



Cyber pirates and hack-activists A clear and present danger

Vlasis Theodorou
Sales Director
Obrela Security Industries

Digital Ships, Digital Crime

DESPITE THE SIGNIFICANT BUSINESS AND OPERATIONAL COSTS ASSOCIATED WITH A SYSTEM BREACH, BOTH SHORE AND SHIP SIDES ARE STILL LACKING IN ABILITY OR WILLINGNESS TO MANAGE THE RISK THROUGH A COMPREHENSIVE RESPONSE TO CYBERCRIME.



Digital Ships, Digital Challenges

THE LEVEL OF IT/OT CYBERSECURITY SKILLSET NEEDED IS INCREASING AND SO IS THE COST OF FINDING SPECIALISTS

IN AN EXPANDING DIGITAL SURFACE, THAT INCLUDES IT AND OT, NON-UNIFIED STACKS INCREASE COMPLEXITY

TRADITIONAL CONSOLE MONITORING OF ALERTS IS NOT COST/TIME EFFECTIVE

TECHNOLOGY PRODUCTS ALONE CANNOT OVERCOME LACK OF PROCESS, EXPERTISE, AND RESOURCES

RISK OF NONCOMPLIANCE WITH IMO, RELEVANT NATIONAL, INTERNATIONAL AND FLAG STATE REGULATIONS OR GUIDELINES IS JUST TOO BIG TO IGNORE



Digital Ships, Digital Opportunities

IN AN INCREASINGLY COMPETITIVE MARITIME INDUSTRY, LEADING SHIPPING COMPANIES ARE USING TECHNOLOGY TO TRANSFORM THEIR BUSINESSES AND INCREASE THEIR COMPETITIVENESS.

AS CYBER ATTACKS AGAINST VESSELS INCREASE, GLOBAL CHARTERERS AND OIL MAJORS WILL HAVE TO MANAGE SUCH RISK, THROUGH REVISED VETTING SCORES.

INSURERS ARE ALSO ADDRESSING CYBER RISK MANAGEMENT AND BUILDING IT INTO THEIR RATES OR OFFERING CYBER INSURANCE AS AN ADD ON. CYBER SECURED VESSELS WILL HAVE AN OPERATIONAL COST ADVANTAGE.



What types of threats?

OBRELA'S DIGITAL UNIVERSE STUDY FOR Q2 2021

OIL & GAS EXPERIENCED THE BIGGEST INCREASE IN ATTACKS:

- 18% INCREASE IN ATTACKS ON ITS USERS AND ENDPOINTS
- 22% INCREASE IN ATTACKS ON ITS CLOUD ENVIRONMENTS
- 12% INCREASE IN ATTACKS ON ITS IT INFRASTRUCTURE
- 29% INCREASE IN ATTACKS ON ITS SYSTEM / PERIMETERS
- 14% INCREASE IN WEB ATTACKS
- 22% INCREASE IN APT / MALWARE ATTACKS



