Analysis of and Mitigation Strategies for Real World OT Security Incidents

Nico Fechtner

Technical University of Munich, Arcisstraße 21, 80333 Munich, Germany
nico.fechtner@tum.de
https://www.tum.de/en/

Abstract. The abstract should briefly summarize the contents of the paper in 150–200 words. The goal is to communicate: Background/motivation/context, Aim/objective(s)/problem statement, Approach/method(s)/procedure(s), Results, Conclusion(s)/implications.

Keywords: OT Security · Security Incident · Triton.

1 Introduction

2 Related Work

3 Comparative Overview of OT Security Incidents

3.1 Targets

3.2 Threat Actors

3.3 Techniques

3.4 Dwell Times and Reactions

3.5 Detection and Mitigation Strategies

3.6 Impacts

4 Detailed Analysis of the Triton Attack

4.1 The Petro Rabigh Oil Refinery

4.2 The Attackers' Approach

4.3 Impact

4.4 Attribution

4.5 Prevention of Attacks Targeting SIS

5 Conclusion

References