Putting Big Data to Work in DFIR

Jason Mical, Global Cybersecurity Evangelist

July 17, 2020

Go Beyond the Constraints of Traditional Security Analytics, Logging, and Monitoring Tools

Purpose-built

Collect 20X the volume of machine data and meet the crushing demand of automation and algorithms consuming it, no re-architecting required

Put More Data to Work, Now

Enrich and combine machine data with other datasets to go beyond isolated views and unlock the compounding value of your data

Game-Changing Economics

Use more data, unlock new business use cases, all while shrinking operational costs and infrastructure footprint

Challenges of Pivoting from Investigating to Hunting

What are the top factors contributing to lengthy investigations?

Poor Visibility

78% *report lack of visibility into IT security infrastructure*

Low Fidelity Alerts

68% *report too many alerts to chase*

Impact to Respond

67% *report information overload*

Isolated Threat Data

51% *report inability to capture actionable intelligence*

Slow Investigations

56% *report inability to prioritize threats*

DEVO

LET THE ANALYSTS ANALYZE WHAT MATTERS MOST.

Analysts' time should not be spent curating information from disparate tools and wading through high noise, low signal alerts.

Automatic enrichment up-levels analysts' work and allows for increased experimentation and innovative analysis

DEVO

It’s time to close the gap between detection and response

The Devo Approach:
Empower Analysts with a Workflow to Focus on What Matters

Detection

Reduce false positives and alert fatigue

Investigation

Increase confidence by operationalizing threat data

Speed triage and investigation

Response

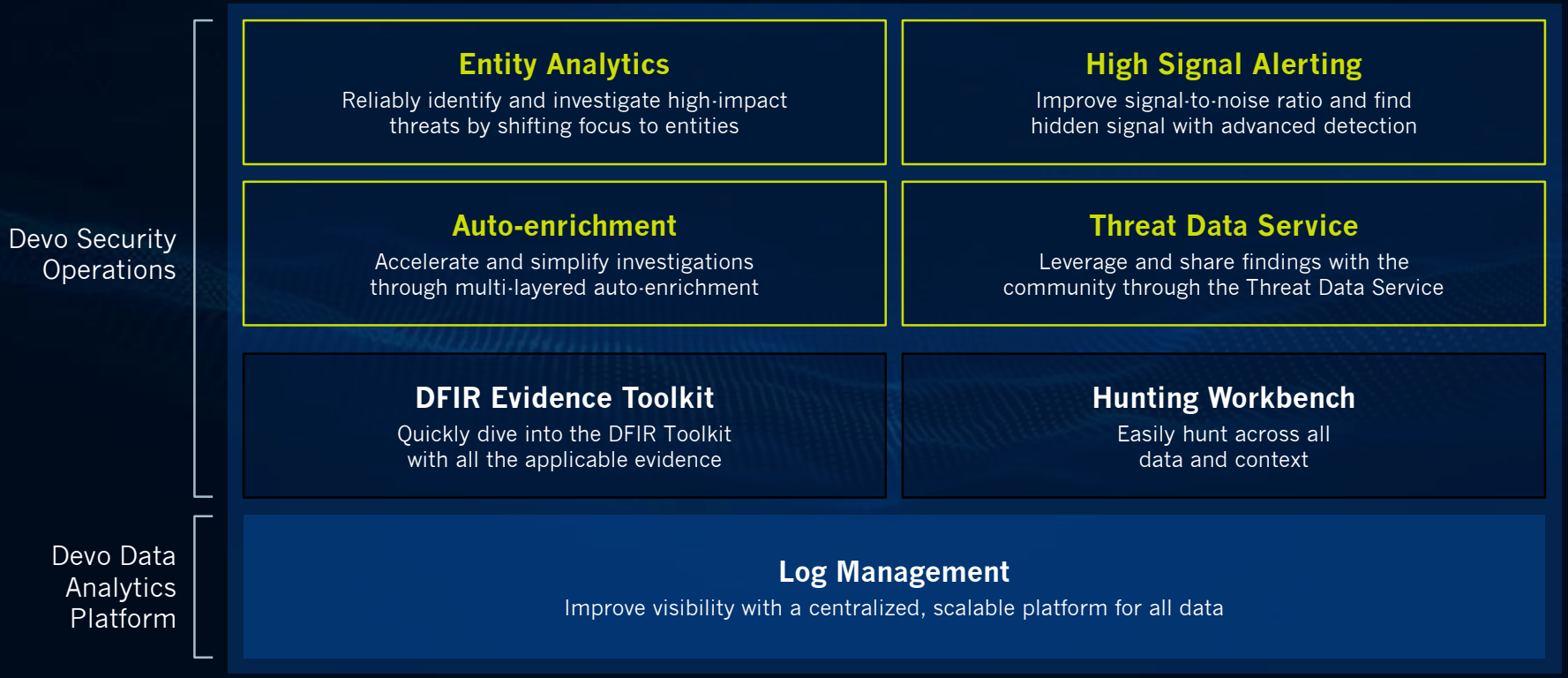
Give analysts the right evidence at the right time

