ORACULUM
AI DATA-DRIVEN SECURE ARBITRATOR

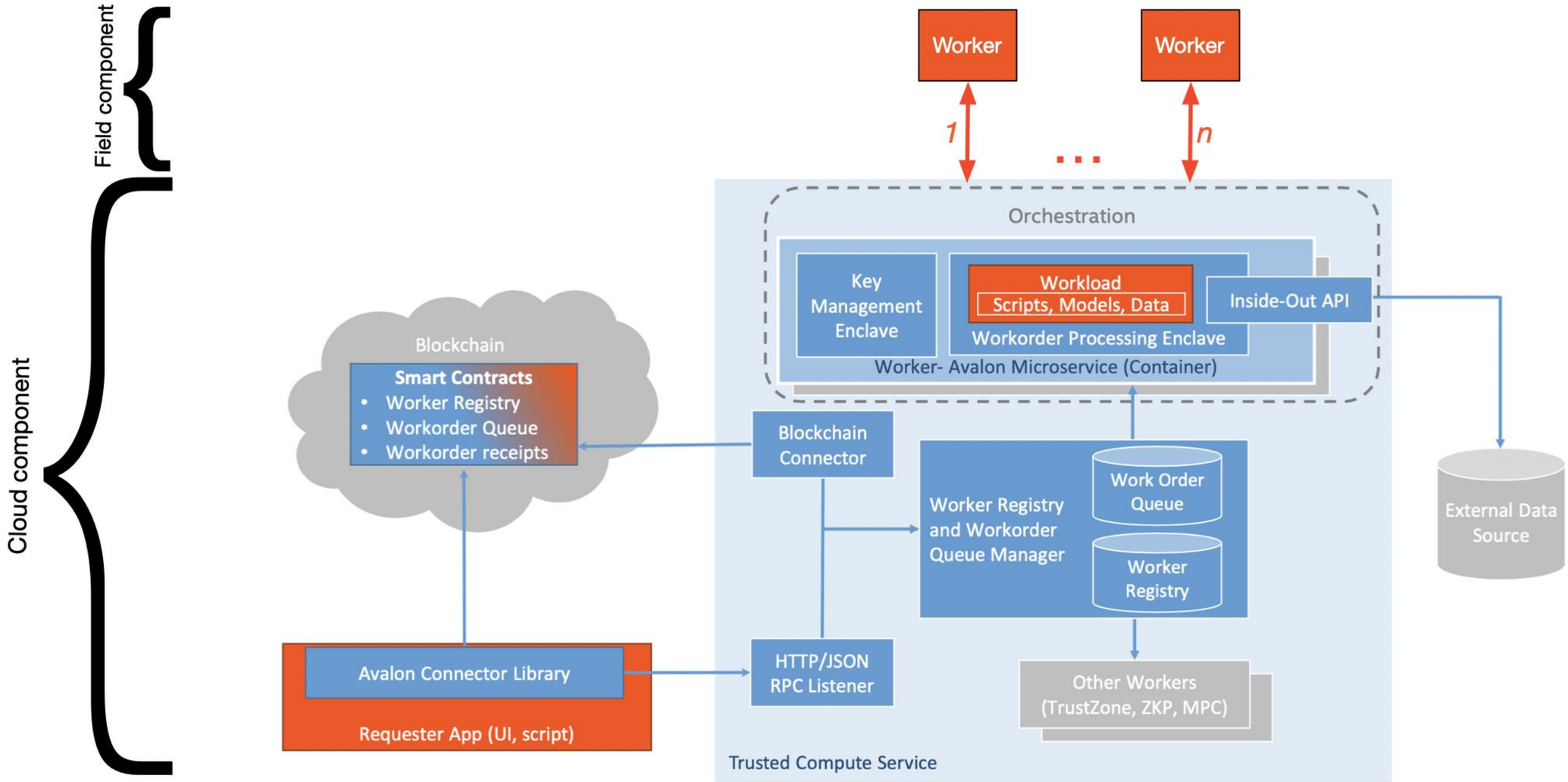
General solution possibilities

Data validation and protection

"Blind", autonomous, censorship-resistant confirmation of the execution of operations by participants and individual elements / nodes of the system

