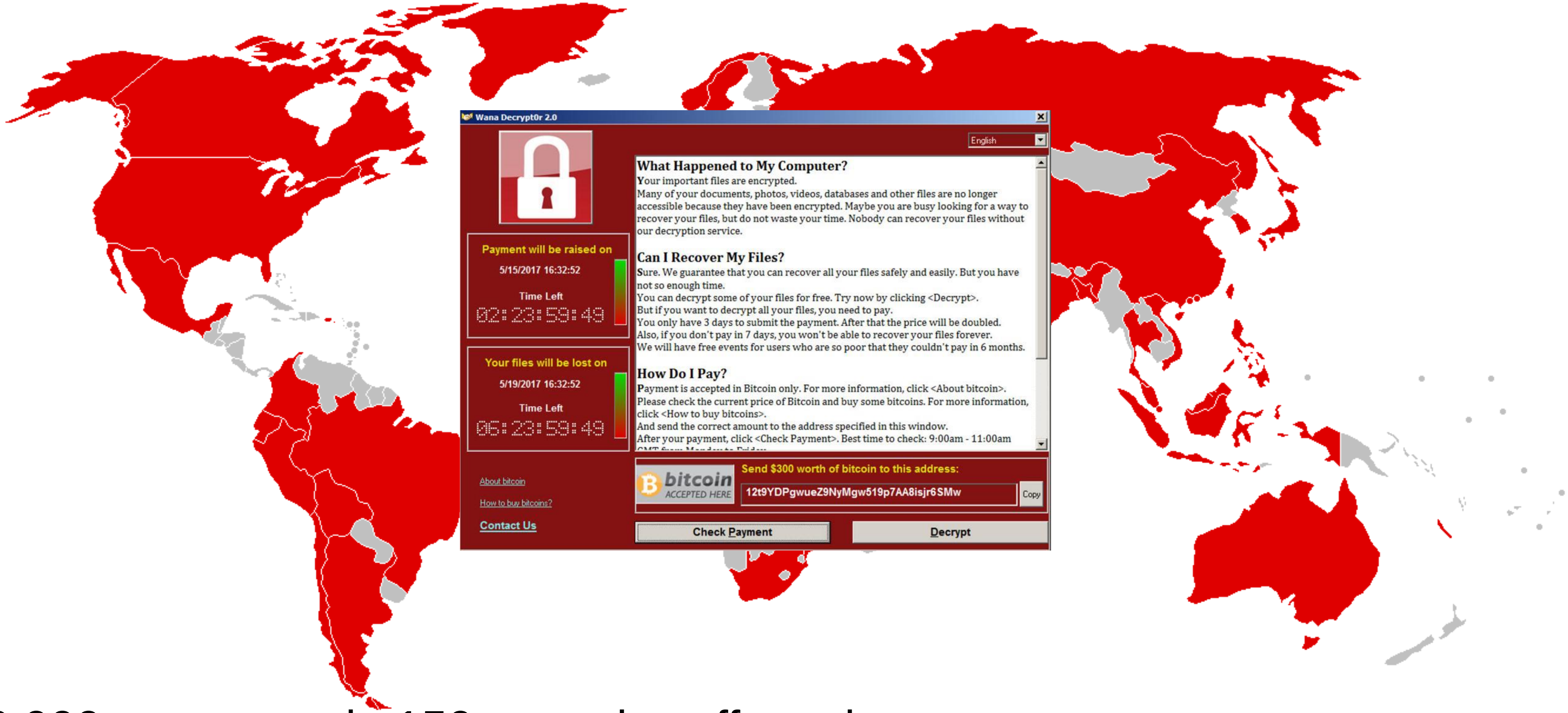
Connected Vehicle Cybersecurity Volvo Group Trucks Technology

Christian Sandberg, Volvo GTT
Presentation material:
Andreas Bokesand, Christian Sandberg

Chalmers, DAT300, 2018-10-10

WannaCry Ransomware Attack 2017-05-12



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

230 000 computers in 150 countries affected

- British Hospitals severely impacted
- Maersk reported financial impact 250M$
- ...

Imaginary – not a real case!

Your car ?

- impacting your ability to travel

STOP!
Pay $5,000 to
unlock this car

http://virusguides.com/wp-content/uploads/2016/09/ransomware-attacks-cars.jpg
https://www.intelligentenvironments.com/wp-content/uploads/2016/11/Ransomware-Car.png

Imaginary – not a real case!

Trucks ?

- Impacting transportation of goods!

In the first 24 hours…

- Hospitals will run out of necessary supplies.
- Service stations will begin to run out of fuel.
- Just-in-time manufacturing get component shortages.

In just 2-3 days…

- Food shortages, consumer hoarding and panic.
- Garbage will start piling up in urban areas.
- Container ships will sit idle in ports and rail transport will be disrupted

In just one week…

- Automobile travel will cease due to lack of fuel.

(US-centric scenario)

https://www.tdsource.com/2016/08/03/if-trucking-stops

Volvo Group - What we do

We are one of the world’s leading manufacturers of **trucks, buses, construction equipment and marine and industrial engines**.

ON THE ROAD

Our products help ensure that people have food on the table, can travel to their destination and roads to drive on.

IN THE CITY

Our products are part of the daily life. They take people to work, distribute goods and collect rubbish. We are developing tomorrow’s public transport solutions.

AT THE SITE

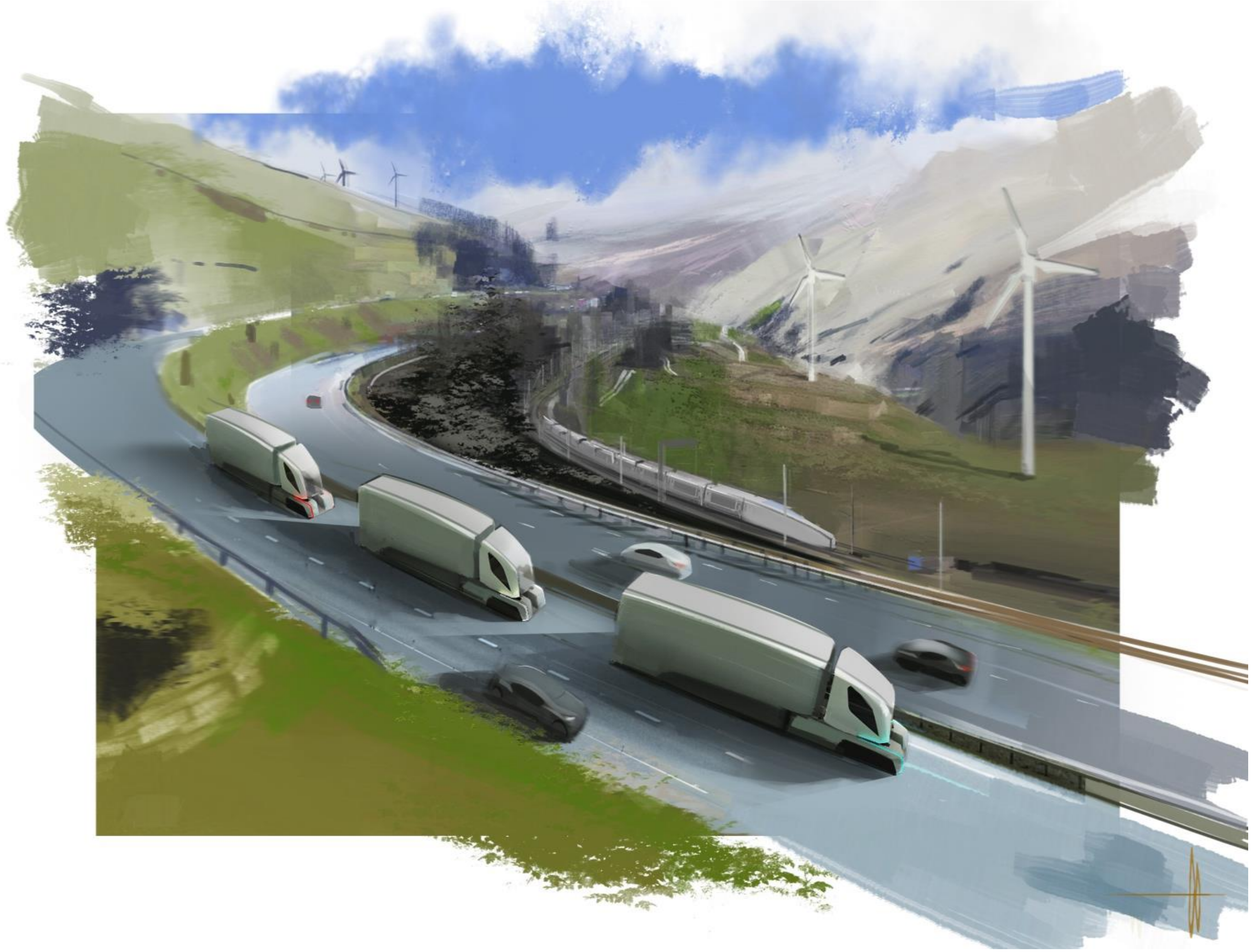
We contribute to the extraction of some of the world’s most important raw materials. Our engines, machines and vehicles can be found at mining and construction sites and in the middle of forests.

AT SEA

Our products and services are with you, regardless of whether you are at work on a ship or on holiday in your pleasure boat.

