



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**.*

A dark, atmospheric photograph of an offshore oil and gas platform at night. The platform is illuminated by various lights, with a prominent bright flare on the left side. The sky is dark with some clouds, and the water is visible in the foreground.

CONNECT@PLANT
SECURE ACCESS TO YOUR PLANTS

THREATS

TARGETED ATTACKS

Tidens hackerangrep mot Norge

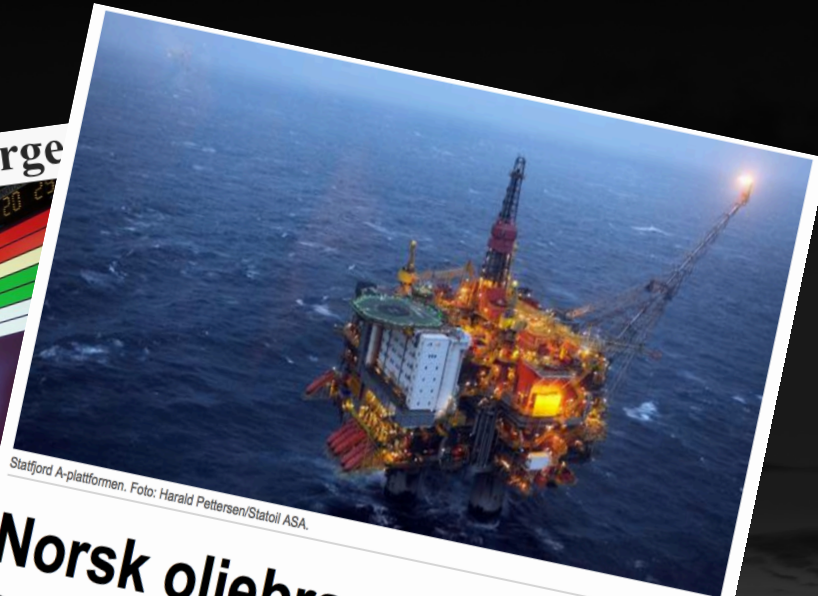


FOTO: HEIKO JUNGE NTB SCANPIX

Oljebransjen angripes av hackere
50 bedrifter bekrefter at de er angrepet, og ytterligere 250 får nå varsel fra Nasjonal Sikkerhetsmyndighet.



bedrifter ikke er klar over hvilke verdier d



Statfjord A-plattformen. Foto: Harald Pettersen/Statoil ASA.

Norsk oljebransje rammet av tidens hackerangrep

– Omtrent 300 virksomheter får nå varsel fra oss, sier NSM-direktør Hans Christian Pretorius.

Artikkel av: Øystein Byberg (Hegnar.no - 26.8.14 22:21)

CHALLENGES

INDUSTRIAL CONTROL SYSTEMS

- Land based personnel need access to critical Industrial Control Systems (ICS) 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



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

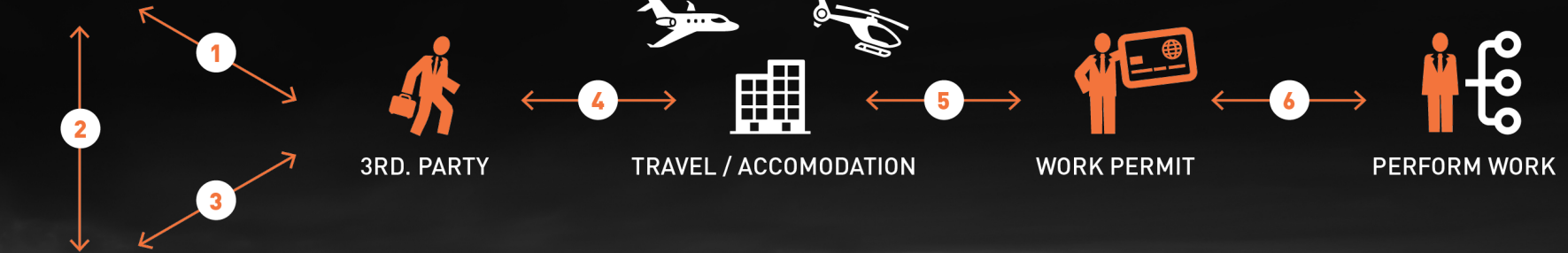
CONNECT@PLANT
SECURE ACCESS TO YOUR PLANTS