ORACULUM

Main components scheme

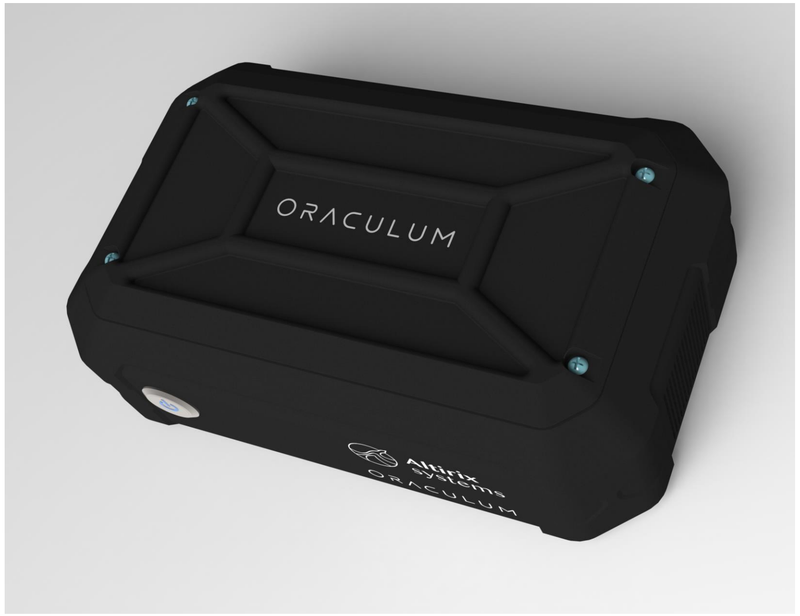


Color map:
blue – Reusable Avalon framework
orange – Custom app specific

Worker's technical characteristics

Power	10 W	15 W
AI Performance	14 TOPS	21 TOPS
CPU	ARM v8.2 64bit 6 core freq 1200 to 1600 MHz	
GPU	384-core NVIDIA CUDA with 48 Tensor cores freq from 800 to 1100 MHz	
RAM	8 Gb @1600 MHz	
Storage (up to 1 Gb SSD)	16 Gb eMMC 5.1	
Ports	3xUSB 2.0, 1xUSB 3.1, 2xHDMI 2.0, 1x SDIO, 2x SPI, 3xUART, 2x I2S, 4xI2C, 1xCAN, GPIOs	
Supporting devices	up to 6 int cams 1080p 4K (up to 36 with virt channels), LIDARs, temperature sensors, G-sensors etc. up to 30 Gbps	
Onboard IS mechanisms	Hybrid TEE (CPU + GPU), customizing OS	
Autonomy	up to 20 h with 5.1v@18650 mAh Li-ion, 5 TOPS up to 8 h with 5.1v@18650 mAh Li-ion, 10 TOPS	
Dimensions	103mm x 34mm x 90.5mm 150mm x 45mm x 100mm (IP4 case)	

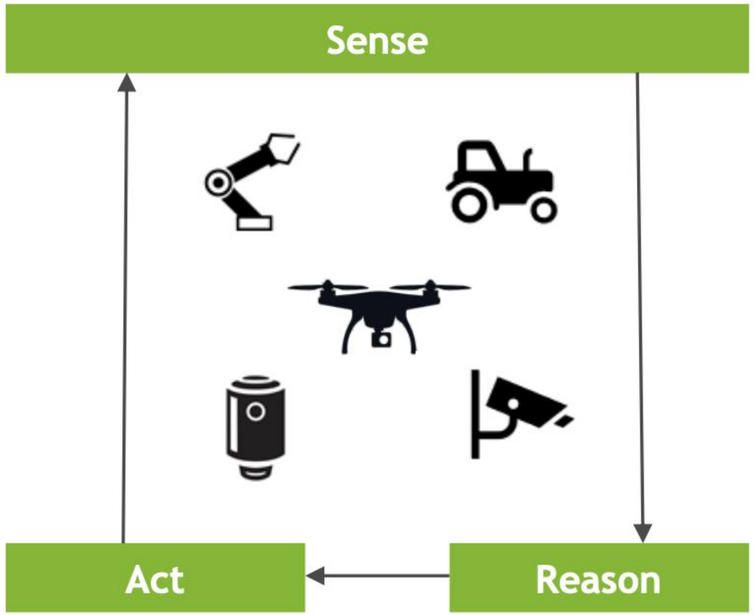
Worker (version L)



