Unternehmensweite Echtzeit Risikobewertung

Tanium - Stefan Molls –Technical Account Manager

Wie priorisieren Sie sicherheitsrelevante Vorfälle aktuell?

Problemstellung

- Das Passwort eines Benutzers taucht im Internet auf
- Ein Antivirenprogram findet Spuren von einem „Credential Dumper“ auf einem System

- Wissen Sie wie „mächtig“ Ihre Active Directory Gruppen sind?
- Wie viele Domänenadministratoren haben Sie?
- Und wo sind die überall angemeldet?

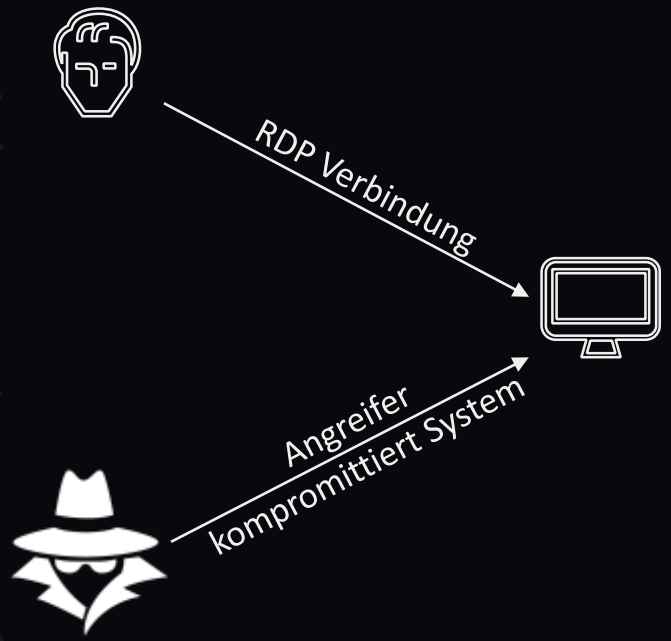
- Antivirenalarme auf einem Serversystem
- Endlos lange Listen mit Schwachstellen. Wo fängt man an?
- Ein Server zeigt auffälliges Verhalten

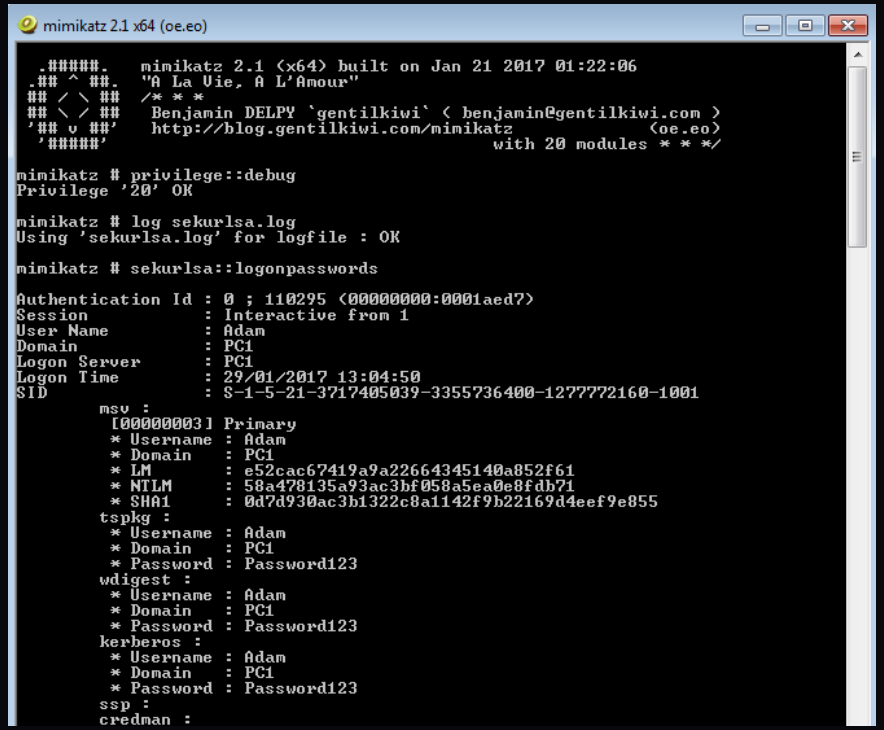
Herausforderungen

- Komplexe & nicht transparente Berechtigungen von Benutzern und Gruppen
- „Bauchgefühl“ bzw. rein funktionale Sicht bei der Bewertung des Impacts
- Betrachtung meist erst „Nach“ einem Vorfall. Keine pro-aktiven Analysen