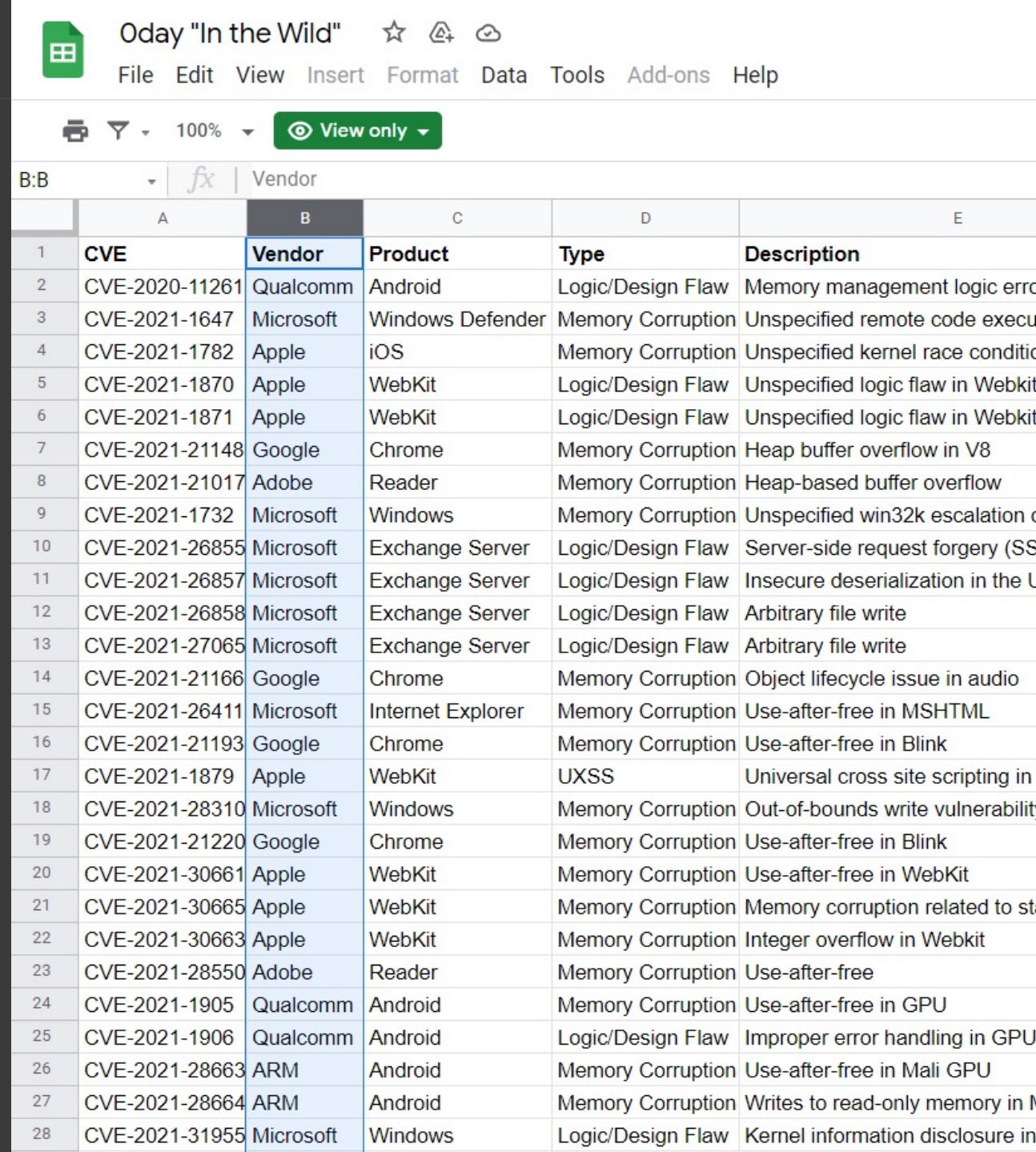
Emerging threat: Zero-Day Exploits

A ZERO-DAY EXPLOIT IS A SOFTWARE SECURITY FLAW THAT CYBERCRIMINALS ARE AWARE OF AND CAN EXPLOIT IT UNTIL THE VENDOR CREATES THE PATCH TO FIX THE FLAW.

THE SEPT 2021 MIT TECHNOLOGY REVIEW SHOWS THAT SO FAR IN 2021 WE HAVE HAD 66 NEW ZERO-DAY EXPLOITS, ALMOST DOUBLE THE ONES WE HAD LAST YEAR.

ONCE DISCOVERED ZERO-DAY VULNERABILITIES CARRY A PRICE TAG OF UPWARD OF \$1M IN BIDDING WARS BETWEEN GOVERNMENT SPONSORED HACKERS AND ORGANIZED CYBERCRIME.

THE TIME IT TAKES FOR AN OEM VENDOR TO BECOME AWARE OF THE FLAW AND PRODUCE A PATCH, IS THE TIME GAP THAT CYBERCRIMINALS THRIVE ON.