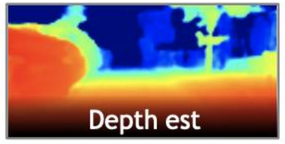
ORACULUM

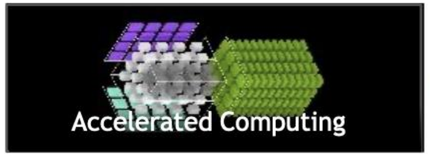
Technological stack

AI over all process

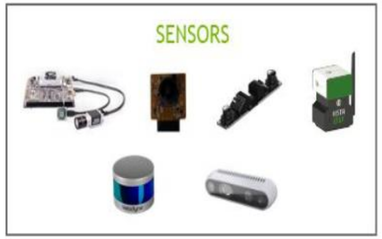


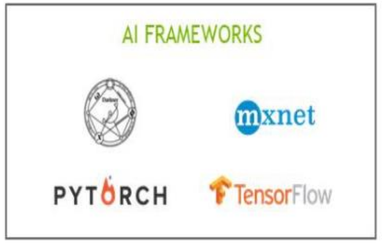
Best practices





Ecosystem





HYPERLEDGER

ethereum

ORACULUM

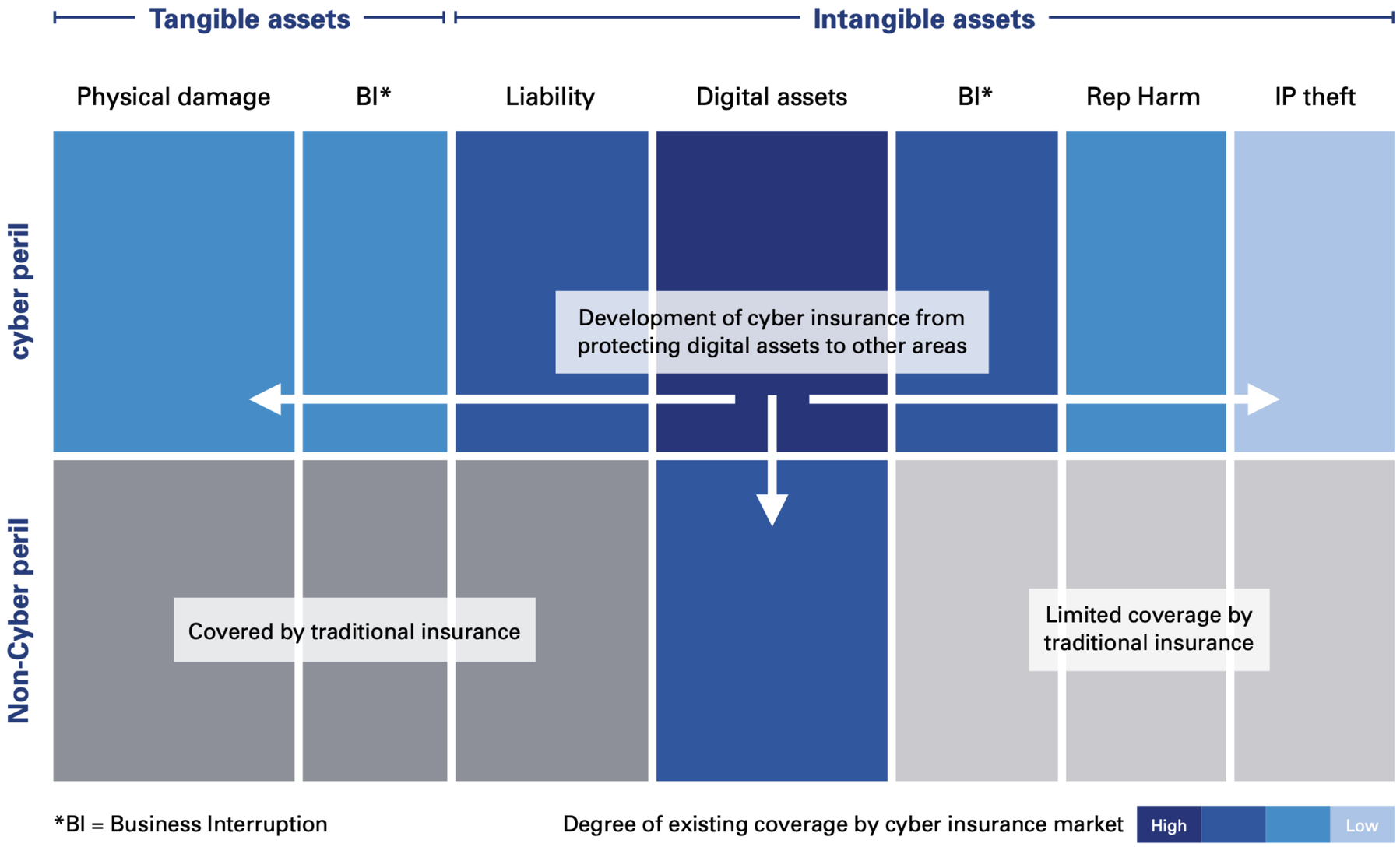
Use Case - Cyber Risk Scoring

New Age of Insurance:

