cegal

CONNECT@PLANT

SECURE ACCESS TO YOUR PLANTS

WHO WE ARE

OUR VISION

Be the most innovative provider of IT services and Geoscience Solutions to the global oil and gas industry.

CONNECT@PLANT
SECURE ACCESS TO YOUR PLANTS

THREATS

TARGETED ATTACKS

CONNECT@PLANT

SECURE ACCESS TO YOUR PLANTS

CHALLENGES

INDUSTRIAL CONTROL SYSTEMS

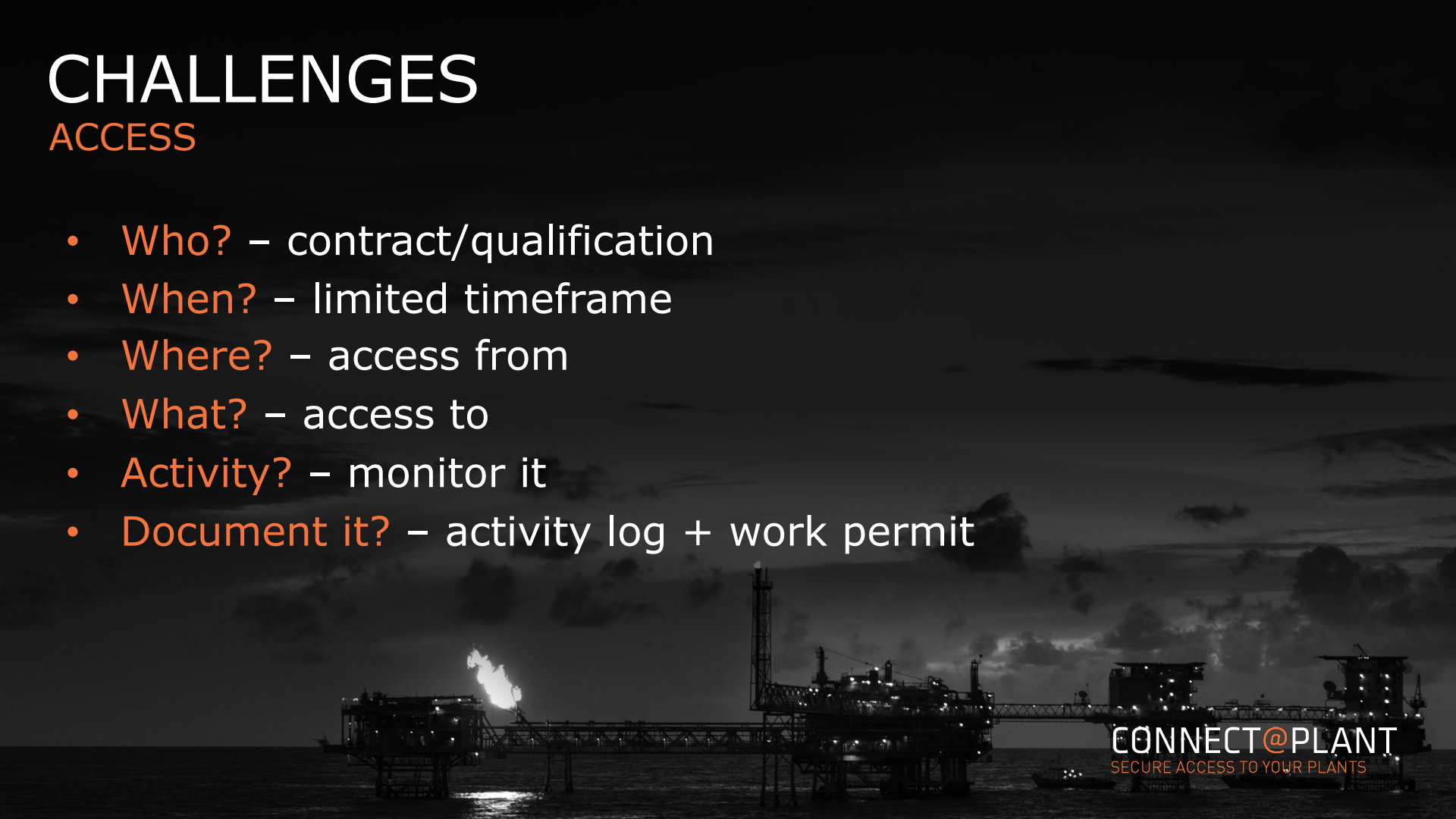
- Land based personnel need access to critical Industrial Control Systems (ICT) offshore in a secure way.

- NOG -104: Objective of the guideline:
  The objective of the guideline is to improve the overall information security of the offshore industry and thereby improving the safety and regularity of the operations on the Norwegian continental shelf.

