CARDINALOPS
Detection Posture Management

CASE STUDY – REPSOL

Repsol Increases SOC Efficiency and Productivity While Fixing Detection Gaps

Leveraging automation to maximize their current coverage and reduce threat exposure

REPSOL

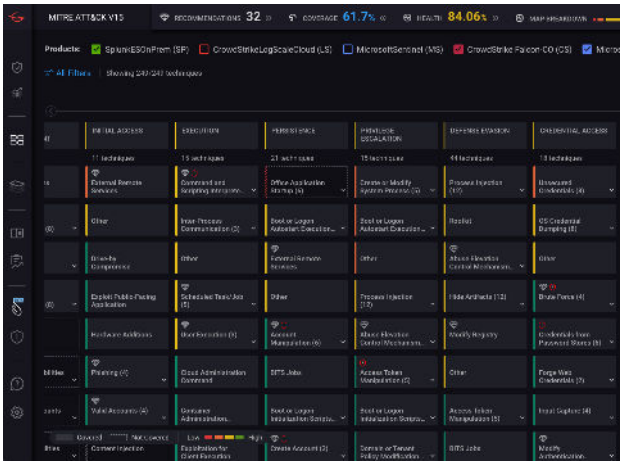
REPSOL

PROFILE

- HQ: Madrid, Spain
- Revenue: $57 Billion
- Employees: 24,000+
- Industry: Energy, Oil & Gas

CHALLENGES

- Multiple-SIEMs
- Increasing volume of data
- Need for more automation



PROBLEM

With over 24,000 employees and global operations, Madrid-based Repsol is a global multi-energy provider that has committed to the ambitious goal of becoming a net zero emissions company by 2050. In order to reach this goal, Repsol is leveraging a wide array of digital transformation initiatives to make operations more efficient and less wasteful. However, this increased reliance on technology also brings additional risk due to a significant increase in the attack surface, both in the cloud and in physical facilities. Combined with the continuously-evolving threat landscape, global geopolitical tensions, and the scarcity of cybersecurity talent, this requires a strategic focus on maximizing the effectiveness of security operations.

SOLUTION

To counter rapidly expanding risks, Repsol brought in the CardinalOps Detection Posture Management platform to accelerate security operations effectiveness. Repsol evaluated different technologies and chose CardinalOps as the best fit to meet its SOC needs and provide visibility and improvement to their overall security posture. In the implementation, the team brought together alignment with the MITRE ATT&CK framework, up-to-date maintenance with CVEs, and internal analysis identifying TTPs of likely threat actors targeting Repsol.

CardinalOps automatically and seamlessly integrates these elements with Repsol's SIEM platforms and provides immediate verification capability of rules so that SOC analysts can be informed on where they have detection coverage and where they have gaps.

CASE STUDY – REPSOL

Maximize Detection Coverage and Fidelity

"CardinalOps is the key piece for us in order to optimize our SOC with automation and the knowledge and expertise of attacker perspectives that they bring. This has led to significant improvements in our ability to detect and respond to attacks more quickly,"

Javier García Quintela
Global CISO, Repsol

RESULTS

As a result of implementing CardinalOps at Repsol, the SOC has successfully improved their detection posture by increasing both the health and coverage of their rules. In only three months, the team configured four times the previous number of rules weekly, increased MITRE ATT&CK coverage from 23% to 56%, received 179 recommendations and fixed 125 rules, and configured precise alerts for critical zero-day and new CVEs.

With CardinalOps, Repsol SecOps significantly increased its speed of response and improved its cost efficiency. The company is now well positioned to build its next-generation SOC based on intelligent automation.

CardinalOps continuously assesses and improves the detection coverage of your SIEM and other detection tools to enable a stronger, more resilient defense.

- Map your current detection coverage to MITRE ATT&CK® for continuous visibility
- Automatically detect and fix broken, misconfigured, and noisy rules
- Receive new, deployment-ready rules and recommendations for the threats relevant to you
- Automate manual tasks to free up team members to perform high-value work