The Right Alerts, Data, and Context at Analysts' Fingertips

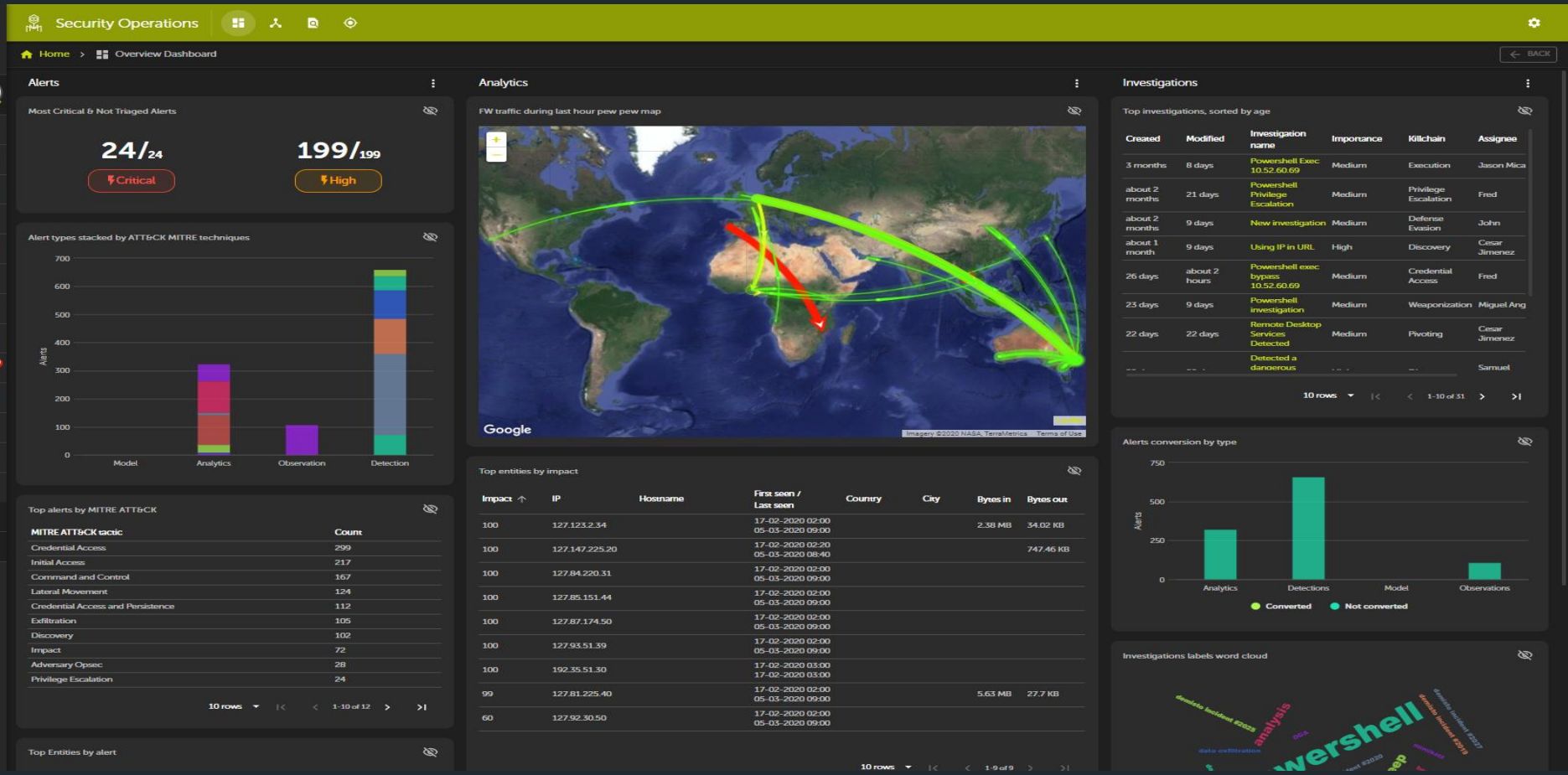
