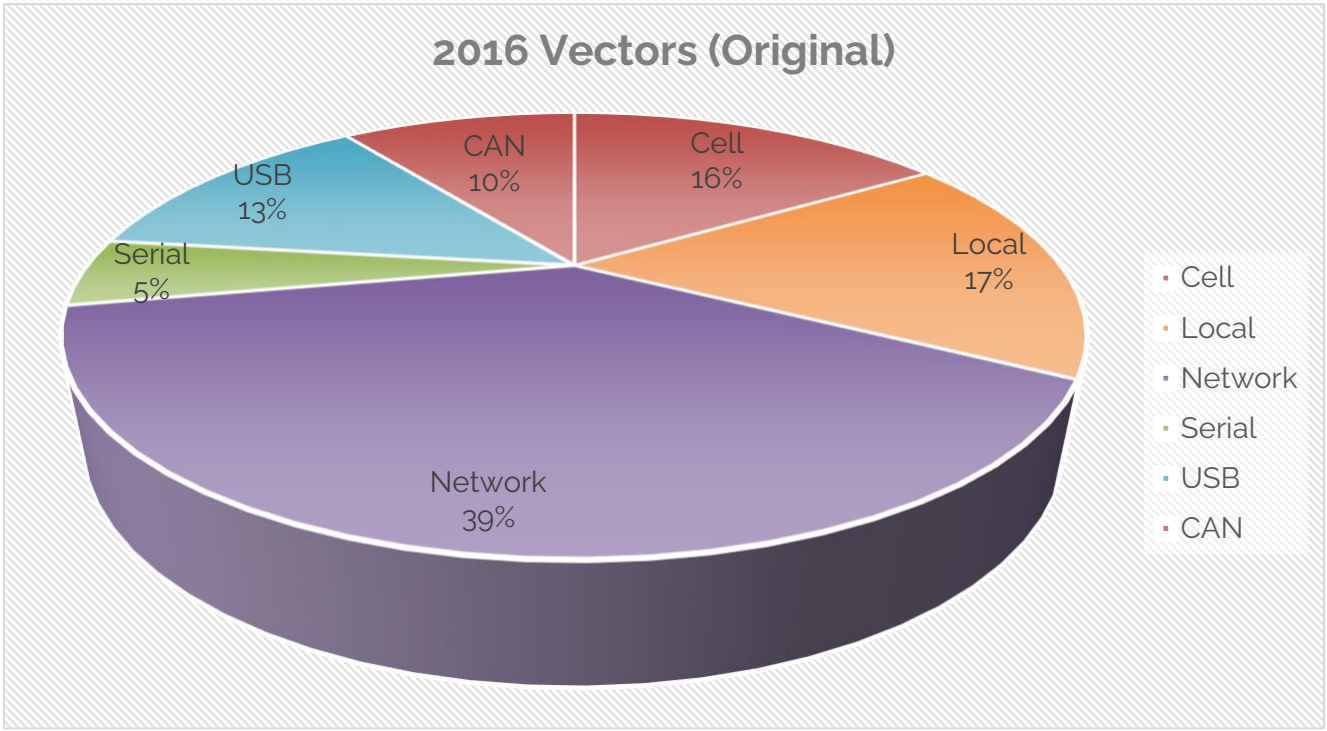


10-year Trend

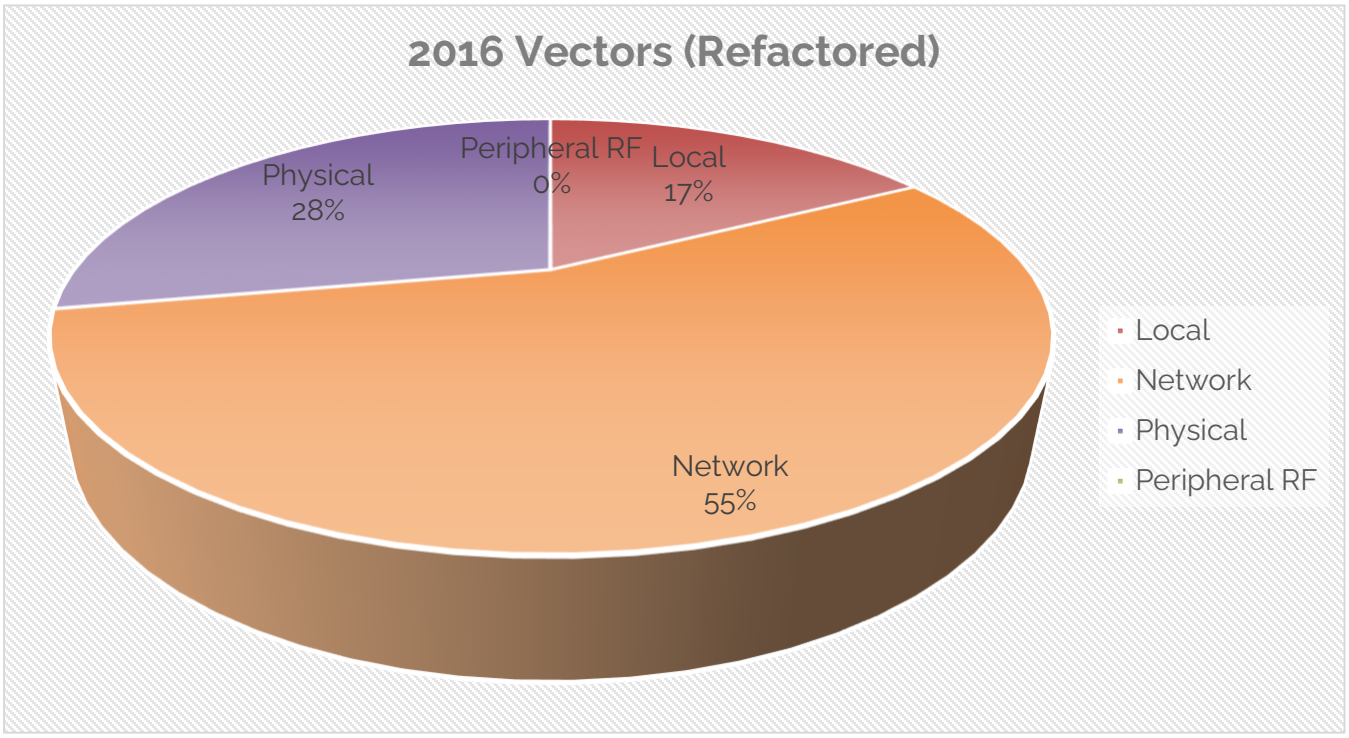


Attack Vectors

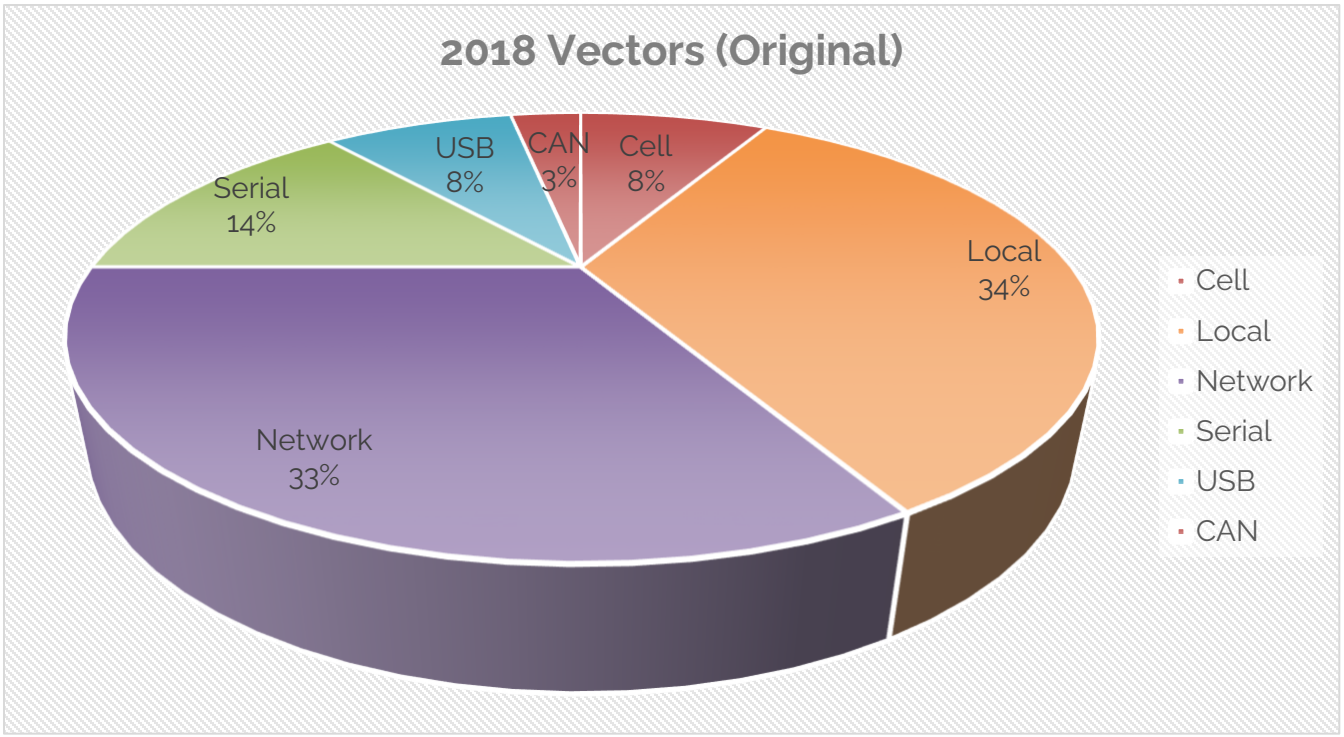
