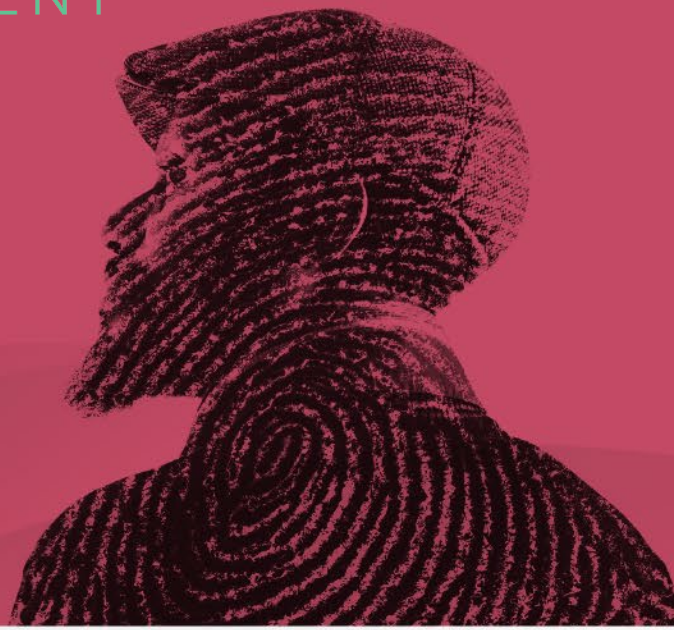
RSAC Sandbox

RSAConference2020

HUMAN ELEMENT



SESSION ID: SBX1-R7

Supply Chain Security in the Software Era

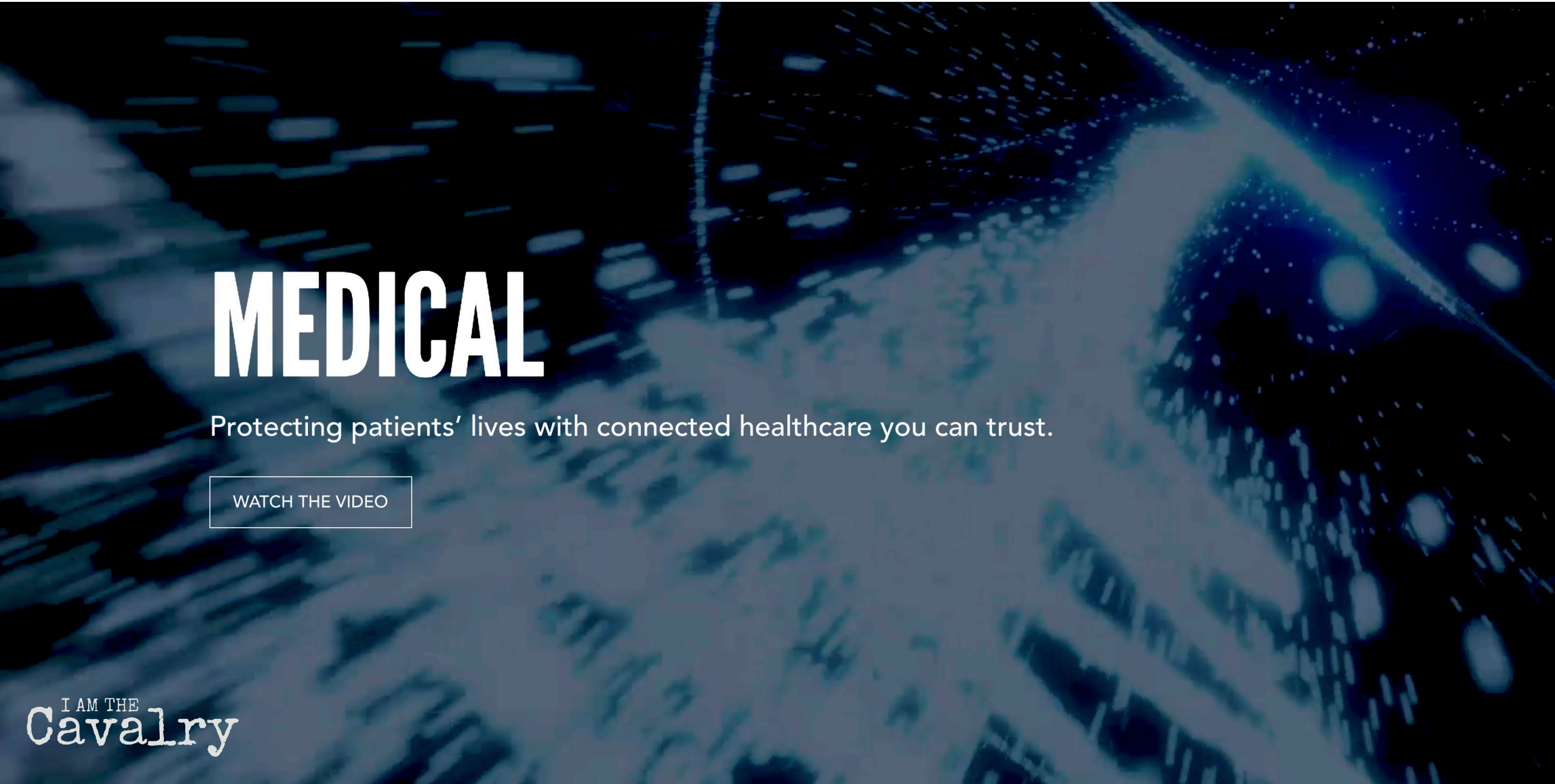
Beau Woods

Cyber Safety Advocate
I Am The Cavalry
@beauwoods


I AM THE
Cavalry

Pentest a MRI – What could go wrong?


I AM THE
Cavalry


MEDICAL
Protecting patients' lives with connected healthcare you can trust.
WATCH THE VIDEO
I AM THE
Cavalry


WIND
WHEN IT MATTERS, IT RUNS ON WIND RIVER.
Contact Us
Search
Menu
VxWorks
WATCH THE VIDEO
I AM THE
Cavalry

URGENT/11


I AM THE
Cavalry

Green Hills Platform for Avionics

- The proven provider
- Absolute reliability
- Proven in safety-critical systems
- In-house certification expertise
- Proven pedigree
- Complete safety-critical line

Green Hills Software products are the leading choice for the avionics industry. The company's full line of safety and security critical products are being used in almost every current and next-generation aircraft, including: the Airbus A380, Boeing 777, Boeing 787, Lockheed Martin F-35 Joint Strike Fighter, F/A-22, Eurofighter Typhoon, Lockheed Martin