DEVO

Introducing Devo Security Operations

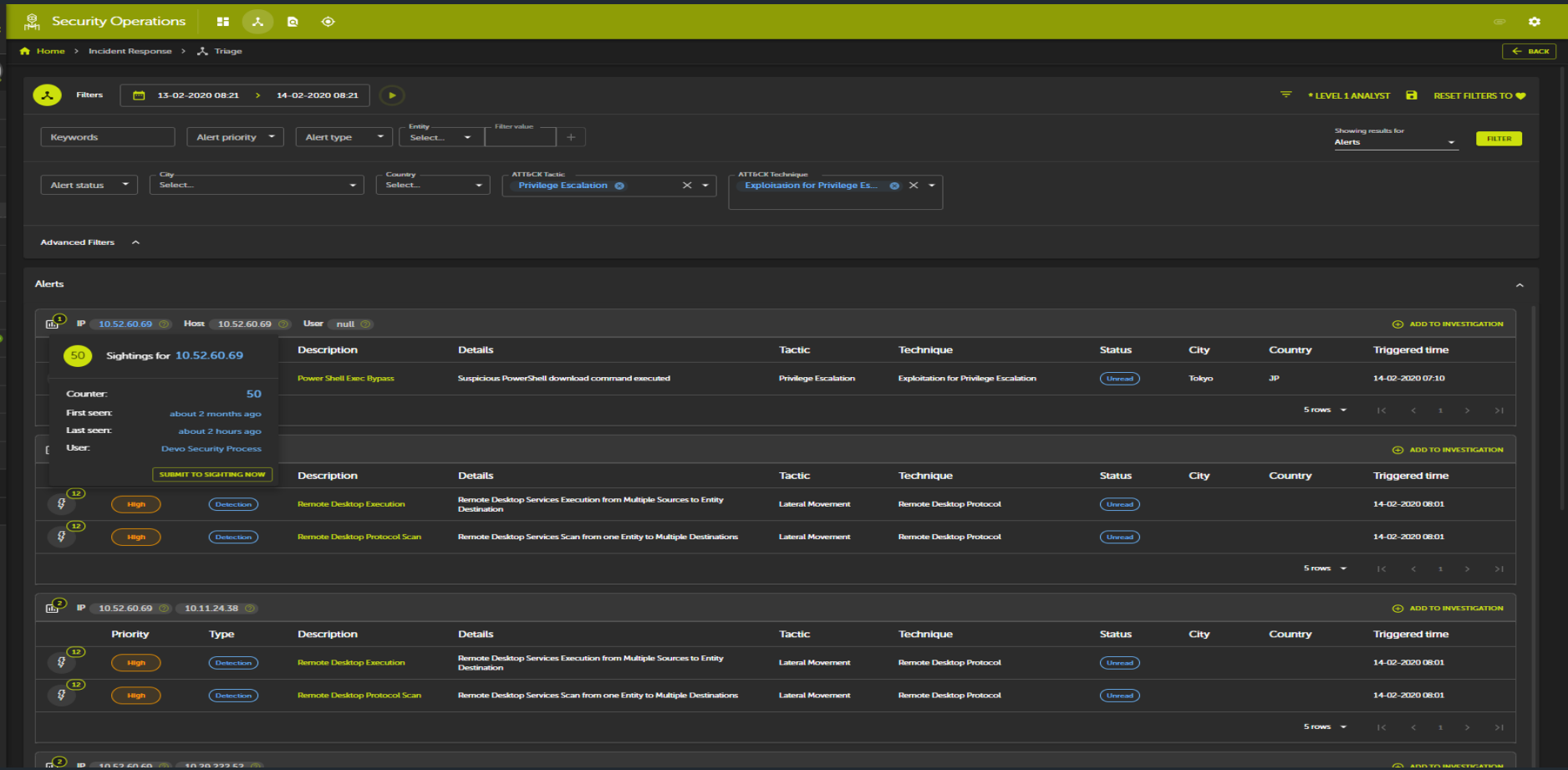
Bringing it all Together