	A	B	C	D	E
1	CVE	Vendor	Product	Type	Description
2	CVE-2020-11261	Qualcomm	Android	Logic/Design Flaw	Memory management logic error
3	CVE-2021-1647	Microsoft	Windows Defender	Memory Corruption	Unspecified remote code execu
4	CVE-2021-1782	Apple	iOS	Memory Corruption	Unspecified kernel race conditio
5	CVE-2021-1870	Apple	WebKit	Logic/Design Flaw	Unspecified logic flaw in Webkit
6	CVE-2021-1871	Apple	WebKit	Logic/Design Flaw	Unspecified logic flaw in Webkit
7	CVE-2021-21148	Google	Chrome	Memory Corruption	Heap buffer overflow in V8
8	CVE-2021-21017	Adobe	Reader	Memory Corruption	Heap-based buffer overflow
9	CVE-2021-1732	Microsoft	Windows	Memory Corruption	Unspecified win32k escalation o
10	CVE-2021-26855	Microsoft	Exchange Server	Logic/Design Flaw	Server-side request forgery (SS
11	CVE-2021-26857	Microsoft	Exchange Server	Logic/Design Flaw	Insecure deserialization in the U
12	CVE-2021-26858	Microsoft	Exchange Server	Logic/Design Flaw	Arbitrary file write
13	CVE-2021-27065	Microsoft	Exchange Server	Logic/Design Flaw	Arbitrary file write
14	CVE-2021-21166	Google	Chrome	Memory Corruption	Object lifecycle issue in audio
15	CVE-2021-26411	Microsoft	Internet Explorer	Memory Corruption	Use-after-free in MSHTML
16	CVE-2021-21193	Google	Chrome	Memory Corruption	Use-after-free in Blink
17	CVE-2021-1879	Apple	WebKit	UXSS	Universal cross site scripting in
18	CVE-2021-28310	Microsoft	Windows	Memory Corruption	Out-of-bounds write vulnerability
19	CVE-2021-21220	Google	Chrome	Memory Corruption	Use-after-free in Blink
20	CVE-2021-30661	Apple	WebKit	Memory Corruption	Use-after-free in WebKit
21	CVE-2021-30665	Apple	WebKit	Memory Corruption	Memory corruption related to st
22	CVE-2021-30663	Apple	WebKit	Memory Corruption	Integer overflow in Webkit
23	CVE-2021-28550	Adobe	Reader	Memory Corruption	Use-after-free
24	CVE-2021-1905	Qualcomm	Android	Memory Corruption	Use-after-free in GPU
25	CVE-2021-1906	Qualcomm	Android	Logic/Design Flaw	Improper error handling in GPU
26	CVE-2021-28663	ARM	Android	Memory Corruption	Use-after-free in Mali GPU
27	CVE-2021-28664	ARM	Android	Memory Corruption	Writes to read-only memory in M
28	CVE-2021-31955	Microsoft	Windows	Logic/Design Flaw	Kernel information disclosure in

It gets worse: OT is exposed

BY DEFINITION, ZERO-DAY ATTACKS ARE DIFFICULT TO DEFEND AGAINST.


THE ABILITY TO ANALYZE LOGS AND IDENTIFY EXPLOIT-LIKE BEHAVIOR IS KEY TO MINIMIZE THE TIME WINDOW FOR DAMAGE AND RISK.

WHILE THE MARITIME INDUSTRY HAS ADDRESSED CYBERSECURITY ON THE SHORE, THE SHIP IT REMAINS EXPOSED AND THE SHIP OT EVEN MORE SO.

ON THE SHORE SIDE CYBERCRIME TRANSLATES TO RANSOMWARE COSTS AND DOWNTIME.

ON THE SHIP SIDE, AND ESPECIALLY ON THE OT SYSTEMS HUMAN ERRORS, INSIDER THREATS OR EXTERNAL CYBER-ACTORS CAN POSE A DANGER TO THE CREW, DAMAGE THE VESSEL OR CAUSE AN ENVIRONMENTAL DISASTER.





**We keep your business
in business**

**WE USE SECURITY ANALYTICS AND SOPHISTICATED RISK
AND THREAT MANAGEMENT TECHNOLOGY TO
DYNAMICALLY PROTECT OUR CLIENTS BY IDENTIFYING,
ANALYZING PREDICTING AND PREVENTING CYBER THREATS
IN REAL-TIME**



**YOUR
OPERATIONAL
TECHNOLOGY**



**YOUR
APPLICATIONS &
INFRASTRUCTURE**



**YOUR
CLOUD**

**WE COVER ALL YOUR DIGITAL UNIVERSE,
ROUND THE CLOCK AND IN REAL TIME**



**YOUR VESSELS
IN THE SEA**



**YOUR WORK FROM
HOME USERS**



**YOUR BRAND
REPUTATION**

OSI's Services

MANAGED THREAT DETECTION AND RESPONSE (MDR)