2016 (Old)



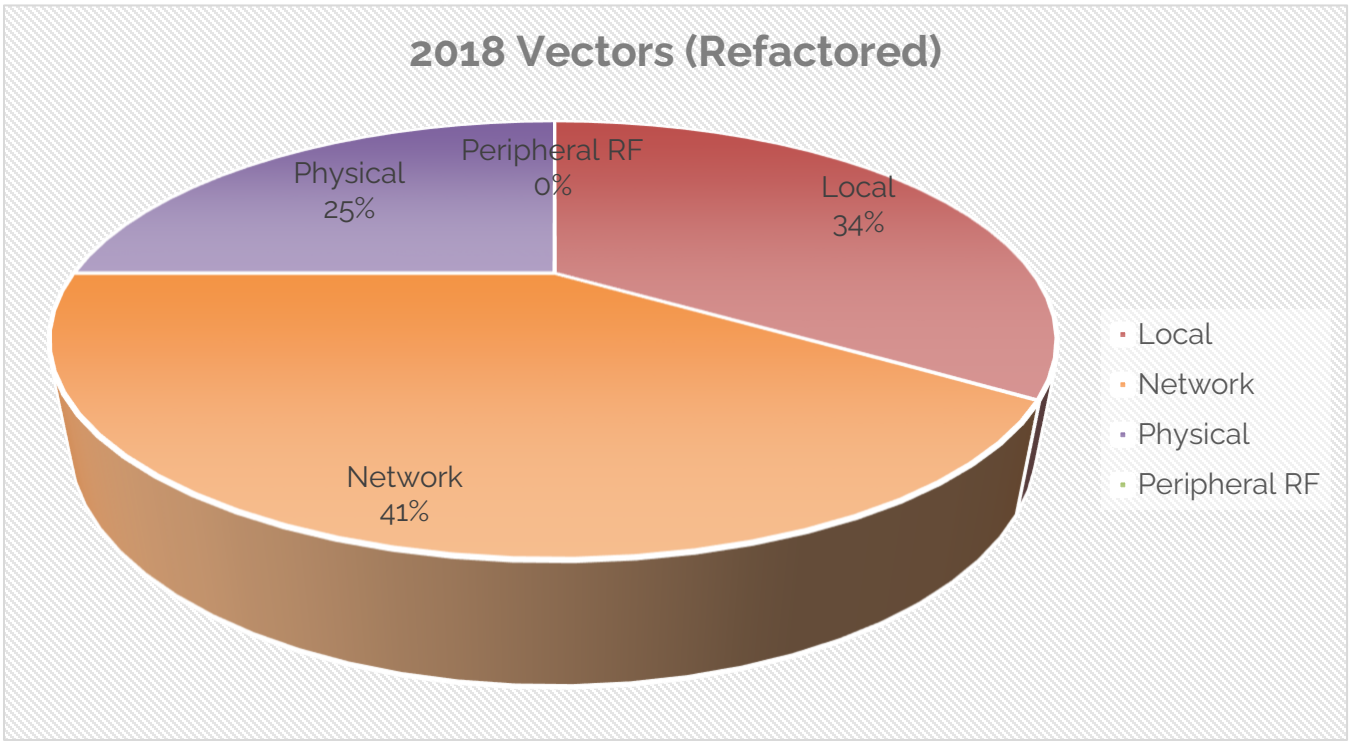
2016 (New)



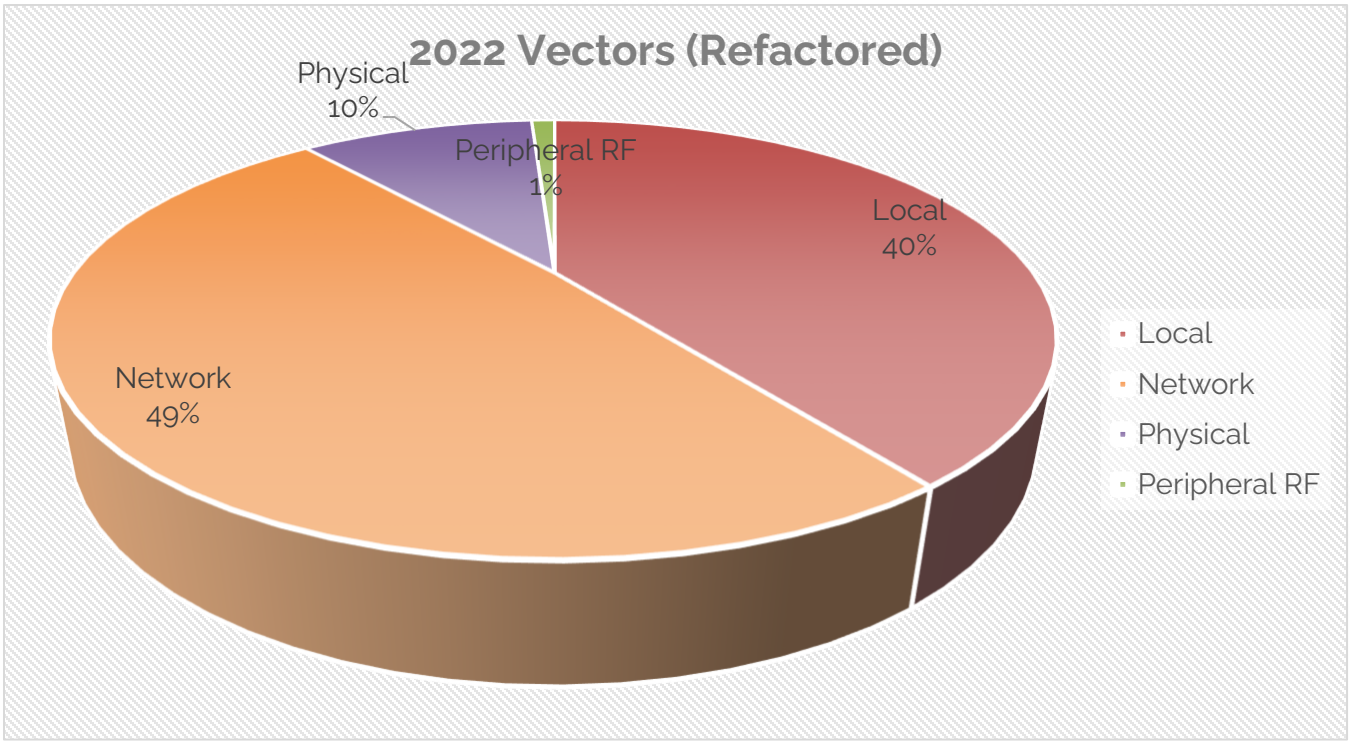
2018 (Old)