F-16, Bell Helicopter UH-1Y and AH-1Z helicopters (on the Northrop Grumman mission computers), the Textron RQ-7B Shadow UAS (on the Rockwell-Collins mission computer), and more.

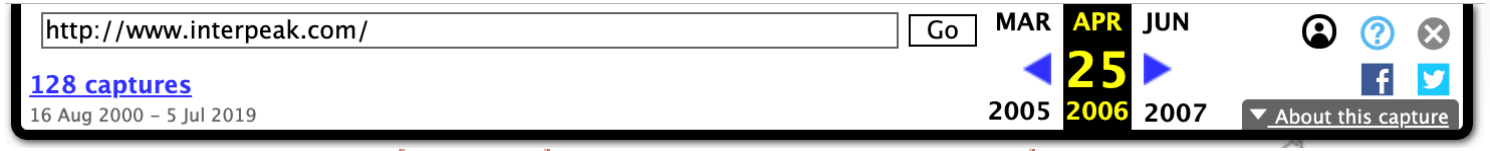
The proven provider of safety & security solutions

Green Hills Platform for Avionics combines the INTEGRITY-178 RTOS with support for aviation industry standard ARINC 653-1 application software interface, and the documentation required for FAA safety certification. INTEGRITY-178 has proven iteself many times by being certified to this top safety-critical level in multiple applications. It is now the leading RTOS choice for the avionics industry for current and next generation aircraft.

The list of avionics suppliers that have selected Green Hills Software solutions is the who's who for this industry and includes: BAE Systems, Boeing, CMC Electronics, EADS, General Electric, Honeywell, Lockheed Martin, Northrop

URGENT/11


interpeak
secure networking software



interpeak

secure networking software

- > INTEGRITY
- > ITRON
- > Linux/MontaVista
- > MQX
- > Nucleus
- > OSE, OSEck
- > ThreadX
- > velOSity
- > VxWorks