A TURNKEY THREAT DETECTION AND RESPONSE SERVICE THAT SIGNIFICANTLY REDUCES THE MEAN TIME TO DETECT AND RESPOND TO CYBERATTACKS

MANAGED CYBER RISK AND CONTROLS (MRC)

A COMPREHENSIVE SUITE OF RISK MANAGEMENT SERVICES THAT ENHANCE SECURITY OPERATIONS WITH REAL TIME VISIBILITY IMPROVING SITUATIONAL AND RISK AWARENESS

ADVISORY SERVICES

OBRELA'S ELITE TEAM OF CYBERSECURITY EXPERTS PROVIDE SERVICES TO INCREASE YOUR ORGANIZATION'S RESILIENCE

The Vessel Threat Management Solution

OBRELA'S VESSEL THREAT MANAGEMENT SYSTEM (VTMS) IS A CENTRALISED, SELF-CONTAINED PASSIVE NETWORK MONITORING SOLUTION BASED ON A VIRTUAL APPLIANCE, THAT ALSO SUPPORTS LOG COLLECTION FROM THE VESSEL'S INFRASTRUCTURE

OBRELA EDRaaS IS A STATE-OF-THE-ART ENDPOINT DETECTION AND RESPONSE SOLUTION FOR THE IT SYSTEMS ON BOARD (OPTIONAL)

OBRELA SOCaaS LEVERAGES THE VIRTUAL APPLIANCE TO COLLECT LOGS FROM IT AND OT THREAT DETECTION DEVICES, ENABLING SOC-AS-A-SERVICE MONITORING AND THREAT HUNTING