WP – WORKFLOW

OLD SCHOOL

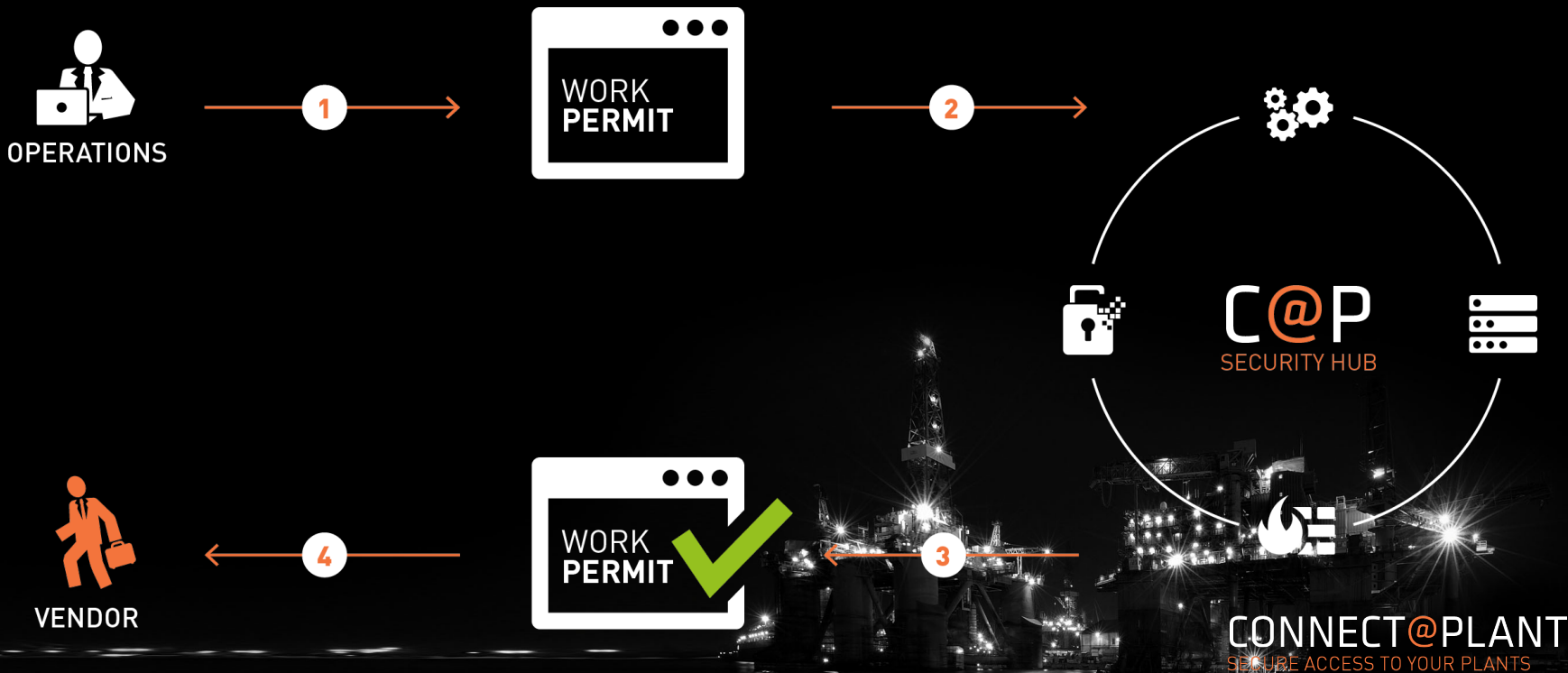
ONSHORE

OFFSHORE



WP – WORKFLOW

C@P WAY



REMOTE CONNECTION

DEVICE CONTROL



SMS / MOBILE



VENDOR

ANTI VIRUS



WINDOWS
UPDATE

1

SECURE CONNECTION



C@P
SECURITY HUB



2



✓ PATCH
VIRUS SCAN



FILE TRANSFER



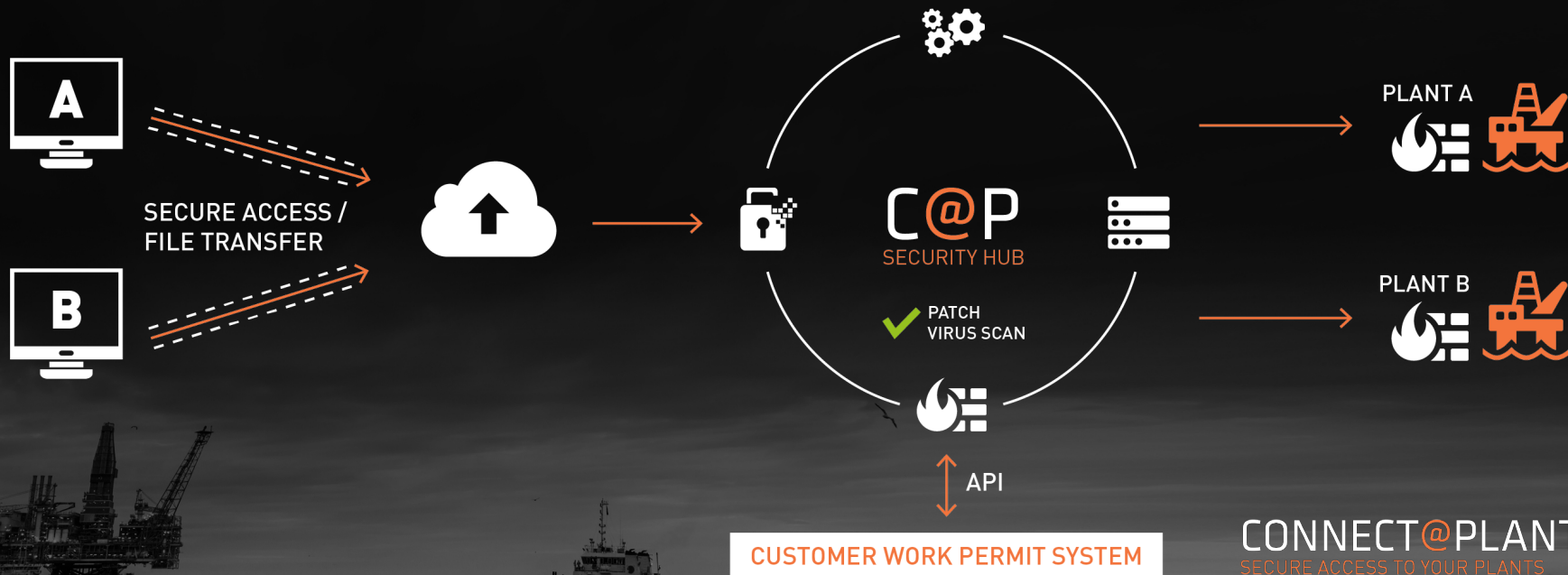
CONNECT@PLANT
SECURE ACCESS TO YOUR PLANTS

SECURITY HUB

OVERVIEW

VENDOR

PLANT



CONNECT@PLANT
SECURE ACCESS TO YOUR PLANTS

ADMISSION CONTROL SYSTEM

DASHBOARD

http://dashboard/ IT Store

Select all Sort on: Name (a-z)

- APP-ALCATEL-4760**
Access to Alcatel 4760 Server
[Request](#) [More...](#)
- APP-DC-UPS-100**
Access DC-UPS-100
[Request](#) [More...](#)
- APP-Plant-HMI Client**
Access to Plant - HMI Client
[Request](#) [More...](#)
- APP-SAS-PureFlex-Chassis**
Access to SAS PureFlex Chassis
[Request](#) [More...](#)
- Create AD groups for new Service**
Creates group for Endservice Access and a group for User Qualification to the service
[Request](#) [More...](#)
- Create new user**
Lets the supervisor create new users.
[Request](#) [More...](#)
- Create Work Permit**
Manual registration of new Work Permit
[Request](#) [More...](#)
- Notepad Service**
Creates and edits text files using basic text formatting.
[Request](#) [More...](#)
- Register e-mail address**
Register your e-mail address for use with self-service password management.
[Request](#) [More...](#)
- Report - Weekly Transactions**
Report of this weeks transactions
[Request](#) [More...](#)
- Self-service Password Reset**
Self-service password reset allows end users to reset their password 24/7, 365 days per year without the need ...
[Request](#) [More...](#)