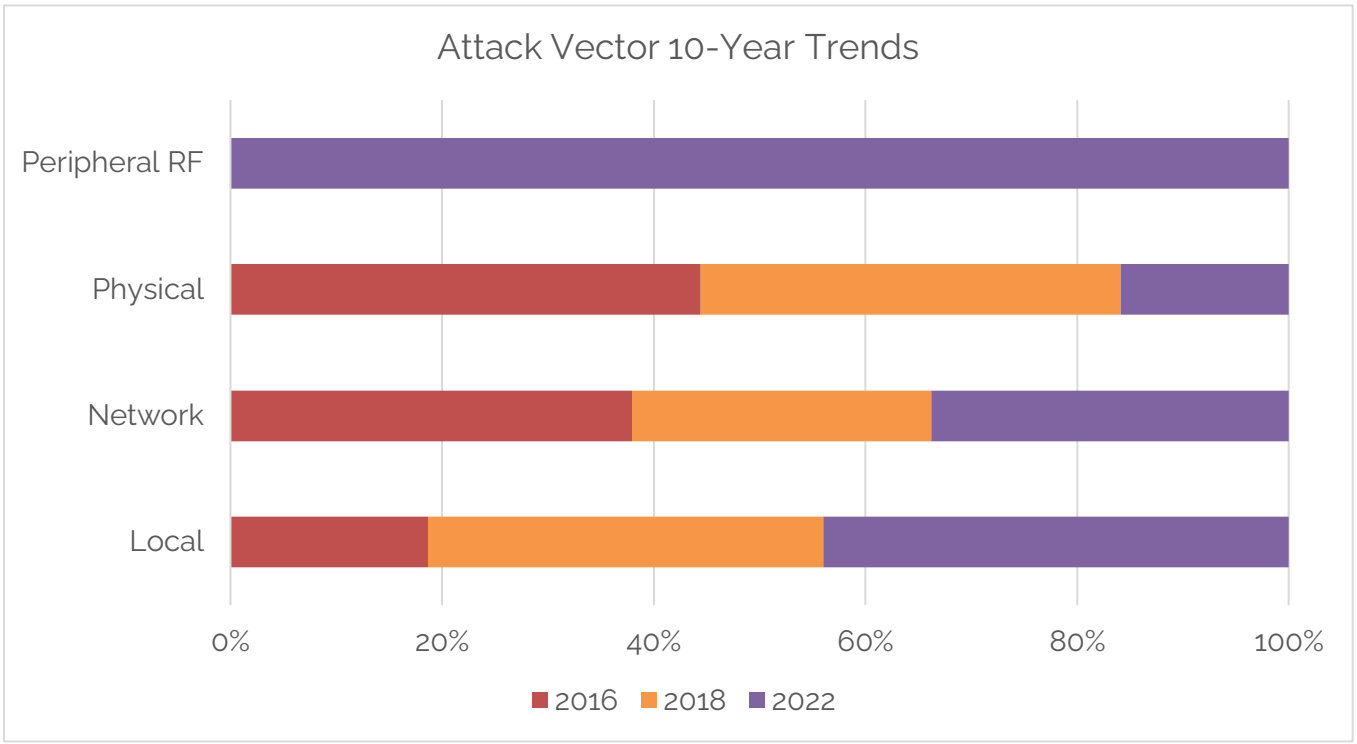
2018 (New)