- The rise of risk aggregators
- Demand for new products and solutions as businesses develop different risk profiles
- The future of excess capacity
- Customers demanding broader solutions, rather than just insurance products
- Collaborative development of solutions to meet emerging customer needs
- Cognitive computing advancements creating value through sophisticated analytics
- The changes to business models and requirements for more agile operating models

© 2017 KPMG International Cooperative (“KPMG International”)

Use Case - Cyber Risk Scoring

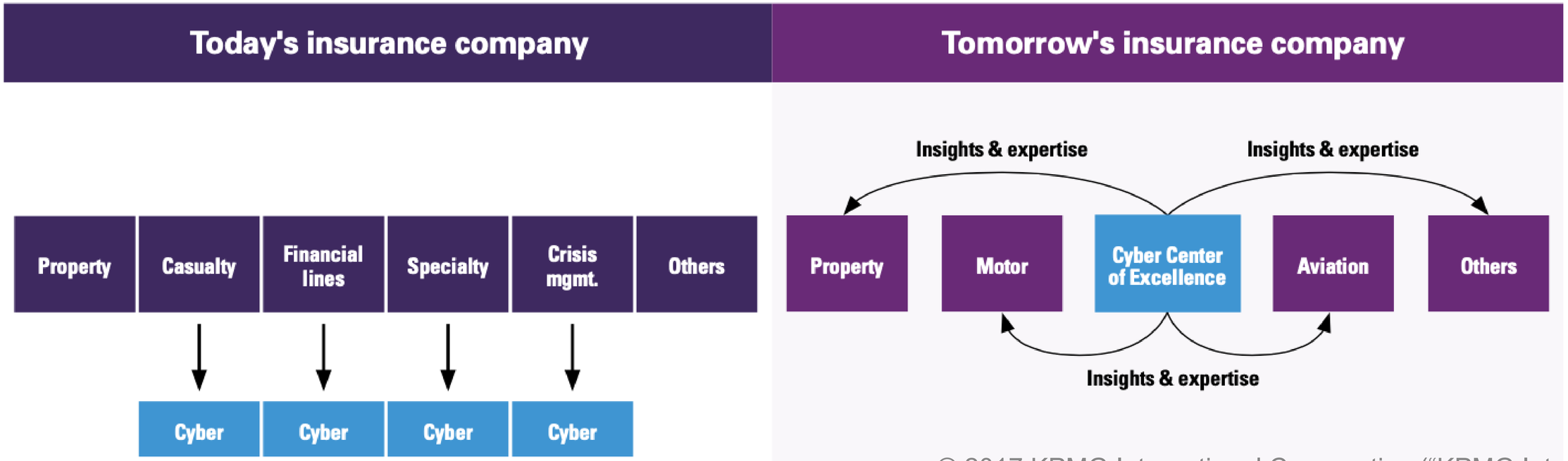


© 2017 KPMG International Cooperative (“KPMG International”)

ORACULUM

Use Case - Cyber Risk Scoring

Insurance company of the future



© 2017 KPMG International Cooperative ("KPMG International")

