Security Investigations

- Incident Investigation and Forensics
  - Creating a timebound picture of network activity
  - Detecting Supernova web shell malware
  - Enriching suspicious email domains
  - Investigating a ransomware attack
  - Reconstructing a website defacement
  - Visualizing processes and their parent/child relationships

- Incident Response and Reporting
  - Detecting REvil ransomware infections
  - Detecting the use of randomization in cyberattacks