2022

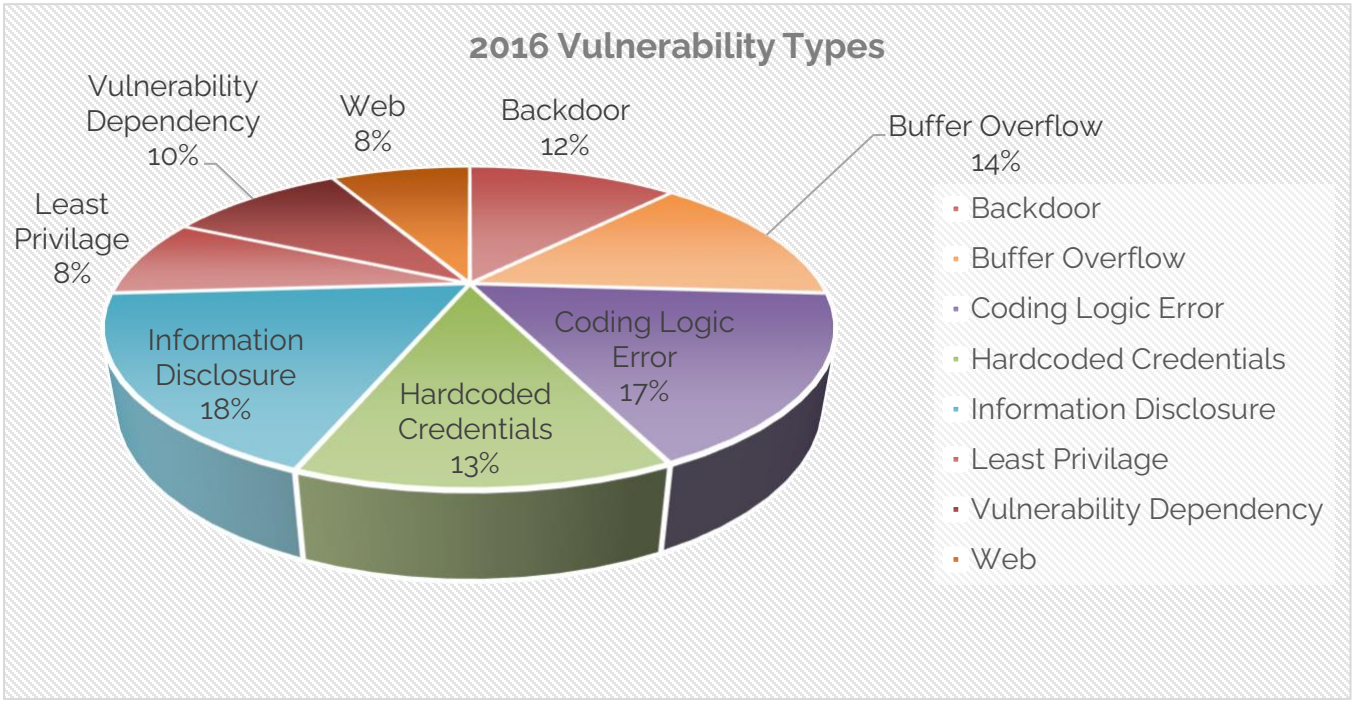


10-year Trend

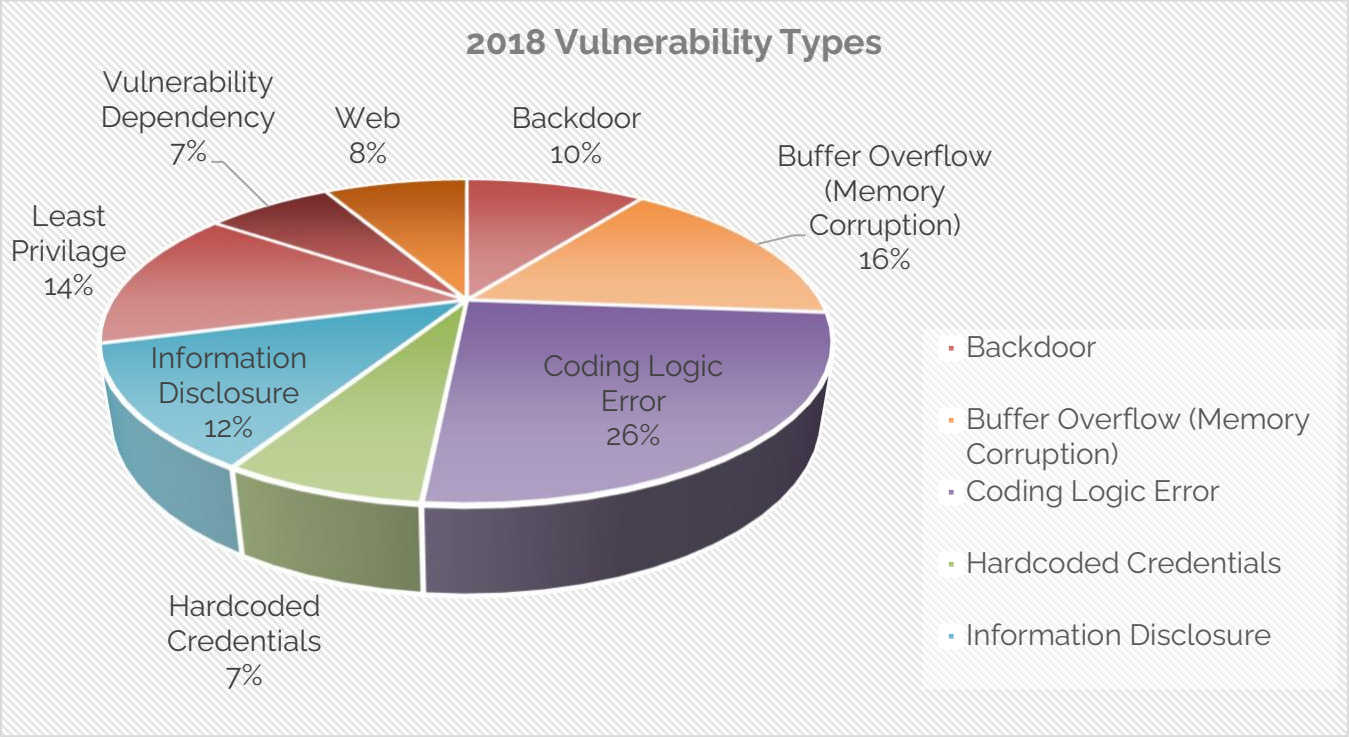


Vulnerability Types

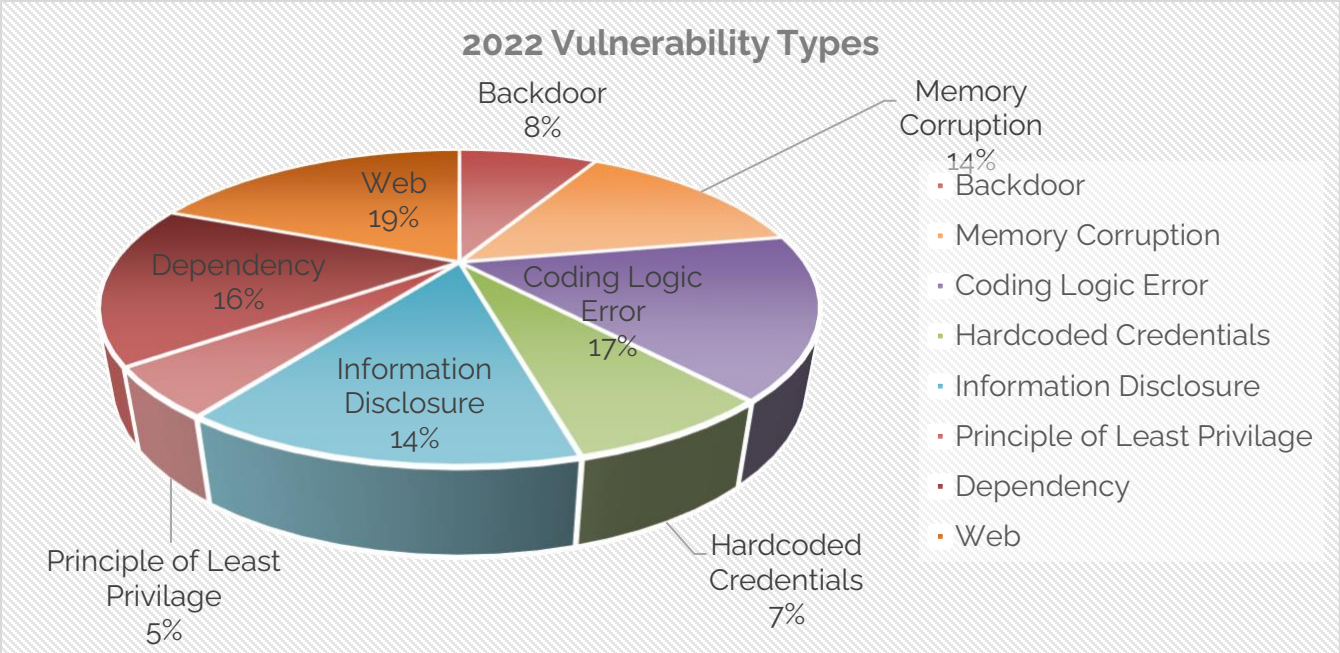
2016



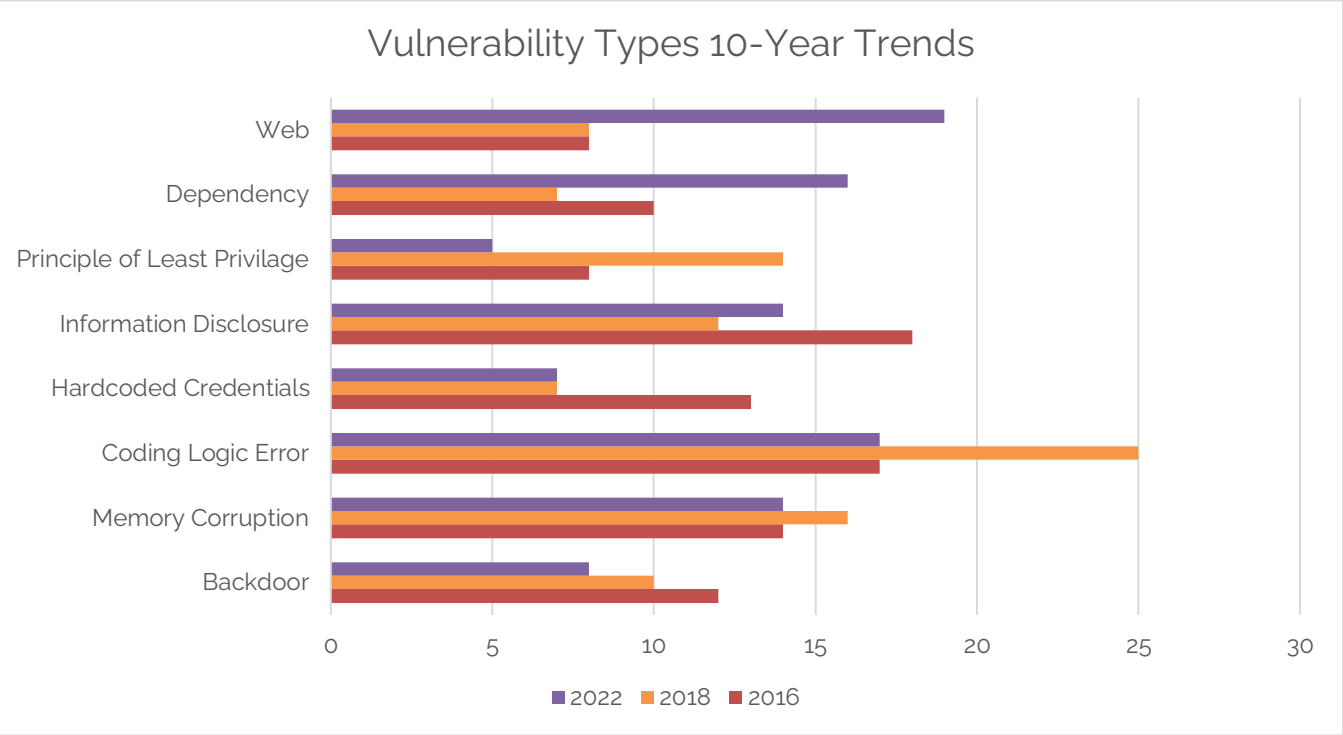
2018



2022

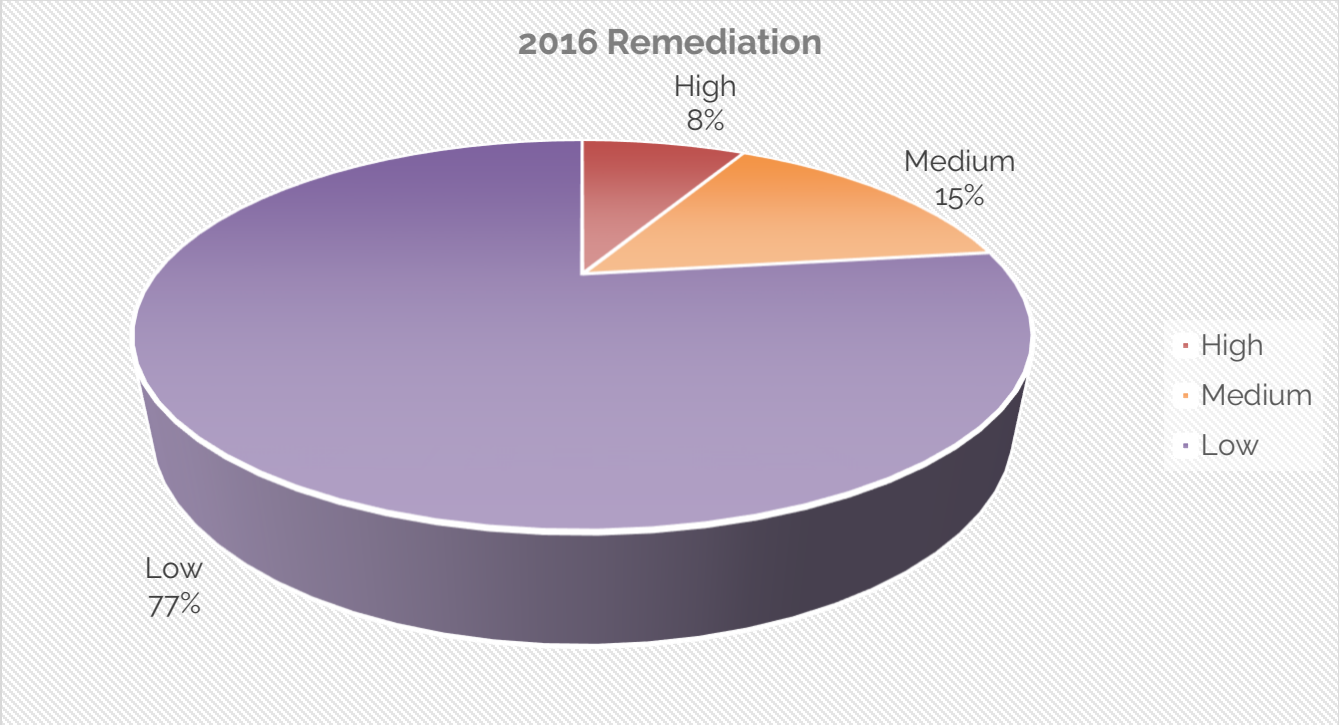


10-year Trend

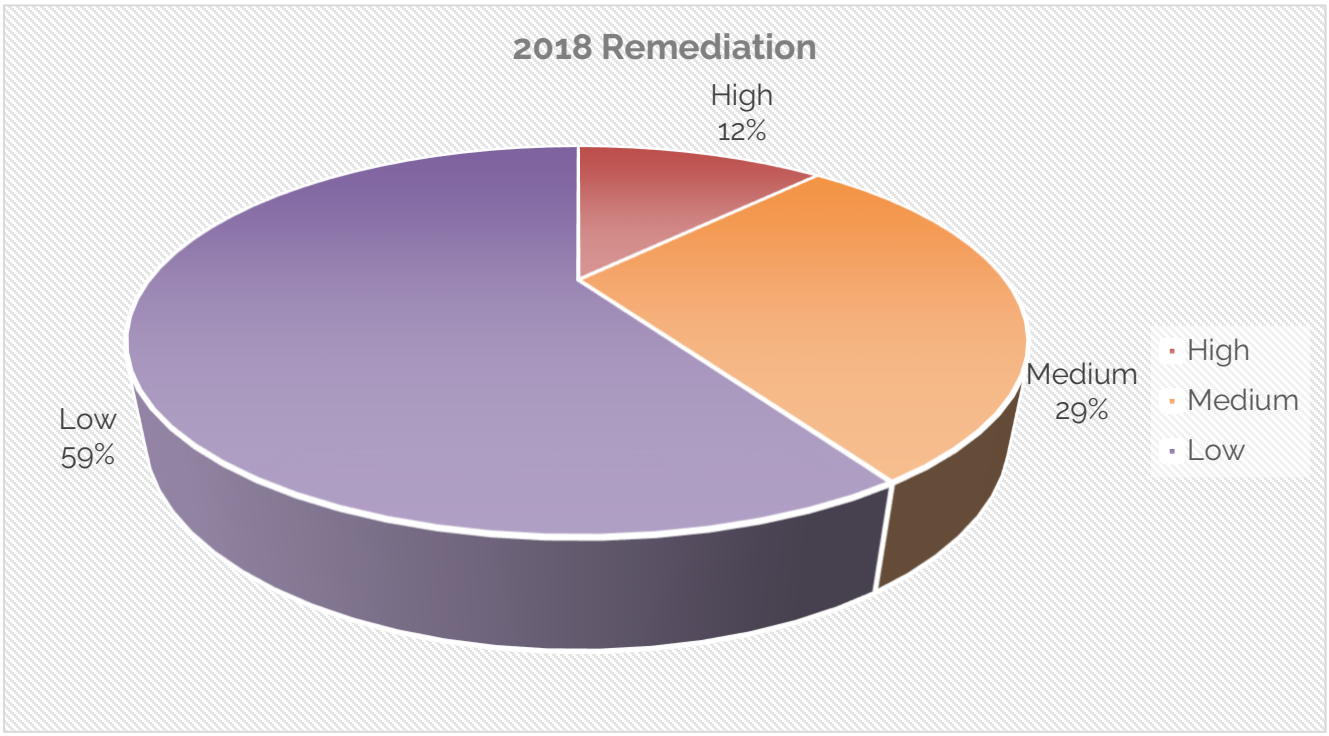


Critical Impact Remediation

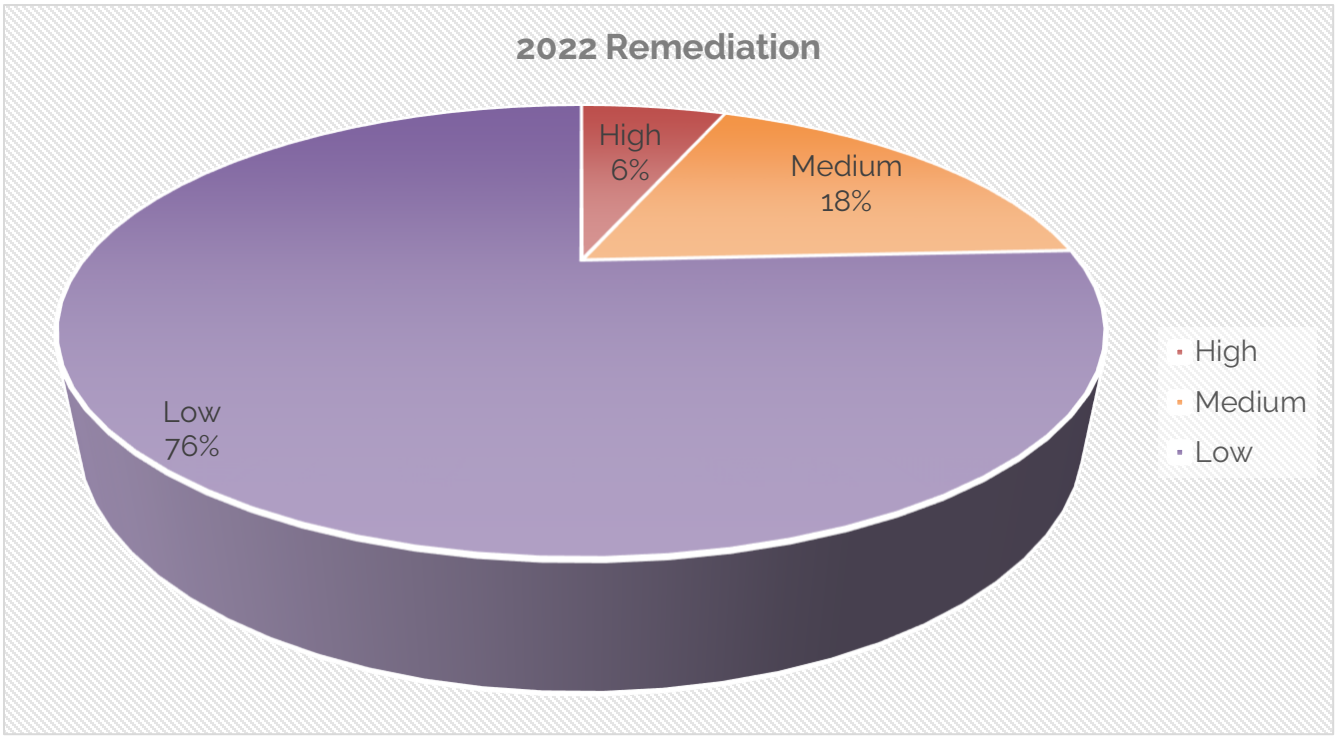
2016



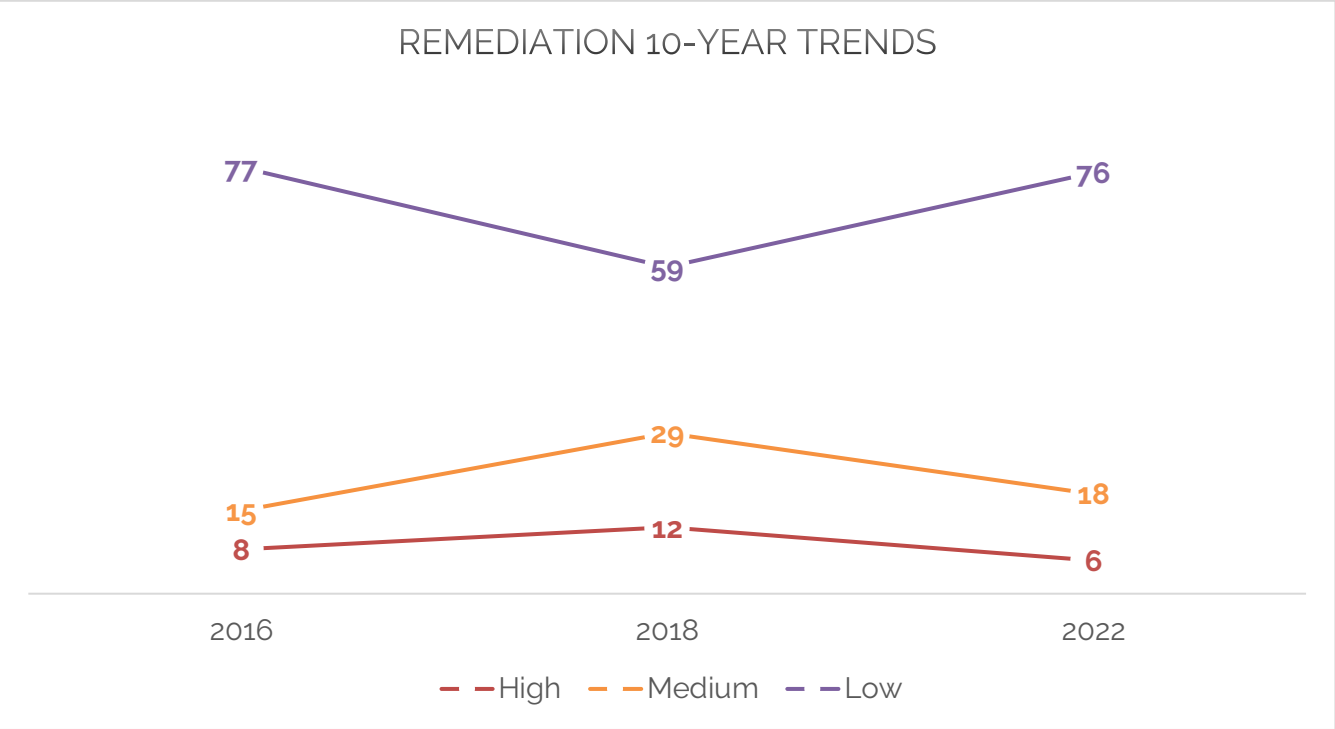
2018



2022

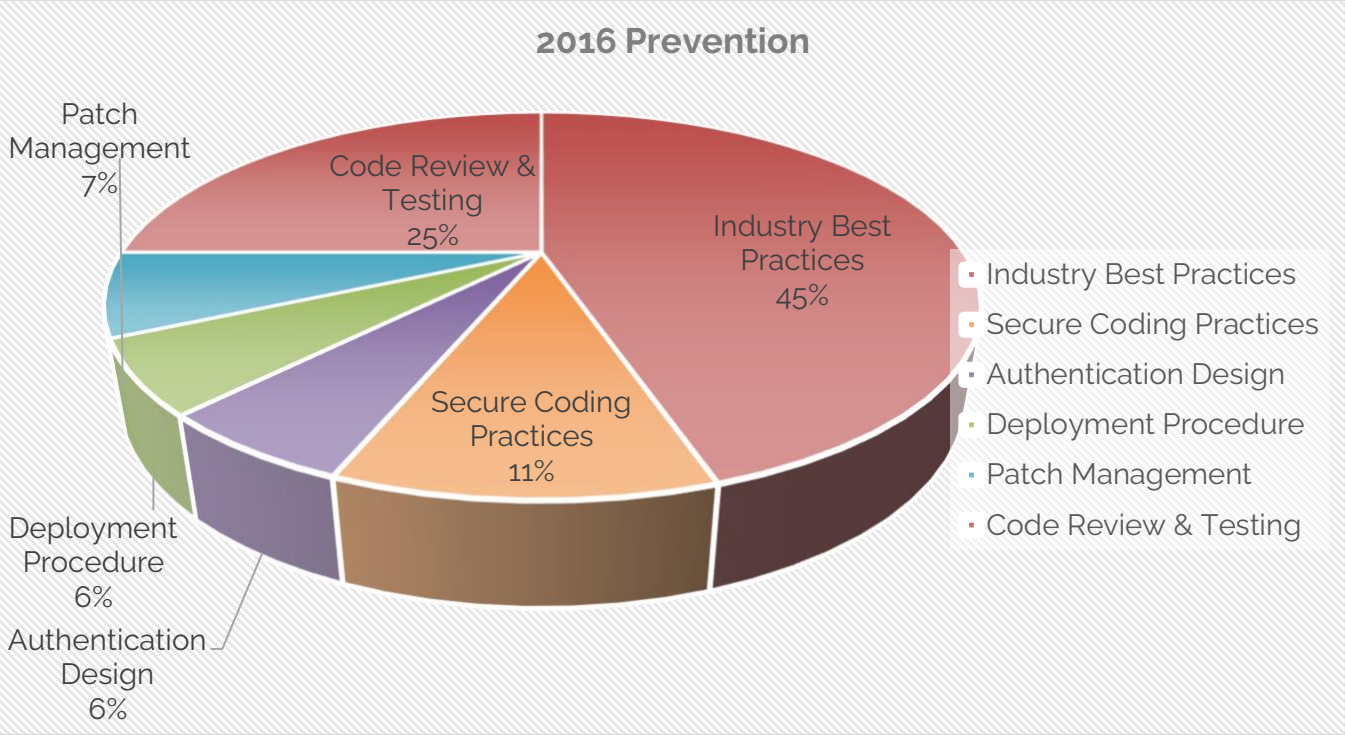


10-year Trend

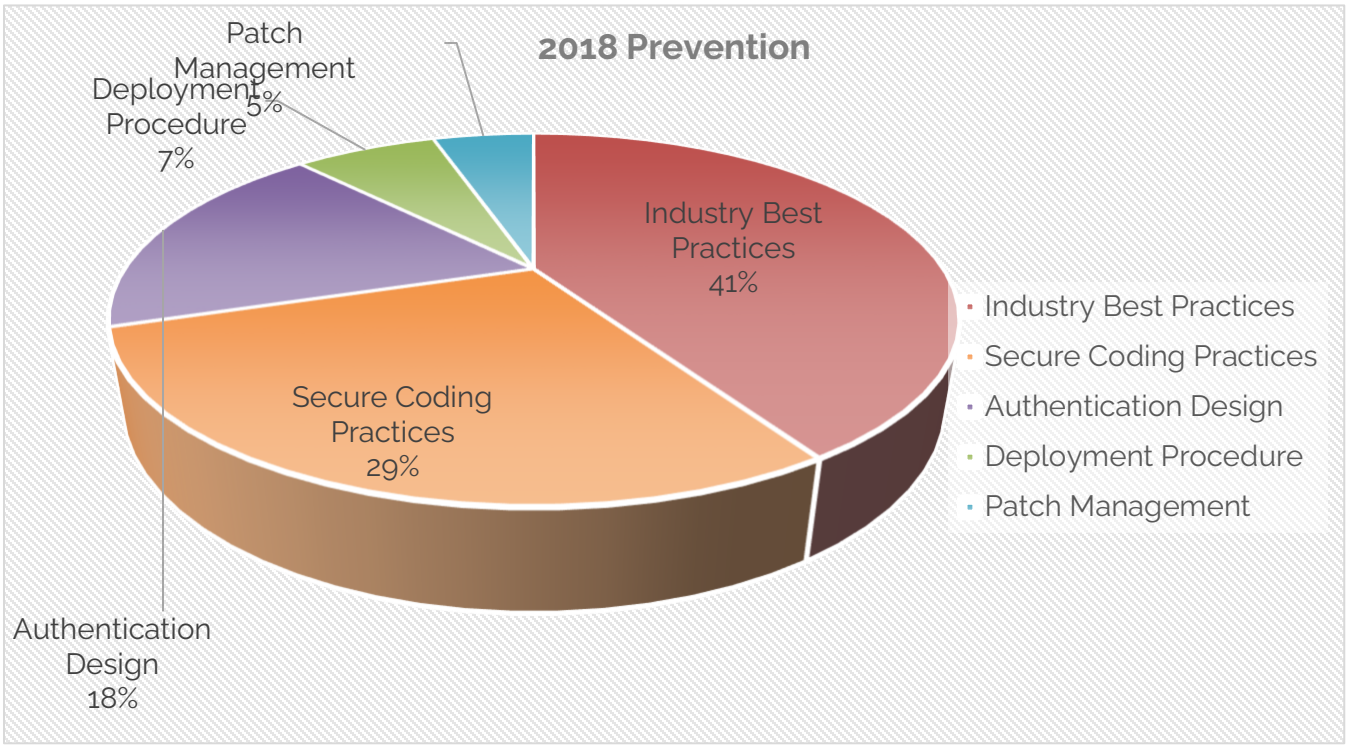


Ounce of Prevention

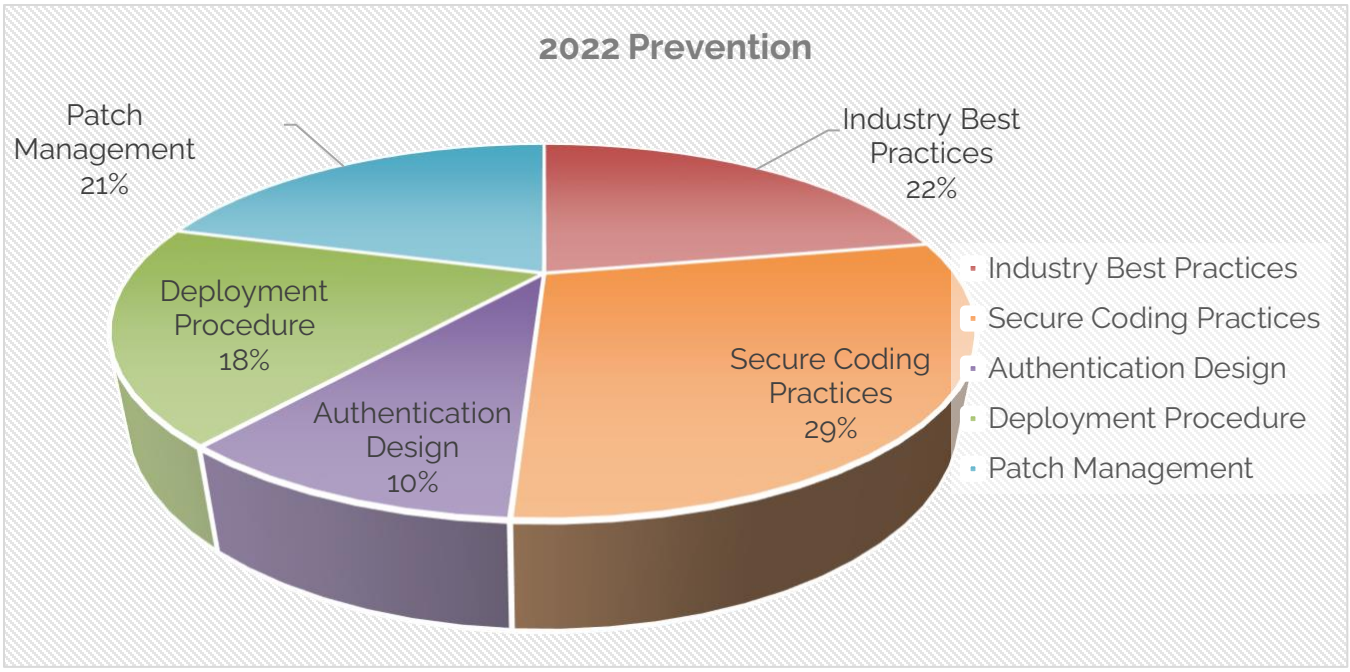
2016



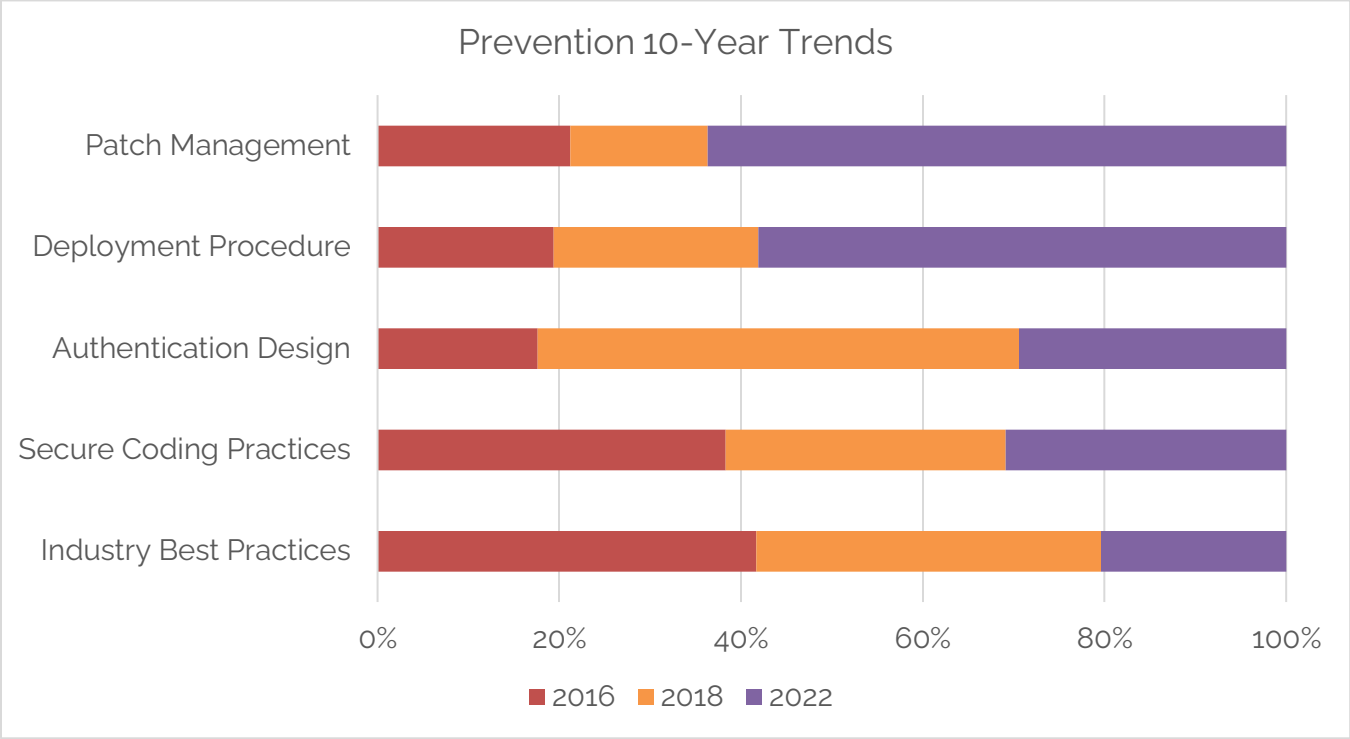
2018



2022



10-year Trend



References

(2021).Audi Skysphere Concept - Design Sketch. *Skysphere.* AUDI AG, Ingolstadt.

Auto-ISAC, Inc. (2022). *Automotive Information Sharing and Analysis Center*. Retrieved from Auto-ISAC: https://automotiveisac.com/