Use Case - Cyber Risk Scoring

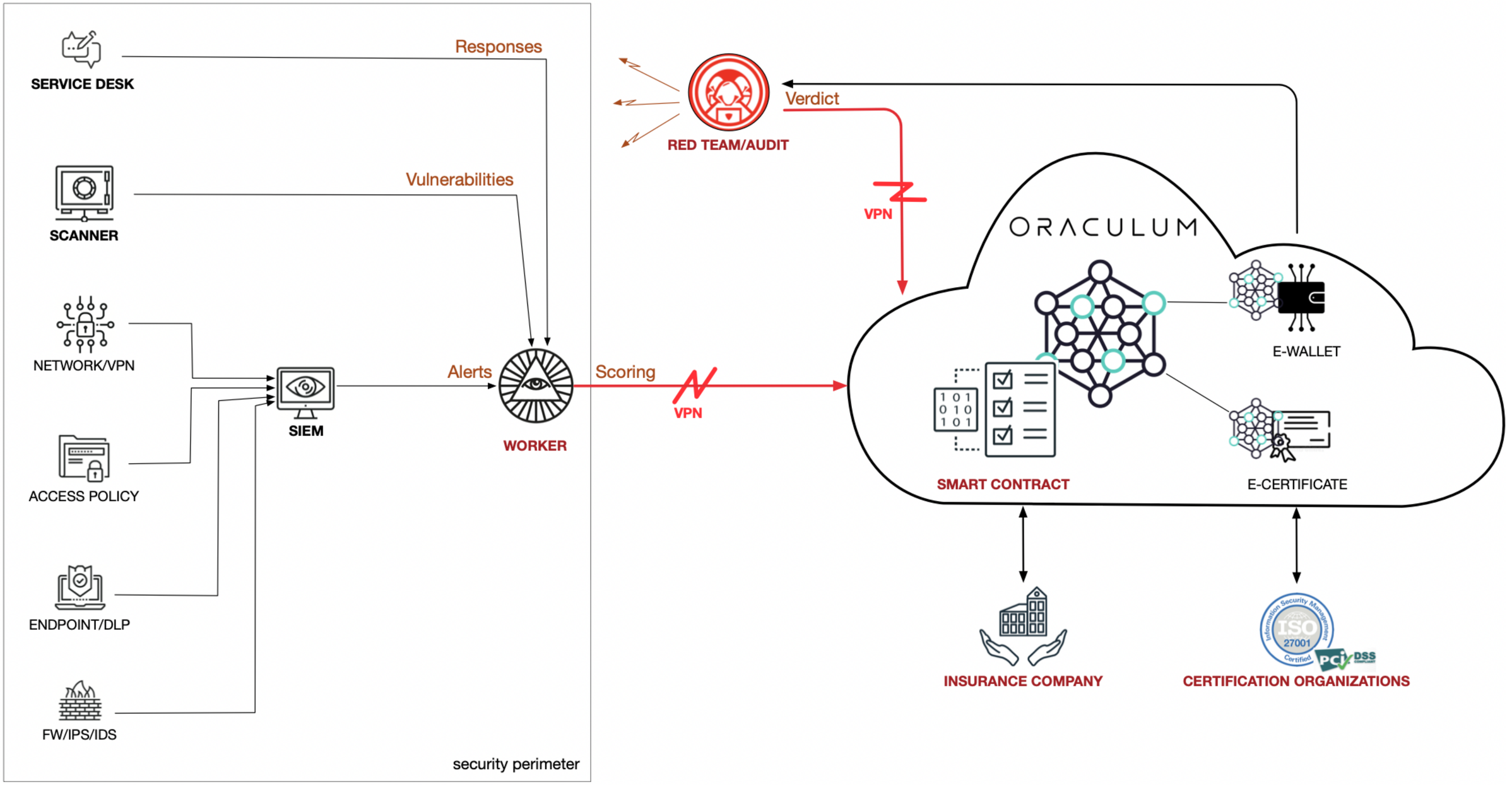
Challenges of Cyber Insurance:

- Cyber risks continue to evolve*
- Cyber incidents are not only the main threat around the world but are also among the
- Companies are facing the problem of larger and more costly data breaches, increasing ra
- High potential cost with a full-scale pre-insurance audit
- Lack of tools for the determination and settlement of insurance claims
- Lack of qualified specialists in the field of cyber risk insurance
- The trend for remote work and the reduction of the human factor