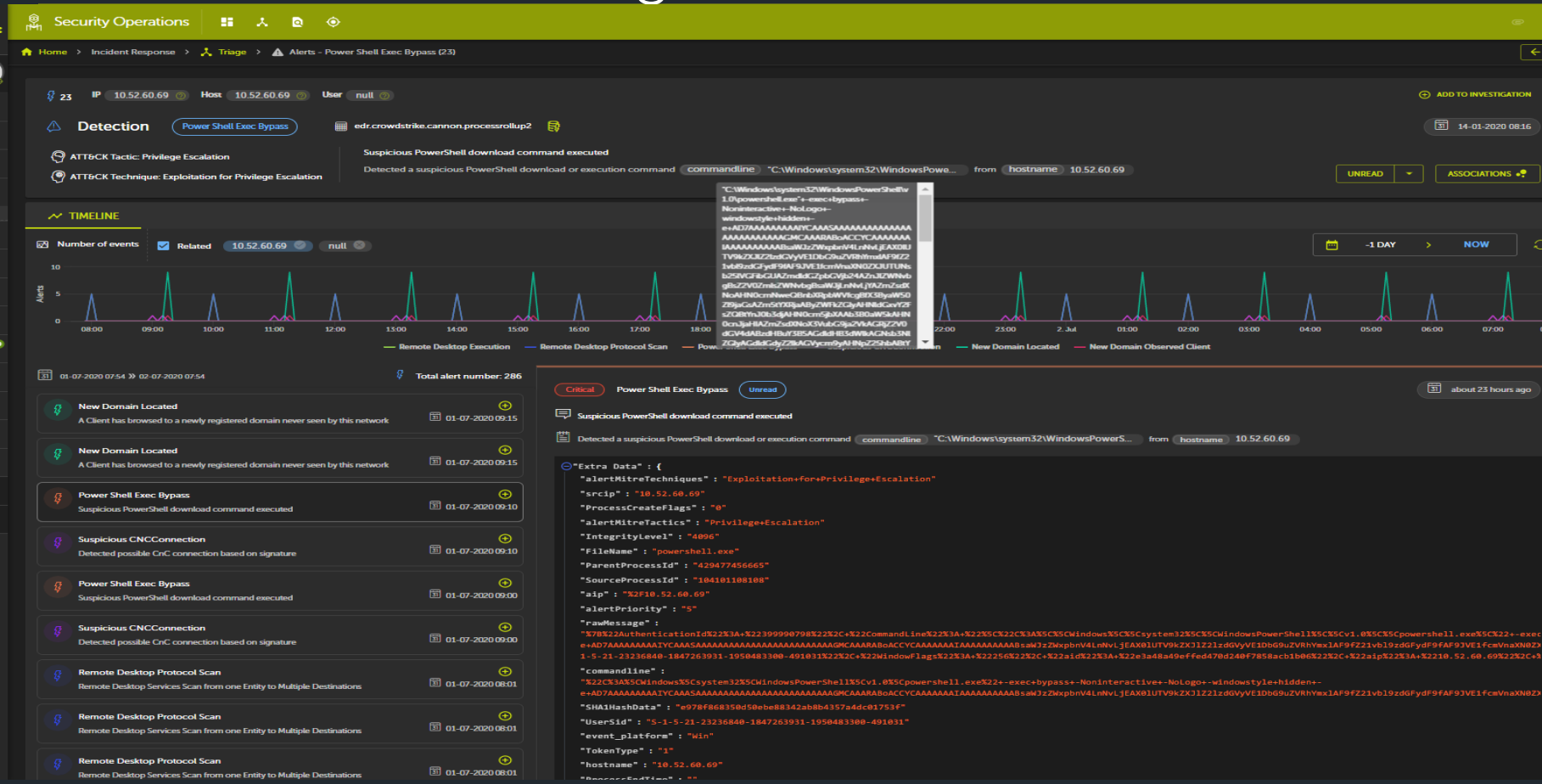
Analysts at the Heart of SOC Technology Design



