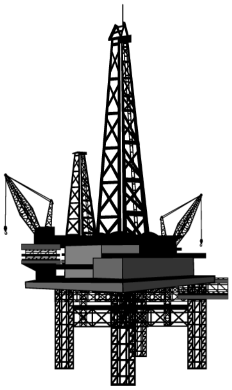
ObsidianRift Energy Co.

Abyssal Pearl



Incident Brief: ICS Compromise on Offshore Platform – Abyssal Pearl
Prepared for: ObsidianRift Energy Co. – Mobile Cybersecurity Response Team
Date: October 1, 2025
Location: Eastern Pacific Ocean, 200 nautical miles off the U.S. West Coast

Our newest and premier fixed offshore oil production platform, the Abyssal Pearl, has been in continuous operation for the past 18 months. The facility currently produces approximately 2,000 barrels of crude oil per day, supported by an integrated industrial control system (ICS) managing wellhead flow, separation, gas compression, flaring, and export operations. These barrels currently are the main source of crude oil for the Western areas of the United States.

An ongoing cyber event is affecting the Abyssal Pearl's ICS infrastructure. Preliminary findings suggest that the compromise originated from equipment introduced by a third-party maintenance contractor, who was onboard the platform for a brief period to service refrigeration units in the rig's galley.

Approximately eight days after the contractor's departure, platform personnel began observing intermittent communication disruptions within the ICS environment. This escalated into a complete 40-second blackout, resulting in all ICS devices simultaneously ceasing communication.

Two days ago, the situation escalated significantly, beginning with the gas compression system, which experienced an unexpected overpressure condition, resulting in a protective shutdown. All HMI terminals across the platform began displaying outdated system data, indicating a possible replay attack or historian compromise. Simultaneously, the flare pilot valve opened, but the igniter failed to activate, posing a severe risk of unburned gas release to the atmosphere. Although fire and gas detection systems remained operational, log data was discovered to be redirected to an unauthorized local storage node, suggesting deeper system manipulation.

As our corporate mobile cybersecurity response team, you are being deployed and stationed on-site at the Abyssal Pearl. Your primary mission is to conduct a comprehensive investigation into the suspected ICS compromise, contain any ongoing threat activity, and prevent escalation that could result in further production disruption, equipment damage, or risk to personnel safety. Your assessment and actions will be critical in determining the operational viability of the platform and guiding the next steps for recovery and system restoration.