* Allianz Risk Barometer 2020©

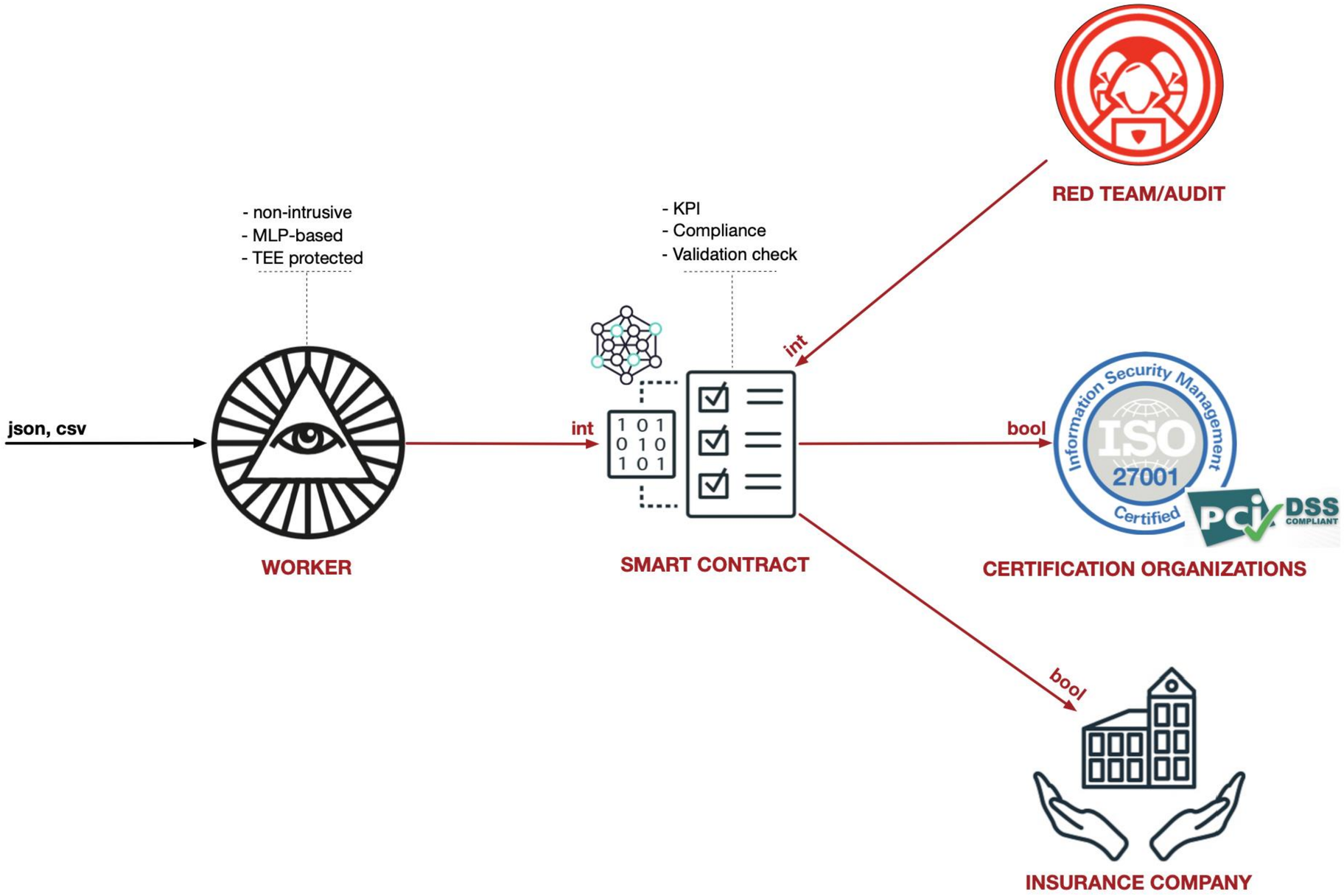
ORACULUM

Use Case - Cyber Risk Scoring



ORACULUM

Use Case - Cyber Risk Scoring



Use Case - Cyber Risk Scoring

INSURANCE BI (BUSINESS RISKS): property interests of the Insured associated with the occurrence of unforeseen expenses as a result of a cyber security incident that led to illegal blocking of access to computer information, inaccessibility of the website, information systems (including information security systems), cloud service on which the assets of the Insured are located due to the following events:

- data encryption with ransomware;
- malfunctioning of the information system caused by malicious software;
- DoS / DDoS attacks;
- APT attacks;
- cyber attacks on the provider;
- attacks on vulnerabilities (zero day) in system software;
- lost profits are covered - in terms of the wage fund.

Use Case - Cyber Risk Scoring

Advantages:

- The data does not go outside the Company, the risk ratio is calculated within the protected perimeter of the company
- Clients with a high level of information security have discounts and reduced insurance rates
- No one outside can distort the risk ratio
- The client and the insurance company receive a continuous and objective assessment of the client's information security
- Automation of certification of information security processes

THANK YOU

> “Let's try to protect everything that's important to us.”
>
> Nick Szabo