CHALLENGES

ACCESS

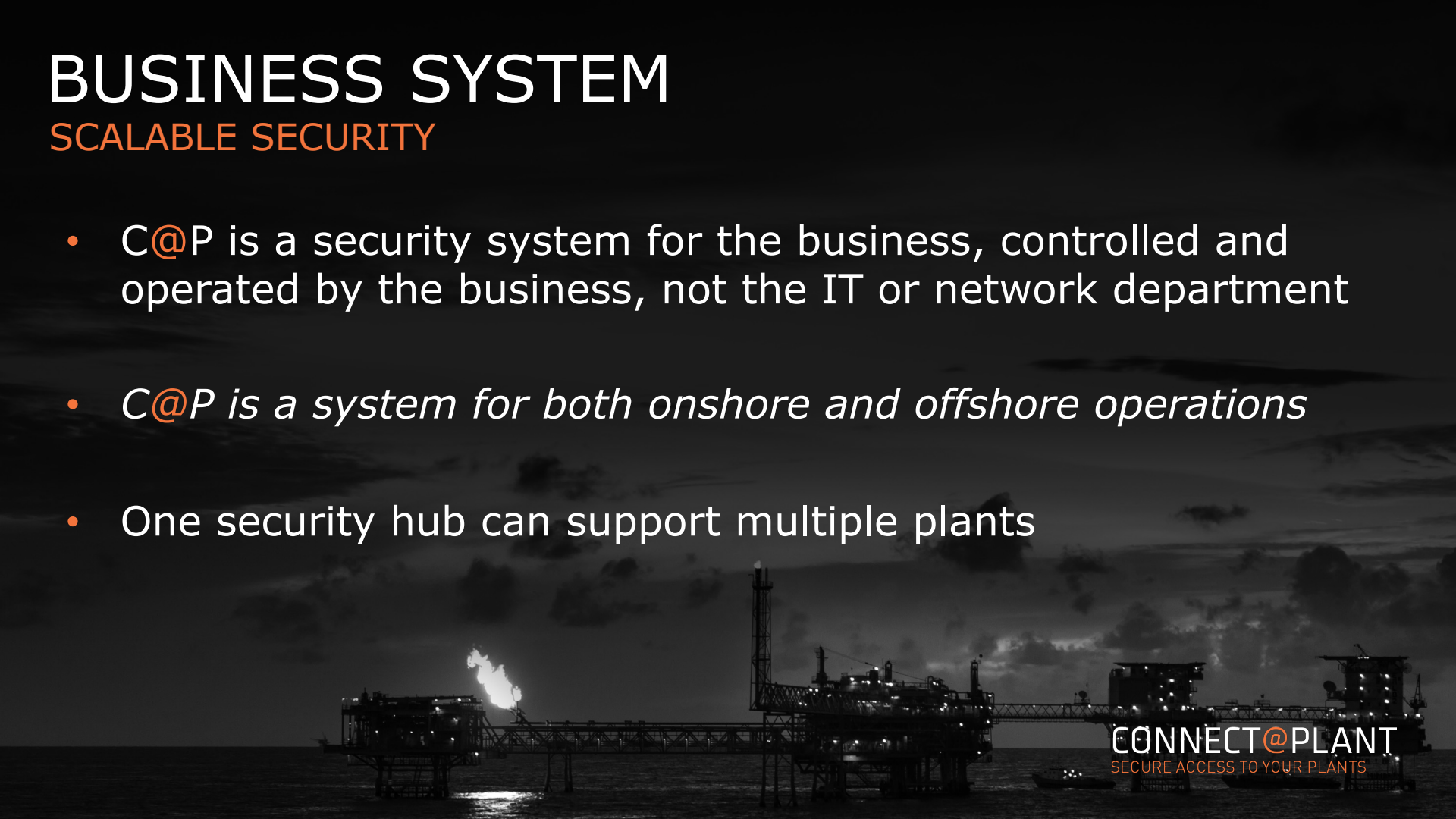
- Who? – contract/qualification
- When? – limited timeframe
- Where? – access from
- What? – access to
- Activity? – monitor it
- Document it? – activity log + work permit



BUSINESS SYSTEM

SCALABLE SECURITY

- C@P is a security system for the business, controlled and operated by the business, not the IT or network department
- *C@P is a system for both onshore and offshore operations*
- One security hub can support multiple plants



CONNECT@PLANT
SECURE ACCESS TO YOUR PLANTS

KEY FUNCTIONALITY

WHAT YOU GET

End point control
(Virus and Windows Updates)

Secure file transfer with multiple virus scan and threat emulation

User authorization

All traffic encrypted – double layer

Only access with a valid work permit

Only access to predefined system, based on skills

User qualifications – skills

User specific dashboard based on skills and work permit

CONNECT@PLANT
SECURE ACCESS TO YOUR PLANTS

KEY FUNCTIONALITY

WHAT YOU GET

Easy overview for Work Permit planning

Selfservice for user administration, qualifications and systems

All traffic logged, users, permits, accesses, ports, system

All traffic encrypted – double layer

Dynamic firewall rules

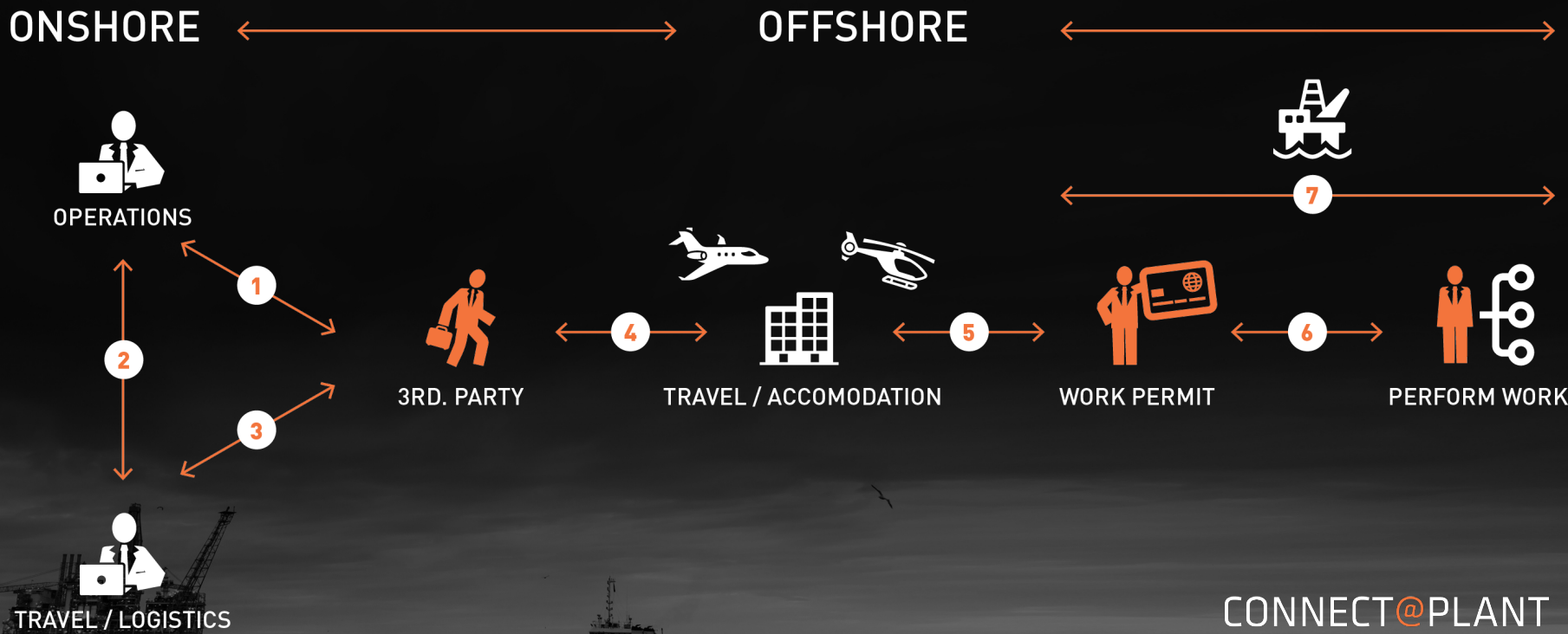
Emergency cut off – shut down all remote access by the touch of a button