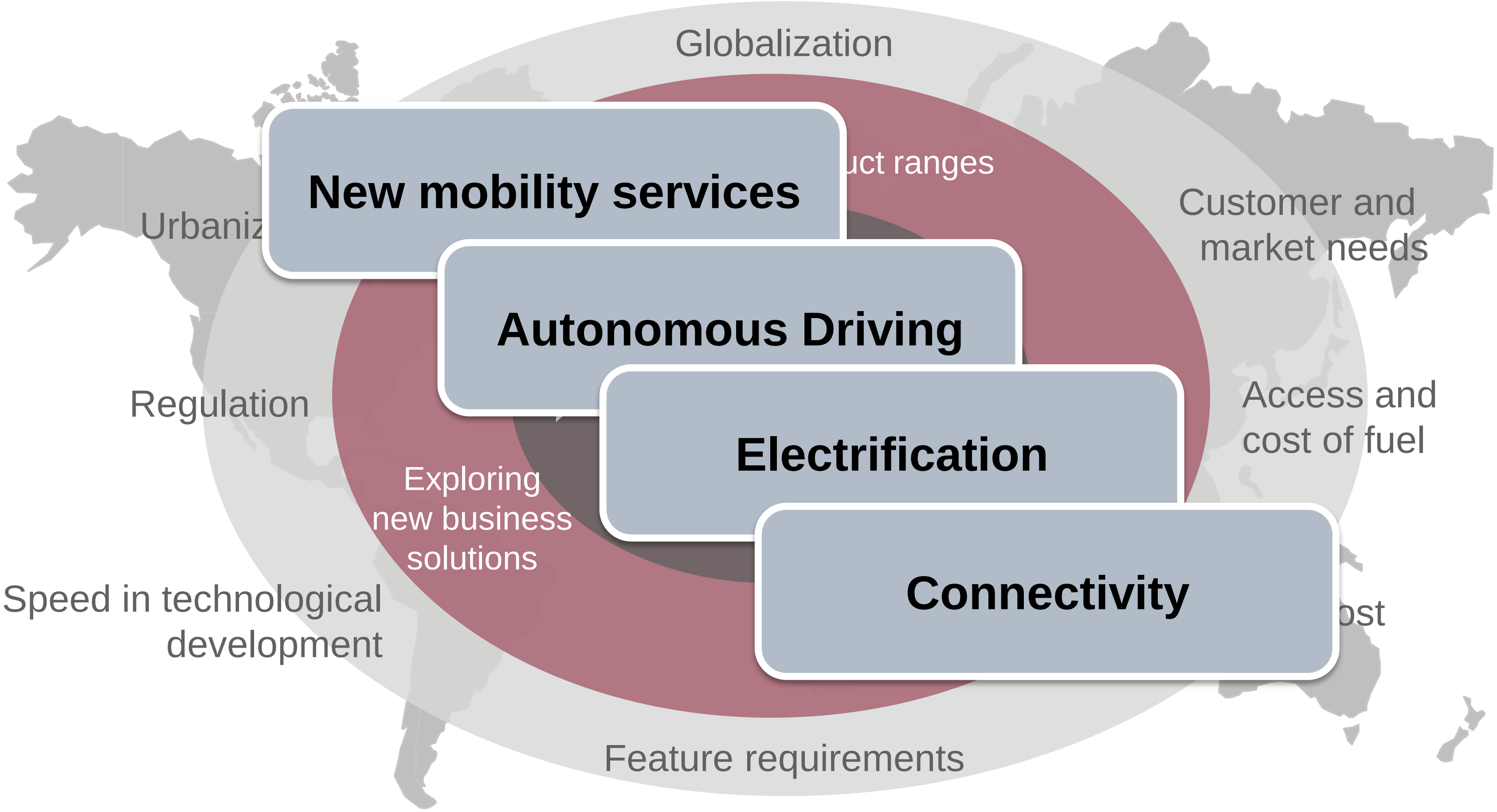
Group Trucks Technology

Our organization for **research and product development** of complete vehicles, powertrain, components and service offering.



The World Evolve

- Drivers for new technology



The classic vehicle

... was a self-contained system

The modern vehicle

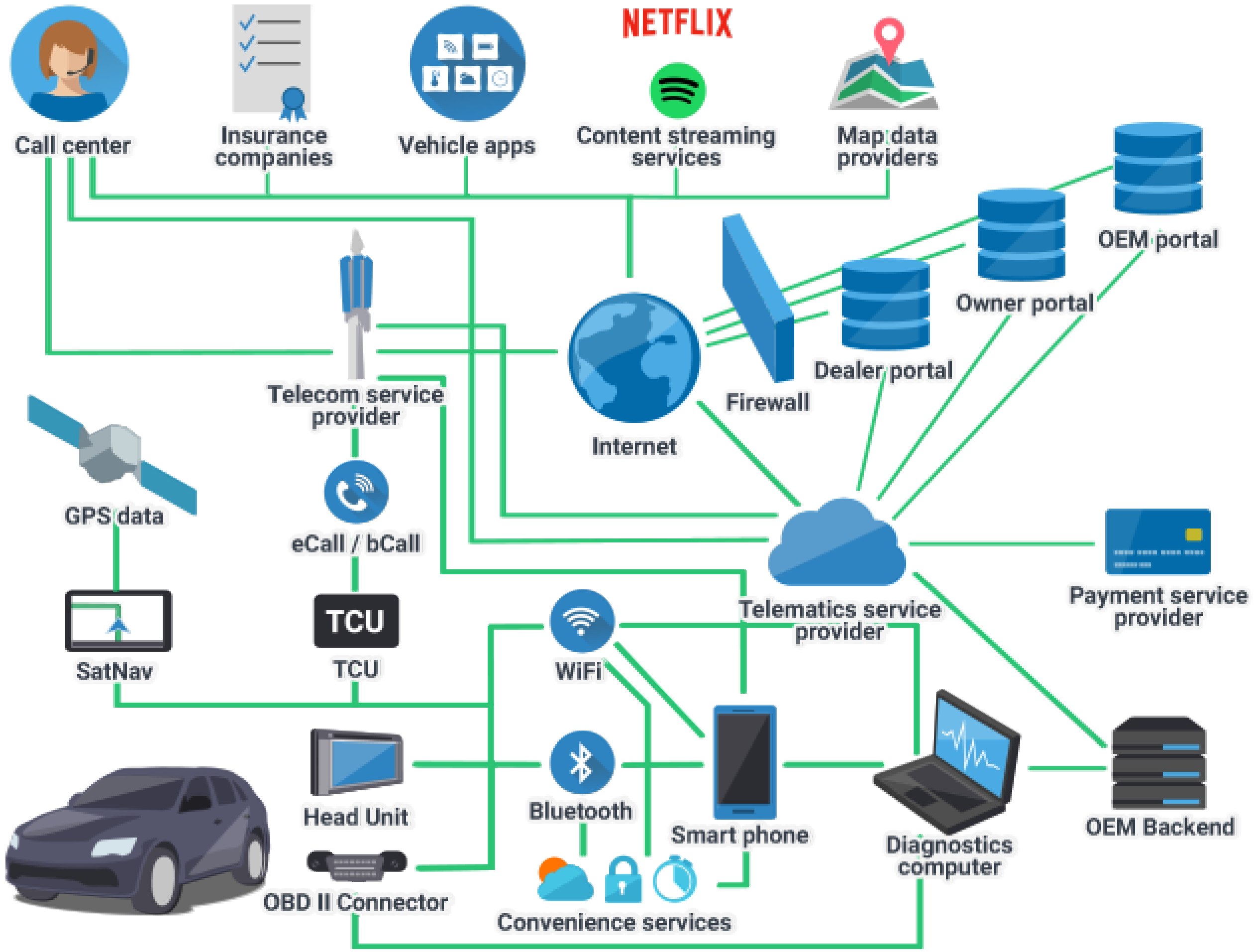
... is essentially a full IT infrastructure, on wheels!

((XM))
P
R·D·S
TCU
GLOBETROTTER
VOLVO
FH

http://www.starhub.com/content/dam/starhub/2016/business/resources/blog/mobile-security-breaches-you-need-to-prevent-today/content-image-unsecured-network.jpg

Connected vehicles

- The more things are connected, the higher the security concern



Researchers demonstrate the potential

July 21, 2015: "Hackers remotely kill a Jeep on the highway"
Source: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
Details: http://illmatics.com/Remote%20Car%20Hacking.pdf

Feb 24, 2016: "Nissan Leaf easily hacked through browser-based attacks"
Source: http://www.bbc.com/news/technology-35642749/
Details:http://www.troyhunt.com/2016/02/controlling-vehicle-features-of-nissan.html

Sep 20, 2016: "Researchers remotely hack Tesla Model S"
Source: https://www.washingtonpost.com/news/the-switch/wp/2016/09/20/researchers-remotely-hack-tesla-model-s/

Aug 2, 2016: "Hackers hijack big rig truck's accelerator and brakes"

Source: https://www.wired.com/2016/08/researchers-hack-big-rig-truck-hijack-accelerator-brakes/

Attackers and Motivations

Researcher may want to showcase and increase awareness

Hacker wants Fun, Fame

Third party developers want to offer add-ons and tuning

Criminal wants to disable vehicle to steal goods

Competitor can be interested in intellectual property

Authorities may require functionality for law enforcement, **owner** want to circumvent

Driver want higher road speed limit, **owner** want to control fuel consumption

Fleet/Vehicle owners may want to “upgrade” their own vehicles

Thief wants to disable alarm or immobilizer, copy/add keys

Criminals can earn money by vehicle ransom

Attackers and Attack vectors

Tool access (unauthorized program licence, ECU reprogramming)

Remote access

- Telecom network access (radio / base station)
- VPN entry points (Back-office)
- Portals exposed to the Internet

Physical access (Using OBD connector, tampering with ECU's and/or CAN buses)

Proximity access (Wifi/Bluetooth)

Attacks on infrastructure

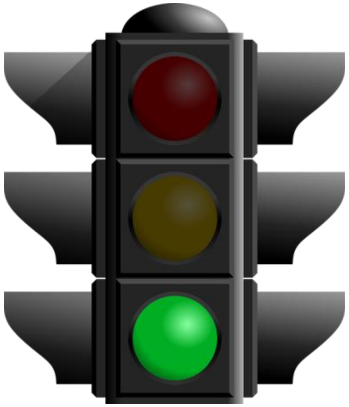
ElectriCity – Bus 55

- Wireless connection
- Charging stations, 600+ Volts
  - Safety implications
- Supplier / consumer
  - Threat of fraud (billing)
- Something to think about:
  - Impact on society of a cyber attack on the power grid from transportation point of view: Electrical vs fossil fuel vehicles?

Attacks on infrastructure

V2I – Example use cases and threats

- **Road works warning**
  - False warnings
  - Jamming legitimate information
- **Green light priority** (heavy vehicles wear down pavement more when stopped. Energy consuming to decelerate and accelerate)
  - Cheating. Attackers getting green light.
  - Traffic disruption by spoofing heavy traffic (or emergency service vehicles)



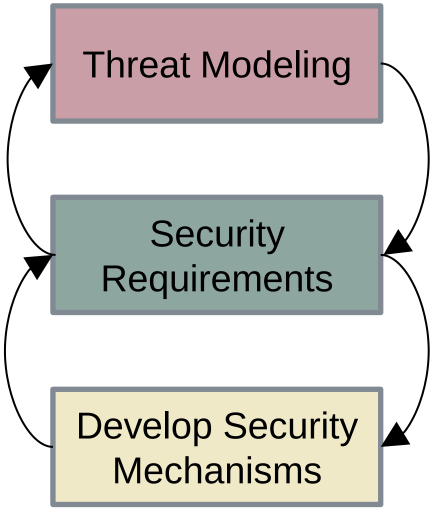
Security Engineering principle

The principle for Security Engineering is a **risk based approach**.