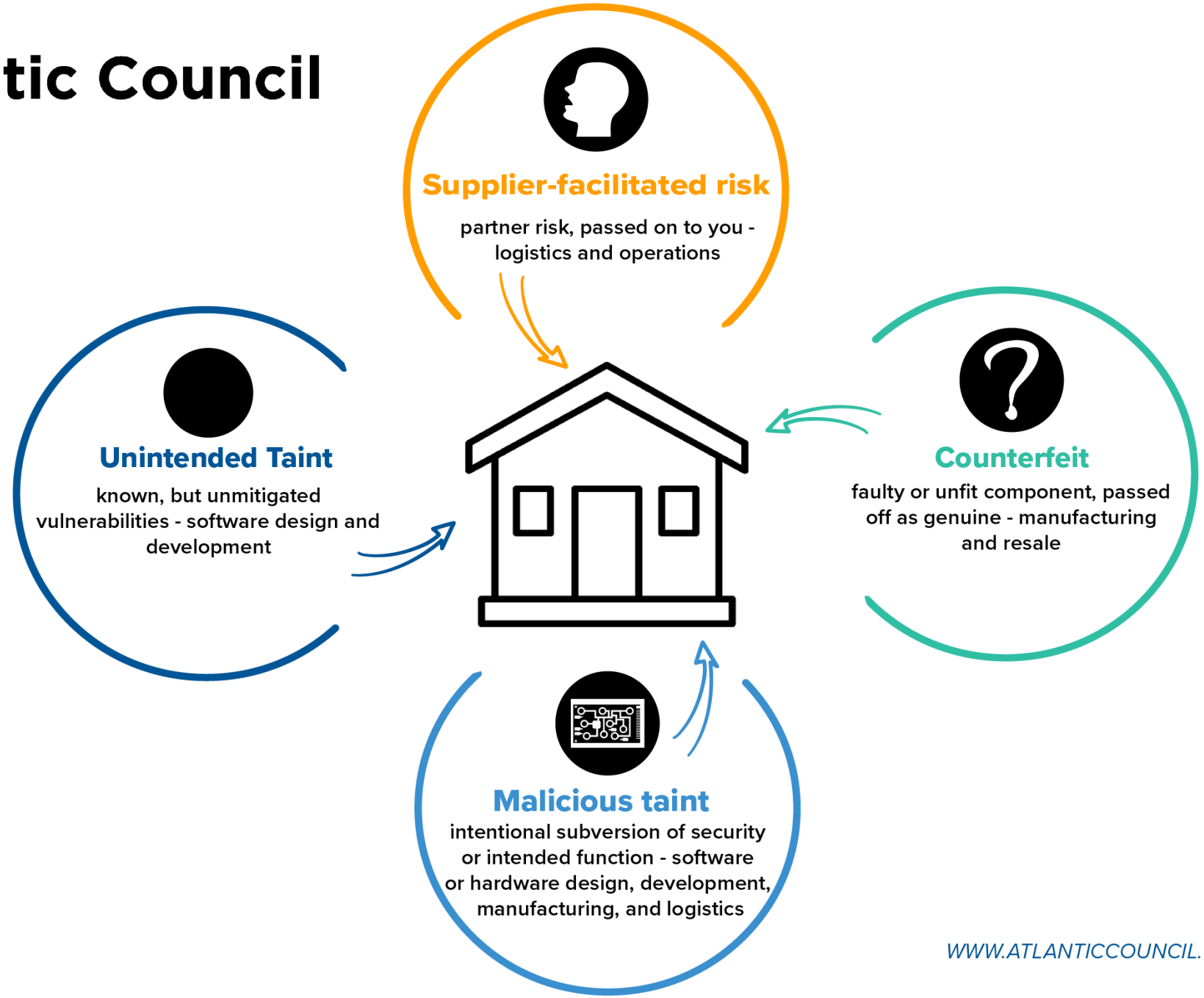

FDA


U.S. DEPARTMENT OF HOMELAND SECURITY


[Everyone disliked that.]
I AM THE
Cavalry

Why is this the case?

Atlantic Council



Atlantic Council

Unintended Taint:

DESCRIPTION

Authorized, authentic, validated components with publicly known software vulnerabilities

ADVERSARY

All adversaries

EXAMPLE

Equifax was breached through a known flaw in Apache Struts

Supplier-facilitated risk

DESCRIPTION

Operational security or reliability risks due to partner security issues

ADVERSARY

Criminals and nation states

EXAMPLE

Criminals breached Target by coming through a maintenance supplier

Counterfeit

DESCRIPTION

Inauthentic and/or unvalidated products or components, typically used to lower costs, and security or operating model subversion is often unintended

ADVERSARY

Typically criminals

EXAMPLE

Pirated software often contains malware

Malicious taint

DESCRIPTION

Authorized, authentic products, containing unvalidated components that can subvert the security or operating model