CONNECT@PLANT

SECURE ACCESS TO YOUR PLANTS

WP – WORKFLOW

OLD SCHOOL

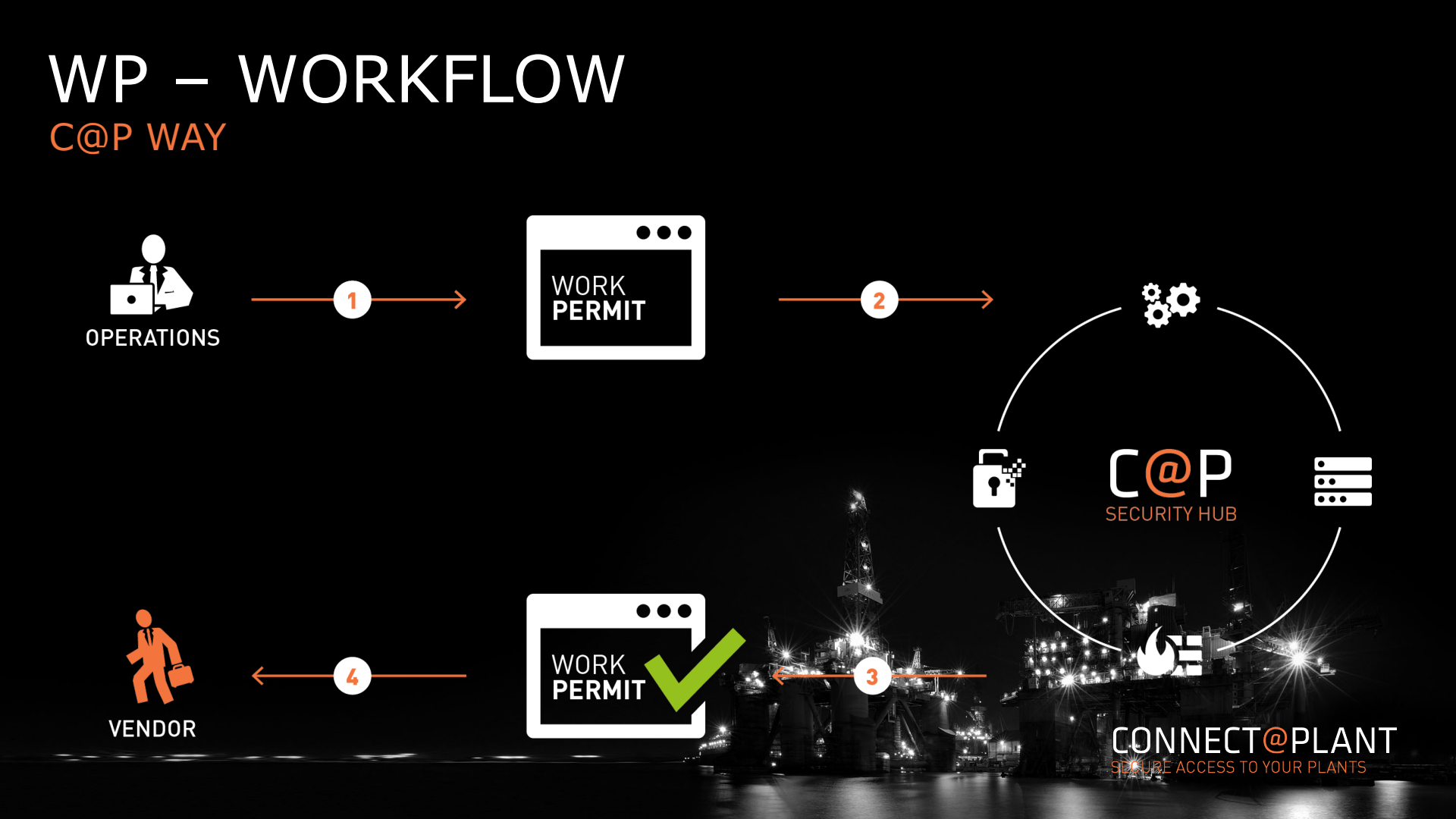


CONNECT@PLANT

SECURE ACCESS TO YOUR PLANTS

WP – WORKFLOW

C@P WAY



REMOTE CONNECTION

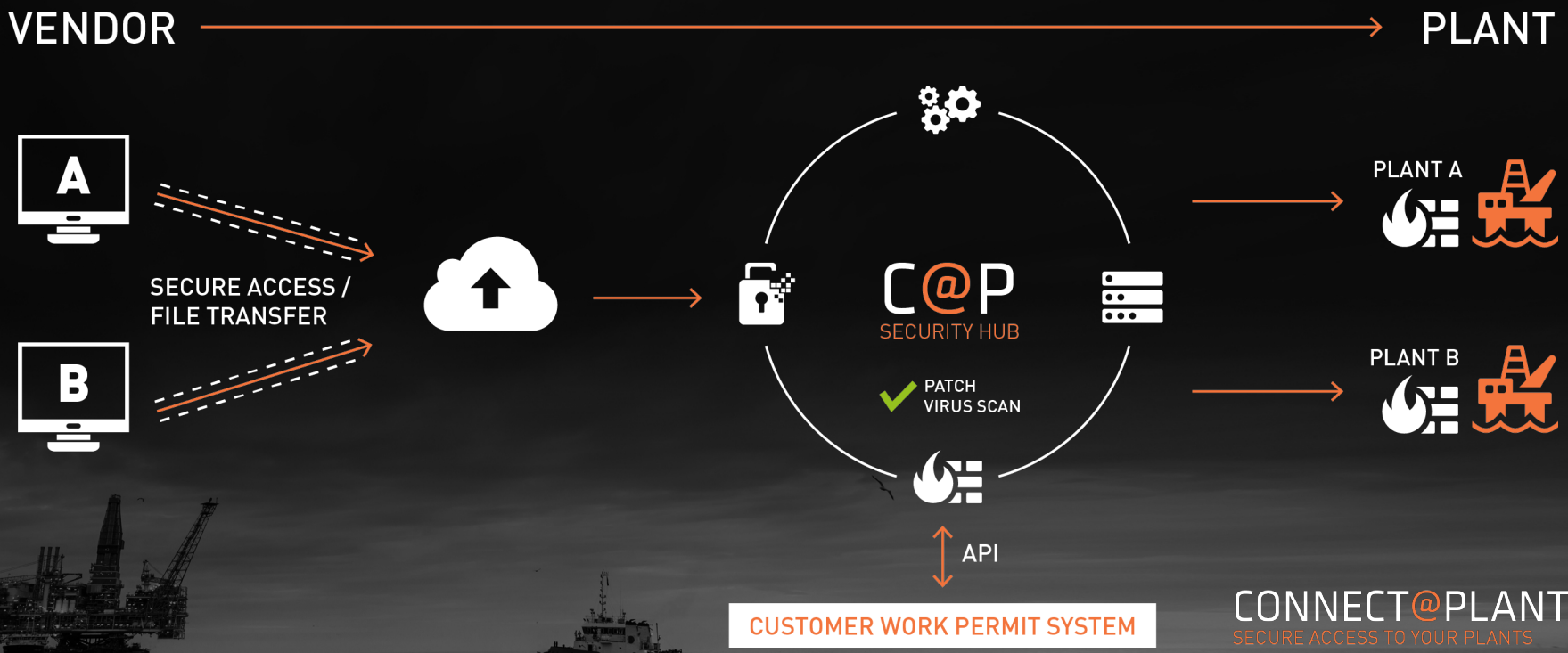
DEVICE CONTROL

CONNECT@PLANT

SECURE ACCESS TO YOUR PLANTS

SECURITY HUB