Security requirements are derived using a

structured engineering process and based on:

- identification of threats
- risk assessment (likelihood and impact)
- mitigate or accept the risk associated with the threat

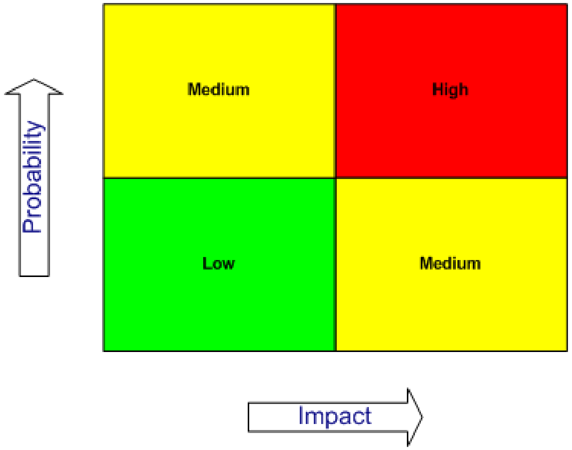


Source: Myagmar, Yurcik

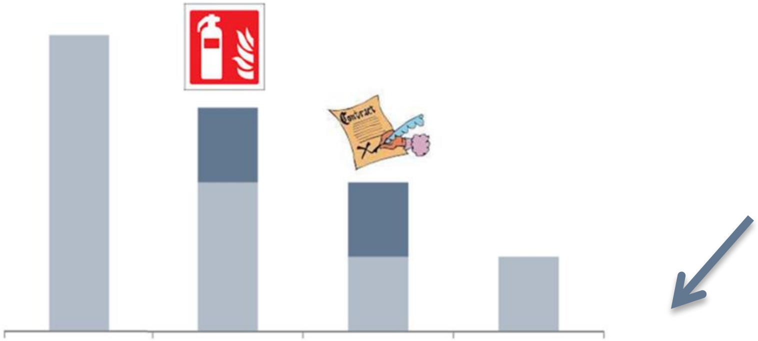
Note: Mature areas can have standardized, minimum security requirements (compliance)

Risk Management

- A very quick introduction



Medium	High
Low	Medium

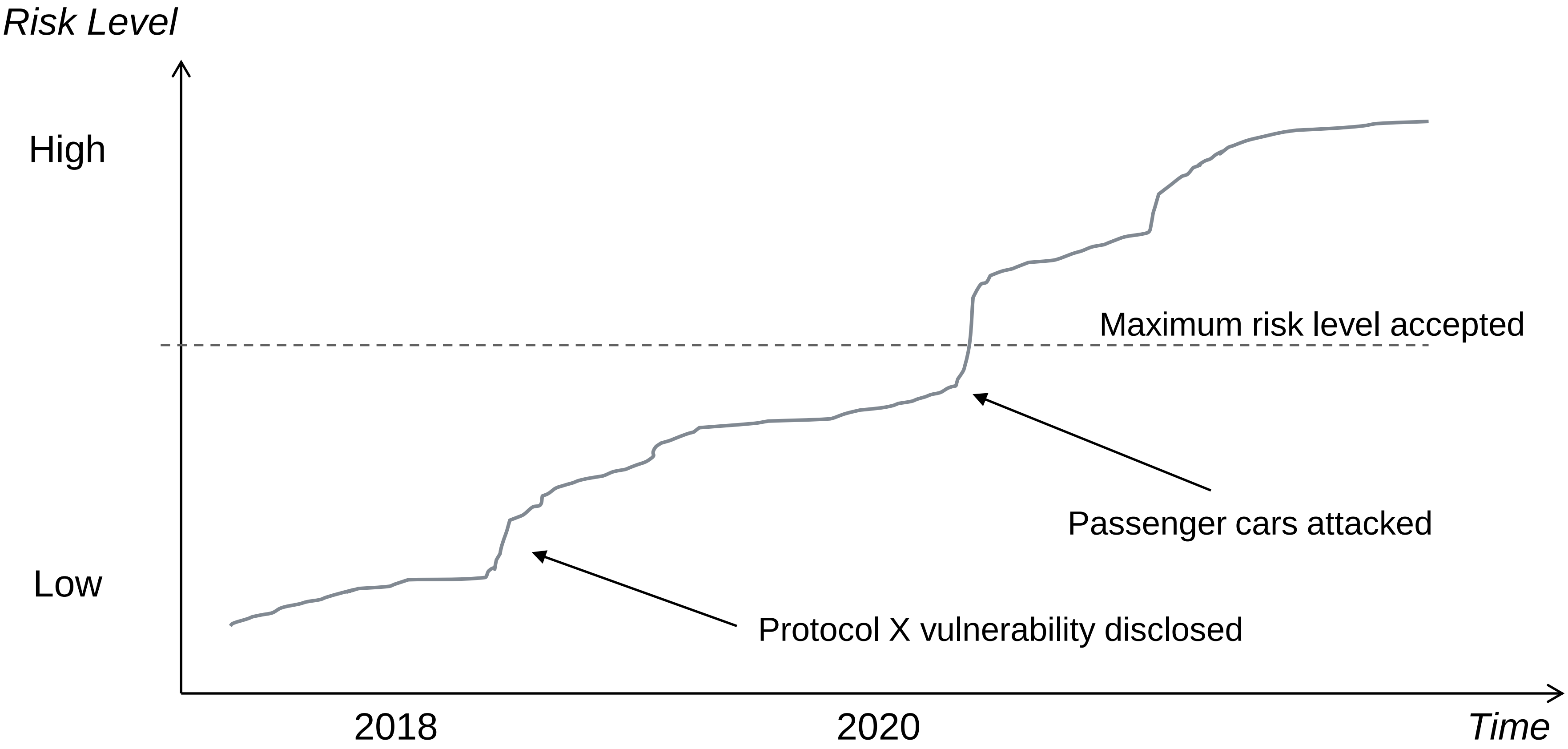


Impact Control Transfer Accept / Avoid

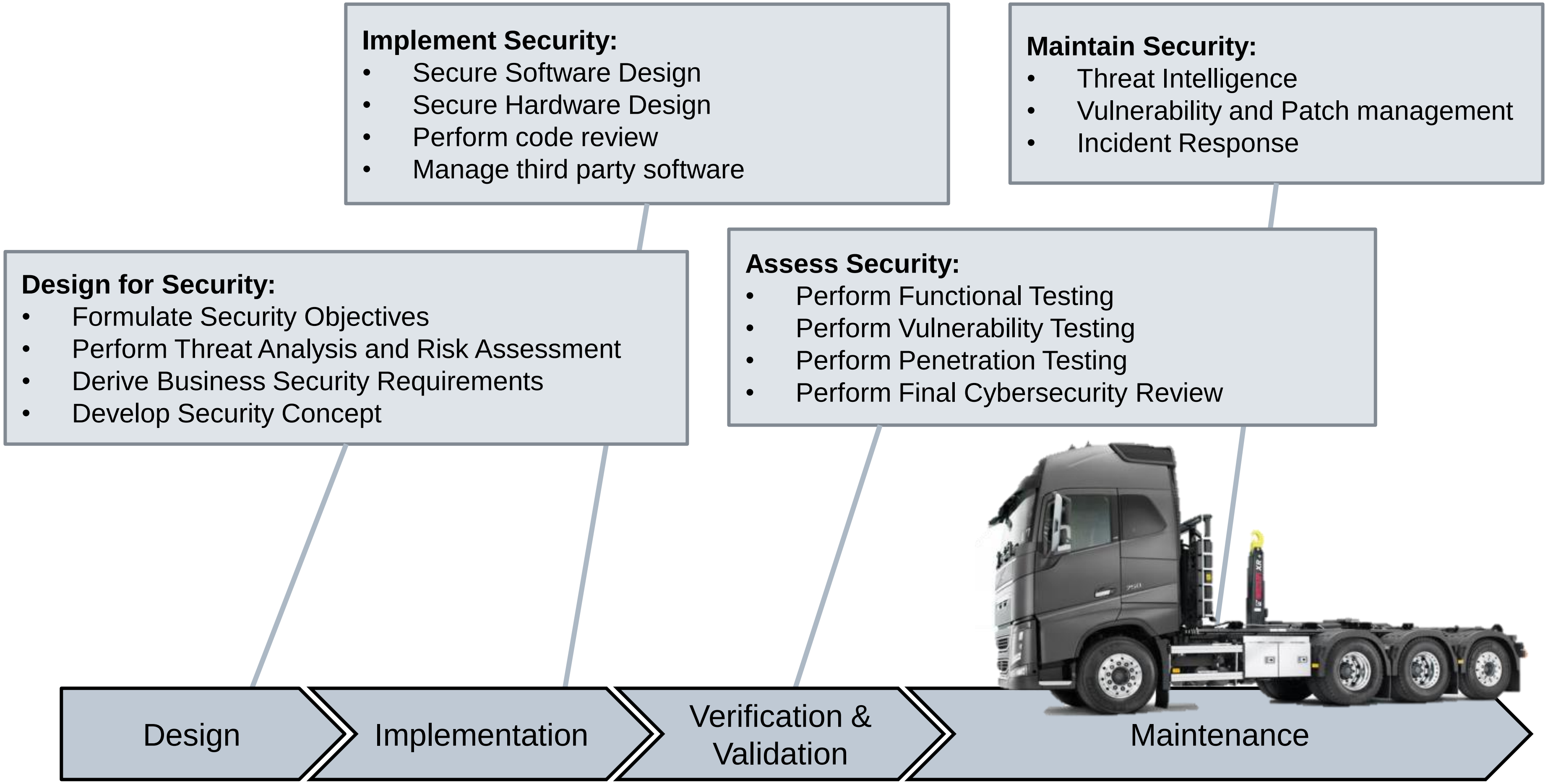
Accepted Risk

$
NEW FEATURE!

Security risks are dynamic
- risk level at product release will not remain



Cybersecurity and Vehicle Lifecycle



Implement Security:

- Secure Software Design
- Secure Hardware Design
- Perform code review
- Manage third party software

Maintain Security:

- Threat Intelligence
- Vulnerability and Patch management
- Incident Response

Design for Security:

- Formulate Security Objectives
- Perform Threat Analysis and Risk Assessment
- Derive Business Security Requirements
- Develop Security Concept

Assess Security:

- Perform Functional Testing
- Perform Vulnerability Testing
- Perform Penetration Testing
- Perform Final Cybersecurity Review

Design

Implementation

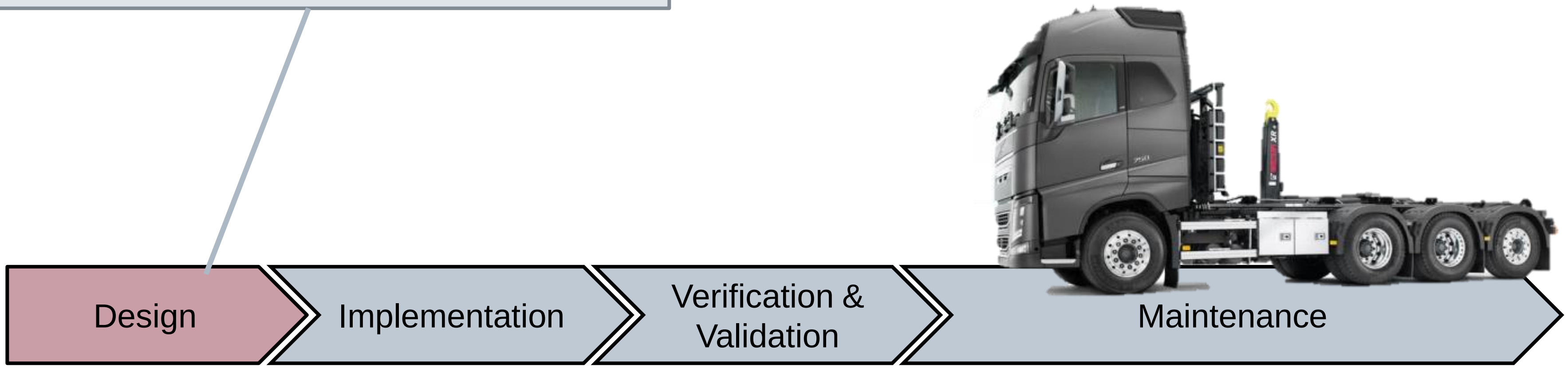
Verification &
Validation

Maintenance

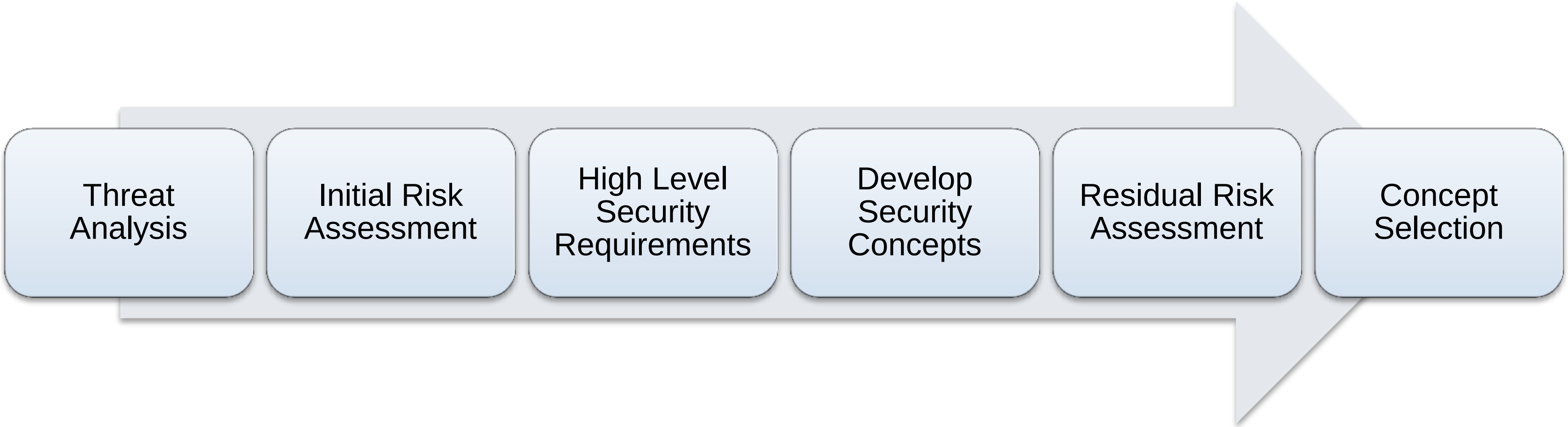
Design for Security

Design for Security:

- Formulate Security Objectives
- Perform Threat Analysis and Risk Assessment
- Derive Business Security Requirements
- Develop Security Concept



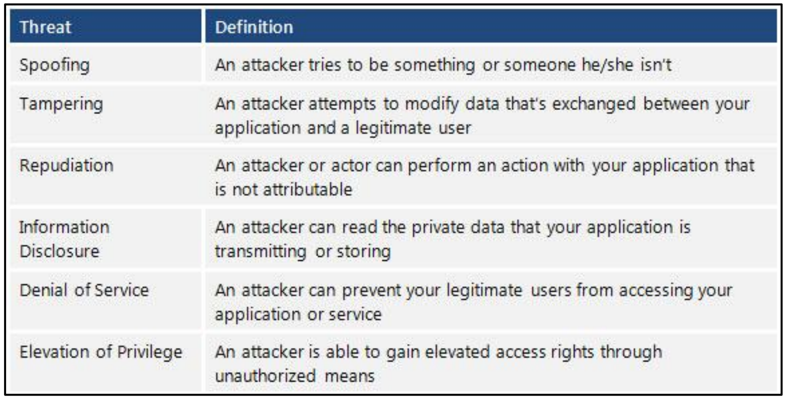
Design for Security



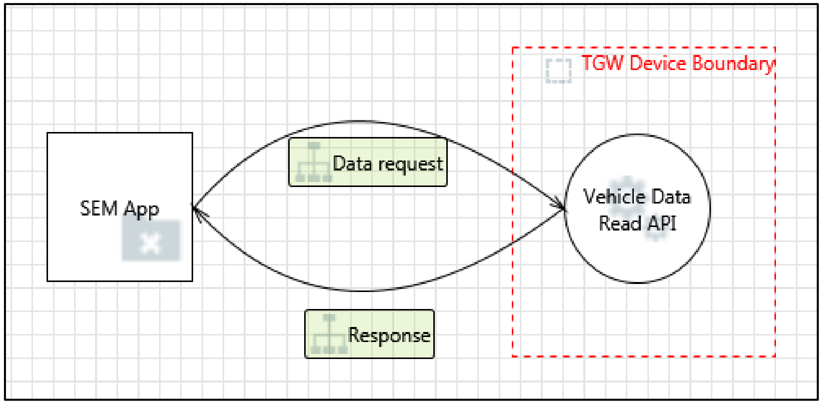
- Threat Analysis to identify possible cybersecurity threats.
- Assess impact level of the identified threats/attacks (less focus on threat level)
- Formulate high level security requirements to mitigate the identified risks.
- Develop security concepts to be implemented.
- Assess Threat Level considering the security concepts in place
- Results in residual design risks (Accept or Avoid)

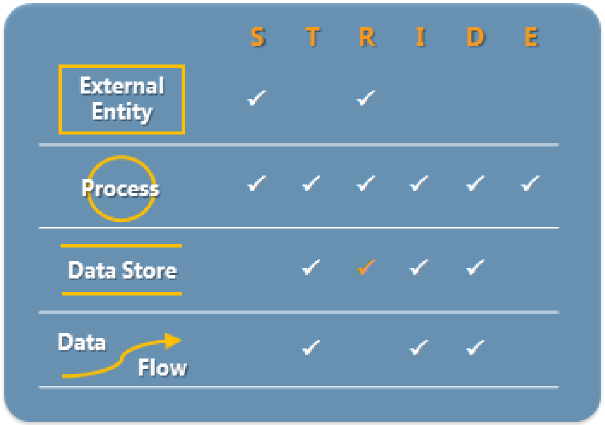
Threat Analysis

- System model
- STRIDE analysis

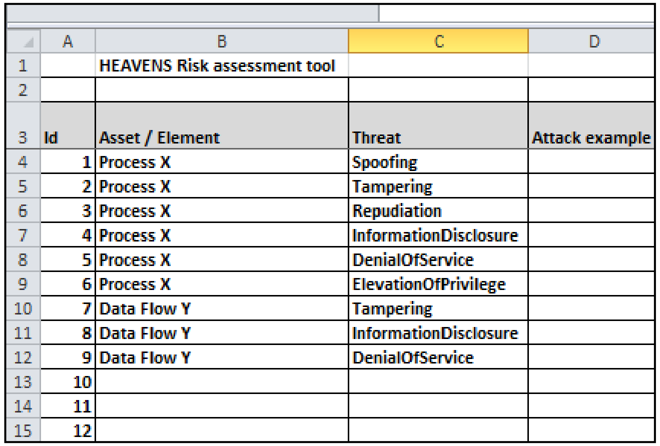


Threat	Definition
Spoofing	An attacker tries to be something or someone he/she isn't
Tampering	An attacker attempts to modify data that's exchanged between your application and a legitimate user
Repudiation	An attacker or actor can perform an action with your application that is not attributable
Information Disclosure	An attacker can read the private data that your application is transmitting or storing
Denial of Service	An attacker can prevent your legitimate users from accessing your application or service
Elevation of Privilege	An attacker is able to gain elevated access rights through unauthorized means





	S	T	R	I	D	E
External Entity	✓		✓			
Process	✓	✓	✓	✓	✓	✓
Data Store		✓	✓	✓	✓	
Data Flow		✓		✓	✓	



	A	B	C	D
1		HEAVENS Risk assessment tool		
2				
3	Id	Asset / Element	Threat	Attack example
4	1	Process X	Spoofing	
5	2	Process X	Tampering	
6	3	Process X	Repudiation	
7	4	Process X	InformationDisclosure	
8	5	Process X	DenialOfService	
9	6	Process X	ElevationOfPrivilege	
10	7	Data Flow Y	Tampering	
11	8	Data Flow Y	InformationDisclosure	
12	9	Data Flow Y	DenialOfService	
13	10			
14	11			
15	12			

Risk Assessment – Impact level

Safety (ISO26262 severity)

No injury	[✓ 0]
Light/moderate injury	10
Severe/life-threatening injury	100
Life-threatening/Fatal injury	1000

Financial (Operating Income)

<X MSEK	0
X-X MSEK	[✓ 10]
X-X MSEK	80
X-X MSEK	700
> X MSEK	1000

Operational (Disturbance)

No impact	0
Low	[✓ 1]
Medium	10
High	100

Privacy and Legislation

No impact	0
Low	[✓ 1]
Medium	10
High	100

Impact Level Calculation

Sum of IL parameter values	Impact Level	IL Value
0	None	0
[✓ 1 – 19]	Low	1
20 – 99	Medium	2
100 – 999	High	3
>= 1000	Critical	4

Risk Assessment – Threat level

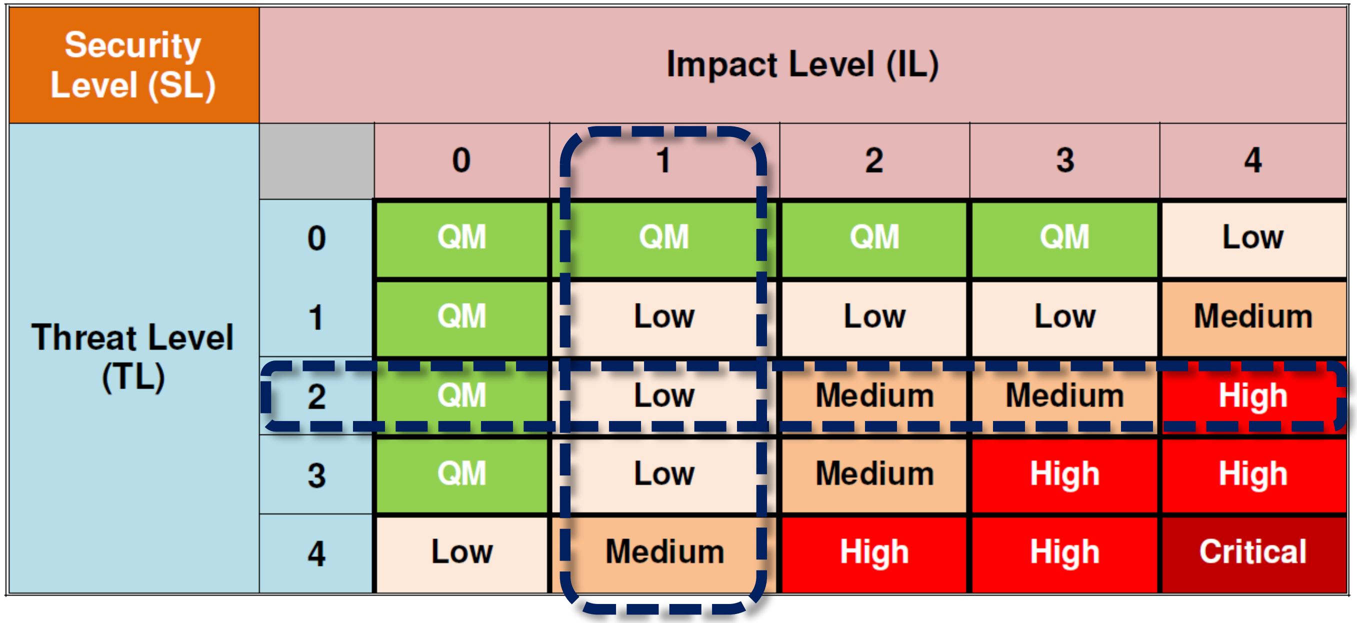
Expertise	
Layman	0
Proficient	[✓ 1]
Expert	2
Multiple experts	3
Knowledge about TOE	
Public	0
Restricted	1
Sensitive	[✓ 2]
Critical	3
Window of opportunity-Accessibility	
Indirect wireless	0
Direct wireless	[✓ 1]
No vehicle disassembly	2
Disassembly of vehicle	3
Component disassembly	4
Window of opportunity-Exposure time	
Infinite	0
Frequent	[✓ 1]
Sporadic	2
Rare	3
Equipment	
Standard	0
Specialized	[✓ 1]
Bespoke	2