Logout
Messages
English

CONNECT@PLANT
SECURE ACCESS TO YOUR PLANTS

ADMISSION CONTROL SYSTEM

SYSTEM DETAILS



Work Permit for "Platform - HMI Client - Netop"

About

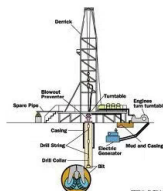


Request

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 communication 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.



HR OVERVIEW

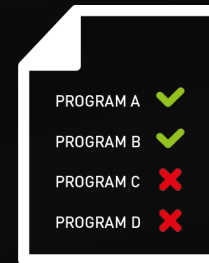
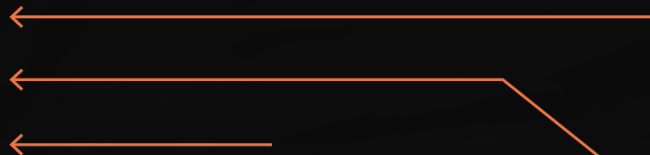
ACCESS MATRIX



VENDOR



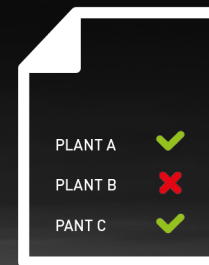
CONTRACT



PREDEFINED APPLICATIONS



EXTERNAL CHECKS



PREDEFINED PLANTS

CONNECT@PLANT
SECURE ACCESS TO YOUR PLANTS

HR OVERVIEW

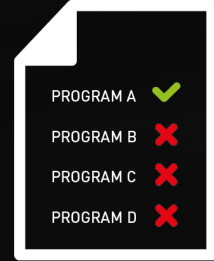
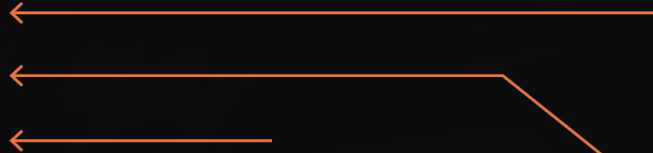
WORK PERMIT



