

# AUSCERT2022

Cyber Security Conference

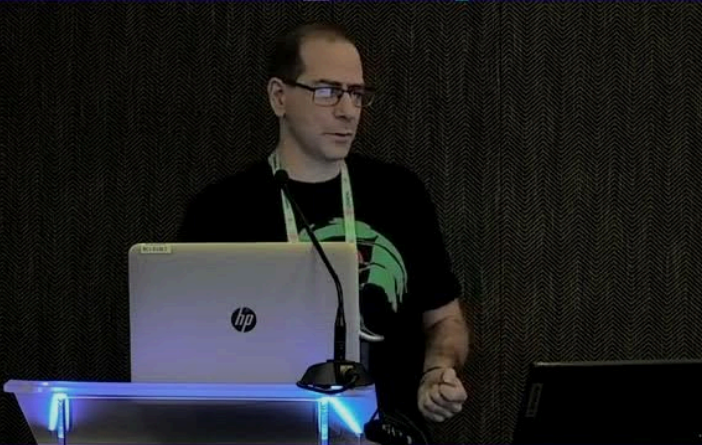
## Data sources

- Windows generates a large number of logs, and more can be enabled.
- This can cause a lot of logs to be forwarded and increases the cost of storing and querying the logs.
- Typically there is a tradeoff between logs and detection.
- Many event logs are not specifically oriented towards detection
  - A lot of non-relevant events generated from multiple sources

8

© 2022 RAPID7

Google Videos



21st Annual AusCERT Cyber Security Conference\_

10 13 May 2022 The Star Hotel, Gold Coast AUS

0:00 / 34:10

⏮ ⏪ ⏩ ⏭ 🔊 ⚙️ 📺 🖥️ 🗖️