Threat Level Calculation

Sum of TL parameter values	Threat Level	TL Value
> 9	None	0
7 – 9	Low	1
[✓ 4 – 6]	[✓ Medium]	[✓ 2]
2 – 3	High	3
0 – 1	Critical	4

Very low
↑
Probability
↓
High

Risk Assessment – Security Level



Security Level (SL)		Impact Level (IL)				
		0	1	2	3	4
Threat Level (TL)	0	QM	QM	QM	QM	Low
	1	QM	Low	Low	Low	Medium
	2	QM	Low	Medium	Medium	High
	3	QM	Low	Medium	High	High
	4	Low	Medium	High	High	Critical

Security Requirements

- After determining the risk for identified threats, security requirements can be derived for each threat

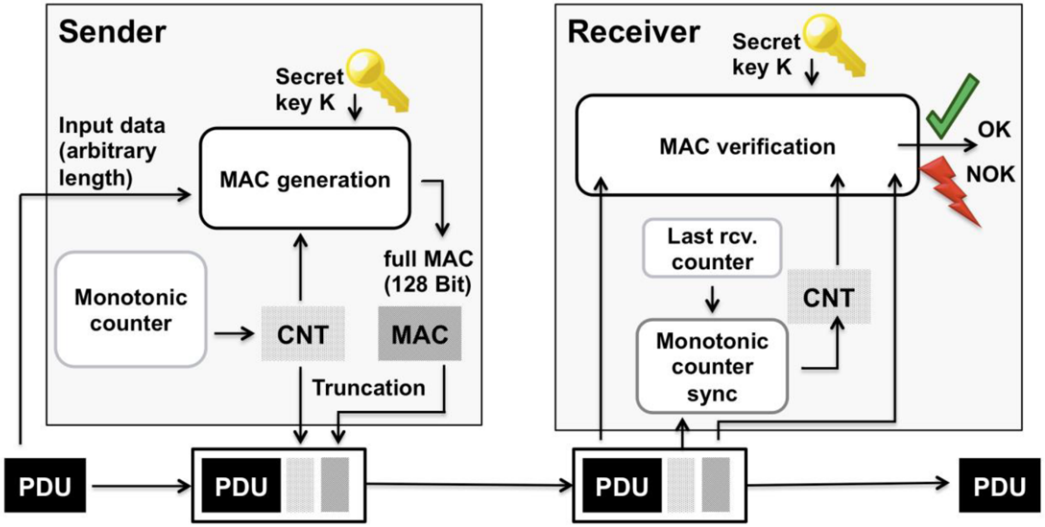
No.	Asset	Threat	Security Attribute	Security Level
1	Vehicle Data Response	Tampering of Vehicle Data Response	Integrity	Low
…				

- High level security requirement #1:
  The integrity of the Vehicle Data Response shall be ensured

Example of a Security Concept

Security Requirement: The integrity of message X shall be ensured

- Integrity protection is e.g. included in AUTOSAR Secure Onboard Communication protocol (adding message authentication codes (MAC) to the original data)

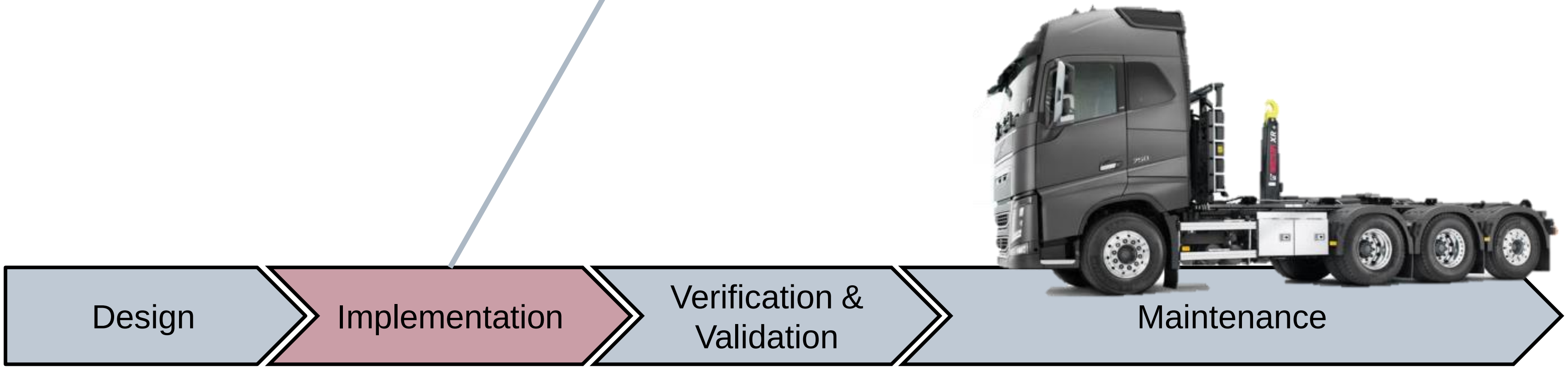


- Mechanism clear, but security relies on good key management

Implement Security

Implement Security:

- Secure Software Design
- Secure Hardware Design
- Perform code review
- Manage third party software



Design

Implementation

Verification & Validation

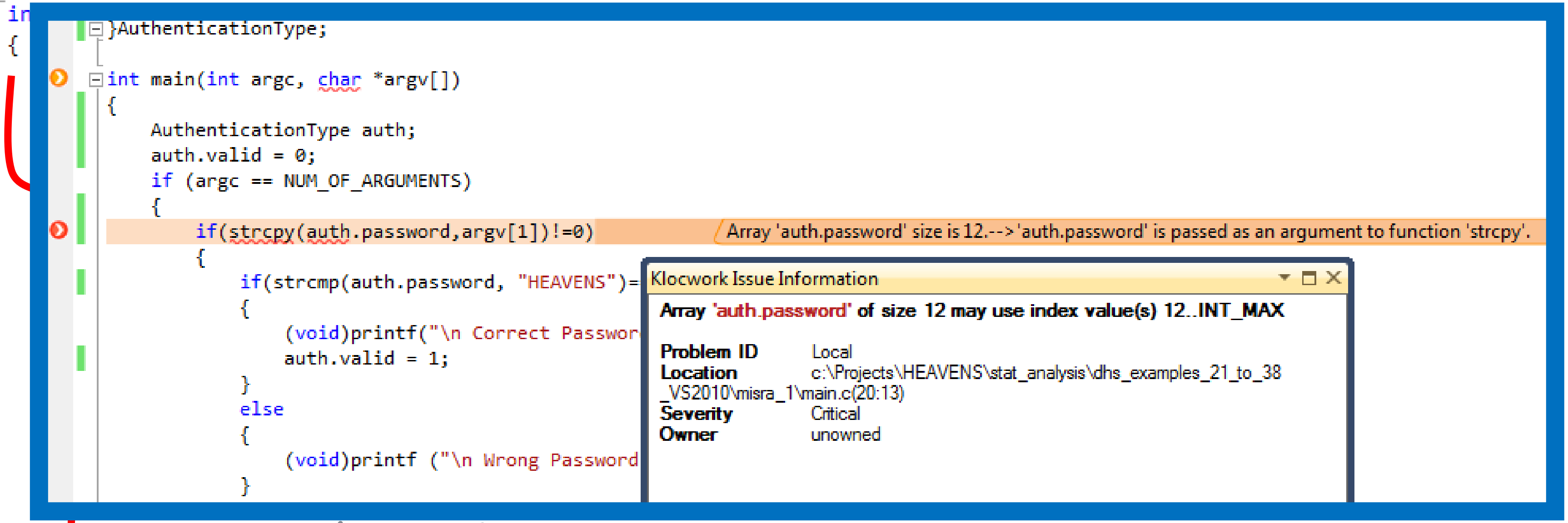
Maintenance

Static code analysis

Buffer overflow example of MISRA C Clean code.
MISRA C compliance != secure

```
#define NUM_OF_ARGUMENTS 2
typedef struct
{
  BYTE password[12];
  BOOL valid;
}AuthenticationType;

in
{
```



```
}AuthenticationType;

int main(int argc, char *argv[])
{
    AuthenticationType auth;
    auth.valid = 0;
    if (argc == NUM_OF_ARGUMENTS)
    {
        if(strcpy(auth.password,argv[1])!=0)
        {
            if(strcmp(auth.password, "HEAVENS")=
            {
                (void)printf("\n Correct Passwor
                auth.valid = 1;
            }
            else
            {
                (void)printf ("\n Wrong Password
            }
```

Array 'auth.password' size is 12.-->'auth.password' is passed as an argument to function 'strcpy'.

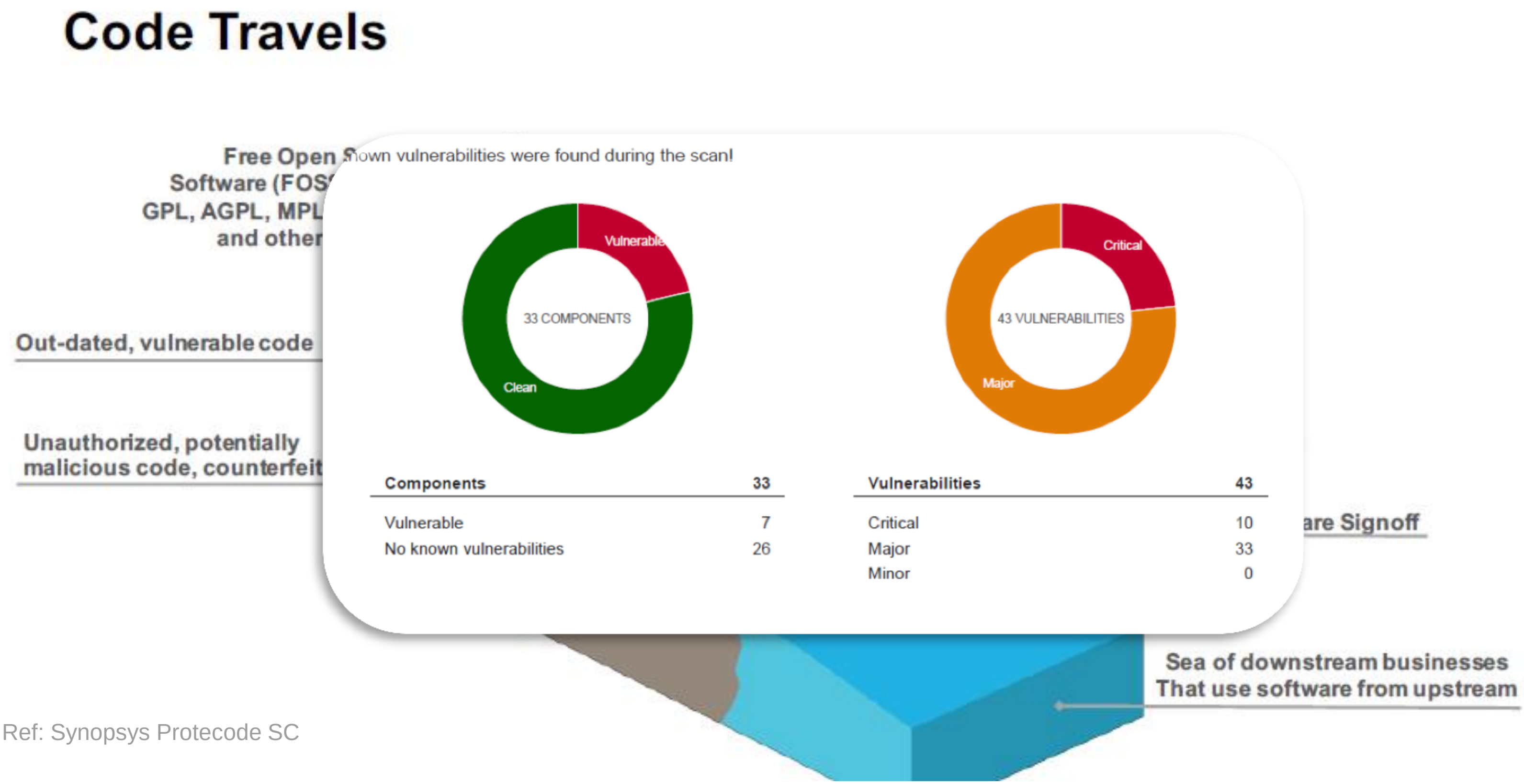
Klocwork Issue Information

Array 'auth.password' of size 12 may use index value(s) 12..INT_MAX

Problem ID	Local
Location	c:\Projects\HEAVENS\stat_analysis\dhs_examples_21_to_38_VS2010\misra_1\main.c(20:13)
Severity	Critical
Owner	unowned

```
    if(auth.valid!=0)
    {
     (void)printf ("\n Security level 1 access granted \n");
    }
   }
  }
```