NATIVE INTEGRATION WITH OT SECURITY MONITORING PLATFORMS SUCH AS **TENABLE.OT**

From Raw Data to Finished Intelligence as a managed service

RAW INTELLIGENCE DATA



FINISHED ACTIONABLE INTELLIGENCE



24/7 MONITORING AND ALERT MANAGEMENT

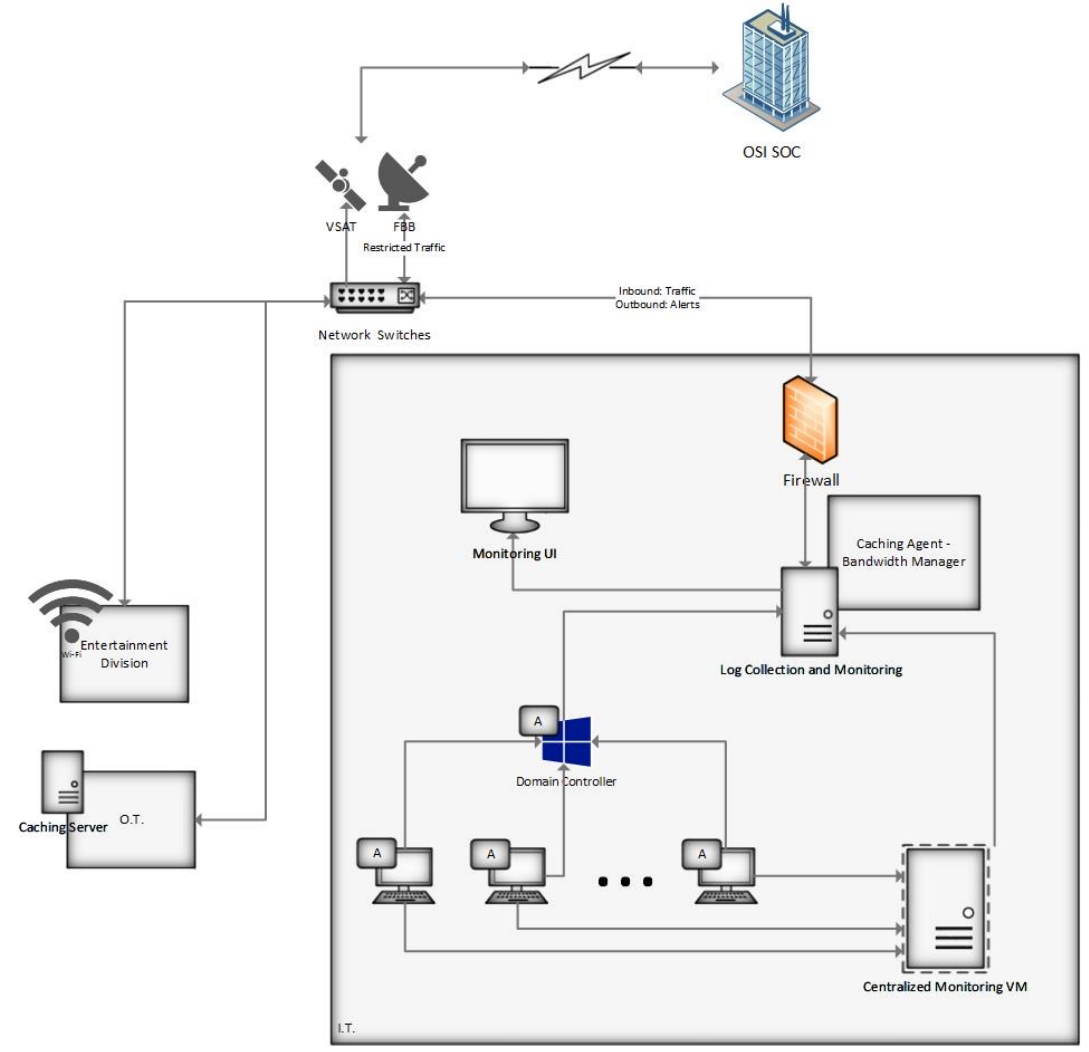
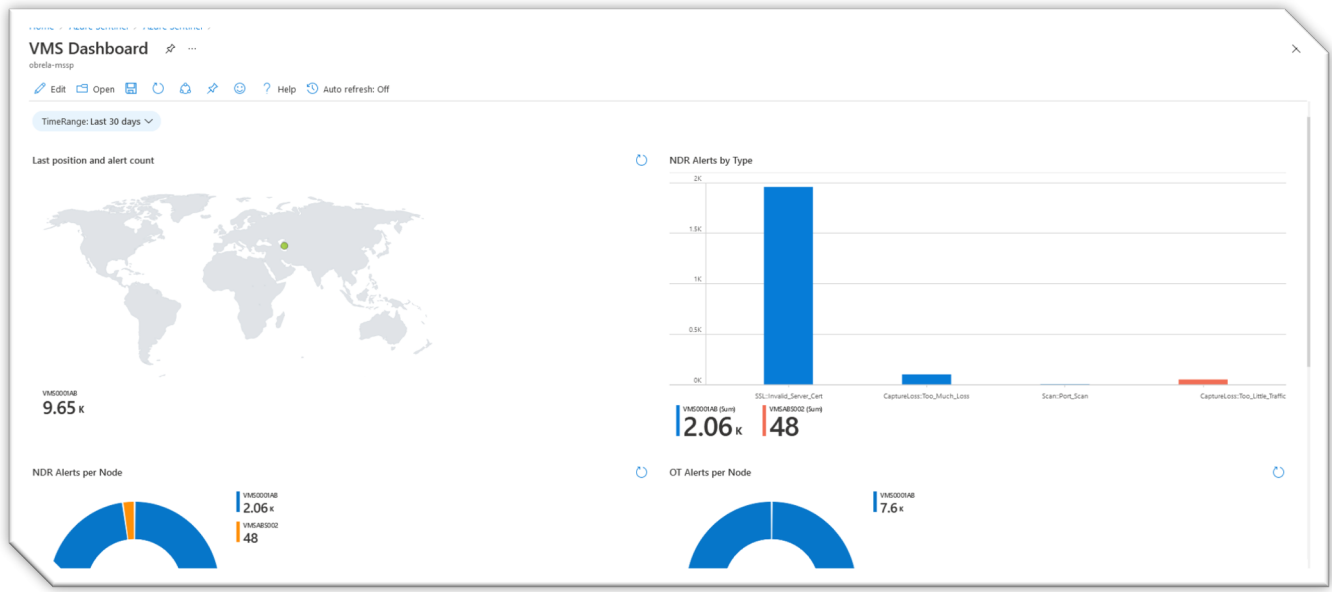


