



Search Threat Detection Marketplace

Uncoder AI

In production

Q Detection Rules



Platform Repositories

Select All

SOC Prime

Roota

Threat Bounty

SigmaHQ/sigma

Azure/Azure-Sentinel

Community

Active Threat IOCs

Blitzkrieg/sigma-rules

The-DFIR-Report/Sigma-Rules

Espresso/sigma-rules

Platform Repos My Repos HOT OSINT Indicators

Possible RDP Resource Redirection Patterns (via file_event)

Author: SOC Prime Team

Possible Rogue RDP via Outlook Attachment (via file_event)

Author: SOC Prime Team

Possible Msedg Dynamic Library Side-Loading Attempt (via image_load)

Author: SOC Prime Team

Possible Screen Capture (via powershell)

Author: SOC Prime Team

Possible Microsoft Console File Created In Unusual Folder (via file_event)

Author: SOC Prime Team

Possible EDR Disablement Attempt Using WDAC (via file_event)

Author: SOC Prime Team

1-10 of 82 10

< 1 2 3 4 5 ... 9 >

Search Threat Detection Marketplace content right from Uncoder AI. Supports both platform and custom repositories. Threat Detection Marketplace is the world's largest repository of public, private and Threat Bounty-made detection rules and queries, indexing over 15 open-source repos, and sporting over 500,000 detection rules in 48 languages. Every rule that exists is in Threat Detection Marketplace, as long as its author's license permitted that.

- Easily find detections for task at hand
- Conveniently open custom rules
- Discover ideas and inspiration for detection content