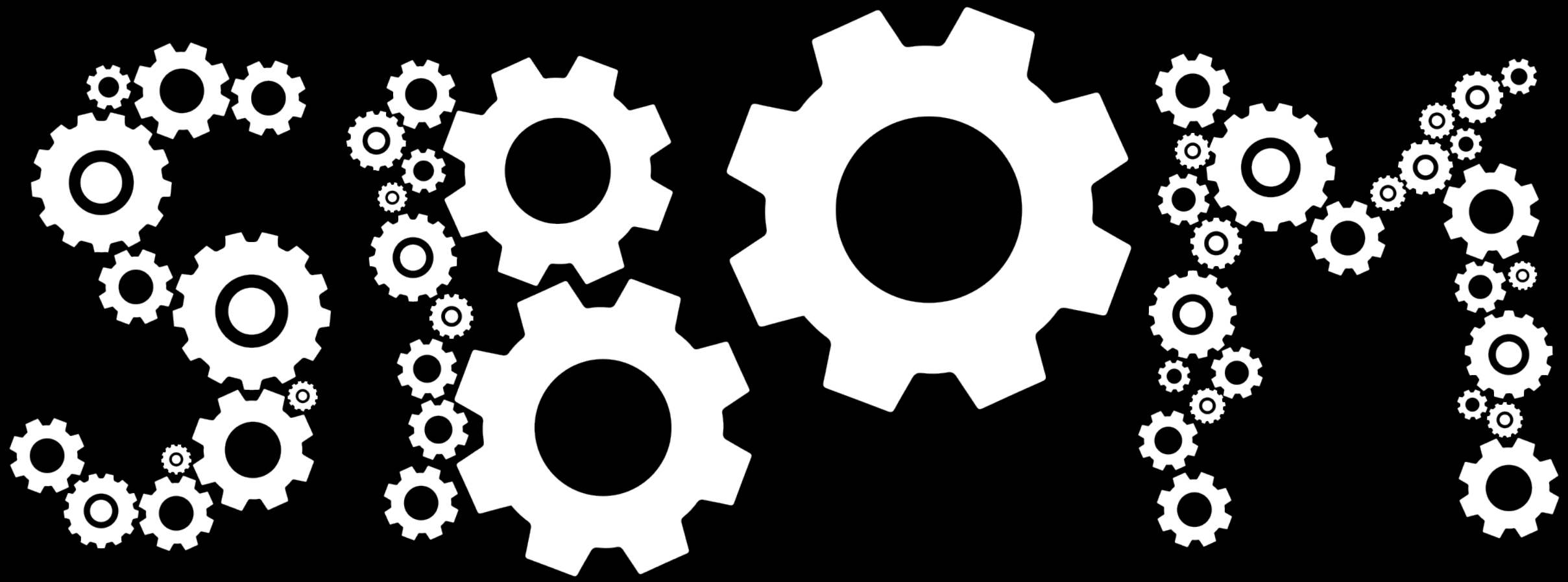
ADVERSARY

Typically nation states

EXAMPLE

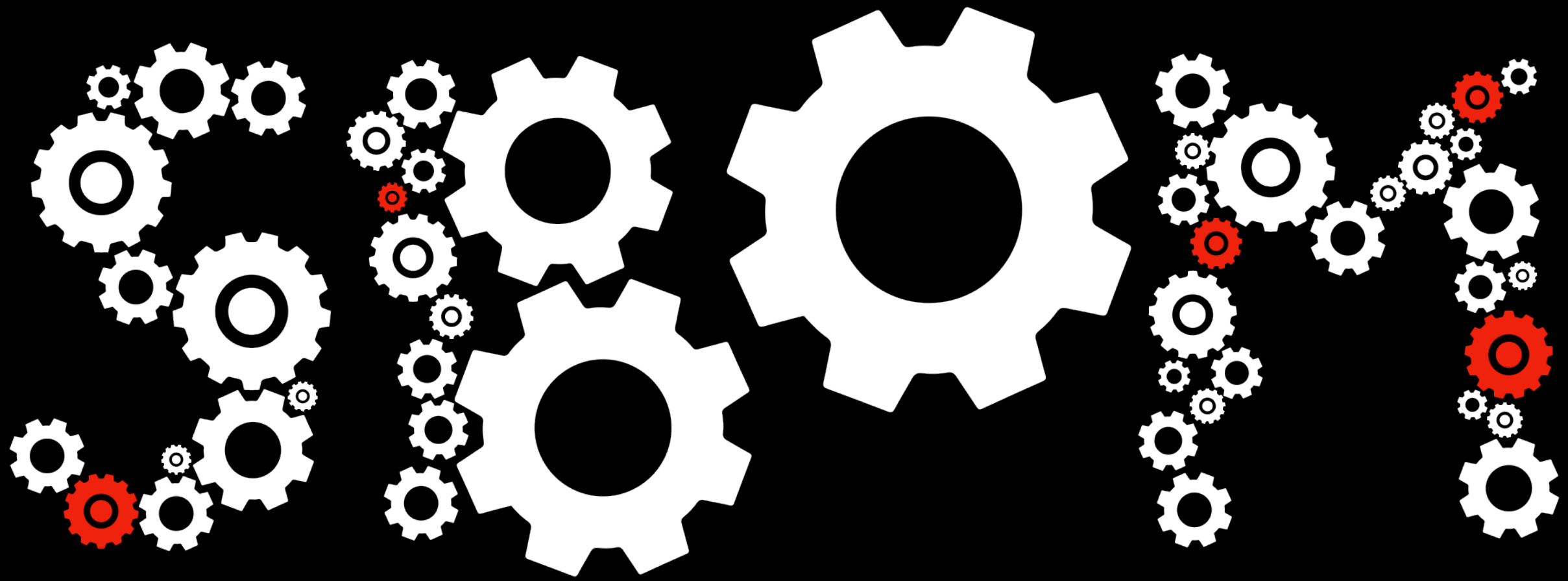
Havex used compromised upgrades on legitimate manufacturer site

What can we do about it?



Software Bill of Materials

I AM THE Cavalry



Software Bill of Materials

I AM THE Cavalry

Suppliers to the new BMW 5 Series

Image source: BMW AG

ROOF MODULE WITH GESTURE RECOGNITION SYSTEM
DELPHI

HARMAN KARDON SOUND SYSTEM
HARMAN/BECKER

PYROTECHNICAL SAFETY SWITCH
AUTOLIV

NEXT GEN CARBON CANISTER
KAUTEX TEXTRON

COMPRESSOR WITH CLUTCH
DENSO

CYLINDER HEAD GASKET
DANA

CLASSICAL SUNROOF
WEBASTO

OIL FILTER MODULE
UFI FILTERS

SMART OPENER
BROSE

MECHANICAL PUMP
SALERI

TRANSMISSION OIL COOLER
MAHLE

SOUND DEADENER PACKAGE
FAIST CHEMTEC

THERMO MANAGEMENT MODULES
SCHAEFFLER

CO-EXTRUDED ARMREST SEAL [TIER 2]
COBA PLASTICS

FRONT ARMREST DAMPERS
CULTRARO AUTOMAZIONE ENGINEERING

DAMPER FORKS
HIRSCHVOGEL UMFORMTECHNIK

PNEUMATIC LUMBAR SUPPORT
KONGSBERG AUTOMOTIVE

SEALING SIDE PANEL
RÖCHLING AUTOMOTIVE

FRONT & REAR WIPER SYSTEM
VALEO

LASER WELDED BLANK
VOESTALPINE

TRUNK LIGHT STRIP
GRUPO ANTOLIN

ROOF MOULDINGS
SMIA

EXHAUST TRIM
TAJCO A/S

BACKLITE
CARLEX

DOUBLE NUT
AMTEK TEKFOR

VALVE COTTERS
FEDERAL-MOGUL

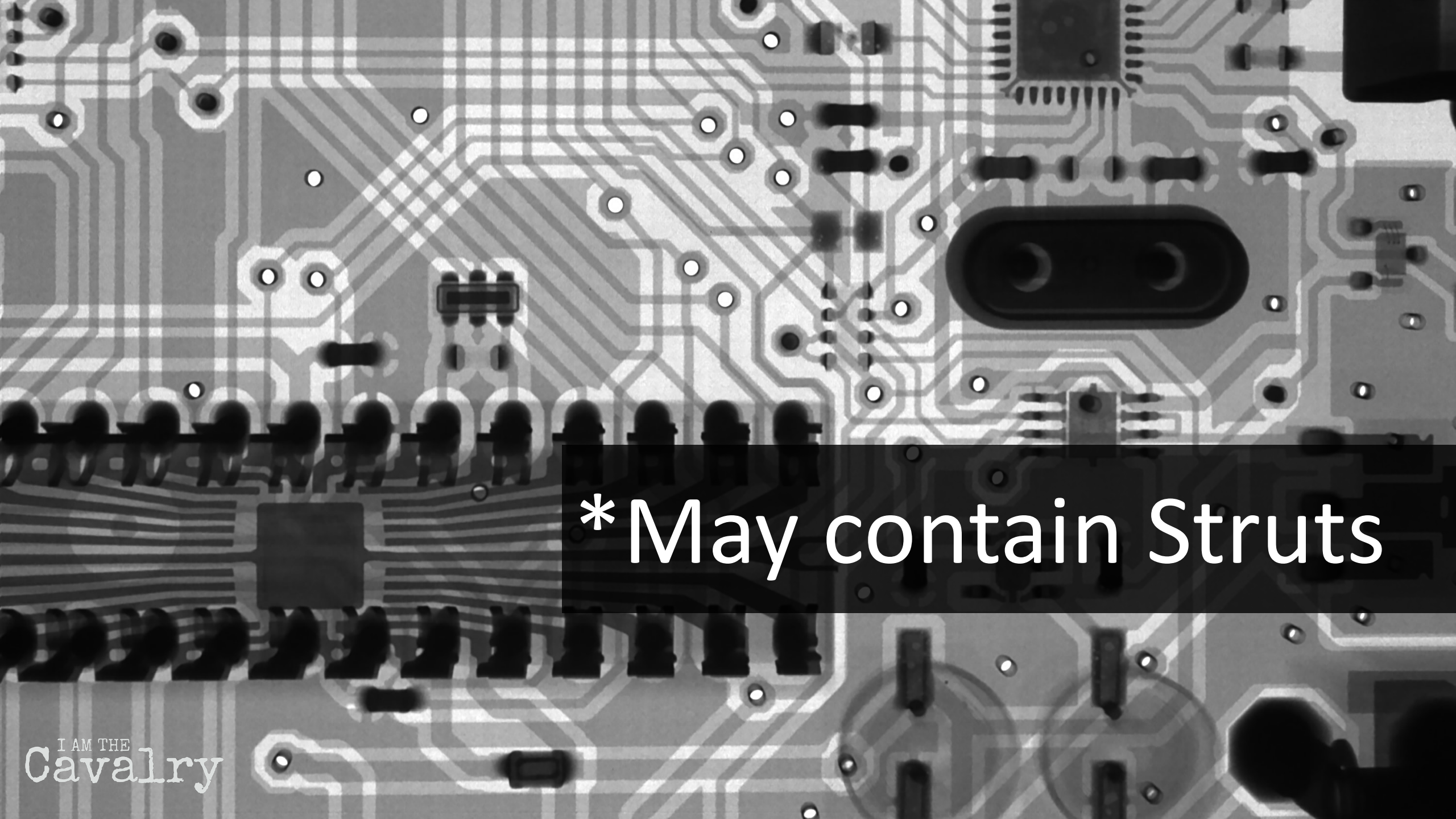
FRONT & REAR SEATBELTS
AUTOLIV

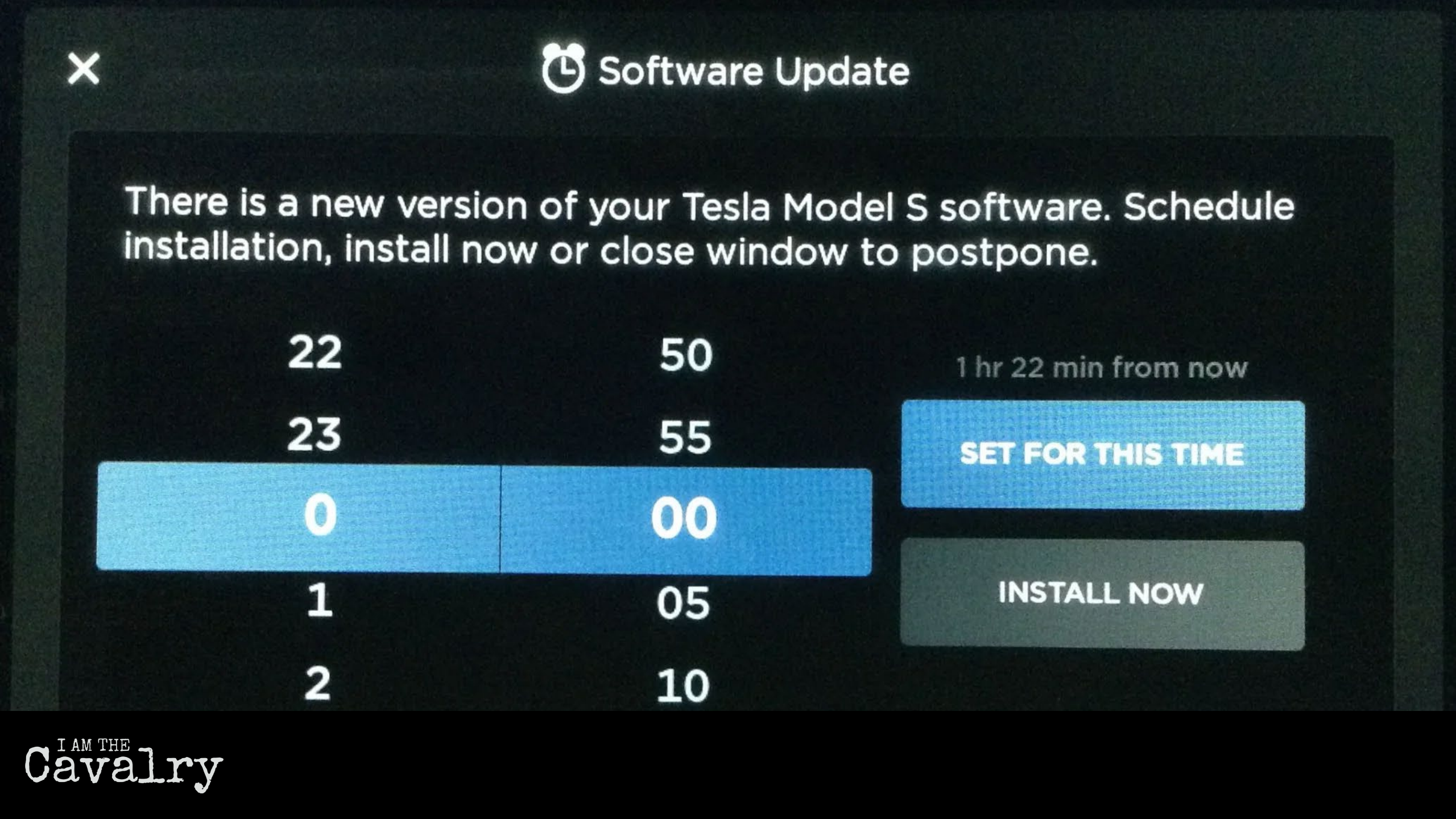
TRAILER COUPLING SWITCH
MARQUARDT

STORAGE COMPARTMENT
MEGATECH INDUSTRIES

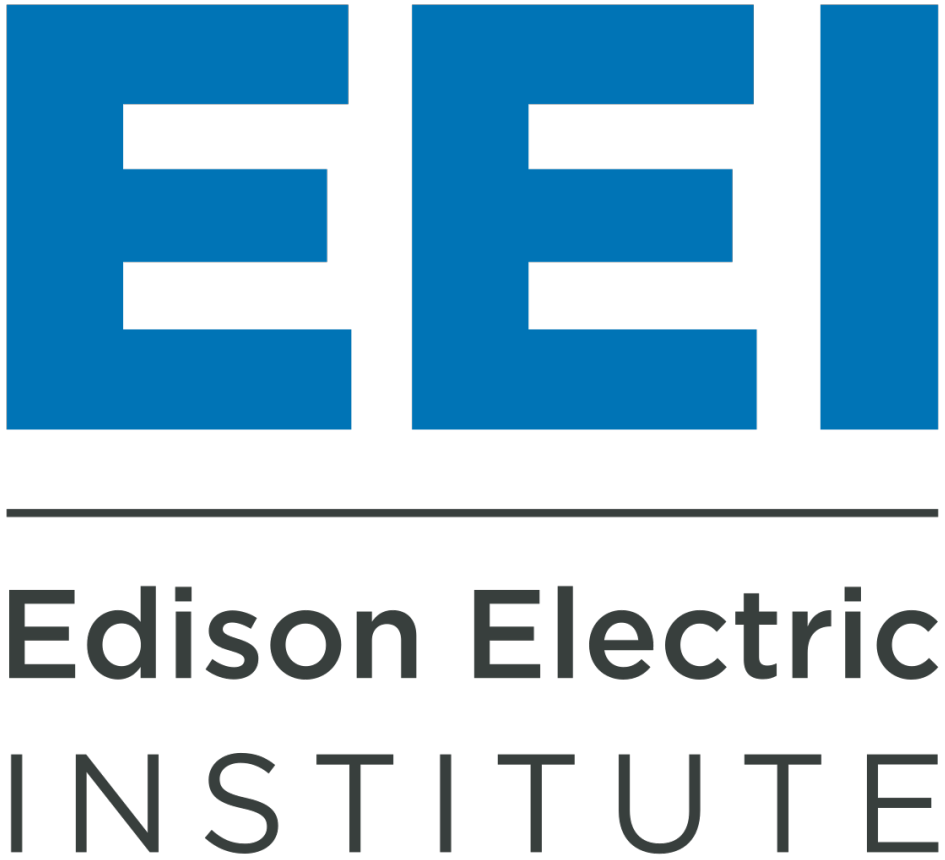
FORGING WHEELS
SUPERALLOY INDUSTRIAL CO. LTD

I AM THE Cavalry


*May contain Struts
I AM THE
Cavalry



Model Procurement Language



I AM THE Cavalry


New Liability Models
I AM THE
Cavalry

What to do next

RSAC Sandbox

- Visit the Supply Chain Sandbox!
- Talk to your procurement officer
  - What do they need to make it easy to get you what you need?
- Ask sellers if they provide SBOMs
  - If they can't tell you what is in their product, your costs to protect your environment go up.
- Consider accountability and responsibility
  - Who does what when, and what happens if they don't?

Resources

RSAC Sandbox

- Supply Chain in the Software Era (Issue Brief)
  - https://atlanticcouncil.org/in-depth-research-reports/issue-brief/supply-chain-in-the-software-era/
- NTIA SBOM Project
  - https://ntia.gov/sbom
- Supply Chain Sandbox materials
  - https://supplychainsandbox.org

One more thing…

#WeHeartHackers

The #WeHeartHackers initiative

#WeHeartHackers connects independent security researchers with industry, to collaborate, assess, and address potential issues that could cause harm to human life, public safety, and public trust.

Developed by industry and the security research community with support from federal government partners, the **#WeHeartHackers** initiative acts as a public private partnership that accelerates security maturity across and within critical infrastructure sectors.

In 2019, **#WeHeartHackers** saw 10 medical device makers pledge high-trust collaboration with the security researcher community. These industry partners provided security researchers with more than 30 medical devices, learning adversary tactics and improved security approaches. Among other output, research from this event contributed to FDA and DHS communications about critical infrastructure, coordinated first with the affected companies.

The **#WeHeartHackers** initiative is expanding to other sectors in 2020 with the help of DHS, sector specific agencies, such as the FDA, industry partners and other security researcher-led non-profit organizations to galvanize support from critical infrastructure manufacturers. We welcome those who support good faith cybersecurity research to ensure we are ***safer, sooner, together.***

Tweet #wehearthackers

Join #WeHeartHackers

Healthcare | Aerospace | Industrial Controls Systems

I AM THE Cavalry

Thermo Fisher Scientific

Medtronic

Siemens Healthineers

Philips Health

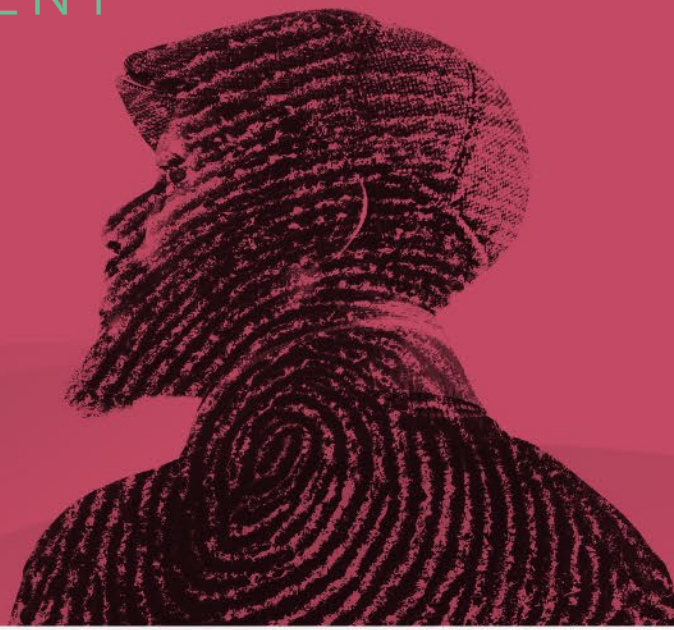
ResMed

ICU Medical

RSAC Sandbox

RSAConference2020

HUMAN ELEMENT



SESSION ID: SBX1-R7

Supply Chain Security in the Software Era

Beau Woods

Cyber Safety Advocate
I Am The Cavalry
@beauwoods