Malta Pharmaceuticals Limited

RDP Brute Force & Credential Compromise Investigation

Credential-Based Remote Access Intrusion Simulation

Organisation: Malta Pharmaceuticals Limited

Sector: Pharmaceutical Manufacturing & Medical Equipment

Information Security Function: Blue Team (SOC)

Lead Analyst: Joseph Christopher

Date: 02 February 2026

Organisational Overview

Organisation Name:

Malta Pharmaceuticals Limited

Industry:

Pharmaceutical Manufacturing & Medical Equipment Production

Organisation Size:

Mid-sized pharmaceutical organisation with manufacturing, finance, operations, and IT staff.

Business Context

Malta Pharmaceuticals Limited operates critical pharmaceutical manufacturing and medical equipment supply operations from its London-based facilities. Internal Windows endpoints and remote administrative access are used to support operational continuity, financial systems, and internal services.

Due to the sensitivity of intellectual property, operational data, and regulated business processes, secure remote access controls are critical. Credential-based compromise of internal systems presents a material risk to business continuity, regulatory compliance, and organisational reputation.

Introduction

This document presents the final incident response and investigation report for a credential-based RDP intrusion conducted within the Malta Pharmaceuticals internal environment.

Objectives of the Investigation

- Simulate a realistic brute force and credential abuse attack over RDP
- Validate detection and response capabilities across endpoint, SIEM, and network telemetry
- Perform root-cause analysis using evidence-based SOC workflows
- Assess control effectiveness and detection gaps
- Produce professional, audit-defensible documentation suitable for portfolio presentation

All findings were validated using correlated telemetry, and no conclusions were drawn from single-source alerts.

Scope of Investigation

In Scop

Windows endpoint authentication telemetry

RDP access and authentication behaviour

Account lockout policy enforcement

SIEM correlation and investigation (Splunk)

Firewall and IDS telemetry

Endpoint detection visibility (Microsoft Defender XDR)

SOC investigation, response, and review

Out of Scope

Data access or modification

Privilege escalation attempts

Persistence mechanisms

Full memory or disk forensics

Cloud identity systems

Tools & Telemetry Sources

The investigation relied on multiple corroborating telemetry sources:

Kali Linux (Remmina RDP Client) Manual credential testing

Windows Security Event Logs Authentication and account activity

Splunk Enterprise Centralised log ingestion, correlation, and investigation

pfSense Firewall Network traffic visibility

Suricata IDS Network intrusion detection

Microsoft Defender XDR Endpoint detection and automated investigation

Investigation Methodology

The investigation followed a structured SOC Workflow

Detection → Triage → Correlation → Investigation → Response → Review

All analysis was time-bounded to the confirmed incident window (19:15–20:30 UTC) and conducted manually to mirror real-world SOC operations.

Detection & Analysis Approach

An evidence-based correlation model was applied:

Windows authentication failures analysed for brute force patterns

Account lockout events validated to confirm policy enforcement

Successful RDP authentication correlated with prior failed attempts

Network telemetry reviewed to validate access paths

Endpoint detection tools reviewed for alerting and response behaviour

No alert was treated in isolation. All conclusions were supported by log correlation.

Artifacts & Evidence

Indicators & Forensic Artifacts Reviewed

Repeated failed RDP authentication events (Windows Event ID 4625)

Account lockout enforcement (Windows Event ID 4740)

Successful RDP login using valid credentials (Windows Event ID 4624)

Authentication source IP correlation

Network telemetry indicating internal east–west traffic

Endpoint detection telemetry (absence of alerts)

All artifacts were reviewed and correlated within Splunk.

MITRE ATT&CK Mapping

Observed activity was mapped as follows:

T1110 – Brute Force

T1110.001 – Password Guessing

T1078 – Valid Accounts

T1021.001 – Remote Services (RDP)

No Evidence Observed Of:

Execution

Persistence

Privilege escalation

Lateral movement

Response & Containment Actions

Upon confirmation of successful credential-based RDP access, the following actions were taken:

RDP session immediately terminated after access validation

No commands executed and no data accessed

Compromised account identified for credential reset (real-world action)

Authentication telemetry reviewed for additional misuse

Continued monitoring applied during and after the incident window

No persistence or follow-on activity was observed.

Mitigation & Hardening Measures

Post-incident actions focused on reducing future risk:

Enforce Multi-Factor Authentication (MFA) for all RDP access

Restrict RDP exposure using IP allow-listing or gateways

Strengthen SIEM alerting for authentication abuse

Review and reduce unnecessary RDP-enabled endpoints

Improve east–west traffic visibility

Playbook, Process & Operations

The investigation adhered to a repeatable SOC playbook:

Detection → Triage → Correlation → Investigation → Response → Review

Although manual investigation was used, all workflows are compatible with automation and SOAR integration.

MTTR & SOC Performance Metrics

Mean Time to Detect (MTTD): Minutes after brute force escalation

Mean Time to Investigate (MTTI): 45 minutes

Mean Time to Respond (MTTR): Within the same operational window

Lessons Learned

Aligned with NIST CSF principles:

Identify: Credential exposure remains a critical attack vector

Protect: Account lockout policies significantly reduce brute force impact

Detect: SIEM correlation is essential for valid-credential attacks

Respond: Rapid session termination prevents escalation

Recover: Continuous monitoring closes the incident lifecycle

Recommendations & Future Improvements

Enforce MFA for all remote administrative access

Implement RDP gateways or Zero Trust access models

Enhance detection for credential abuse scenarios

Formalise SOC response playbooks for authentication incidents

Conduct regular credential hygiene reviews

Final Summary

This project demonstrates Malta Pharmaceuticals Limited’s SOC capability to detect, investigate, and respond to a credential-based RDP intrusion using industry-standard tools and professional methodologies.

The investigation was evidence-driven, structured, and aligned with real-world SOC best practices, accurately reflecting mature Blue Team operations within a regulated pharmaceutical environment.