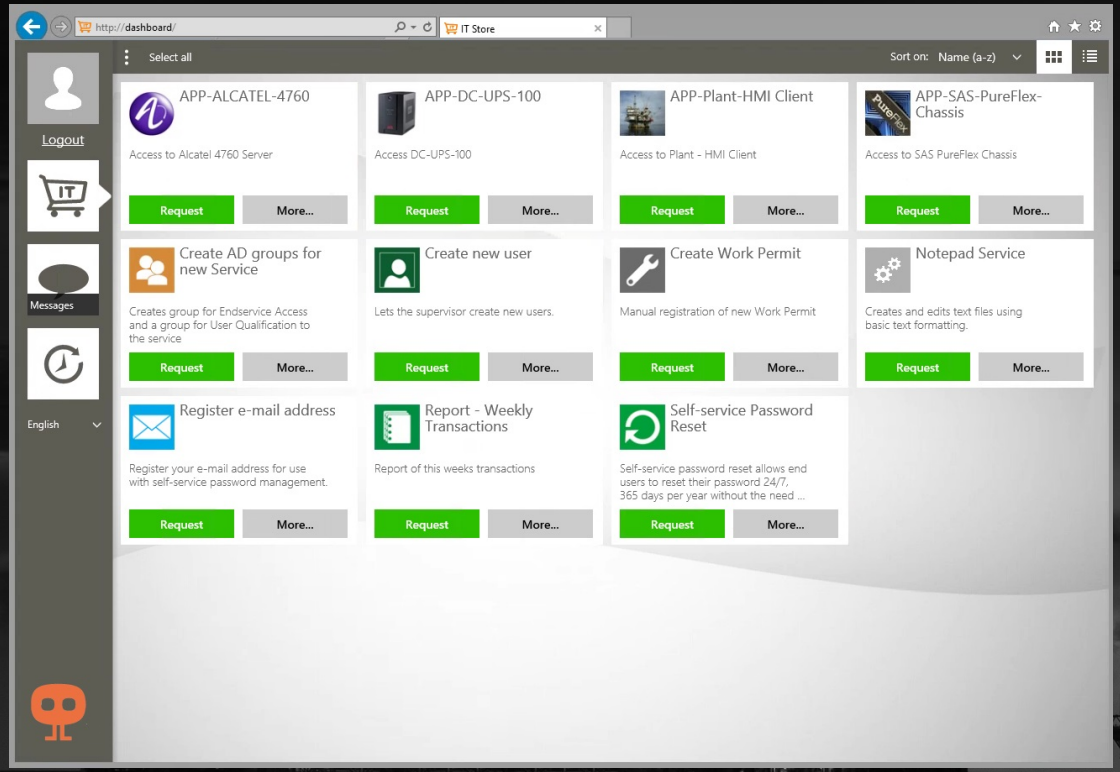
OVERVIEW



CONNECT@PLANT
SECURE ACCESS TO YOUR PLANTS

ADMISSION CONTROL SYSTEM

DASHBOARD



CONNECT@PLANT

SECURE ACCESS TO YOUR PLANTS

ADMISSION CONTROL SYSTEM

SYSTEM DETAILS

Work Permit for "Platform - HMI Client - Netop"

About

Request

Apply for work permit.

