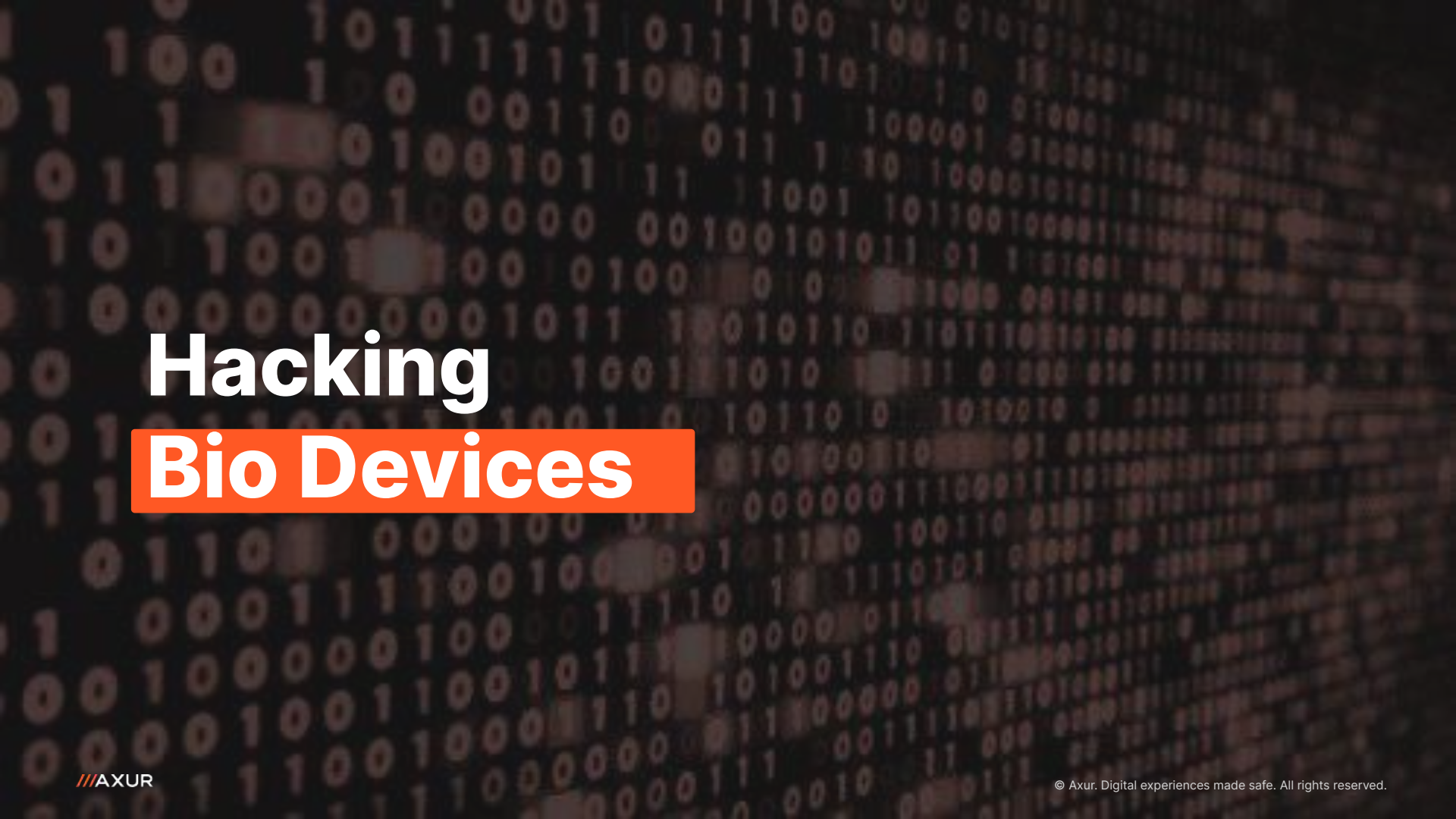


///AXUR

Thiago Bordini

Head of Cyber Threat Intelligence at Axur

Over 20 years of experience in the field of cybernetic intelligence, acting with analysis and threat and fraud prevention and disseminating educative content about the topic for professionals and companies.

Technical coordinator for Post Gradiation on Cyber Threat Intelligence and a professor of post-graduate courses of Cyber Security and Computational Forensics at IDESP.

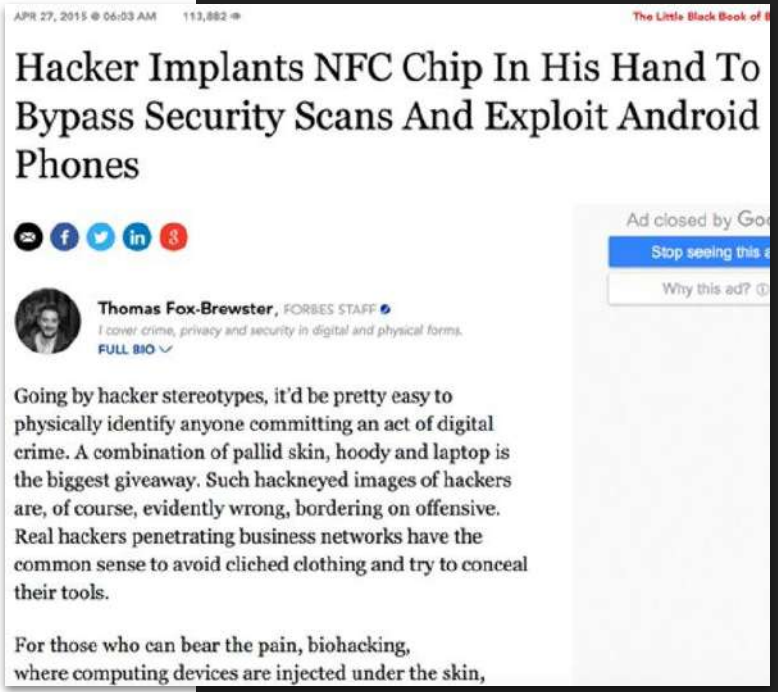
Spokesman in many national and international events, such as YSTS, EkoParty, H2HC, CIAB, Security BSides, SANS, HTCIA, CoronaCon and more.

Member of HTCIA (High Technology Crime Investigation Association). Member of Security BSides SP Organization. Mentor for Cyber Security Girls.

linkedin.com/in/thiagobordini/

///AXUR

Fiction or reality?



APR 27, 2015 @ 06:03 AM 113,882

The Little Black Book of

Hacker Implants NFC Chip In His Hand To Bypass Security Scans And Exploit Android Phones

Ad closed by Goo

Stop seeing this

Why this ad?

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms.

FULL BIO

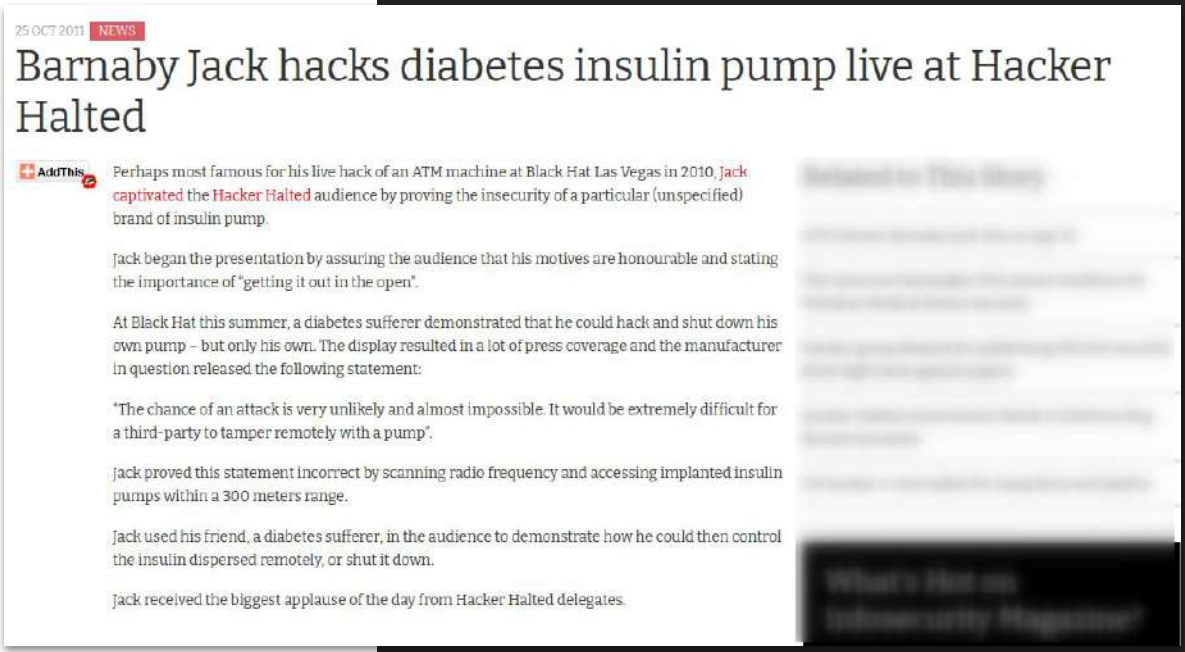
Going by hacker stereotypes, it'd be pretty easy to physically identify anyone committing an act of digital crime. A combination of pallid skin, hoody and laptop is the biggest giveaway. Such hackneyed images of hackers are, of course, evidently wrong, bordering on offensive. Real hackers penetrating business networks have the common sense to avoid cliched clothing and try to conceal their tools.

For those who can bear the pain, biohacking, where computing devices are injected under the skin,

SOURCE: FORBES

///AXUR

Fiction or reality?



25 OCT 2011 NEWS

Barnaby Jack hacks diabetes insulin pump live at Hacker Halted

Perhaps most famous for his live hack of an ATM machine at Black Hat Las Vegas in 2010, Jack captivated the Hacker Halted audience by proving the insecurity of a particular (unspecified) brand of insulin pump.

Jack began the presentation by assuring the audience that his motives are honourable and stating the importance of "getting it out in the open".

At Black Hat this summer, a diabetes sufferer demonstrated that he could hack and shut down his own pump – but only his own. The display resulted in a lot of press coverage and the manufacturer in question released the following statement:

"The chance of an attack is very unlikely and almost impossible. It would be extremely difficult for a third-party to tamper remotely with a pump".

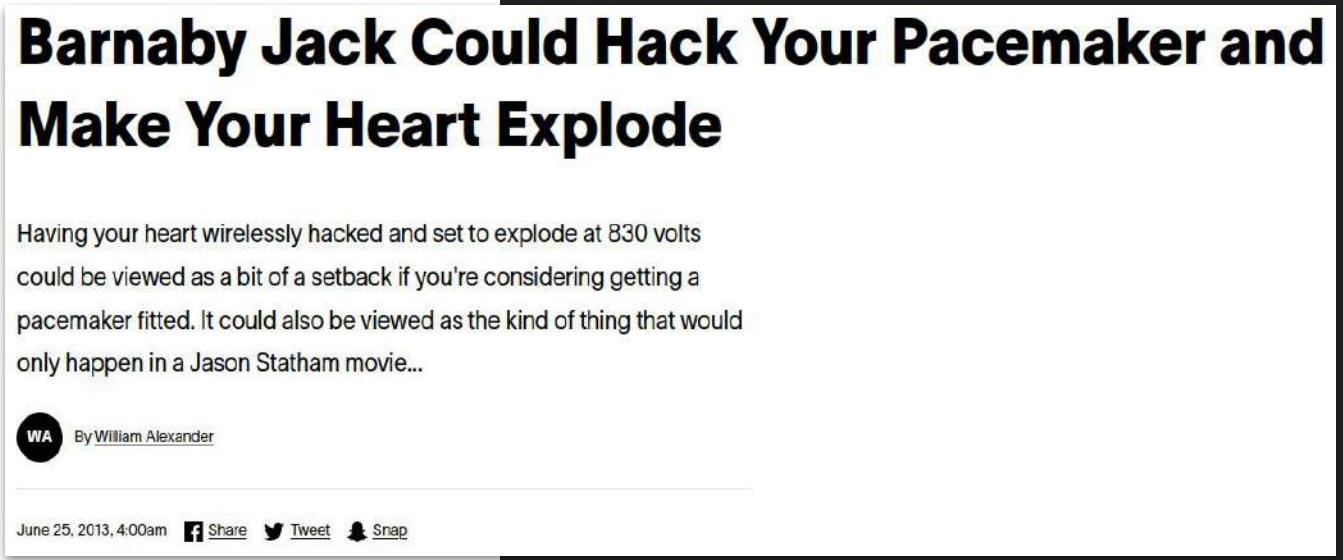
Jack proved this statement incorrect by scanning radio frequency and accessing implanted insulin pumps within a 300 meters range.

Jack used his friend, a diabetes sufferer, in the audience to demonstrate how he could then control the insulin dispersed remotely, or shut it down.

Jack received the biggest applause of the day from Hacker Halted delegates.

SOURCE: InfoSecurity

Fiction or reality?



Barnaby Jack Could Hack Your Pacemaker and Make Your Heart Explode

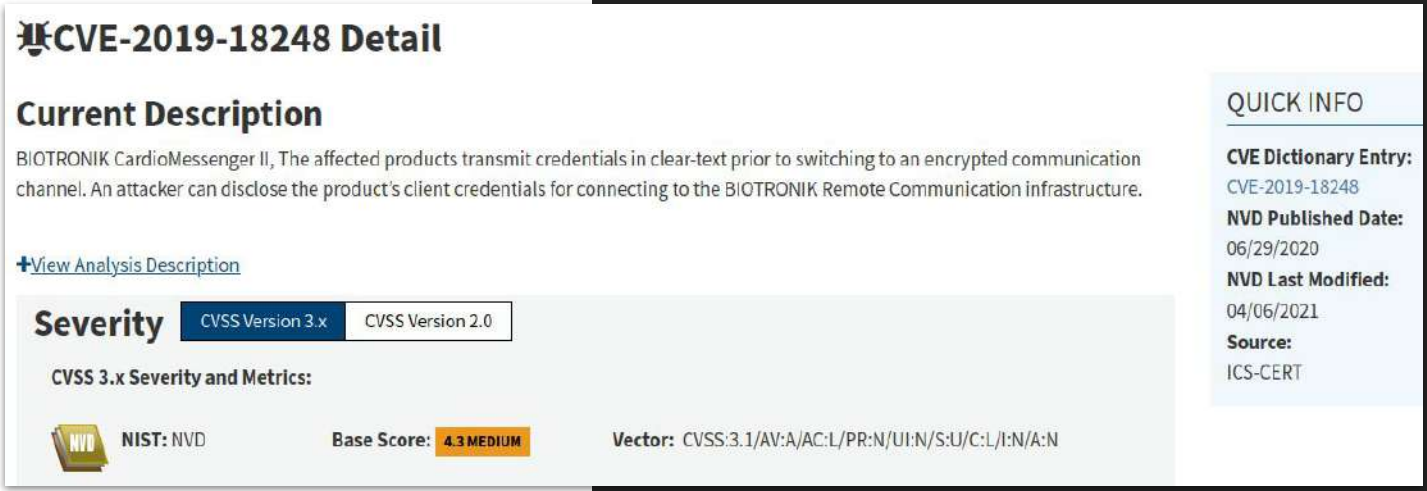
Having your heart wirelessly hacked and set to explode at 830 volts could be viewed as a bit of a setback if you're considering getting a pacemaker fitted. It could also be viewed as the kind of thing that would only happen in a Jason Statham movie...

WA By William Alexander

June 25, 2013, 4:00am Share Tweet Snap

SOURCE: VICE

Fiction or reality?



CVE-2019-18248 Detail

Current Description

BIOTRONIK CardioMessenger II, The affected products transmit credentials in clear-text prior to switching to an encrypted communication channel. An attacker can disclose the product's client credentials for connecting to the BIOTRONIK Remote Communication infrastructure.

+View Analysis Description

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

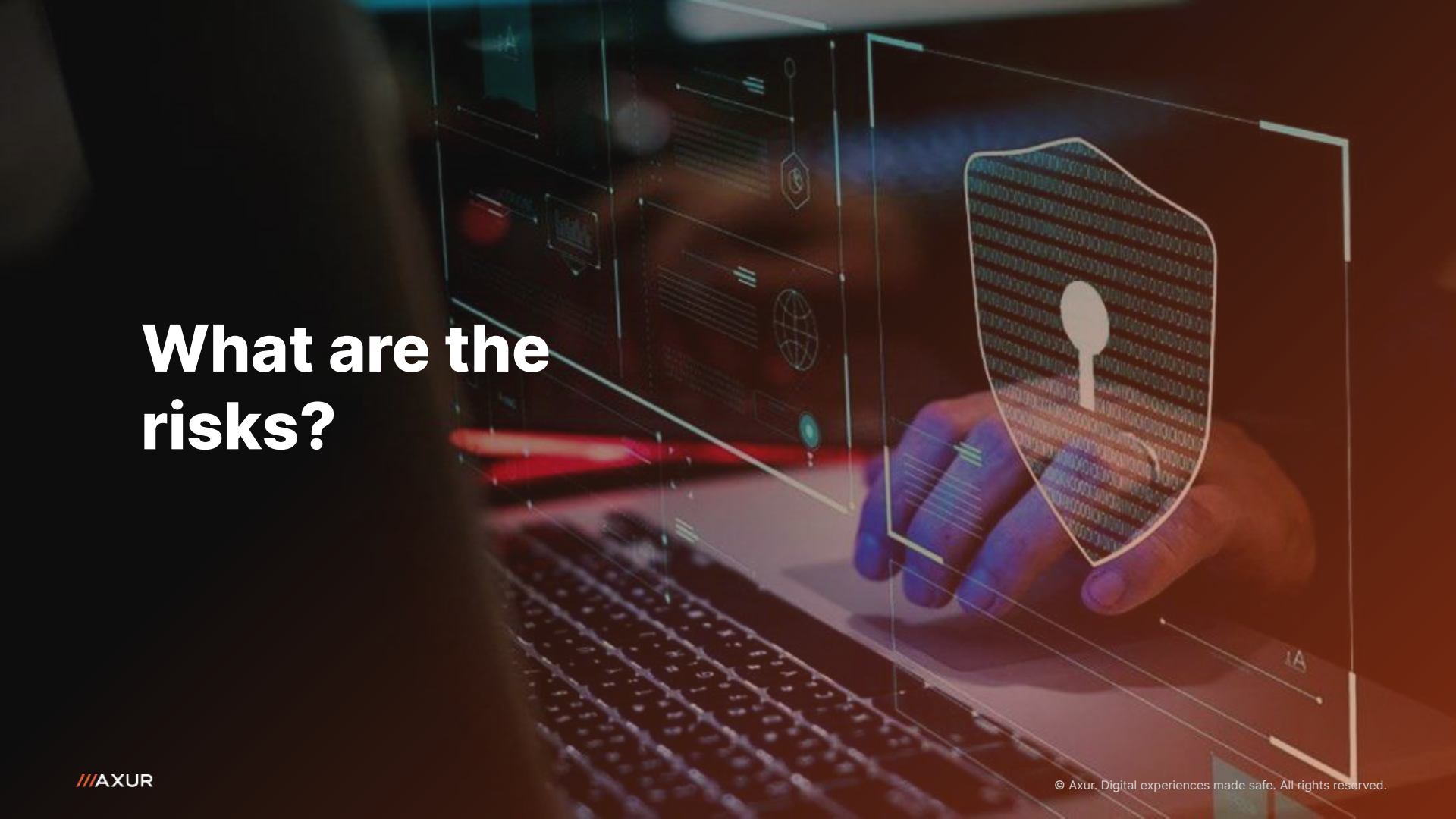
NIST: NVD **Base Score:** 4.3 MEDIUM **Vector:** CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

QUICK INFO

CVE Dictionary Entry: CVE-2019-18248
NVD Published Date: 06/29/2020
NVD Last Modified: 04/06/2021
Source: ICS-CERT

SOURCE: NVD

What are the risks?



///AXUR

Current Scenery:

- Sensitive data collection
- Exposition of health data
- Device data manipulation (rhythm, dosage, etc)
- Murder or health interference
- Use of devices as vector for an attack
- Low maturity related to the sector’s CyberSecurity

///AXUR

Bio Implants as attack vectors?

///AXUR

Attack scenery

Attack scenery

Vídeo demo

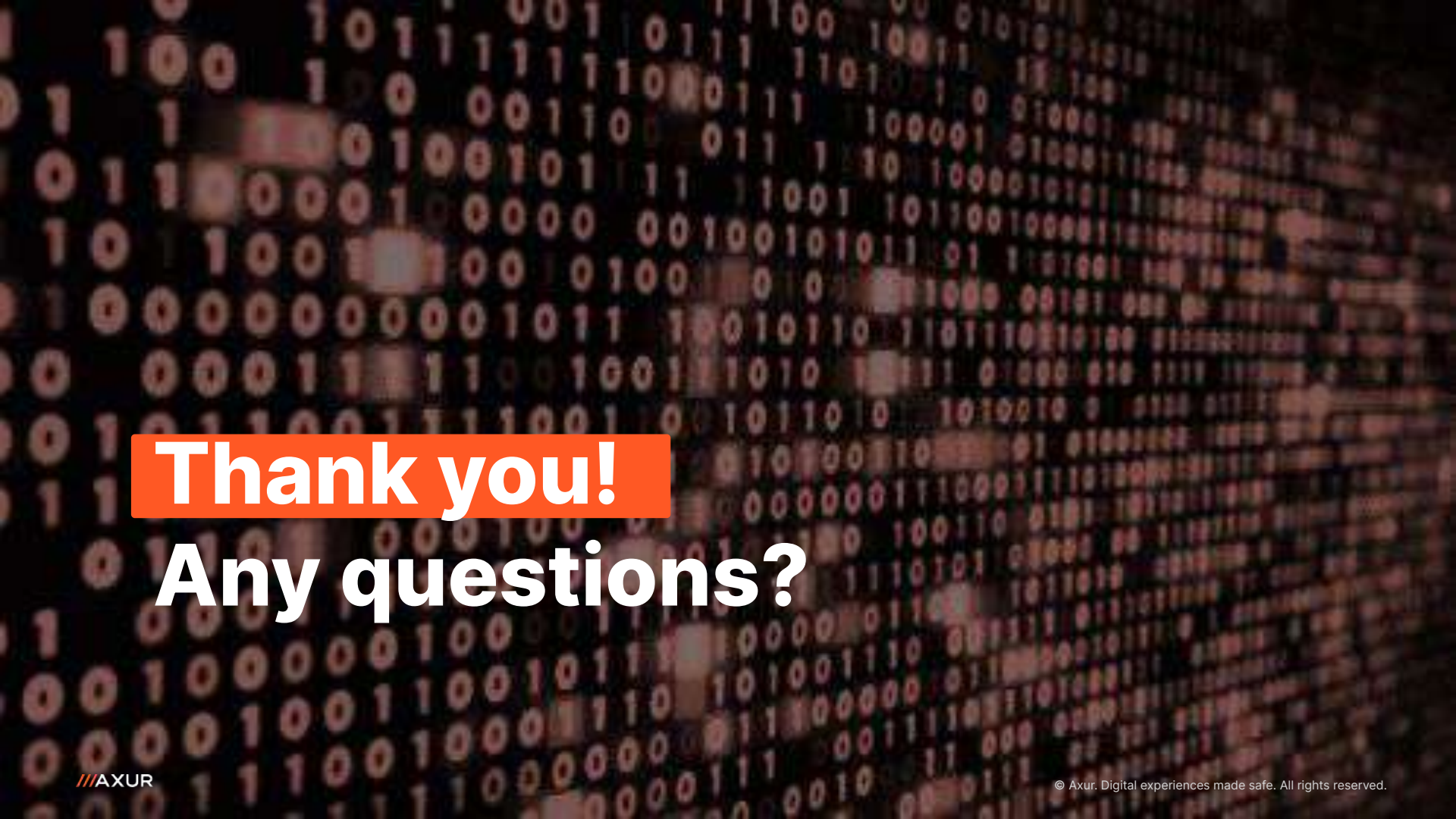
Changes

- Products being conceived with the concept of security and privacy by design
- Investment of the industry in Cyber Security
- People’s awareness regarding to possible risks
- Security must be thought of as risk to an individual’s life

///AXUR

How to handle
Cybernetic threats

End to end:
Axur has monitoring solutions, response and intelligence that look on the entire NIST Framework with the aid of specialized teams and the latest technology.



AXUR