maltiverse
Actionable Threat Intelligence

CASE STUDY

Enhancing OT Security in Water Supply with Maltiverse Threat Intelligence

In the water supply sector, the security of operational technologies (OT) is critical to ensure service continuity and the protection of critical infrastructure. Cyber threats against OT systems are increasingly sophisticated and can have devastating consequences, including service disruptions, physical damage to infrastructure, and public health risks. A leading water supply company faced these challenges, needing a solution that not only detected threats early but also enabled efficient and coordinated responses.
Implemented Solution

The integration of Maltiverse Threat Intelligence marked a significant shift in the company's OT security strategy. Maltiverse offers a threat intelligence platform that gathers, enriches, and analyzes indicators of compromise (IoCs) from multiple sources, providing a detailed view of the threat landscape specific to the water sector.

IMPROVEMENTS IN DETECTION AND PROTECTION

The integration of Maltiverse with Security Orchestration, Automation, and Response (SOAR) solutions enabled the company to automate responses to security incidents, significantly reducing response time. This was achieved through:

- Automation of intelligence gathering and data correlation, freeing up valuable SOC resources for critical tasks.
- Implementation of customized incident response playbooks, which trigger automatic actions such as isolating compromised systems and communicating with affected teams.
- Improved collaboration among security, IT, and operations teams, ensuring a coordinated response to incidents.

ADDRESSED CHALLENGES AND PROPOSED SOLUTIONS

- Proactively identifying emerging threats and targeted attacks: The Maltiverse platform enables the identification and analysis of threats specifically targeting water supply operations, significantly improving detection and protection capabilities.
- Enriching security data with contextual information about threats: This improves detection accuracy.
- Automating the correlation of IoCs with internal security events: Speeds up the identification of potential incidents.

ACHIEVED RESULTS

The adoption of Maltiverse Threat Intelligence transformed the company's ability to face the cyber threat landscape. The results include:

- A 40% reduction in threat detection time, allowing the SOC to act preventively rather than reactively.
- Improved efficiency in incident response processes, with a 50% reduction in response time.
- Increased ability to anticipate targeted attacks, thanks to deep and contextual analysis of threat intelligence.

CONCLUSION

The integration of Maltiverse Threat Intelligence into the OT security strategy of a leading water supply company has been crucial in enhancing threat detection and optimizing SOC response processes through automation with SOAR. This proactive and automated approach to cybersecurity not only improves the company's security posture but also ensures the protection of its assets and the trust of its customers in an increasingly threatening environment.

For more information on how Maltiverse can transform OT security in the water supply sector, visit www.maltiverse.com.