Bevor wir in die Details gehen …

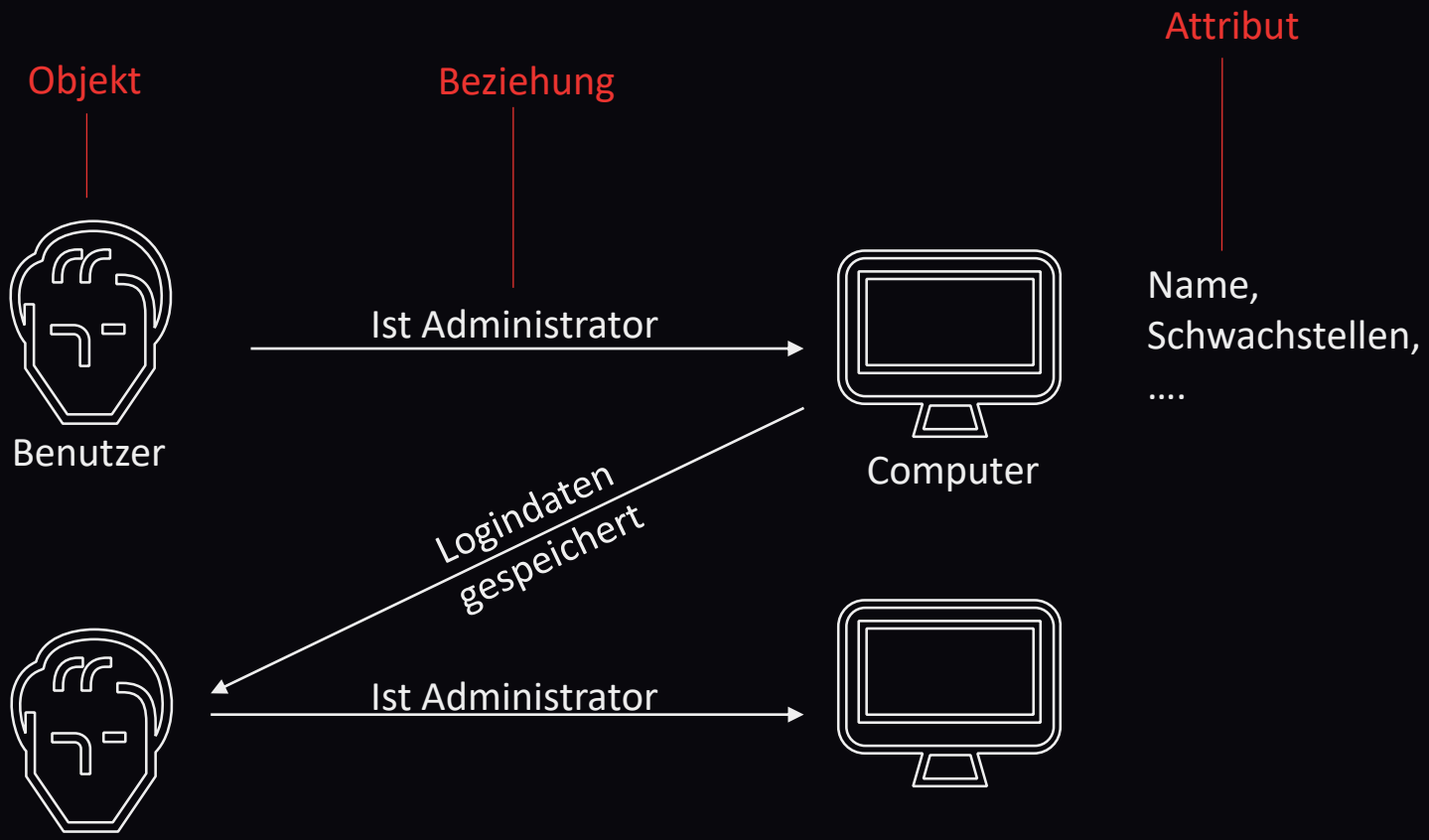
Vorwissen: Was ist “Lateral Movement”





Angreifer hat Zugriff auf Logindaten

Vorwissen: Was ist ein Graph?