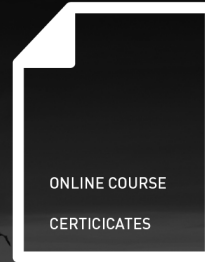
VENDOR



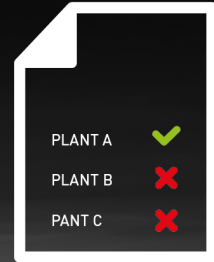
WORK PERMIT



PREDEFINED APPLICATIONS



EXTERNAL CHECKS

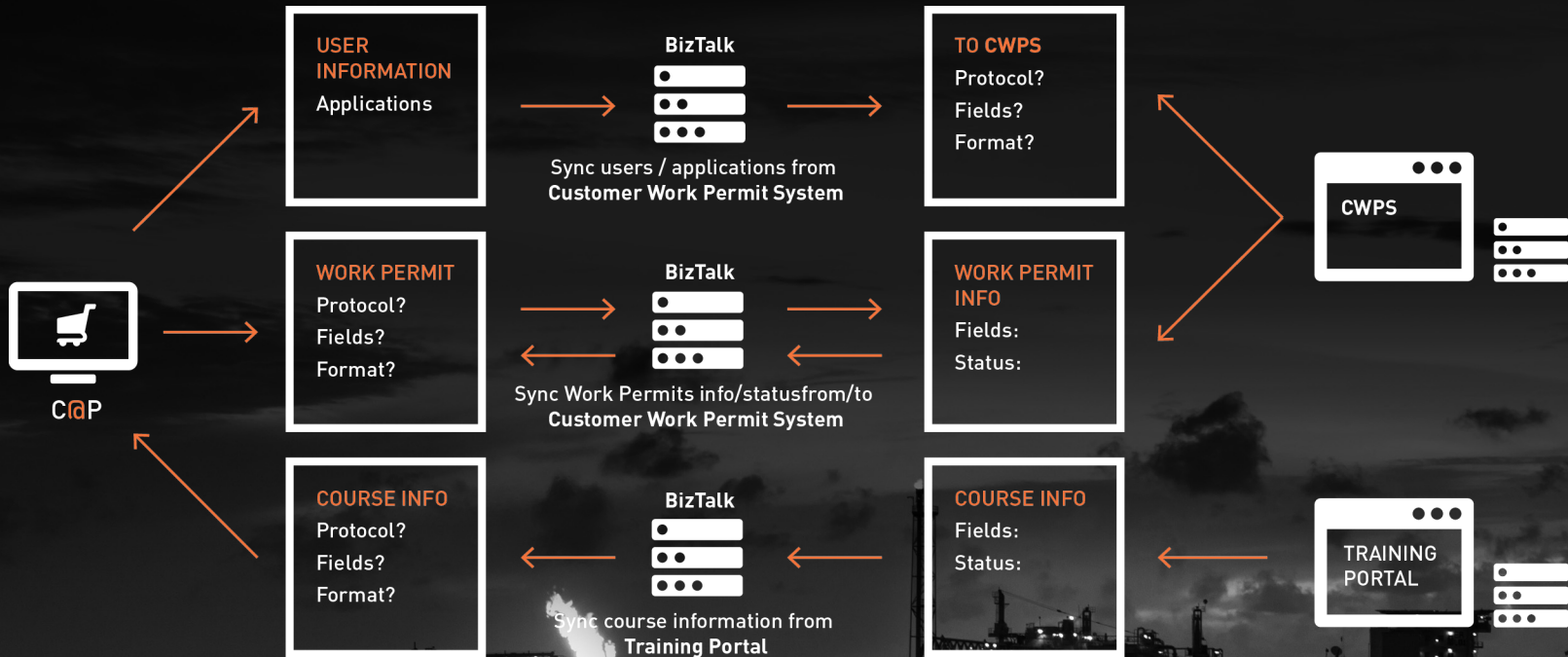


PREDEFINED PLANTS

CONNECT@PLANT
SECURE ACCESS TO YOUR PLANTS

INTEGRATION

BIZTALK



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
- Legal 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

System Status

- Work Permits (active) 2
- Work Permits (pending) 2
- Work Permits (closed) 5 (last 7 days)

System Messages

System Maintenance Scheduled at 05.10.2014 23:00

- AD user sync 06.10.2014 12:40
- WP sync 06.10.2014 12:10

Work Permit Status

Work Permit status: Active Pending Closed Refresh

Work Permit	Status	Percentage
WP-101	Platform - Monitoring	90 %
WP-102	Platform - HMI Client	0 %
WP-103	Platform - OPIS Client	100 %
WP-104	Platform - Drilling status	5 %
WP-105	Platform - HMI Client	0 %

WP-104 Platform - Drilling status

Username: Roger

StartTime: 2014-10-06 08:00

EndTime: 2014-10-10 16:00

Job description: Upgrade software to version 5.0. This version supports the new equipment. The upgrade has been tested and approved by supervisor.

Details: [Click for details](#)