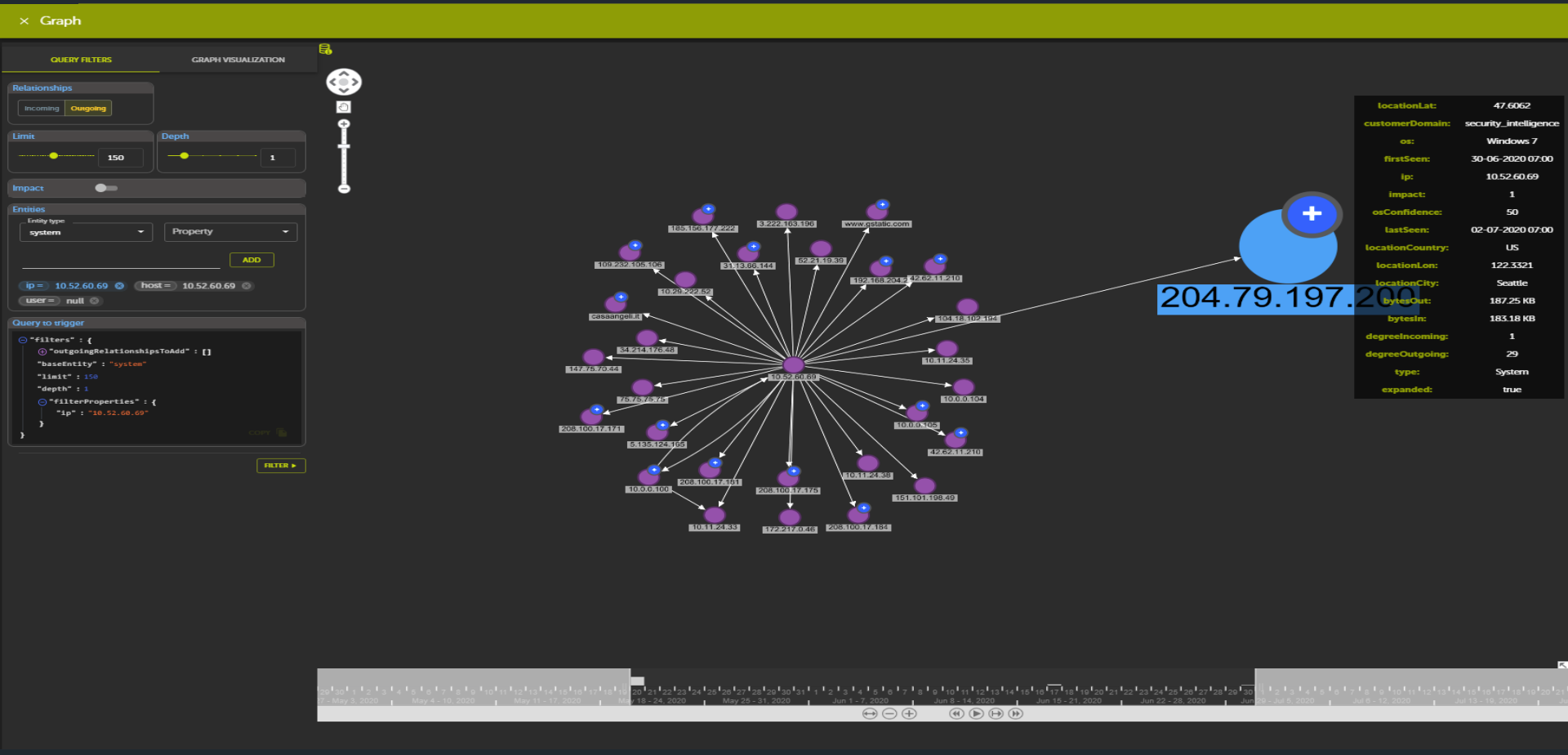
Alert Triage



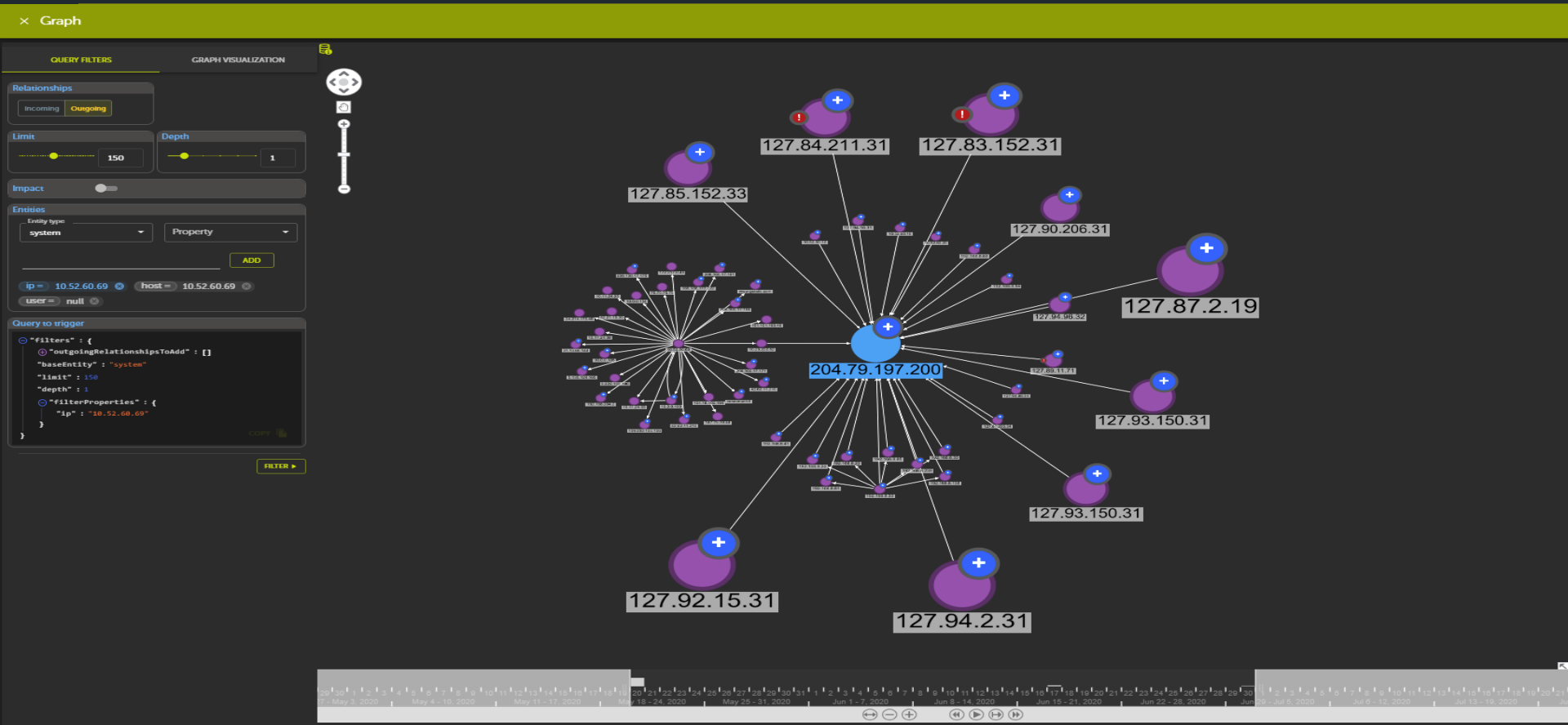
Complete replay of all activity that occurred prior, during and after alert