ACTIONABLE ANALYTICS AND REPORTING



ADVANCED THREAT HUNTING AND INTELLIGENCE

Obrela's Vessel Threat Management Solution



Vessel Threat Management Solution features

REAL TIME SIGNATURE AND ANOMALY BASED THREAT DETECTION

INTELLIGENCE BASED THREAT DETECTION

ALERT CRITICALITY PRIORITIZATION – FORWARDS ONLY IMPORTANT ALERTS

WHEN THE SHIP IS OFFLINE, A MINIMAL WEB UI IS AVAILABLE FOR THE CREW TO MONITOR SECURITY ALERTS

A CASHING AGENT STORES ALERTS AND FORWARDS THEM TO OSI'S SOC FOR ANALYSIS, WHEN SHIP IS BACK ONLINE

AUTOMATIC BANDWIDTH MANAGEMENT OF AVAILABLE CONNECTIVITY OPTIONS (I.E. BETWEEN VSAT and FBB)

REMOTE MANAGEMENT OF VTMS DEPLOYMENT (BASED ON COMPANY'S REMOTE ACCESS POLICY)

OBRELA EDRaaS features

MULTI-LAYERED PROTECTION BUILT INTO THE ENDPOINT AND CLOUD. PROTECTS FROM FILE-BASED MALWARE, MALICIOUS SCRIPTS, MEMORY-BASED ATTACKS AND OTHER ADVANCED THREATS

CONTEXTUAL THREAT REPORTS PROVIDE NEAR REAL TIME VISIBILITY ON HOW THREATS IMPACT YOUR COMPANY

THREAT DISCOVERY, PRIORITIZATION AND REMEDIATION FOR A COMPREHENSIVE THREAT & VULNERABILITY MANAGEMENT

BEHAVIORAL DETECTIONS WITH DEEP INSIGHTS ON KERNEL/MEMORY INTERACTIONS ON SERVERS, W/S AND FILES/IP/URL

THREAT CONTAINMENT MINIMIZES RISK BY RESPONDING WHEN AND WHERE THREATS ARE DETECTED

FROM DETECTION TO REMEDIATION IN MINUTES AND AT SCALE

LEVERAGING AI TO AUTOMATICALLY ANALYSE LOGS, SUGGEST COURSE OF ACTION AND REMEDIATE THREATS IN MINUTES

WATCH YOUR SECURE SCORE IN REAL TIME AS IT RISES DUE TO AUTOMATED ACTIONS THAT PROTECT USERS AND DATA

MULTIPLE DEPLOYMENT OPTIONS TO ACCOMMODATE LOGISTICS AND AVAILABILITY OF VESSEL AND CREW

OBRELA Vessel Monitoring SOCaas features

- 24x7x365 THREAT MONITORING
- EDR BASELINE MANAGMENT: INSTALLATION SUPPORT, BASELINE CONFIGURATION
- ACTIONABLE INCIDENTS MANAGEMENT AND ESCALATION
- ACTIVE INCIDENT CONTAINMENT AT THE ENDPOINT
- THREAT HUNTING
- REMOTE SECURITY INCIDENT SUPPORT UNTIL CLOSURE
- THREAT ERADICATION RECOMMENDATIONS
- LOG RETENTION
- MDR INTEGRATION
- INCIDENT RESPONCE SERVICES: POST INCIDENT INVESTIGATION, MALICIOUS CODE ANALYSIS, ROOT CAUSE ANALYSIS
- ADVISORY SERVICES

WHY OBRELA

- GLOBAL FOOTPRINT AND SCALE
- RECOGNISED BY ANALYSTS, TECHNOLOGY VENDORS AND PEERS SUCH AS GARTNER, MICROSOFT AND ABS GROUP
- DOMAIN EXPERTISE AND INTELLECTUAL PROPERTY ALREADY DEVELOPED ARE OFFERED TO OUR CUSTOMERS
- ZERO TIME TO DEPLOYMENT LEVERAGING EXISTING SCALABLE SaaS MODEL
- SEAMLESS INTEGRATION AND SINGLE VIEW ACROSS DIVERSE TOPOLOGIES OF ASSETS AND TECHNOLOGIES
- OFFERED AS A MANAGED SERVICE WITH MULTIPLE SERVICE AND DELIVERY MODELS TO CHOOSE FROM