Software composition analysis


Code Travels
Free Open S
Software (FOS
GPL, AGPL, MPL
and other
Out-dated, vulnerable code
Unauthorized, potentially
malicious code, counterfeit
are Signoff
Sea of downstream businesses
That use software from upstream
Vulnerable
33 COMPONENTS
Clean
Critical
43 VULNERABILITIES
Major

Known vulnerabilities were found during the scan!

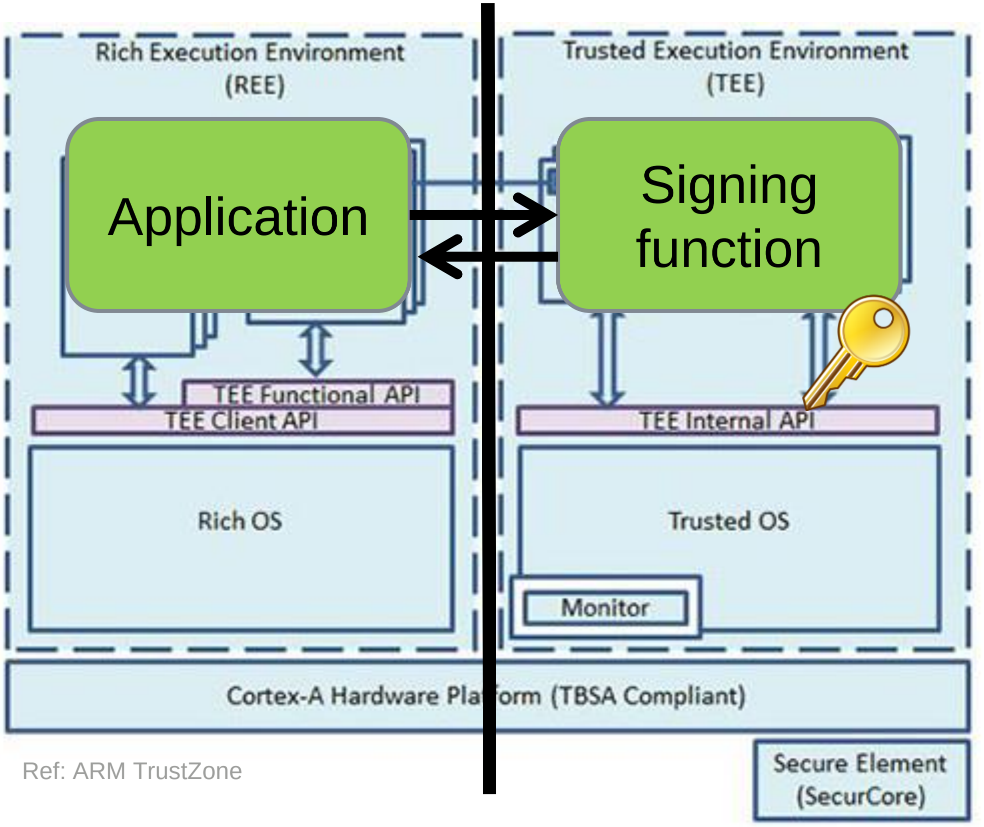
Components	33
Vulnerable	7
No known vulnerabilities	26

Vulnerabilities	43
Critical	10
Major	33
Minor	0

Ref: Synopsys Protecode SC

Software and Hardware design

- Example of isolated execution environment



Ref: ARM TrustZone

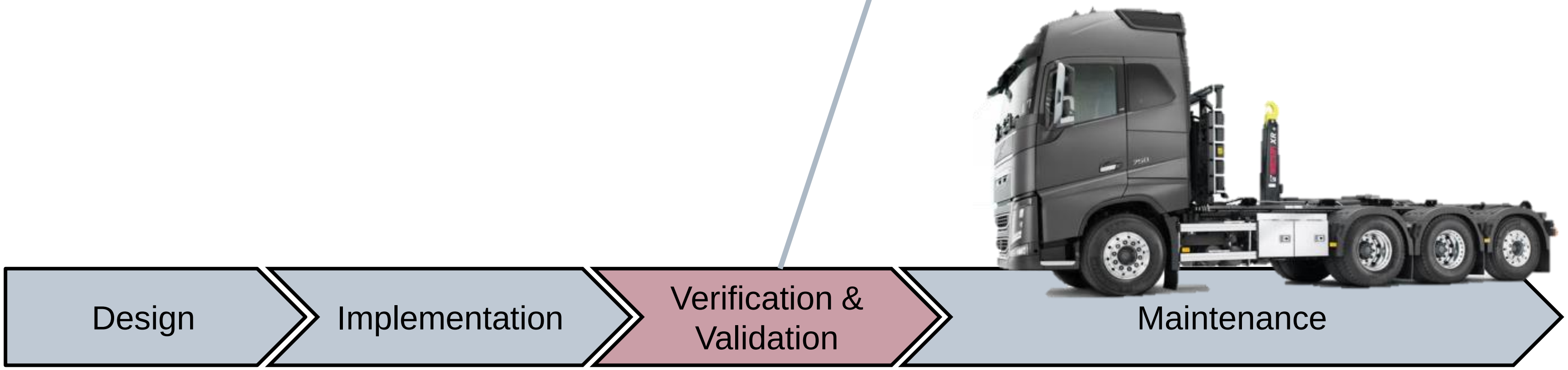
Example use

- Need to protect access to private key
- Application can sign data, but have no access to key
- Even if attacker compromise application, private key is not compromised

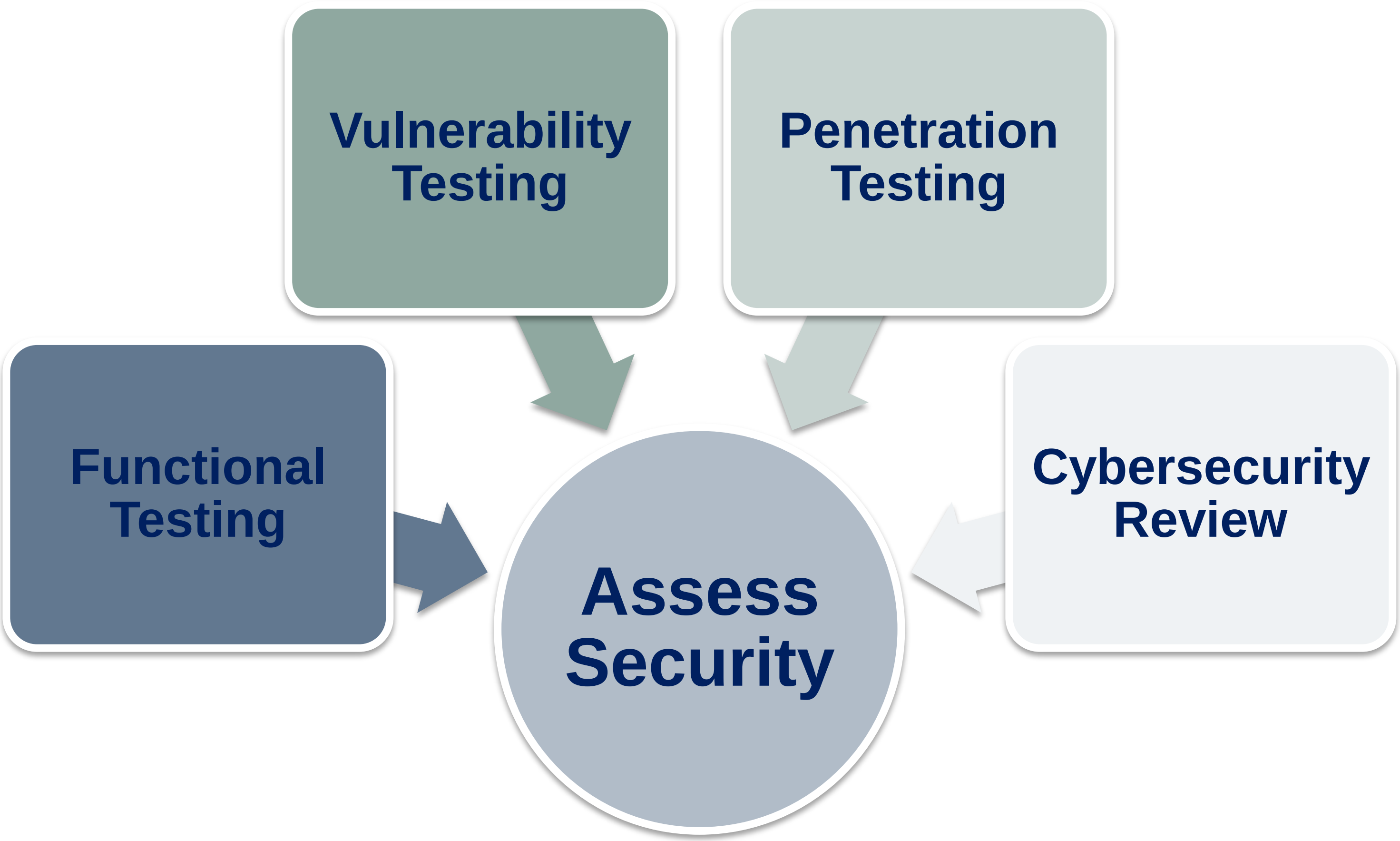
Assess Security

Assess Security:

- Perform Functional Testing
- Perform Vulnerability Testing
- Perform Penetration Testing
- Perform Final Cybersecurity Review



Assess Security



Functional testing
- verify correct implementation of security measures

Correctness

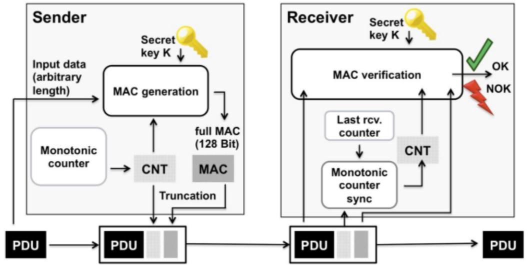
- Positive testing of Algorithms, Protocols, Key Management
- AES, TLS, SecOC, etc

