

Hands-on BloodHound

Intro to Cypher Workshop

November 12, 2018

Bloodhound is an open-source Active Directory object relationship graphing tool. Initially designed for offensive purposes, it has lately become a tool of choice for defense, as well as regular admins wanting to have a clearer picture of their domains/forest.

In this session, attendees will learn the core Bloodhound concepts and UI navigation, before diving into Cypher - the Neo4j database query language. Understanding the basic Cypher syntax is important for users to start writing custom queries, including 'Metric' queries that can not be perform in UI. Various Cypher input techniques will be demonstrated, as well as a custom PowerShell tool build to interact with the Bloodhound Database.

Prerequisites

Basic understanding of core Active Directory concepts.

An Active Directory Summit is offered on November 13, 2018.

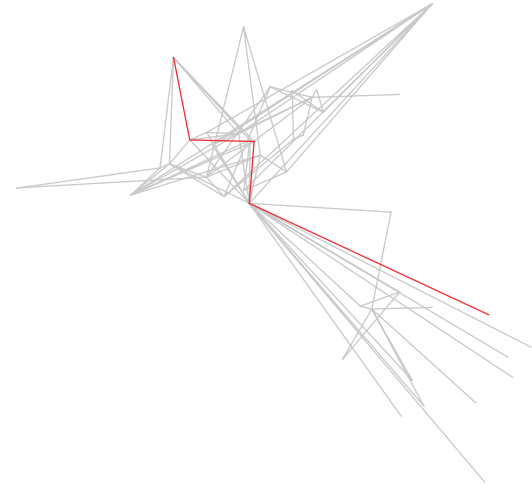
The Hands-On Bloodhound and the Active Directory Summit can be bought as a special package.

Audience

- Reds & Blues
- (Windows) Security Folks
- AD admins
- IT Students

Material required

- Laptop with Windows - min 8GB RAM & NIC (VM is also ok).
- Course material and exercises will be provided as pdf.



Course content

1. What is BloodHound?

- Intro to BloodHound & relational databases
- BloodHound Node types and relationships
- SharpHound: Harvesting and Ingesting AD data
- Initial Setup & Sample DB
- Self Discovery & UI Secrets

2. What is Cypher?

- Intro to neo4j Cypher language
- BloodHound Cypher 101
- Custom Cypher Queries (UI/Browser)
- Cypher over REST API
- Manipulating BH DB with Cypher
- Advanced Neo4j Syntax tricks
- Pulling AD metric from BH DB
- Tool Demo: CypherDog15

3. Session Wrap up

Registration

You can register online on our ticketshop:
<https://tickets.ernw-insight.de/insight/iss2018/>

For further information, please contact us:
registration@ernw-insight.de

The Bloodhound event takes place in English.
The Active Directory event takes place in German.

Price

Hands-On Bloodhound 799€
Bloodhound & Active Directory Package 1499€
plus 19% MwSt.

The price includes the entrance to the event, as well as catering and beverages. The package includes a shared dinner on Monday evening.

Event location

Print Media Academy
Kurfürstenanlage 60
69115 Heidelberg

Event organizer

ERNW Insight GmbH
Carl-Bosch-Strasse 4
69115 Heidelberg
+49 (0) 6221 480390
info@ernw-insight.de
www.ernw-insight.de