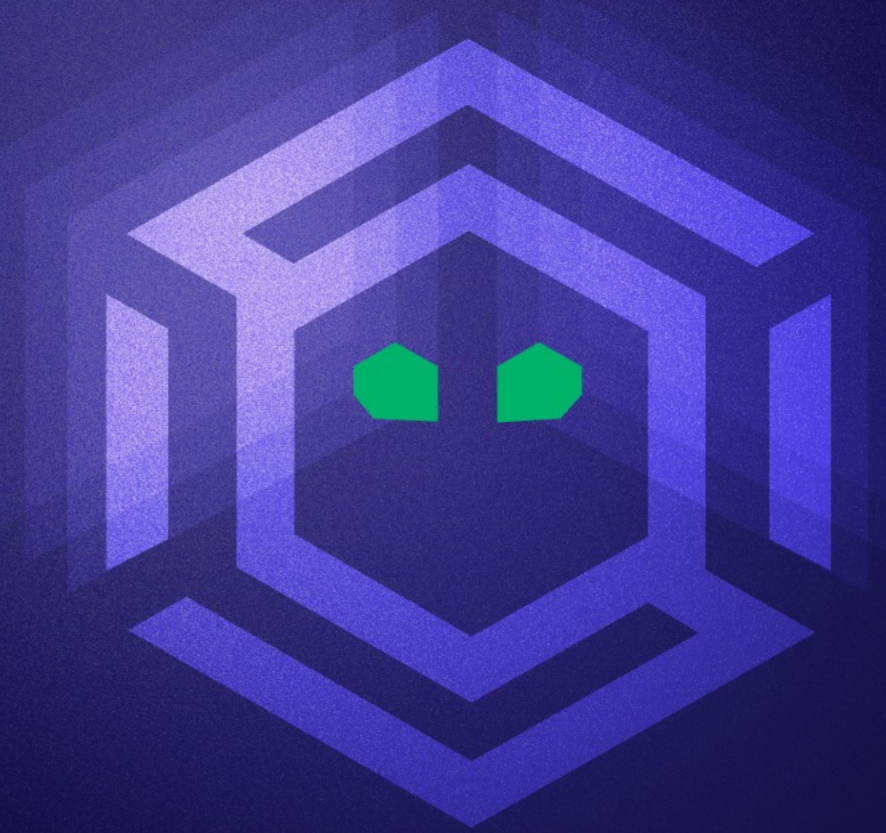
SPECTEROPS

# BloodHound Update

## Spring 2024



Stephen Hinck – Director of Product Management

# What’s new?

Q1 2024 Edition

# New coverage

## Active Directory Certificate Services

- Native collection and processing
- Added support for “Composition” feature
- More research and paths to come!

- Support for:
  - GoldenCert
  - ADCSESC1
  - ADCSESC3
  - ADCSESC4
  - ADCSESC6a, b
  - ADCSESC9a, b
  - ADCSESC10a, b

# Data enhancements

- Mark objects as Owned
- Group Management view
- Power User role

# Ingest and management enhancements

- Native support for .zip upload and extraction
- Support for larger file sizes in UI
- Streaming JSON parser
- Database management
  - Clear data, history, tags

# Thank you, community!

## Community Contributors in Q1, 2024 (Alphabetical)

https://github.com/byinarie

https://github.com/nurfed1

https://github.com/spyr0-sec

https://github.com/stuartw1

https://github.com/uidzeroo

https://github.com/vtrenton

# New sample data set

- Sample AD data set available in GitHub – Link
- Contains
  - Multiple collected domains with trusts
  - Visible, trusted domains without collection
  - Local privileged collection data
  - ADCS escalation paths
- Huge thanks:
  - Jonas Bülow Knudsen (SpecterOps Research)
  - Aaron Smith (SpecterOps Sales Engineering)

# What’s next?

# What’s coming next?

- Next Release
  - Native cypher mutation support
  - ADCS ESC 13 (Blog)
- Going forward
  - Additional path research in Azure
  - Additional ESC research ongoing

# ICYMI

## The BloodHound-Adjacent Edition

- Blogs
  - ADCS ESC 14 (Jonas Bülow Knudsen) – Blog
  - Pwned by the Mail Carrier (Jonas Bülow Knudsen) – Blog
  - Browserless Entra Device Code Flow (Andy Robbins) – Blog
  - Microsoft Breach
    - Technical Deep Dive (Andy Robbins) – Blog
    - How can I see this in BloodHound (Stephen Hinck) – Blog
- Training
  - ***New*** Azure Security Fundamentals Course – Link
  - AD Security Fundamentals – Link

# Deploy BloodHound CE today!

```
curl -L https://ghst.ly/getbhce | docker compose -f - up
```

# Interested in BloodHound Enterprise?

https://bloodhoundenterprise.io/demo/

# Join the BloodHound Gang Slack!

http://ghst.ly/BHSlack

# Thank you!