Credits: Initiale Idee der Darstellung als Graph

https://bloodhoundgang.herokuapp.com/
https://github.com/BloodHoundAD/

Was hat Tanium damit zu tun?

Operations Management

Asset Visibility

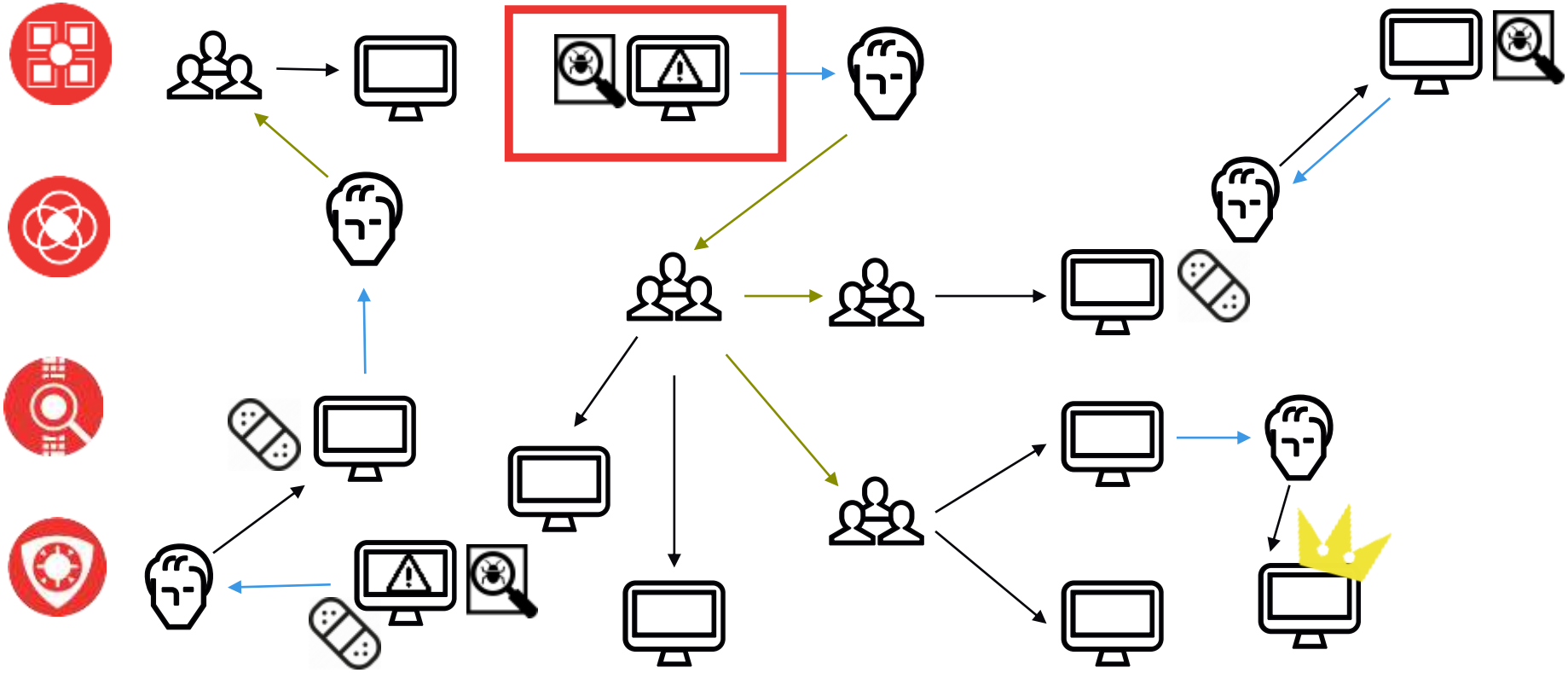
Security Hygiene

Detection & Response

- Voller Überblick über alle Endpunkte in Sekunden
- Schwachstellenscans, Fehlende Patches, Berechtigungen, Identifikation von auffälligem Verhalten …
- Möglichkeit Fehler direkt zu beheben

