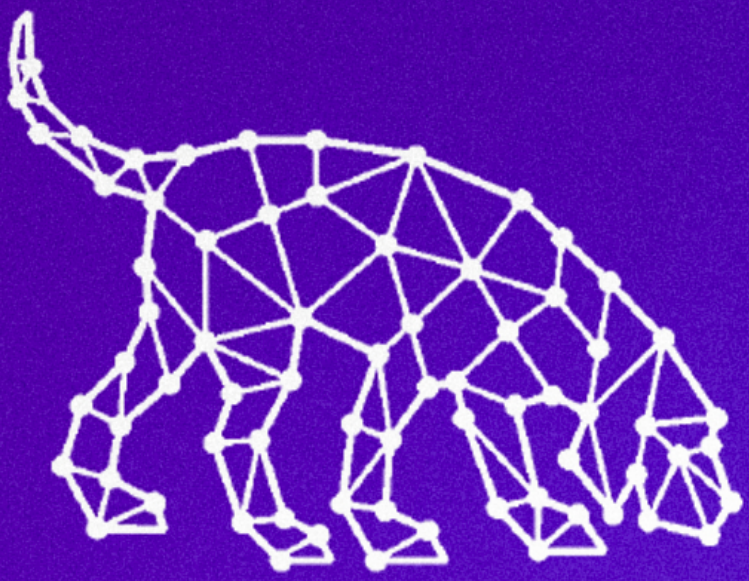
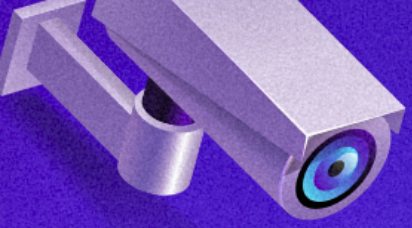


BLOODHOUND

What Is BloodHound?

BloodHound is an open-source tool that shows potential attack paths within an Active Directory environment.

STATIONX



You can analyze this information using BloodHound's GUI to uncover security misconfigurations.
The Bloodhound tool is not a standalone executable. Instead, the tool consists of several key parts:

The SharpHound data collector: This collects the data from the Active Directory environment you are attacking and packages it in a format you can upload to BloodHound for analysis.

The Neo4j backend: BloodHound uses Neo4j as its backend database to store and process the Active Directory data uploaded to the tool. Neo4j creates a graphical view of the data, allowing it to be queried.

The BloodHound GUI: This provides a visual representation of the Active Directory information collected and allows you to interact with this information to discover security misconfigurations.

The BloodHound query language: BloodHound comes with its custom query language called Cypher. This allows you to search the collected data for vulnerabilities, misconfigurations, and reveal hidden relationships between Active Directory entities.

BLOODHOUND

SCANNING...

DO YOU LIKE THIS POST?

SAVE THIS FOR LATER

WWW.STATIONX.NET