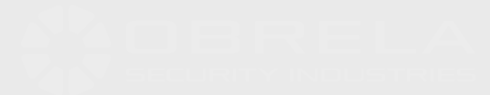
ACKNOWLEDGEMENTS & ACCREDITATIONS



Microsoft
Partner

Silver Application Development
Gold Cloud Platform
Silver Security

Member of
Microsoft
Intelligent
Security
Association



OFFICES

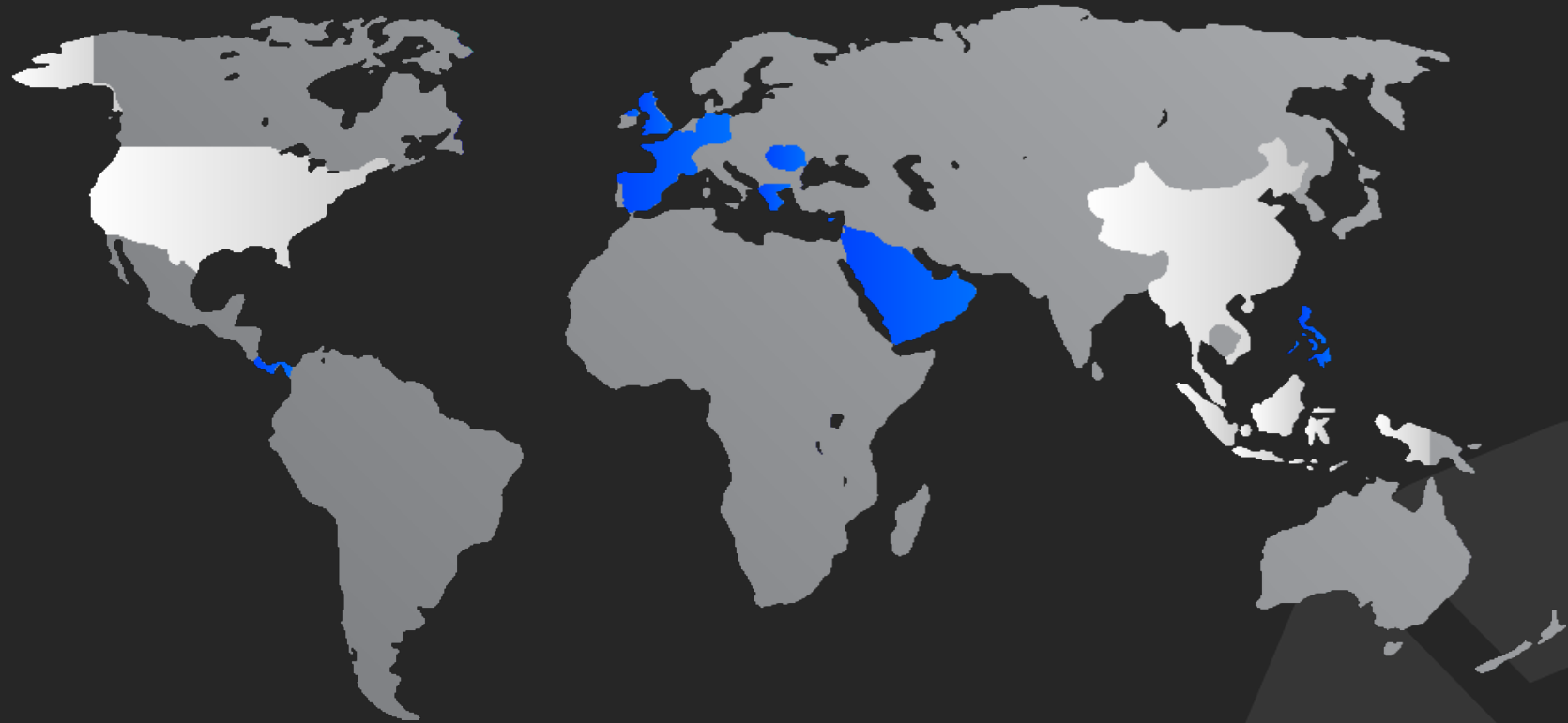
London, HQ

Frankfurt

Athens

Dubai

Riyadh



TECHNOLOGY AND BUSINESS PARTNERS





OBRELA SECURITY INDUSTRIES

© 2021. Published in the UK.
All Rights Reserved.

obrela.com

Thank you