Robustness

- Negative testing, security measures fail correctly
- Abuse the security measures

Performance

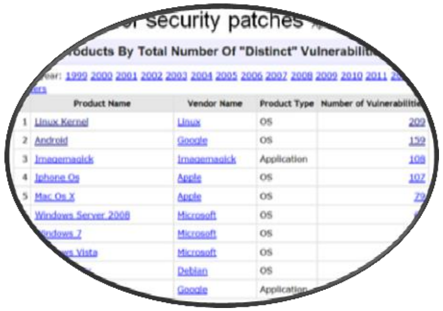
- Execution time, memory usage



Vulnerability and Fuzz testing
- search for known and unknown vulnerabilities

Known vulnerabilites

- Scan for open ports, services exposed.
- Verify known vulnerabilities patched
- Software Composition analysis



security patches

oducts By Total Number Of "Distinct" Vulnerabiliti

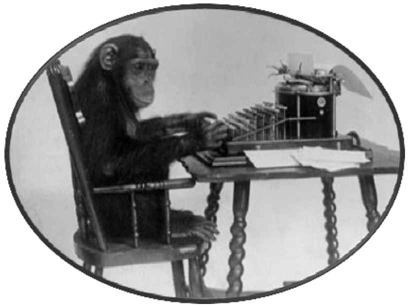
ear: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 20

ers

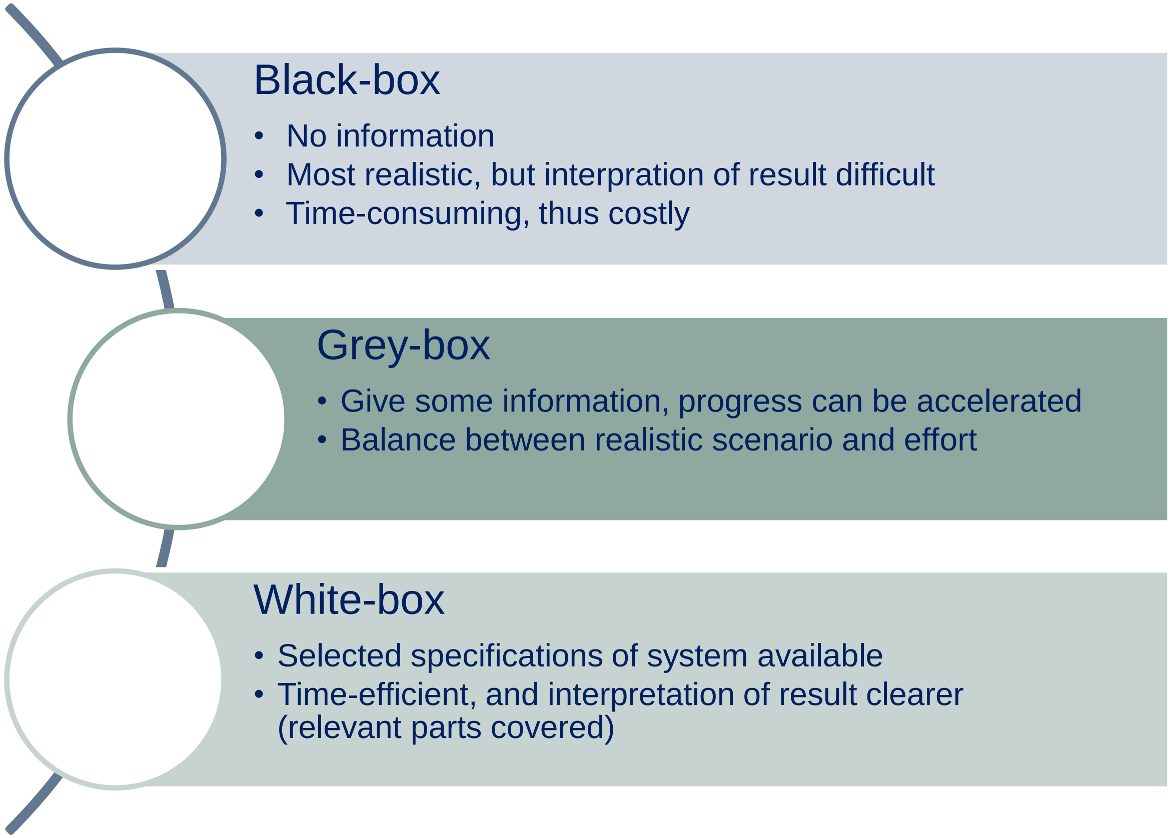
	Product Name	Vendor Name	Product Type	Number of Vulnerabilitie
1	Linux Kernel	Linux	OS	209
2	Android	Google	OS	159
3	Imagemagick	Imagemagick	Application	108
4	Iphone Os	Apple	OS	107
5	Mac Os X	Apple	OS	79
	Windows Server 2008	Microsoft	OS	
	indows 7	Microsoft	OS	
	ws Vista	Microsoft	OS	
		Debian	OS	
		Google	Application	

Unknown vulnerabilites

- Fuzzing, expose interfaces to unexpected input
- Generation-based, protocol aware
- Robustness



Penetration testing
- authorized, simulated attacks on the system



Black-box

- No information
- Most realistic, but interpration of result difficult
- Time-consuming, thus costly

Grey-box

- Give some information, progress can be accelerated
- Balance between realistic scenario and effort

White-box

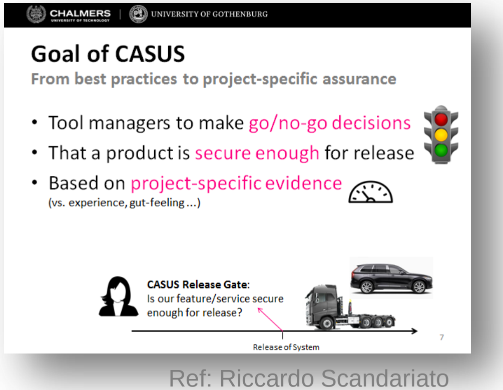
- Selected specifications of system available
- Time-efficient, and interpretation of result clearer (relevant parts covered)

Final Cybersecurity Review

- is the system secure enough for release?

- Recommended in ISO-SAE 21434 and SAE J3061 (process frameworks)
- Review threats, review test results
- But how to argue reasonable effort spent to secure vehicle?

PhD position in research project CASUS



CHALMERS UNIVERSITY OF TECHNOLOGY | UNIVERSITY OF GOTHENBURG

Goal of CASUS

From best practices to project-specific assurance

- Tool managers to make go/no-go decisions
- That a product is secure enough for release
- Based on project-specific evidence (vs. experience, gut-feeling ...)

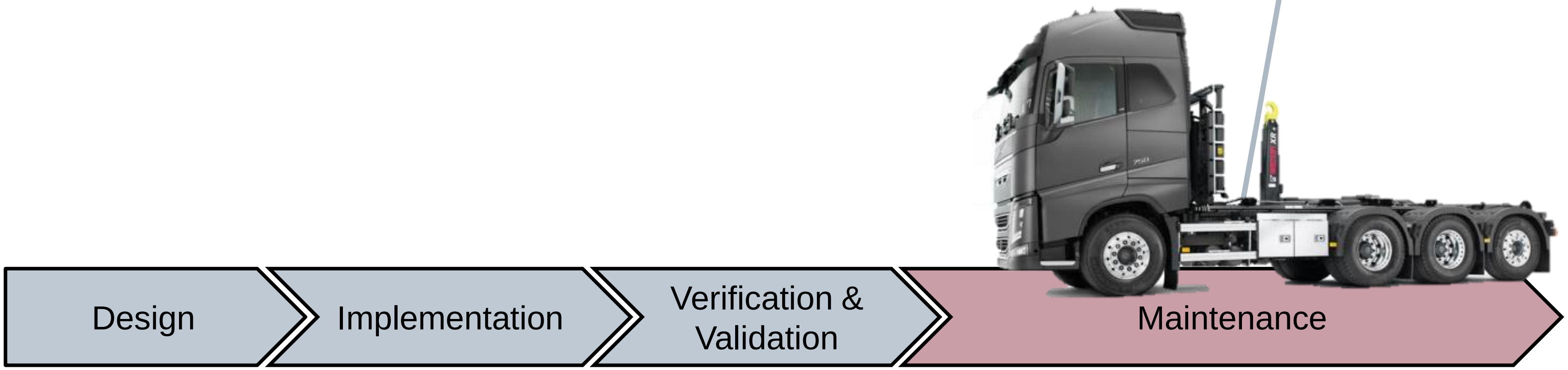
CASUS Release Gate: Is our feature/service secure enough for release?

Ref: Riccardo Scandariato

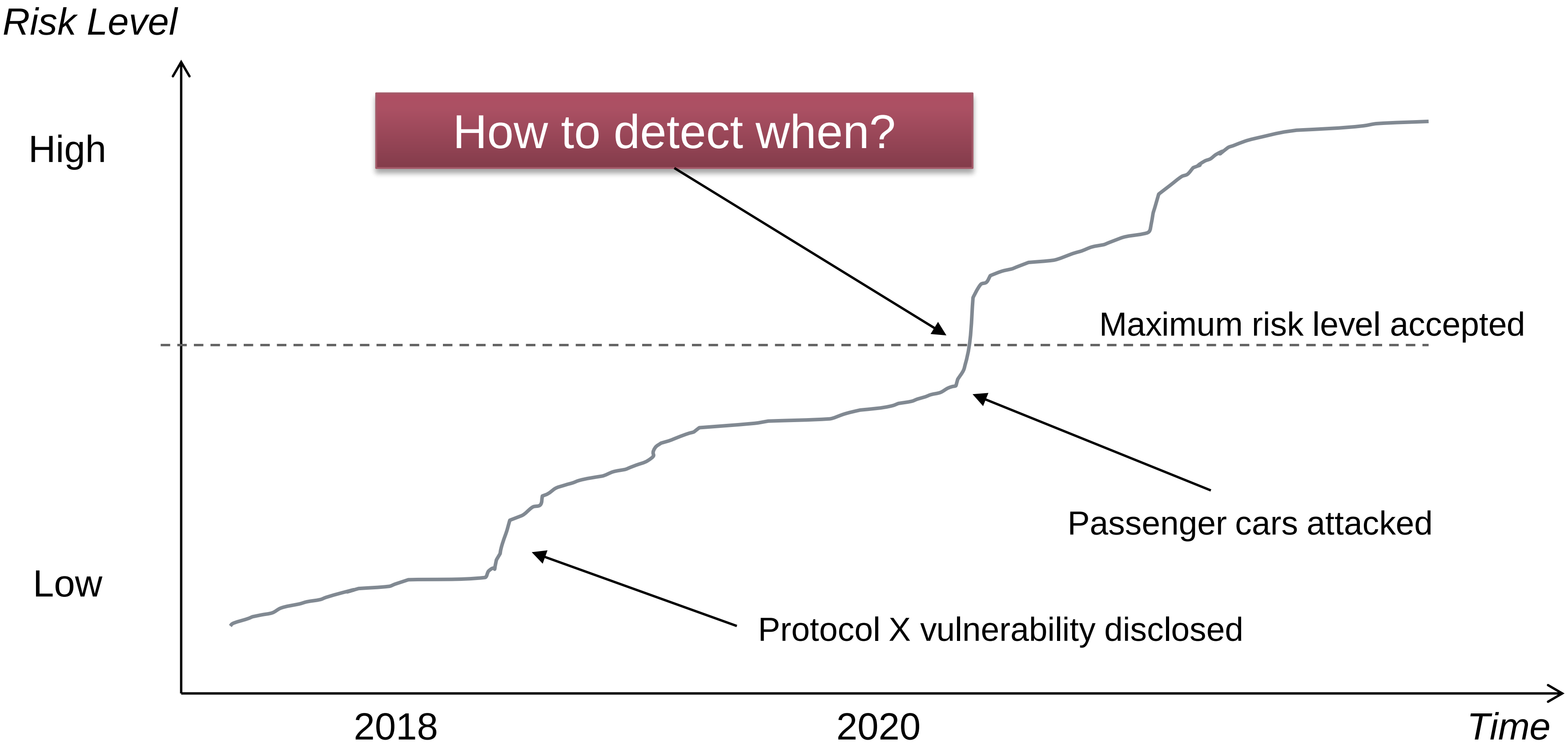
Maintain Security

Maintain Security:

- Threat Intelligence
- Vulnerability and Patch management
- Incident Response



Remember?
- Threat and vulnerabilities change over time



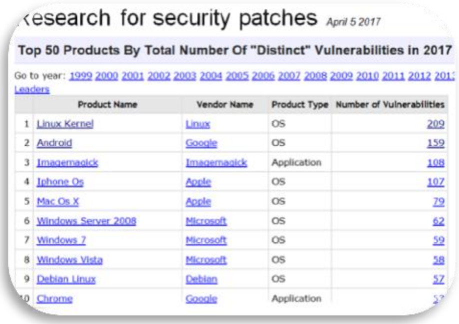
Vulnerability Management

Mainly related to mitigating from **known software vulnerabilities**.

The process is **proactive**, defend against known vulnerabilities **before attacks** take place.

Common types:

- Buffer overflow, over-reads
- Lack of input validation
- Code injection

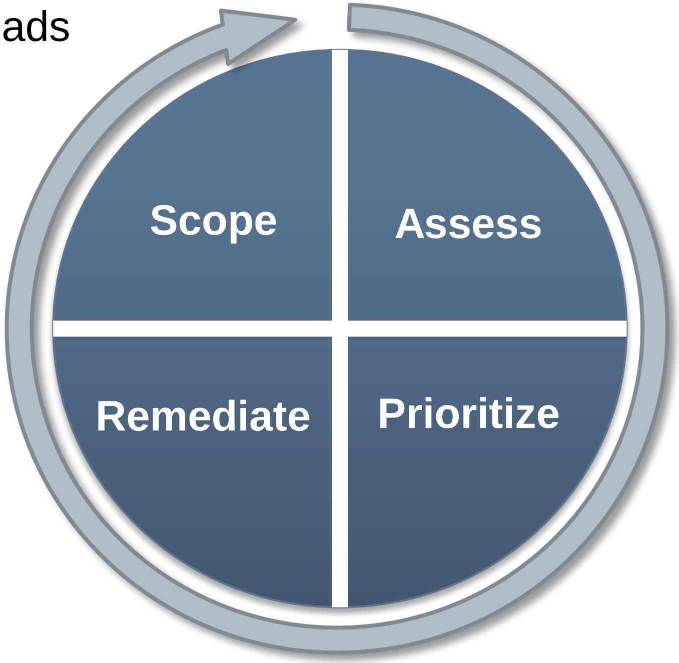


Research for security patches *April 5 2017*

Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2017

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 201
Leaders

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Linux Kernel	Linux	OS	209
2	Android	Google	OS	159
3	Imagemagick	Imagemagick	Application	108
4	Iphone Os	Apple	OS	107
5	Mac Os X	Apple	OS	79
6	Windows Server 2008	Microsoft	OS	62
7	Windows 7	Microsoft	OS	59
8	Windows Vista	Microsoft	OS	58
9	Debian Linux	Debian	OS	57
10	Chrome	Google	Application	52



Scope

- Asset inventory
- Schedule

Assess

- Vulnerabilities feeds
- Scan / research assets
- Determine relevance

Prioritize

- Assess risk
- Plan actions

Remediate

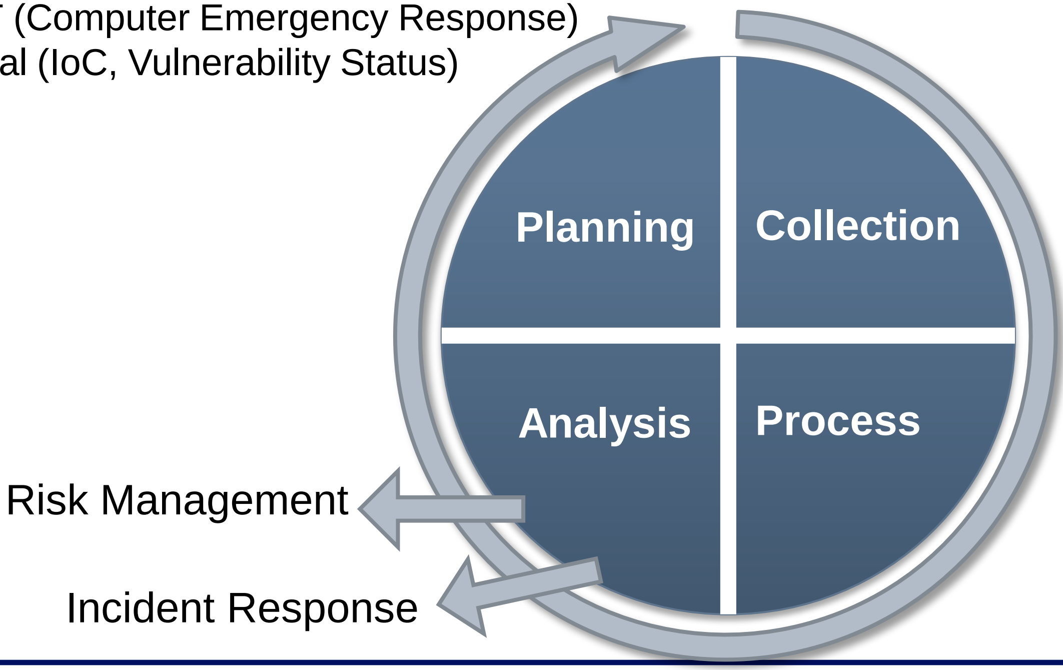
- Deploy security updates
- Report progress

Threat intelligence

Threat Intelligence organize, analyze and refine information about **potential or current attacks**

Type of intelligence sources

- Industry ISAC i.e. Auto ISAC
- Publicly Available sources (OSINT)
- Commercial sources (e.g. Recorded Future)
- CERT (Computer Emergency Response)
- Internal (IoC, Vulnerability Status)



Planning

- Identify attack vectors
- Identify indicators of compromise (IoCs)
- What data to collect

Collection

- Real time evidence (IoC)
- Vulnerability status
- External threat feeds (OSINT, Auto-ISACs)

Process

- Aggregation
- Filter
- Specific internal data
- Generic external data

Analysis

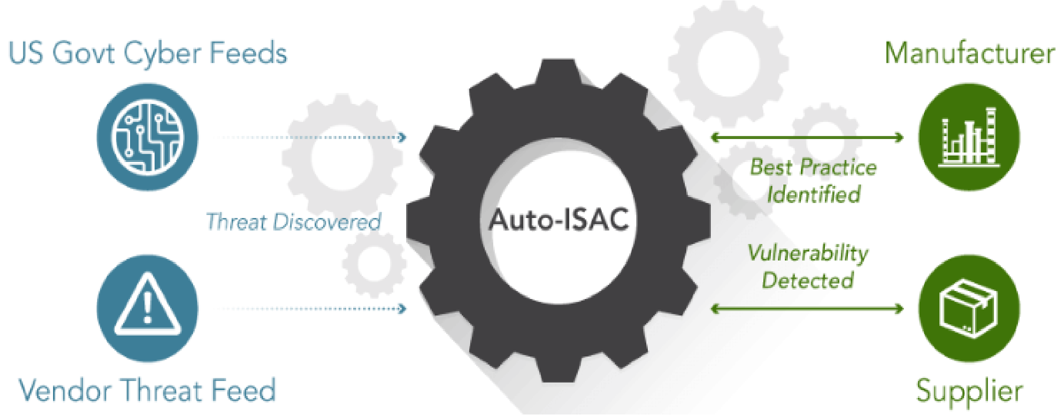
Threat and Risk analysis
Intelligence Reporting

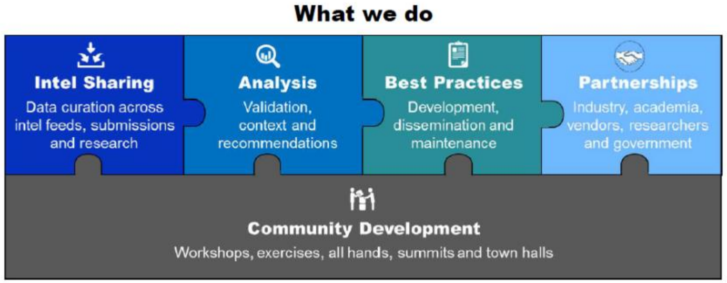
Threat Intelligence example

- Automotive Industry Information Sharing

AUTO-ISAC
Automotive Information Sharing and Analysis Center

To promote collaborative cyber security efforts, the auto industry created the Automotive Information Sharing and Analysis Center (Auto-ISAC) in July 2015.




What we do

Intel Sharing
Data curation across intel feeds, submissions and research

Analysis
Validation, context and recommendations

Best Practices
Development, dissemination and maintenance

Partnerships
Industry, academia, vendors, researchers and government

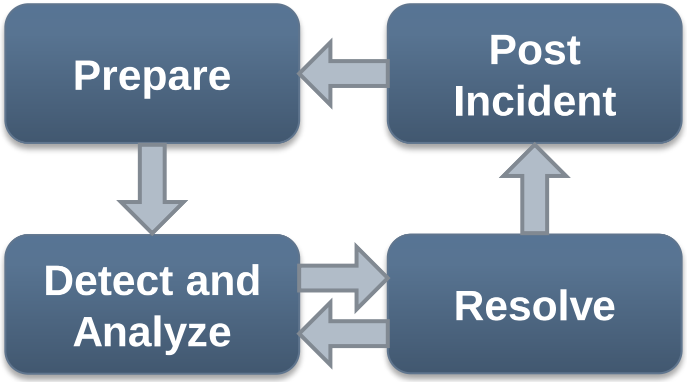
Community Development
Workshops, exercises, all hands, summits and town halls

Ref: Auto-ISAC

Incident Response

Incident Response aims to “shorten the window” from incident detection to applied resolution

Incident response is highly interacting with Threat Intelligence



Prepare

- Create plan
- Identify contact persons
- Train and exercise
- Identify indicators/channels

Detect and Analyze

- Incident channels
- Triage (evaluate and confirm)

Resolve

- Containment
- Develop mitigation
- Recovery

Post-incident

Feedback and Reporting

The bigger picture
- Holistic Cybersecurity Management

Leadership Priority

Awareness & Culture

Policy & Governance

Risk Based Approach

Security by Design

Continuous Risk Management

Incident & Crisis Management

External Collaboration

Regulation & Compliance

Questions