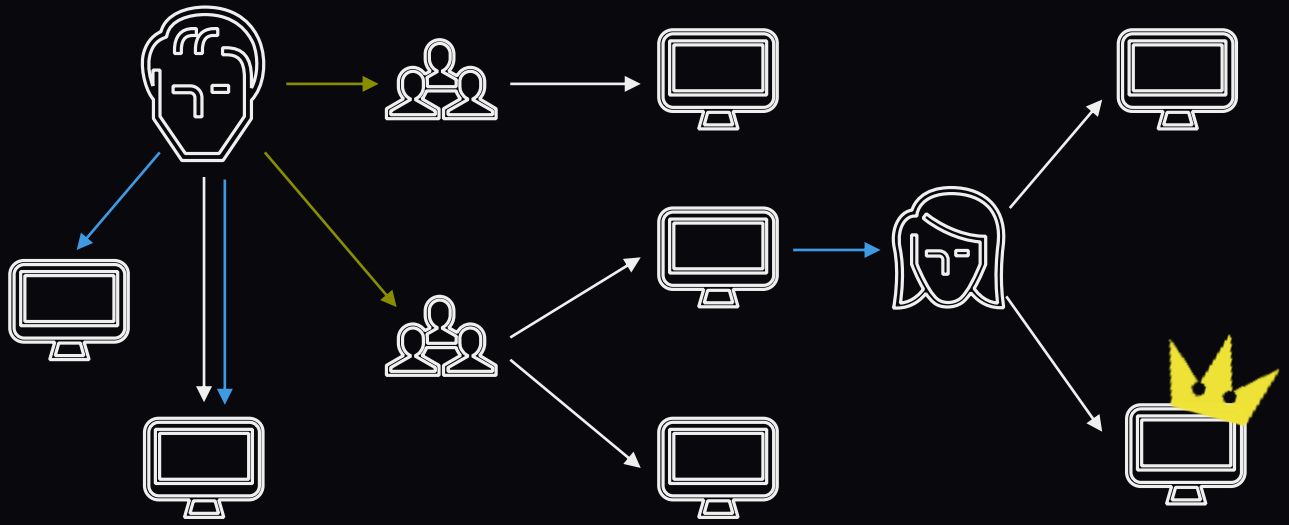
Wie können uns Graphen helfen Risiken besser einzuschätzen?

Visualize, Contextualize, Prioritize



Welche Werte können helfen?

Details: Benutzer

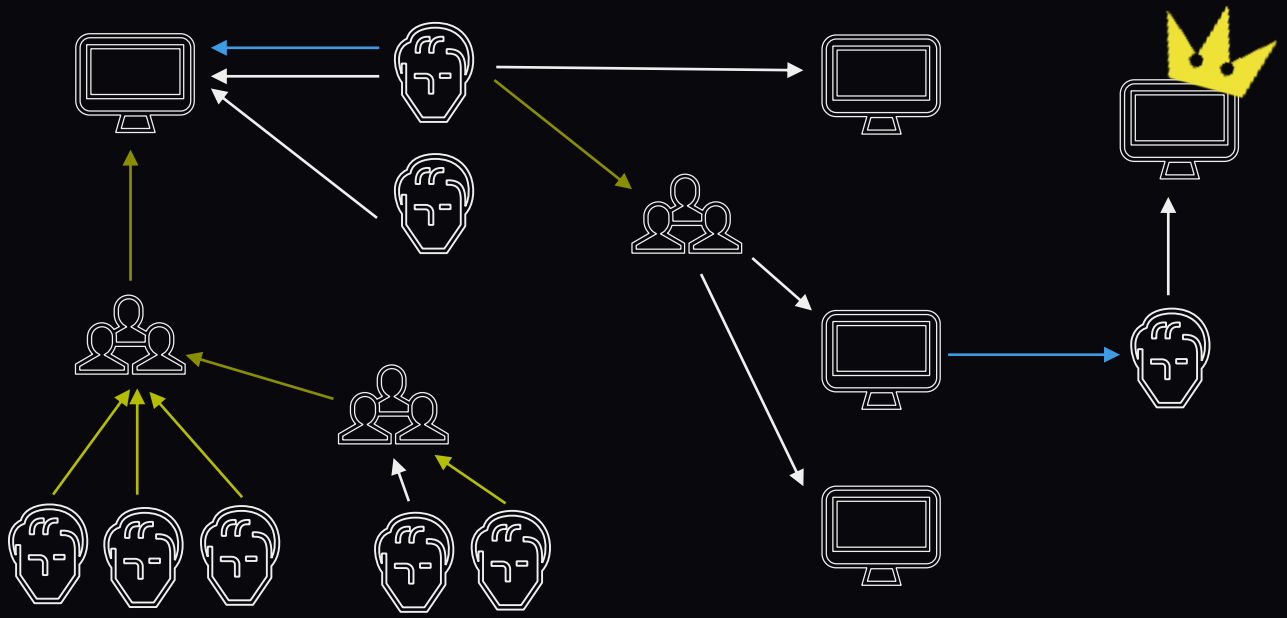


- Name: Bob
- Direkter Admin zu: 1
- Sessions: 2
- Indirekter Admin zu: 3
- Breach Zugriff auf: 2
- Zugriff auf kritische Assets: 1