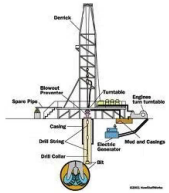
Information Security Baseline Requirement (ISBR)

1. An Information Security Policy for process control, safety and support ICT systems environments shall be documented.
An Information Security Policy is an overall management document that lays down the foundations for information security in the production environment. The policy describes the management intent and direction for information security.

2. Risk assessments shall be performed for process control, safety and support ICT systems and networks.
The risk assessments shall identify probabilities and consequences of security incidents, taking into account the security activities and actions that have been undertaken to mitigate potential risks.

3. Process control, safety and support ICT systems shall have designated system and data owners1.
The function shall have the overall system responsibility and ensure that only authorised applications and services are installed in the ICT systems.

4. The infrastructure shall be able to provide segregated networks, and all communi-cation paths shall be controlled.
The ICT infrastructure must be able to provide segregated networks, so that ICT systems with different levels of security, real-time systems that require a guaranteed network throughput, or especially sensitive systems can be installed in separately divided networks.

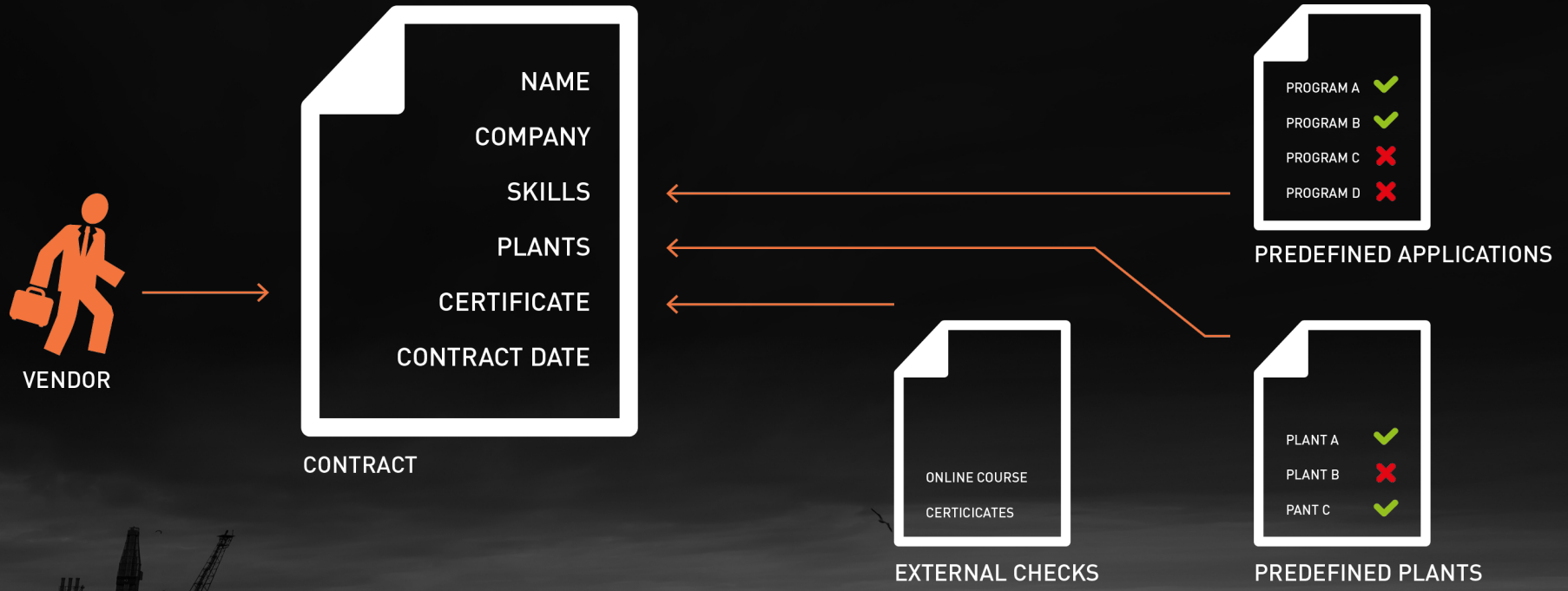


CONNECT@PLANT

SECURE ACCESS TO YOUR PLANTS

HR OVERVIEW

ACCESS MATRIX

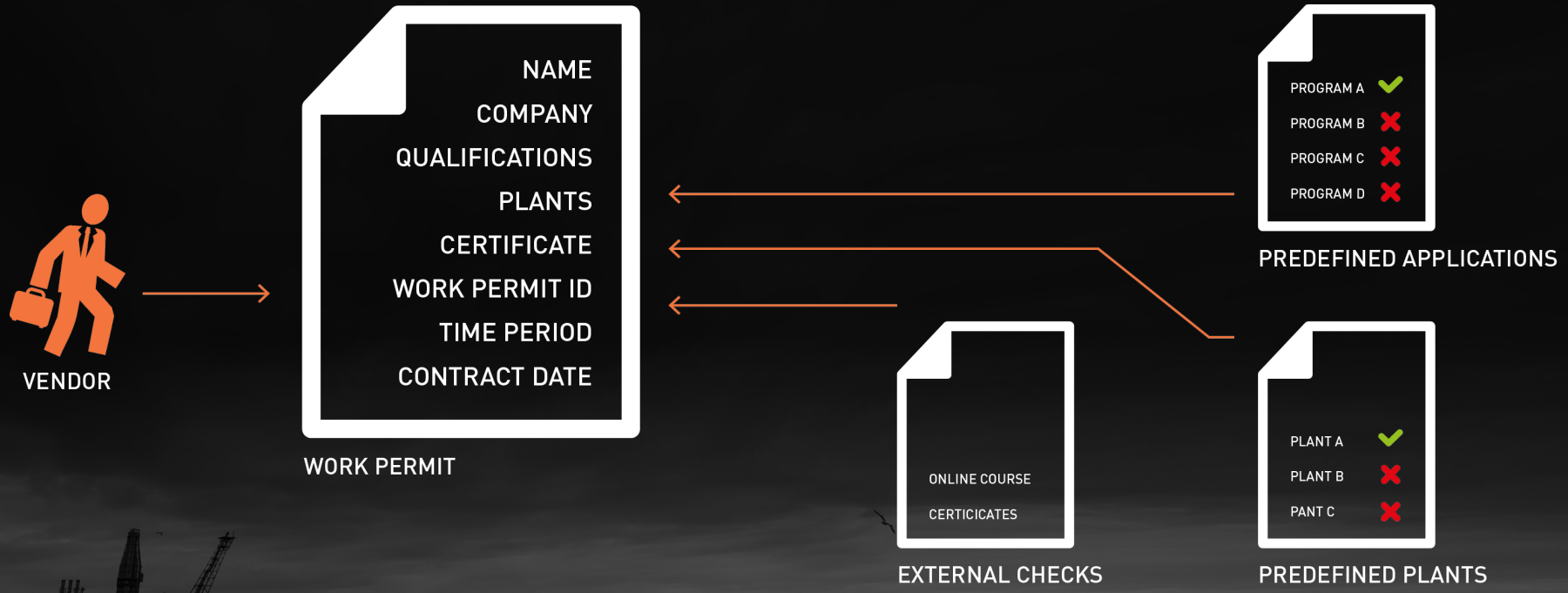


CONNECT@PLANT

SECURE ACCESS TO YOUR PLANTS

HR OVERVIEW

WORK PERMIT

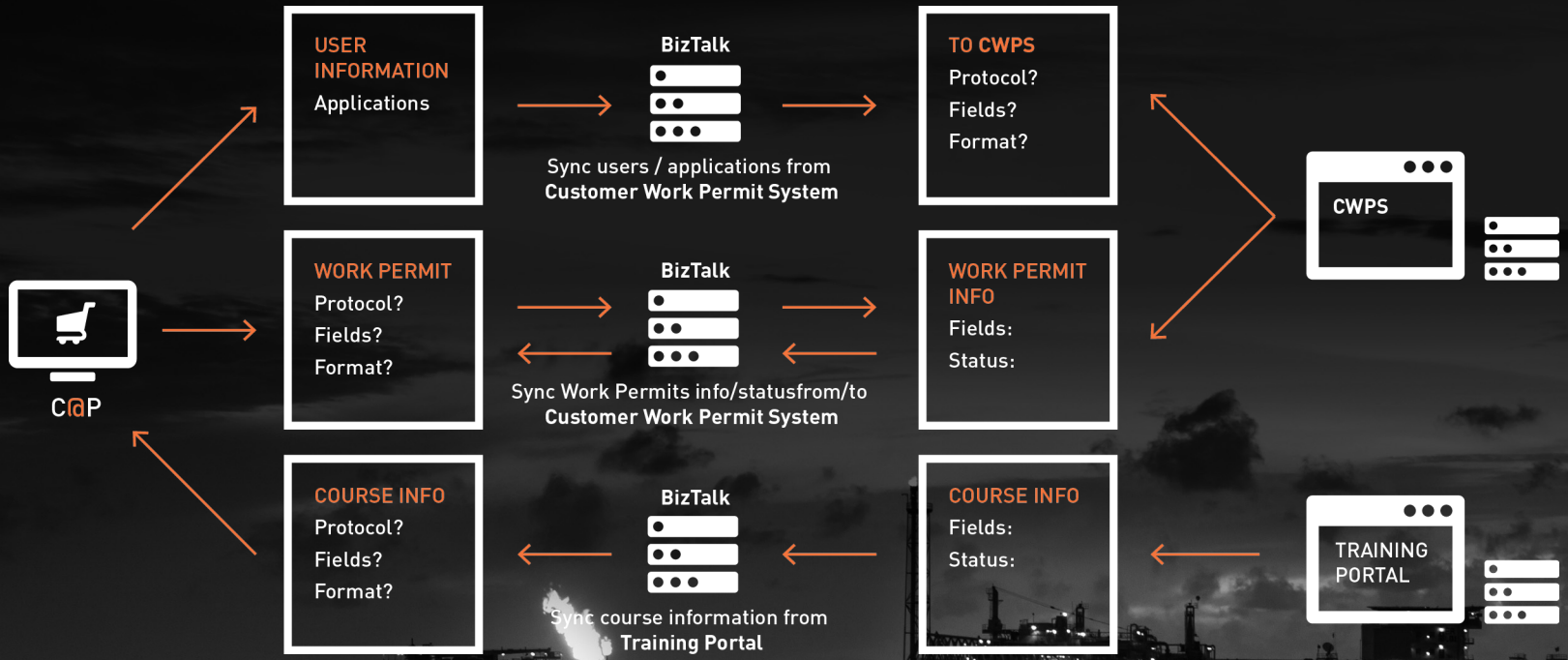


CONNECT@PLANT

SECURE ACCESS TO YOUR PLANTS

INTEGRATION

BIZTALK



CONNECT@PLANT

SECURE ACCESS TO YOUR PLANTS

CONNECT@PLANT

API

- Integrate your current Work Permit system into C@P
- API functionality
  - Create users
  - Create qualification
  - Define connection platform
  - Connect users to qualifications
  - Define access grantors
  - Create Work Permits
- Support 3.party systems through BizTalk

CONNECT@PLANT

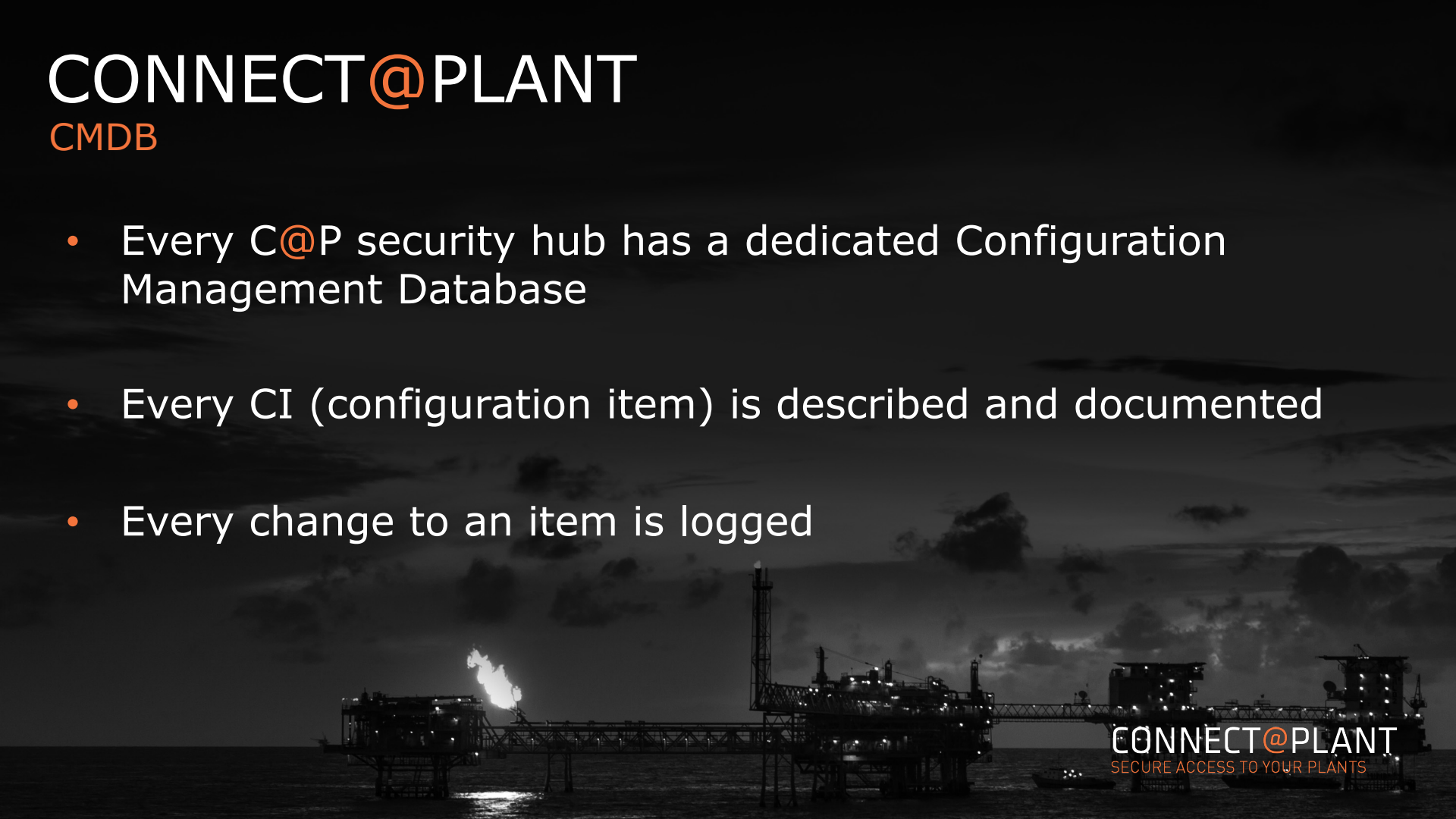
MAINTENANCE

- Access to centralized C@P core components not accessible without a work permit
- Cegal personnel is defined as a vendor
- Need special qualifications to access core components
- Every action is monitored and logged
- Customer controls when updates are done

