



# Rule Deployment into a Data Plane

Uncoder AI

**In production**

Detection Rules

AI Tools

Save As

Contr

Notepad Password Files Discovery

```
1 title: Notepad Password Files Discovery
2 id: 3b4e950b-a3ea-44d3-877e-432071990709
3 status: experimental
4 description: Detects the execution of Notepad to open a fi
5 which may indicate unauthorized access to credentials or
6 references:
7 - https://thedfirreport.com/2025/02/24/confluence-explo
8 - https://intel.thedfirreport.com/eventReports/view/57
9 author: The DFIR Report
10 tags:
11 - attack.discovery
12 - attack.ti083
13 date: 2025-02-21
14 logsource:
15 product: windows
16 category: process_creation
17 detection:
18 selection:
19 ParentImage|endswith: \explorer.exe
20 Image|endswith: \notepad.exe
21 CommandLine|endswith:
22 - password*.txt
23 - password*.csv
24 - password*.doc
25 - password*.xls
26 condition: selection
27 falsepositives:
28 - Legitimate use of opening files from remote hosts by a
```

Deploy to Microsoft Sentinel

Data Plane

Microsoft Sentinel (QA-lab)

Content name ⓘ

Notepad Password Files Discovery

Code

```
"displayName": "Notepad Password Files Discovery by The DFIR Report",
"description": "Detects the execution of Notepad to open a file that has
the string '\\password\" which may indicate unauthorized access to
credentials or suspicious activity. Author: The DFIR Report. Rule ID
: 3b4e950b-a3ea-44d3-877e-432071990709. License: https://github.com
/Neo23x0/sigma/blob/master/LICENSE.Detection.Rules.md. Reference:
https://tdm.socprime.com/tdm/info/.",
"severity": "low",
"enabled": true,
"query": "SecurityEvent | where EventID == 4688 | where
(ParentProcessName endswith @'\\explorer.exe' and NewProcessName
endswith @'\\notepad.exe' and (CommandLine endswith @'password*.txt'
or CommandLine endswith @'password*.csv' or CommandLine endswith
@'password*.doc' or CommandLine endswith @'password*.xls')) | extend
AccountCustomEntity = TargetUserName | extend HostCustomEntity =
```

Cancel Deploy

Translate functions with Gpt-4o-Mini ⓘ

TRANSLATE

Save As

How it works?

# Rule Deployment into a Data Plane

## **Directly deploy rules into your Microsoft Sentinel, Google SecOps or Elastic Stack:**

- Reduces Time-to-Detection by automating the rule deployment pipeline, eliminating manual steps and accelerating threat detection rollout
- Increases operational efficiency by cutting down engineering overhead for security teams managing rule life cycles across multiple SIEM environments
- Improves consistency and accuracy by minimizing human error