Baclawski, K. (2018). The Observer Effect. *2018 IEEE Conference on Cognitive and Computational Aspects of Situation Management* (pp. 83-89). Boston: IEEE.

Beaumont, S. I. (2022). *Commonalities in Vehicle Vulnerabilities, 2022 Remix.* Seattle, WA: IOActive, Inc.

Beaumont, S. I. (2022, June 15). *Conference Program - ESCAR USA 2022.* Retrieved from ESCAR: Embedded Security in Cars: https://escarusaevent.com/wp-content/uploads/2022/06/CommonalitiesVehicle_ESCAR_v2.0.pdf

Combs, G. (1998). Retrieved from Wireshark: http://www.wireshark.org

Dupuy, E. (2019, December 25). *java-decompiler/jd-gui*. Retrieved from GitHub: https://github.com/java-decompiler/jd-gui

Fuloria, S., Anderson, R., Alvarez, F., & McGrath, K. (2011). Key Management for Substations: Symmetric Keys, Public Keys or No Keys. *IEEE Power Systems Conference & Exposition 2011* (pp. 1-6). Phoenix: IEEE.

Hammond, J., & Culiss, J. (2018, September 9). *Commonalities in Vehicle Vulnerabilities.* Retrieved from IOActive, Inc.: https://ioactive.com/wp-content/uploads/2018/10/IOActive_Commonalities-in-Vehicle-Vulnerabilities.pdf

International Organization for Standardization. (2018). *ISO 26262:2018 Road Vehicles - Functional Safety.* Vernier, Geneva, Switzerland: International Organization for Standardization.

International Organization for Standardization. (2021). *ISO/SAE 21434:2021 Road Vehicles - Cybersecurity Engineering.* Vernier, Geneva, Switzerland: International Organization for Standardization.

International School of IT Security AG. (2022, June 15). *ESCAR USA 2022*. Retrieved from Embedded Security in Cars: https://www.escar.info/escar-usa.html

National Institute of Standards and Technology. (2006). *FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems.* Gaithersburg: Federal Information Processing Standards Publications.