Example risk formula:

((Direct Admin Rights + Group Administrators Rights + Total Admin Rights) * (Sessions +1)) * (No of critical assets access + 1)

Details: Computer



- Name: SQL1
- Direct Admins: 2
- Indirect Admins: 5
- Sessions: 1
- Total / Derivative Breach Access: 4
- Access to critical assets: 1

Example risk formula Breach exposure:

(Direct Admin + Indirect Admin + Sessions + Total Breach Access) * (No of critical assets access + 1)

Details: Active Directory Gruppen

- Groupname: service_desk@awesome.local
- Direct Members: 10
- Indirect Members: 5
- Direct Admin to: 25
- Indirect Admin to: 3
- Lateral Movement access to: 50
- Access to critical assets: 2

Example risk formula AD groups:

((Direct Members + Indirect Members) * (Admin to + Indirect Admin To) + Lateral Movement access) * (Critical Assets +1)

Umsetzung in der Praxis (Benutzerdaten)

User Data

Show 10 entries

Search:

Name	Direct Admin to	Indirect Admin to (Group Membership)	Derivative Admin rights (Lateral Movement)	Sessions	No of direct group memberships	Direct Risk Rate	Derivative Risk Rate
AWESOME\SVC_TANIUM	3	7	7	2	2	60	81
AWESOME\JBARBER	3	7	7	1	2	40	54
AWESOME\ADMIN	2	7	7	1	3	36	50
AWESOME\ADMINISTRATOR	1	7	7	1	3	32	46
AWESOME\MMOSS	1	2	7	2	2	18	39
AWESOME\SMOLLS	2	7	7	0	2	18	25
AWESOME\DREYNHOLM	1	1	1	1	1	8	10
AWESOME\RTRENNEMAN	1	1	7	1	1	8	22
AWESOME\ABBOTASH	0	1	1	0	1	2	3
AWESOME\ABBOTDON	0	1	1	0	1	2	3

Umsetzung in der Praxis (Computerdaten)

Computer Data

Show 10 entries

Search:

Name	Direct Administrators	Indirect Administrators (Due to Group memberships)	Derivative Access (Lateral Movement)	Sessions	Missing Critical Patches	Vulnerabilities	Direct Risk Rate	Derivative Risk Rate
TESTRAILTS1.AWESOME.LOCAL	1	5	6	1	7	588	599	605
SPLUNK.AWESOME.LOCAL	2	551	0	1	31	No recorded vulns	585	585
CLIENT2.AWESOME.LOCAL	6	5	6	2	52	No recorded vulns	65	71
JENKINS1.AWESOME.LOCAL	3	6	6	2	29	No recorded vulns	40	46
DC1.AWESOME.LOCAL	1	5	6	2	20	No recorded vulns	28	34
TESTRAILTMS1.AWESOME.LOCAL	1	5	6	1	7	588	14	20
TESTRAILSQL.AWESOME.LOCAL	0	0	0	0	7	585	7	7

