RADAR CYBER SECURITY | Safeguard your digital journey.

# Verstehen, Erkennen und Mitigieren von Angriffsvektoren

## Unterstützt durch MITRE ATT&CK

ISO 27001 CERTIFIED

© RadarServices | Classification: PUBLIC

CONFIDENTIAL

RADAR CYBER SECURITY | Safeguard your digital journey.

# Problem

ISO 27001 CERTIFIED

© RadarServices | Classification: PUBLIC

# Konfrontation mit Cyber Security

- Personal

- Fachwissen

- Verteidigung

© RadarServices | Classification: PUBLIC

CONFIDENTIAL

RADAR CYBER SECURITY | Safeguard your digital journey.

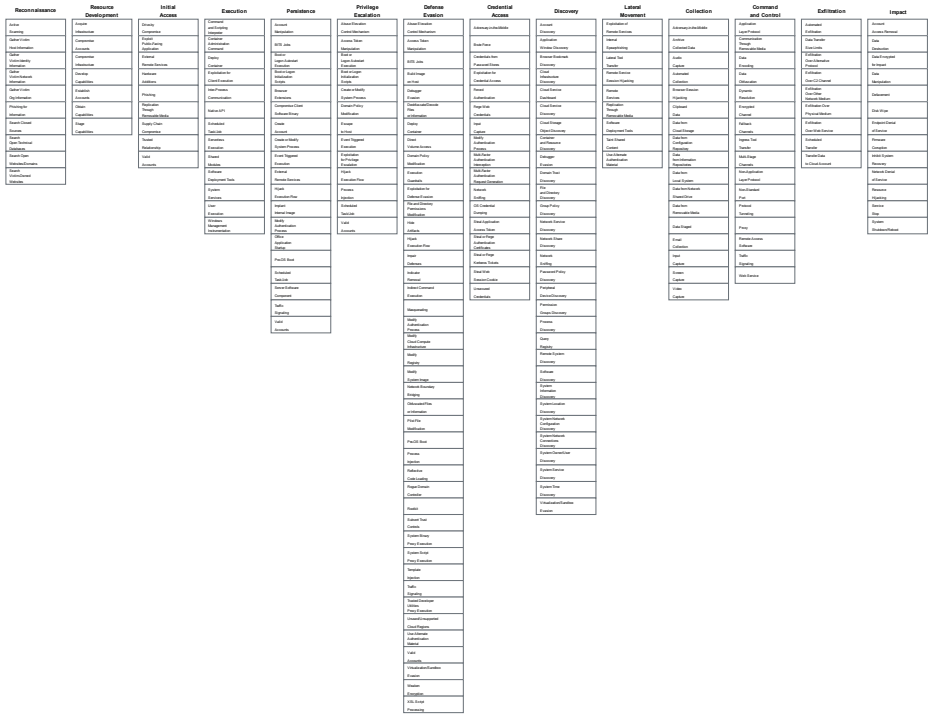
# MITRE ATT&CK

ISO 27001 CERTIFIED

© RadarServices | Classification: PUBLIC

# Aufbau

- Taktiken
- Techniken
- Datenquellen
- Mitigationen
- Software




© RadarServices | Classification: PUBLIC

CONFIDENTIAL

RADAR CYBER SECURITY | Safeguard your digital journey.

# Verständnis

ISO 27001 CERTIFIED

© RadarServices | Classification: PUBLIC

# Verstehen

- Verständnis

- Verteidigung

© RadarServices | Classification: PUBLIC

CONFIDENTIAL

RADAR CYBER SECURITY | Safeguard your digital journey.

# Erkennung

ISO 27001 CERTIFIED

© RadarServices | Classification: PUBLIC

# Erkennen

- Logs


- Regeln


© RadarServices | Classification: PUBLIC

CONFIDENTIAL

RADAR CYBER SECURITY | Safeguard your digital journey.

# Mitigation

ISO 27001 CERTIFIED

© RadarServices | Classification: PUBLIC

# Mitigieren

- Verteidigung
- Angriffsvektoren
- Strategien
- Sicherheitsniveau

© RadarServices | Classification: PUBLIC

CONFIDENTIAL

RADAR CYBER SECURITY | Safeguard your digital journey.

# Beispiel

ISO 27001 CERTIFIED

© RadarServices | Classification: PUBLIC

# Kerberoasting – Verstehen

- TA0006 - T1558.003
  - Ticket Granting Service (TGS) Request
  - RC4 Verschlüsselung
  - Brute Force
- S0357 – Impacket
  - Python Module
- S0194 – PowerSploit
  - PowerShell Module & Skripte
- S1071 – Rubeus
  - C# Toolset

© RadarServices | Classification: PUBLIC

# Kerberoasting – Erkennen

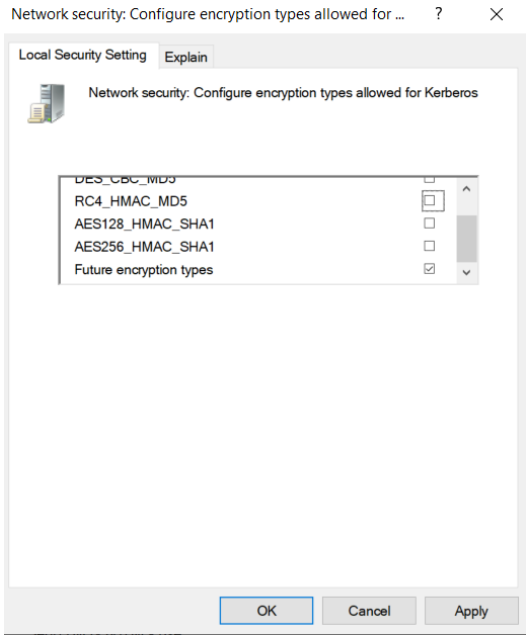
DS0026

```
title: Kerberoasting TGS request detected
id: 4c6746e8-c3d7-447d-b692-b1a431291163
status: production
description: Kerberos TGS with RC4 encryption requested
tags:
   - attack.credential_access
   - attack.t1558.003
author: Tom Perkovic
date: 2023/06/02
logsource:
   product: windows
   service: authentication
detection:
   selection:
      eventID: 4769
      option: 0x40810000
      encryption:
         - 0x17
         - 0x18
      outcome: success
   filter:
      serviceID: *502
      serviceName: *$
   condition: selection AND NOT filter
level: high
```

© RadarServices | Classification: PUBLIC

# Kerberoasting – Mitigieren

- M1041
- Kerberos Encryption Types
  - Computer Configuration\
    Windows Settings\
    Security Settings\
    Local Policies\
    Security Options\
    Network security: Configure encryption types allowed for Kerberos




© RadarServices | Classification: PUBLIC

CONFIDENTIAL

RADAR CYBER SECURITY | Safeguard your digital journey.

# Problem - Lösung

ISO 27001 CERTIFIED

© RadarServices | Classification: PUBLIC

# Lösung

- Startpunkt

- 3-Stufen-Prozess

- Kontinuität

© RadarServices | Classification: PUBLIC

RADAR CYBER SECURITY

Safeguard your digital journey.

Folgen Sie uns

CYBERSECURITY MADE IN EUROPE™

Initiated by ECSO. Issued by eurobits e.V.

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2018

Teilnehmer der Allianz für Cyber-Sicherheit

MSSP Alert TOP 250 MSSPs™ 2021 EDITION

ISO 27001 CERTIFIED