



CHAIRE
CYBERCNI
Sécurité des infrastructures critiques



COLLOQUE IMT
ENTRONS-NOUS DANS UNE NOUVELLE ÈRE
DE LA CYBER-SÉCURITÉ?



Critical Infrastructure Security

Simon Foley
IMT Atlantique



Security of Critical Infrastructure

Davis Besse Nuclear Power Plant

Event: Aug 20, 2003 Slammer worm infects plant

Impact: Complete shutdown of digital portion of Safety Parameter Display System (SPDS) and Plant Process Computer (PPC)

Specifics: Worm started at contractors site

Worm jumped from corporate to plant network and found an unpatched server

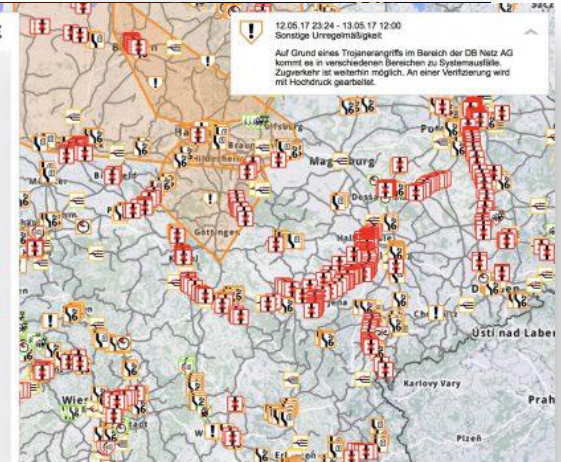
Patch had been available for 6 months



Recovery time:
 * SPDS – 4 hours 50 minutes
 * PPC – 6 hours 9 minutes

Lessons learned:

- Secure remote (trusted) access channels
- Ensure Defense-in-depth strategies with appropriate procurement requirements
- Critical patches need to be applied



Ukrainian postal service hit by 48-hour cyber-attack
 10 August 2017 | Technology

Ukraine's national postal service has been hit by a two-day-long cyber-attack targeting its online system that tracks parcels.

Unknown hackers carried out a distributed denial of service (DDoS) attack against Ukrposhta's website.

The attack began on Monday morning, but ended shortly after 21:00 local time (1900 BST).

However, Ukrposhta reported on Facebook that the DDoS attack continued again on

SWIFT Banking System Was Hacked at Least Three Times This Summer
 September 26, 2016

The SWIFT logo at their headquarters in Brussels, Belgium. Photograph by Jacques Collet—AFP/Getty Images

And cyber attacks on banks are set to intensify.

By Reuters September 26, 2016

SWIFT, the system banks use to send payment instructions worth trillions of dollars each day, was hacked at least three times over the summer and cyber attacks on banks are set to intensify, the cooperative said on Monday.

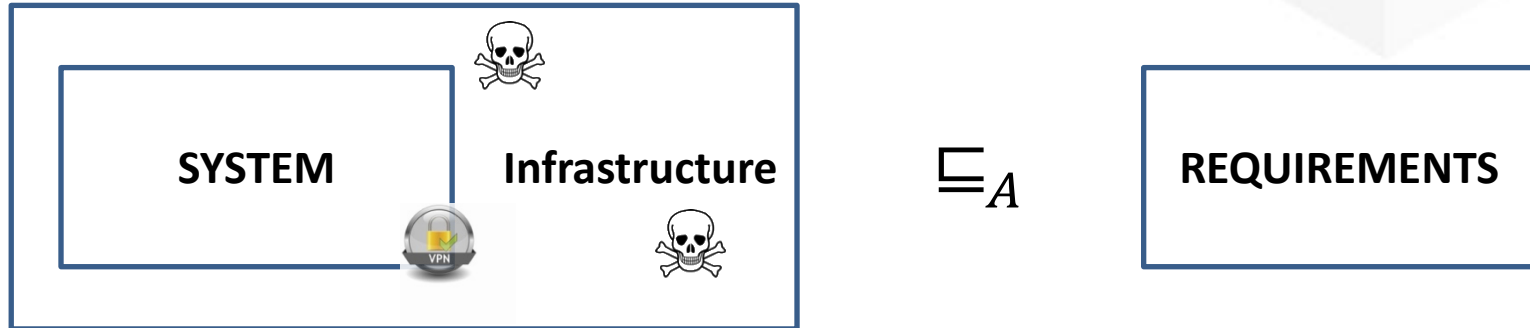
Cyber-attack halts production at Cadbury factory
 By James Ridler
 29-Jun-2017 - Last updated on 30-Jun-2017 at 09:26 GMT

Mondelez was one of a number of food firms caught in the latest wave of cyber-attacks

Cyber-attacks have reportedly halted production at a Cadbury factory in Tasmania, after its owner, global food giant Mondelez, was infected by ransomware.

IT systems at Cadbury's factory in Hobart went down just after 9:30 yesterday (June 27), according to the Australian Manufacturing Workers' Union Tasmanian secretary John Short.

Defining security: *declarative*



System with infrastructure is sufficiently robust to satisfy its requirements in presence of threats

$$S \sqsubseteq_A R \equiv \forall s \in \tau(S). \exists r \in \tau(R). s \uparrow A = r \uparrow A$$

Promising for critical security mechanisms



\subseteq_A



Cisco Router Security Certifications

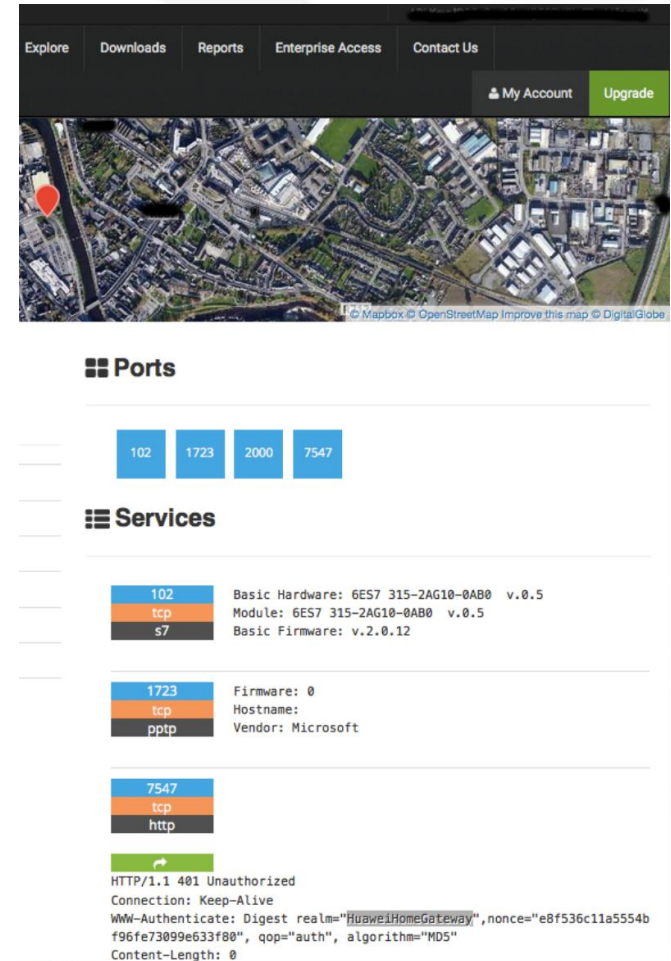
	FIPS 140-2, Level 2	Common Criteria EA1.4	NG Strong Crypto AES-GCM-256
Cisco ISR 890 Series	✓	✓	✓
Cisco ISR 1900 Series	✓	✓	✓
Cisco ISR 2900 Series	✓	✓	✓
Cisco ISR 3900 Series	✓	✓	✓
Cisco ISR 4000 Series	✓	✓	✓
Cisco ASR 1000 Series	✓	✓	✓

ciscolive! BFC 6378 Suite B ^{***} Not supported on older RP1 based ASR 1000s.



The reality

- S7comm on Port 102
 - CVE-2015-2177 ...
- PPTP on Port 1723
 - MS security Advisory 2743314 ...
- CWMP over HTTP
 - CVE-2014-9222, CVE-2014-9223 ...
- Huawei home gateway
 - CVE-2015-7254, CVE-2013-6786 ...
- Siemens FAQ8970169
 - *“Port 102 [...] must be enabled for the complete transfer route”*

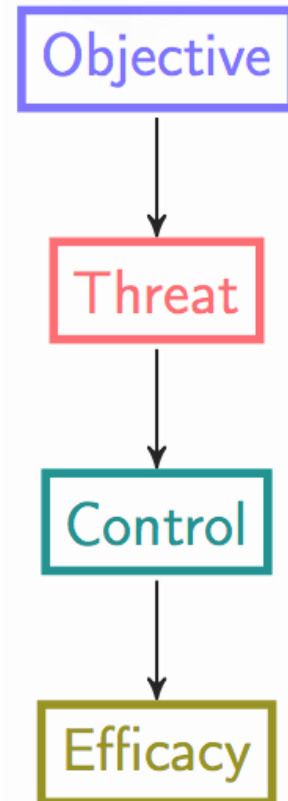
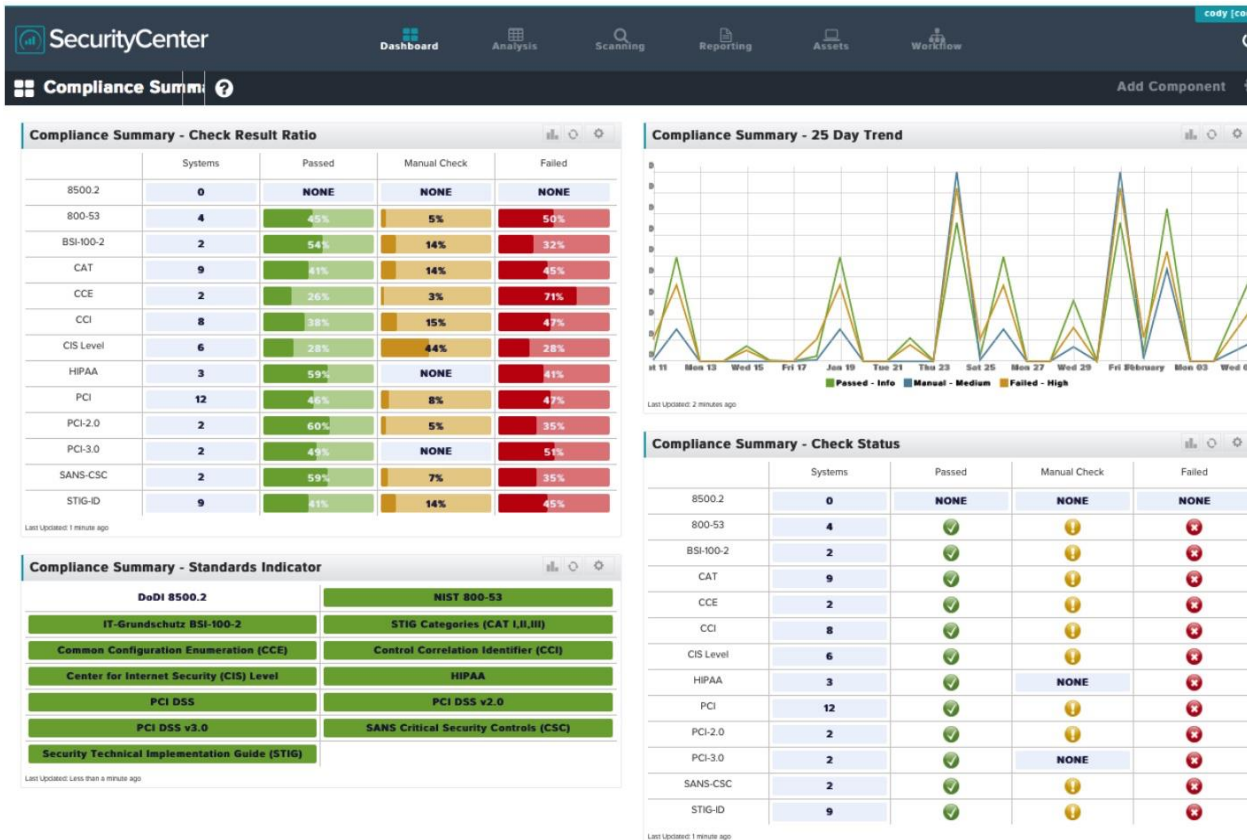


The screenshot shows a web-based network scanner interface. At the top, there are navigation tabs: Explore, Downloads, Reports, Enterprise Access, and Contact Us. On the right, there are links for 'My Account' and 'Upgrade'. Below the navigation is a satellite map of a city area with a red location pin. Underneath the map is a section titled 'Ports' with a grid of four blue buttons labeled '102', '1723', '2000', and '7547'. Below that is a section titled 'Services' with three entries:

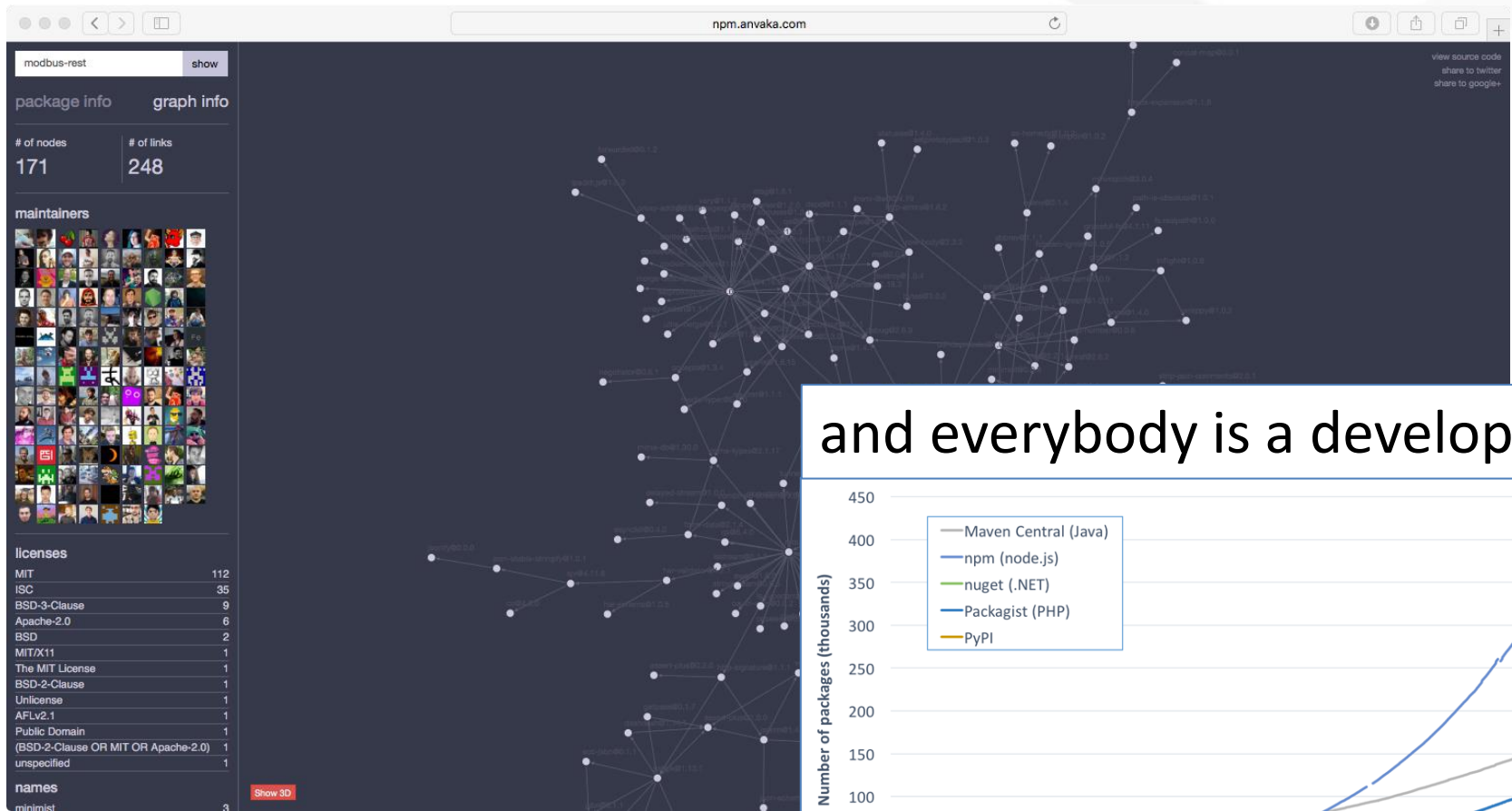
- 102**: tcp, s7. Basic Hardware: 6ES7 315-2AG10-0AB0 v.0.5, Module: 6ES7 315-2AG10-0AB0 v.0.5, Basic Firmware: v.2.0.12
- 1723**: tcp, pptp. Firmware: 0, Hostname: , Vendor: Microsoft
- 7547**: tcp, http

At the bottom, there is a green button with a right-pointing arrow and a block of text: HTTP/1.1 401 Unauthorized, Connection: Keep-Alive, WWW-Authenticate: Digest realm="HuaweiHomeGateway", nonce="e8f536c11a5554bf96fe73099e633f80", qop="auth", algorithm="MD5", Content-Length: 0

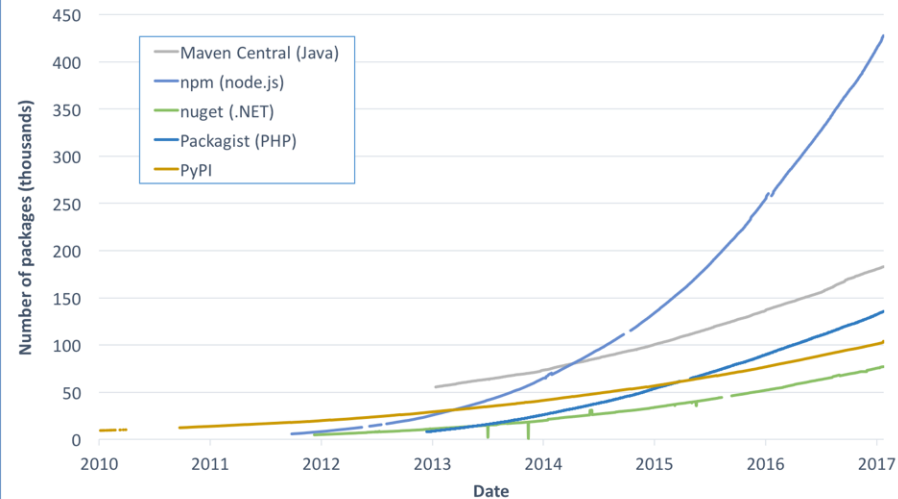
Defining security: *Operational*



Contemporary systems are convoluted,



and everybody is a developer



and built and operated by humans

The New York Times

TECHNOLOGY

Security Experts Expect 'Shellshock' Software Bug in Bash to Be Significant

By NICOLE PERLROTH SEPT. 25, 2014

Long before the commercial success of the Internet, Brian J. Fox invented one of its most widely used tools.

Davis Besse Nuclear Power Plant

Event: Aug 20, 2003 Slammer worm infects plant

Impact: Complete shutdown of digital portion of Safety Parameter Display System (SPDS) and Plant Process Computer (PPC)

Specifics: Worm started at contractors site

- Worm jumped from corporate to plant network and found an unpatched server

- Patch had been available for 6 months



Recovery time:

- SPDS – 4hours 50 minutes
- PPC – 6 hours 9 minutes

Lessons learned:

- Secure remote (trusted) access channels
- Ensure Defense-in-depth strategies with appropriate procurement requirements
- Critical patches need to be

CNET

REVIEWS NEWS VIDEO HOW TO SMART HOME CARS GAMES DOWNLOAD

SEARCH

How Target detected hack but failed to act -- Bloomberg

Despite alerts received through a \$1.6 million malware detection system, Target failed to stop hackers from stealing credit card numbers and personal information of millions of customers, Bloomberg reports.

CSC et HPE Enterprise Services forment désormais DXC Technology.

EN SAVOIR PLUS

DXC.technology

Security



by Lance Whitney
13 March 2014 3:36 pm GMT
@lancewhit



THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine

The Man Who Wrote Those Password Rules Has a New Tip: N3v\$r M1^d!

Bill Burr's 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—he regrets the error

By Robert McMillan
Aug. 7, 2017 12:41 p.m. ET

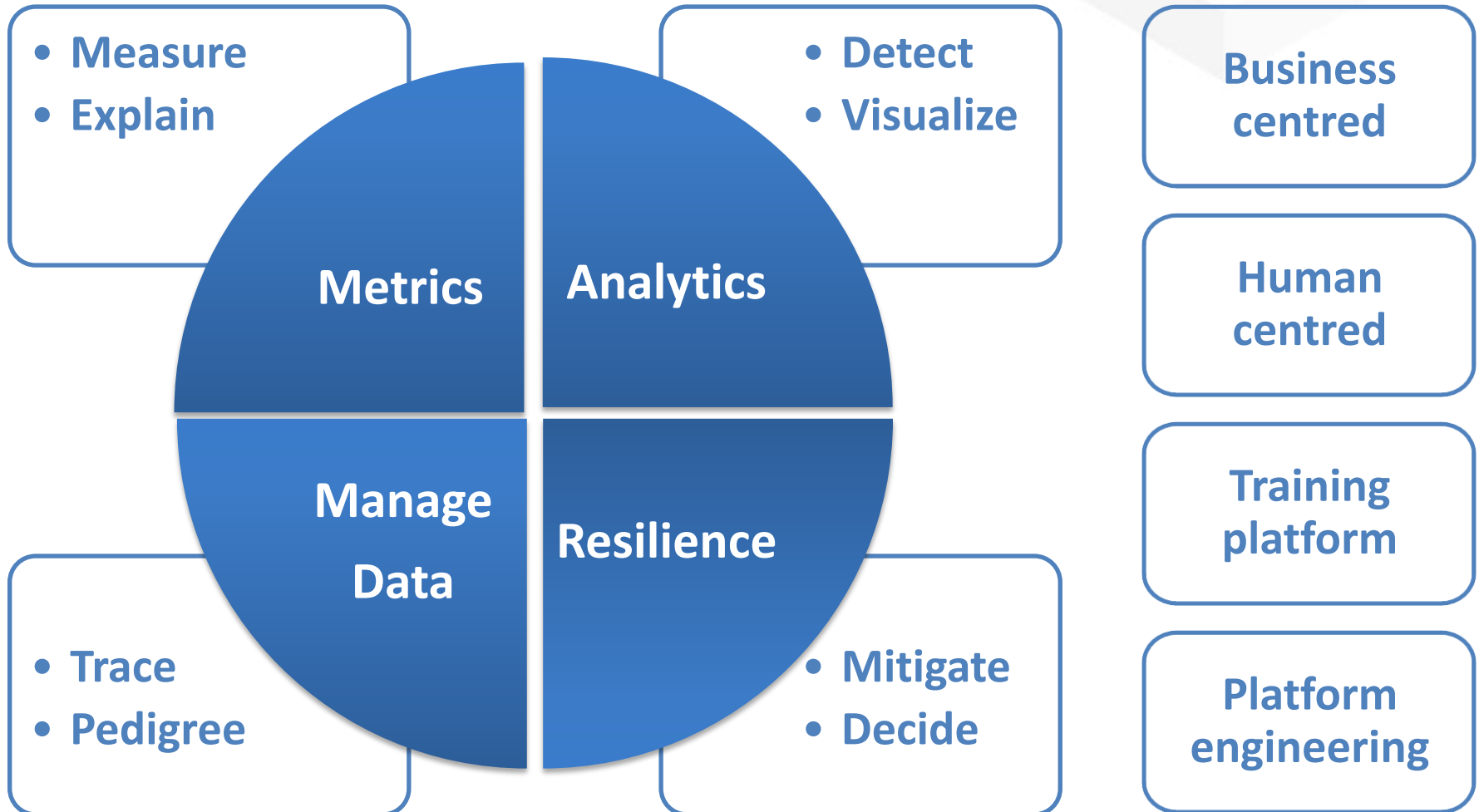
The man who wrote the book on password management has a confession to make: He blew it.

Back in 2003, as a midlevel manager at the National Institute of Standards and Technology, Bill Burr was the author of "NIST Special Publication 800-63, Appendix A." The 8-page primer advised people to protect their accounts by inventing awkward new words rife with obscure characters, capital letters and numbers—and to change them regularly.

Most Popular Videos

- The High-Tech Hunt for Russian Submarines
- One Man's Quest to Save the Holy Yamuna River
- What's Next for Islamic State?

IMT Cyber CNI chair: robust to failure

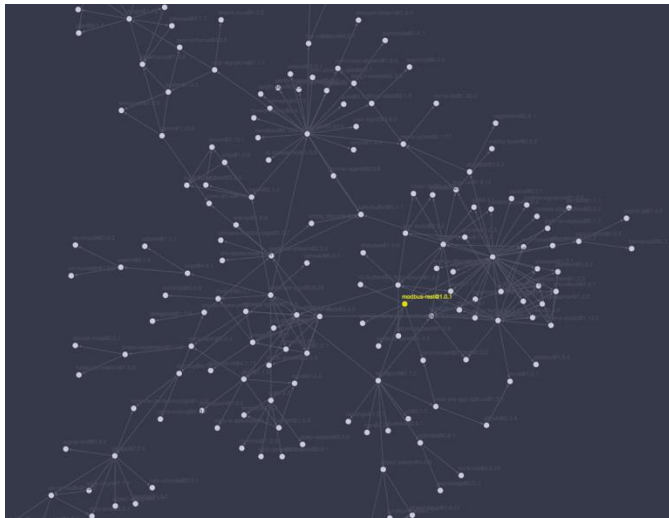


Resilience

resilient | rɪ'zɪliənt |

adjective

- 1 (of a person or animal) able to withstand or recover quickly from difficult conditions: *babies are generally far more resilient than new parents realize* | *the fish are **resilient** to most infections.*



Reason about & provide resilience in complex critical systems

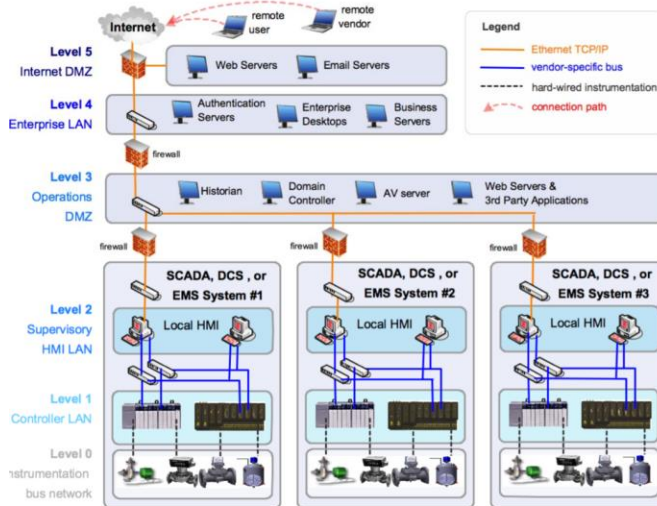
- measure degree of resilience
- make trade-offs, recommendations
- improve and manage resilience

Diagnostics

explanation | ɛksplə'neɪʃ(ə)n |

noun

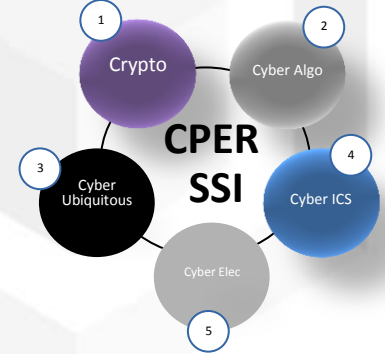
a statement or account that makes something clear: *the birth rate is central to any explanation of population trends.*



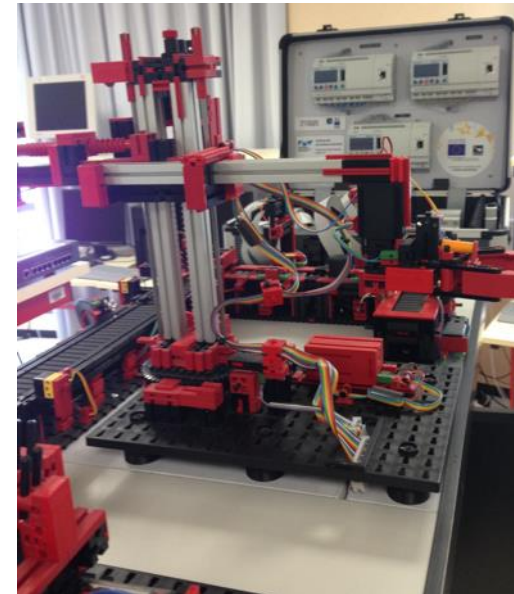
Diagnose security and safety in Industrial Control Systems.

- modelling security threats and safety failures
- Diagnose and explain threats and failures
- Reason about, make trade-offs

Research Laboratory



- Fischertechnik testbeds
- SADA Crouzet, Siemens, Yokagawa, stormshield, ...
- Big data platform
- Cyber Range attack simulator platform



IMT Cyber CNI chair: partners



UNION EUROPÉENNE
UNANIEZH EUROPA



L'Europe s'engage
en Bretagne

Avec le Fonds européen
de développement régional



BNP PARIBAS
La banque d'un monde qui change

NOKIA