Umsetzung in der Praxis

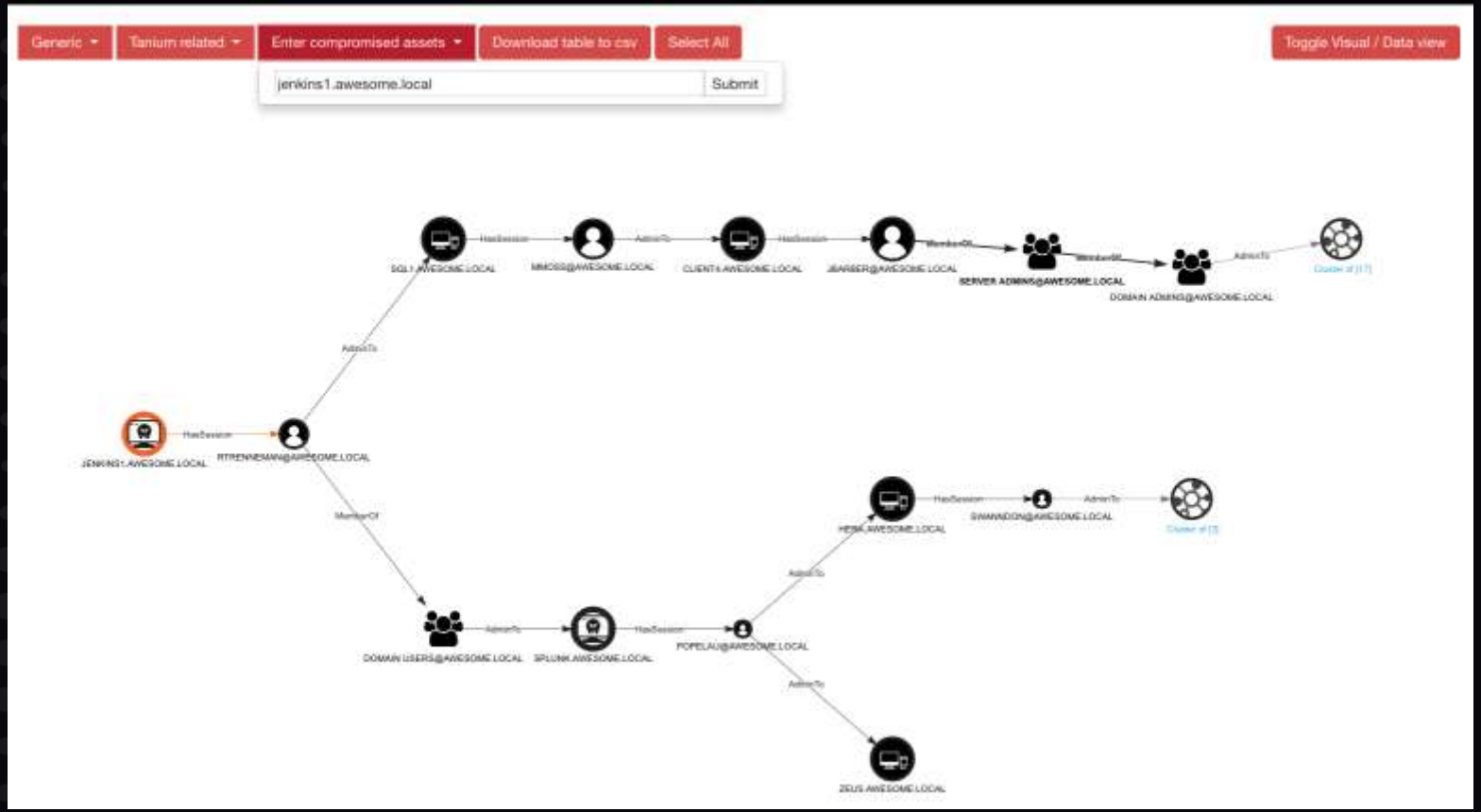
Vulnerability Data

Show 10 entries

Search:

Name	CVSS	Severity	Direct Affected	Derivative Impact
.NET and .NET Core Denial of Service Vulnerability - CVE-2018-0765	5	Medium	3	7
.NET Core Denial Of Service Vulnerability - CVE-2018-0764	5	Medium	2	7
.NET Core Information Disclosure Vulnerability - CVE-2018-8292	5	Medium	0	0
.NET Framework and .NET Core Denial of Service Vulnerability - CVE-2019-0820	5	Medium	3	7
.NET Framework and .NET Core Denial of Service Vulnerability - CVE-2019-0980	5	Medium	3	7
.NET Framework and .NET Core Denial of Service Vulnerability - CVE-2019-0981	5	Medium	3	7
.NET Framework and Visual Studio Remote Code Execution Vulnerability - CVE-2019-0613	9.3	High	3	7
.NET Framework and Visual Studio Spoofing Vulnerability - CVE-2019-0657	4.3	Medium	3	7
.NET Framework Denial Of Service Vulnerability - CVE-2018-8517	5	Medium	3	7
.NET Framework Device Guard Security Feature Bypass Vulnerability - CVE-2018-1039	4.6	Medium	3	7

Umsetzung in der Praxis (Visualisierung)



TANIUM

Besuchen Sie unseren Stand:
Hall 10.1, Stand 420

Stefan Molls | Technical Account Manager – EMEA, Tanium