Reports

Activity last Month Generate

SIEM Status

Source IP	Source Port	Destination IP	Destination Port	Source Bytes	Destination Bytes	Total Bytes	Source Packets	Destination Packets	Total Packets	Protocol	Application
10.200.203.163	60851	10.200.204.11	88	2 842	5 872	2 930	0	10	20	tcp	Misc/Arbiter
10.200.14.35	1985	224.0.0.2	1985	2 596 (C)	0	2 536	26	0	26	udp	Other
10.200.51.41	56372	128.199.163.58	53	237	237	474	2	2	4	udp	Other
10.200.202.10	60775	10.200.204.11	135	1 220	2 428	3 648	12	12	24	tcp	FileTransfer/DCOM
10.200.214.1434	17500	255.255.255.255	17500	1 244 (C)	0	1 244	8	0	8	udp	Other
10.200.204.11	53690	10.157.6.26	53	174	174	348	2	2	4	udp	Misc/domain
10.200.202.181	53173	10.200.204.98	89	7 738	7 726	15 464	16	16	32	tcp	Web/Win.Misc
10.200.201.198	137	10.200.204.11	137	528	528	1 056	6	6	12	udp	FileTransfer/NETBIOS
10.200.210.230	N/A	10.200.110.38	N/A	320	180	500	5	3	8	icmp	ICMP Echo-Reply
10.200.210.44	N/A	10.200.110.1	N/A	128	84	212	2	1	3	icmp	ICMP Echo-Reply
10.200.203.210	57066	10.200.204.109	8320	18 765	18 753	37 518	20	20	40	tcp	Other
10.200.201.155	63160	10.200.204.11	445	5 934	5 922	11 856	22	22	44	tcp	DataTransfer/Windows/rdp
10.200.201.4	123	10.200.204.11	123	84	96	180	1	1	2	udp	Misc/FTP
10.200.202.34	64888	10.200.204.11	135	7 776	1 764	9 540	16	16	32	tcp	FileTransfer/DCOM
10.200.200.67	58804	10.200.204.212	135	5 271	5 259	10 530	16	16	32	tcp	FileTransfer/DCOM
10.200.204.170	57865	27.46.114.191	89	400	448	848	5	5	10	tcp	Web/Win.Misc
10.200.201.691	60956	10.200.200.8	8090	59 128	59 128	100 256	69	69	138	tcp	Other
10.200.201.159	49191	10.200.204.11	445	6 481	6 409	12 890	22	22	44	tcp	DataTransfer/Windows/rdp
10.200.201.216	59687	10.200.204.212	135	5 553	5 541	10 094	16	16	32	tcp	FileTransfer/DCOM
10.200.219.24.96	45553	10.200.210.14	161	168	159	327	2	2	4	udp	Misc/comp
10.200.219.24.96	N/A	10.200.210.14	N/A	64	0	64	1	0	1	icmp	ICMP Echo-Reply
10.200.219.24.96	38918	10.200.210.12	23	64	63	127	1	1	2	udp	RemoteAccess/rdp
10.200.210.230	59737	10.200.204.118	135	3 332	3 320	6 652	13	13	26	tcp	FileTransfer/DCOM
10.200.8.124	53033	10.200.204.211	89	0	831 696 (C)	831 696	0	668	668	tcp	Web/Win.Misc
10.200.201.56	54534	10.200.204.31	22029	59 712 (C)	0	59 712	236	0	236	tcp	Other
10.200.24.21	5100	10.200.49.31	5000	0	2 388 (C)	2 388	0	37	37	udp	Multimedia/Intel
10.200.201.190	60553	10.200.204.31	22029	192 (C)	0	192	3	0	3	tcp	Other
10.200.210.230	59738	10.200.204.200	135	3 340	3 328	6 668	13	13	26	tcp	FileTransfer/DCOM
10.200.209.83	52031	10.166.166.213	443	5 243	5 231	10 474	19	19	38	tcp	Web/SecureShell
10.200.201.20	57600	10.200.204.11	53	160	160	320	2	2	4	udp	Misc/domain
10.200.201.57	64799	127.0.0.105.105	89	184	172	356	5	4	9	tcp	Web/Win.Misc
10.163.13.129	30444	10.195.88.95.67	89	756	756	1 512	5	5	10	tcp	Web/Win.Misc
10.200.210.230	59719	10.200.204.81	1027	119 562	119 510	239 072	218	218	436	tcp	Other
10.200.210.230	59712	10.200.204.81	135	3 208	3 208	6 416	13	13	26	tcp	FileTransfer/DCOM
10.200.201.230	59710	10.200.204.89	135	3 846	3 834	7 680	13	13	26	tcp	FileTransfer/DCOM
10.200.201.230	59708	10.200.204.12	89	3 660	3 660	7 320	12	12	24	tcp	Misc/Arbiter
10.200.208.14	59416	10.200.204.12	89	199	199	398	2	2	4	udp	Misc/domain

SCOM Status

SC Advisor Dashboard

Welcome, Stefan SCU Help Feedback Sign out

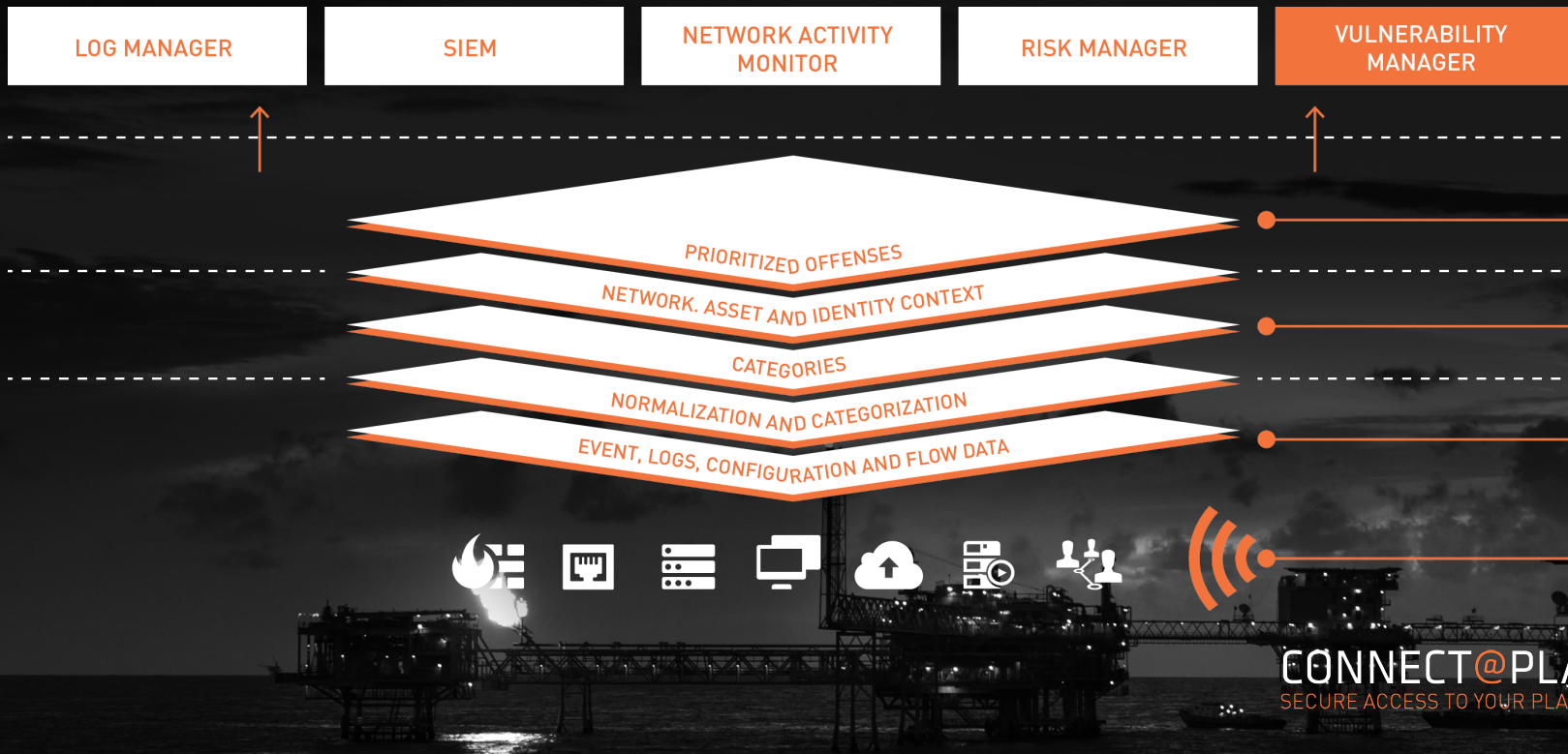
Overview Overall System Status

Alerts View all alerts

By Server: 1 Critical 3 Warning 4 Not Alerts

By Area: SQL Server VMM

IBM QRADAR



IBM QRADAR



CORRELATION

Logs/events
Flows
IP reputation
Geographic location

ACTIVITY BASELINING & ANOMALY DETECTION

User activity
Database activity
application activity
Network activity

OFFENCE IDENTIFICATION

Credibility
Severity
Relevance

TRUE OFFENCE

SUSPECTED INCIDENTS

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