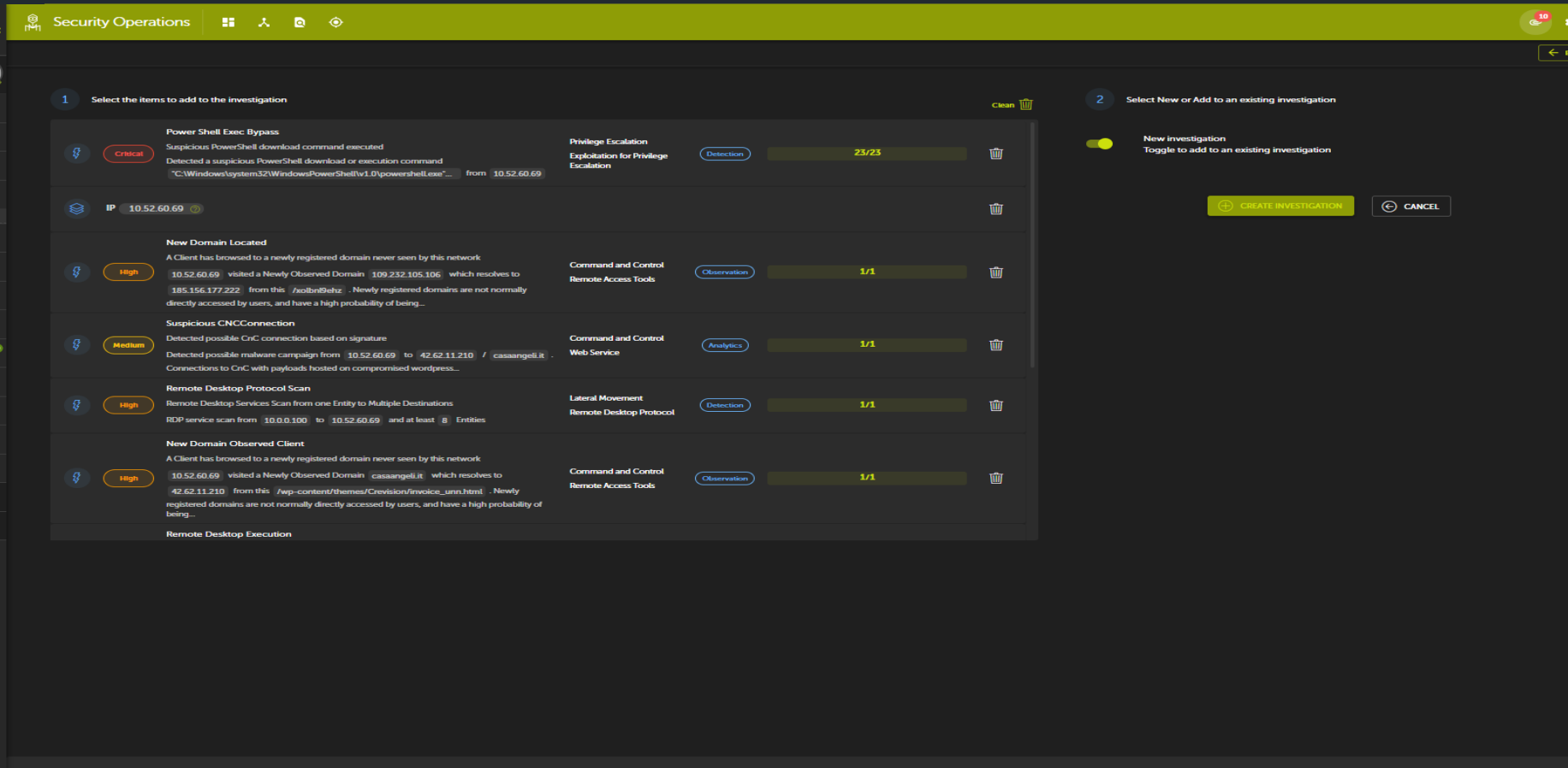
Live Victim associations with automated entity enrichment to determine impact