CONNECT@PLANT

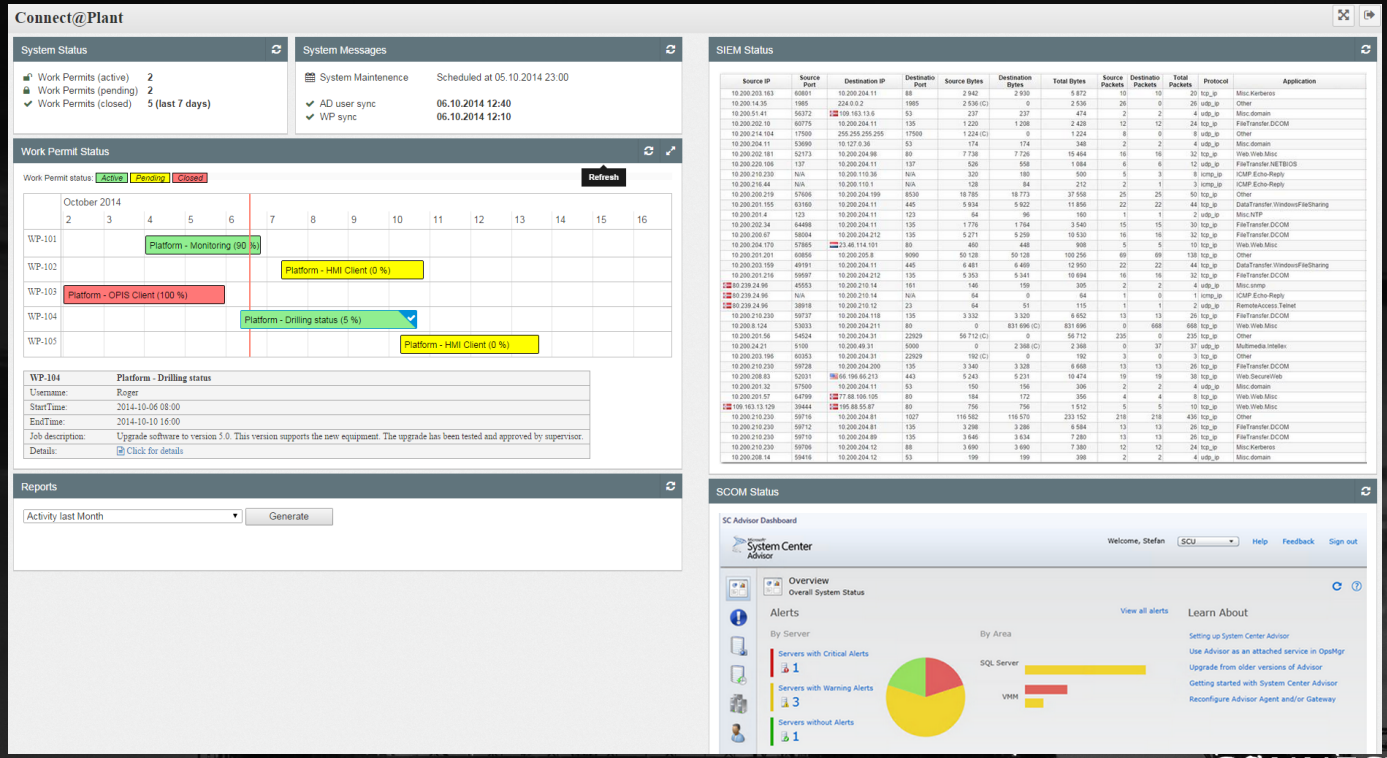
CMDB

- Every C@P security hub has a dedicated Configuration Management Database
- Every CI (configuration item) is described and documented
- Every change to an item is logged



OPERATION MANAGER

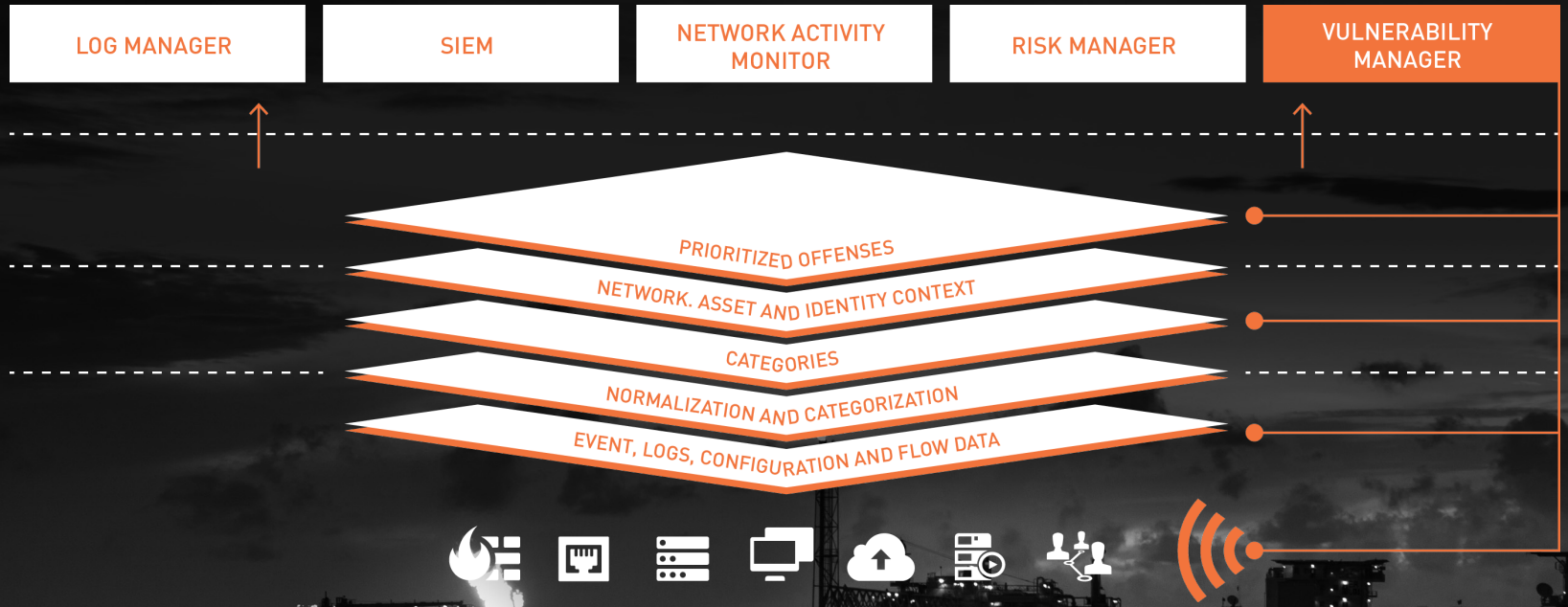
DASHBOARD



CONNECT@PLANT

SECURE ACCESS TO YOUR PLANTS

IBM
QRADAR



CONNECT@PLANT
SECURE ACCESS TO YOUR PLANTS

IBM
QRADAR

CONNECT@PLANT
SECURE ACCESS TO YOUR PLANTS

THE END

THANK YOU FOR YOUR ATTENTION

Arve Osmundsen
Business Development Manager - Solutions
Mob: +47 450 00 250
E-mail: Arve.Osmundsen@cegal.com

Cegal AS
Kanalvegen 11 • 4033 Stavanger • Norway
Tel: +47 81 50 09 55
Fax: +47 52 04 00 01
Web: www.cegal.com

CONNECT@PLANT
SECURE ACCESS TO YOUR PLANTS