National Institute of Standards and Technology. (2011, September). *Information Security Continuous Monitoring for Federal Information Systems and Organizations.* Retrieved from Information Security: NIST Special Publication 800-137: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

National Institute of Standards and Technology. (2012, September). *Guide for Conducting Risk Assessments.* Retrieved from Information Security: NIST Special Publication 800-30 Revision 1: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology. (2017). *NIST Special Publication 800-12 Revision 1: An Introduction to Information Security.* National Institute of Standards and Technology.

Newman, C., Menon-Sen, A., Melnikov, A., & Williams, N. (2010, July). *Salted Challenge Response Authentication Mechanism (SCRAM) SASL and GSS-API Mechanisms*. Retrieved from RFC Editor: tools.ietf.org/html/rfc5802

OWASP Foundation, Inc. (2022). *Fuzzing*. Retrieved from OWASP: https://owasp.org/www-community/Fuzzing

OWASP Foundation, Inc. (2022). *Who is the OWASP Foundation?* Retrieved from OWASP: https://owasp.org/

SAE International. (2021). *J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.* Warrendale: SAE International. Retrieved from https://www.sae.org/standards/content/j3061_202112/

The MITRE Corporation. (2006, July 19). *CWE-200: Exposure of Sensitive Information to an Unauthorized Actor*. Retrieved from Common Weakness Enumeration: https://cwe.mitre.org/data/definitions/200.html

The MITRE Corporation. (2010, January 15). *CWE-798: Use of Hard-coded Credentials*. Retrieved from Common Weakness Enumeration: https://cwe.mitre.org/data/definitions/798.html

Thuen, C. (2016, June 30). *Commonalities in Vehicle Vulnerabilities.* Retrieved from IOActive, Inc.: https://ioactive.com/pdfs/Commonalities_in_Vehicle_Vulnerabilities_WP.pdf

United Nations. (2023, 02). *UNECE R155.* Retrieved from https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf