La force de l'innovation

CYBER SECURITY

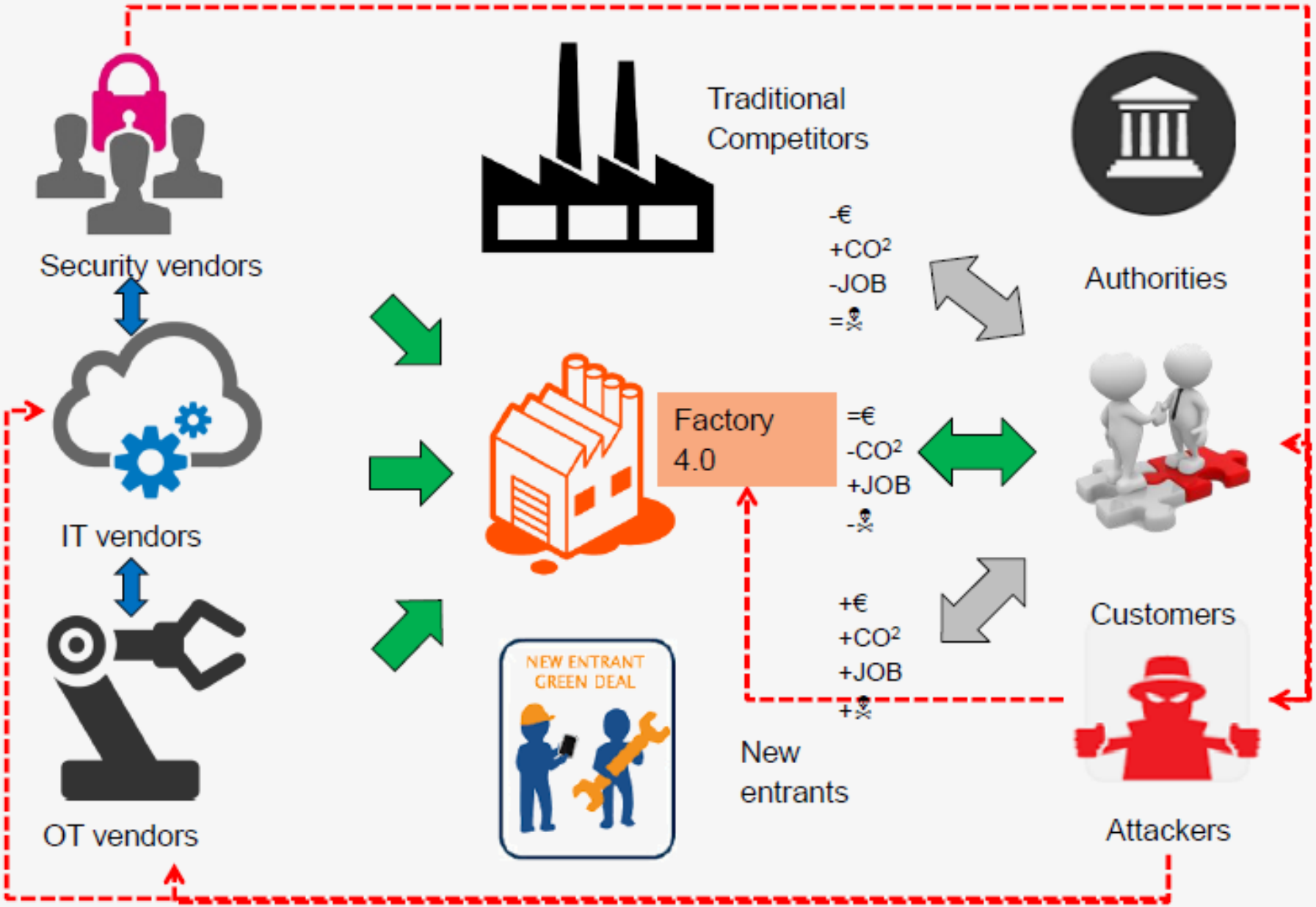
EUROPEAN UNION CONTEXT

- The Directive on security of network and information systems (the NIS Directive) was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. Member States had to transpose the Directive into their national laws by 9 May 2018 and identify operators of essential services by 9 November 2018.
- The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:
  - Member States' preparedness by requiring them to be appropriately equipped,
  - cooperation among all the Member States […].
  - a culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by the Member States as operators of essential services will have to take appropriate security measures

UE WORKSHOP ON CYBERSECURITY HELD LAST OCTOBER

- Any device with software-defined behaviour can be tricked into doing things its creators did not intend
- Any device connected to a network of any sort, in any way, can be compromised by an external party
- If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology
- Progress just means bad things happen faster

Ecosystem overview



UE WORKSHOP ON CYBERSECURITY HELD LAST OCTOBER

La force de l'innovation

➔ Managing industrial cyber security risks : key takeaways

- Broadening the understanding of security : logical, physical and human
- Understanding the potential impact of cyber threats and vulnerabilities (higher cyber risk management maturity)
- Integrating cyber securities best practices into the industrial processes
- Forming multi-disciplinary cyber security teams
- Ensuring the use of secure devices and platforms

CS CYBERSECURITY OFFERING

CONSULTING & AUDIT

SOLUTIONS' INTEGRATION

SECURITY SERVICES

FOCUS ON A PRODUCT : WHAT IS A SIEM ?

- A Security information and event management system (SIEM) :
  - collects and analyzes activity tracks (logs, netflows, etc.) of hosts and infrastructure applications to ensure a unified vision of information system security management for operations.
  - provides real-time event processing to extract alerts, normalize them, correlate them and notify operators in real time of threats within an administration console.
  - provides the capacity to stock and index all system tracks for analysis, reporting and compliance purposes.
- It must :
  - be able to process a very large volume of data in real time
  - Normalize suspicious events and enriches them in a format dedicated to intrusion detection
  - offer advanced correlation capabilities
  - offer all the tools necessary for monitoring and exploiting alerts: notification, ticket and workflow management.
- SIEM capabilities now include combination capabilities with Cyber Threat Intelligence (CTI) or Artificial Intelligence functionalities such as machine learning to improve detection capabilities.

FOCUS ON ONE PRODUCT – PRELUDE

Unified Security Supervision

Detection APT Remediation	Investigation Reporting Steering	Big Data Compliance Risk Management

Alert **Analyse** **Archive**

PRELUDE Smart Security

is based on open-source : https://www.prelude-siem.com/en/

Applications Systems Networks Security

FEATURES

- Completeness
- Power of in depth detection
- IDMEF standard (Intrusion Detection Message Exchange Format)
- Modularity, adaptability, customization
- Proven efficiency
- French based software
  - Open-source core version
  - Enhanced commercial version

La force de l'innovation

PERSPECTIVES