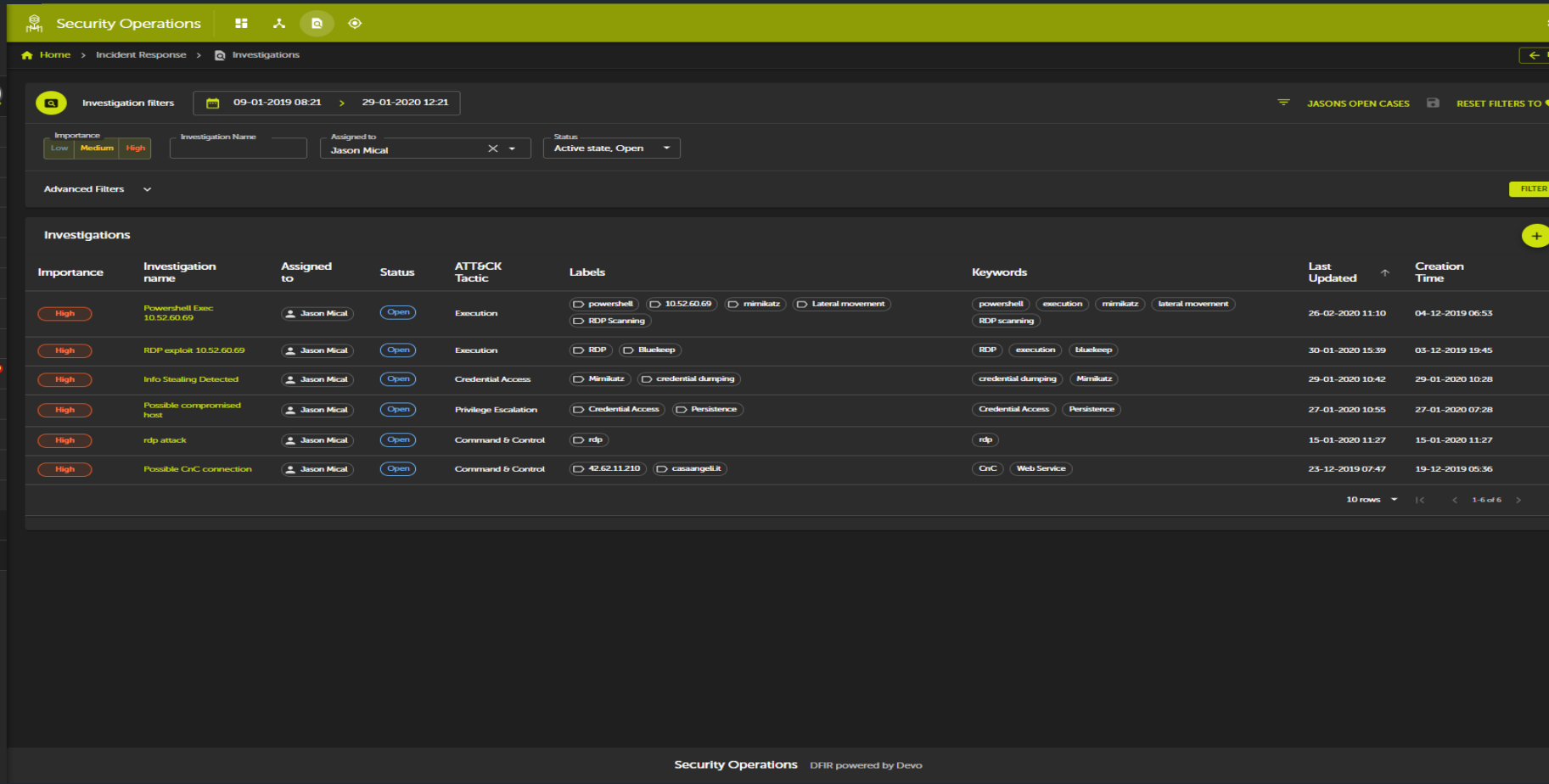
Association expansion with automated additional symptoms observed



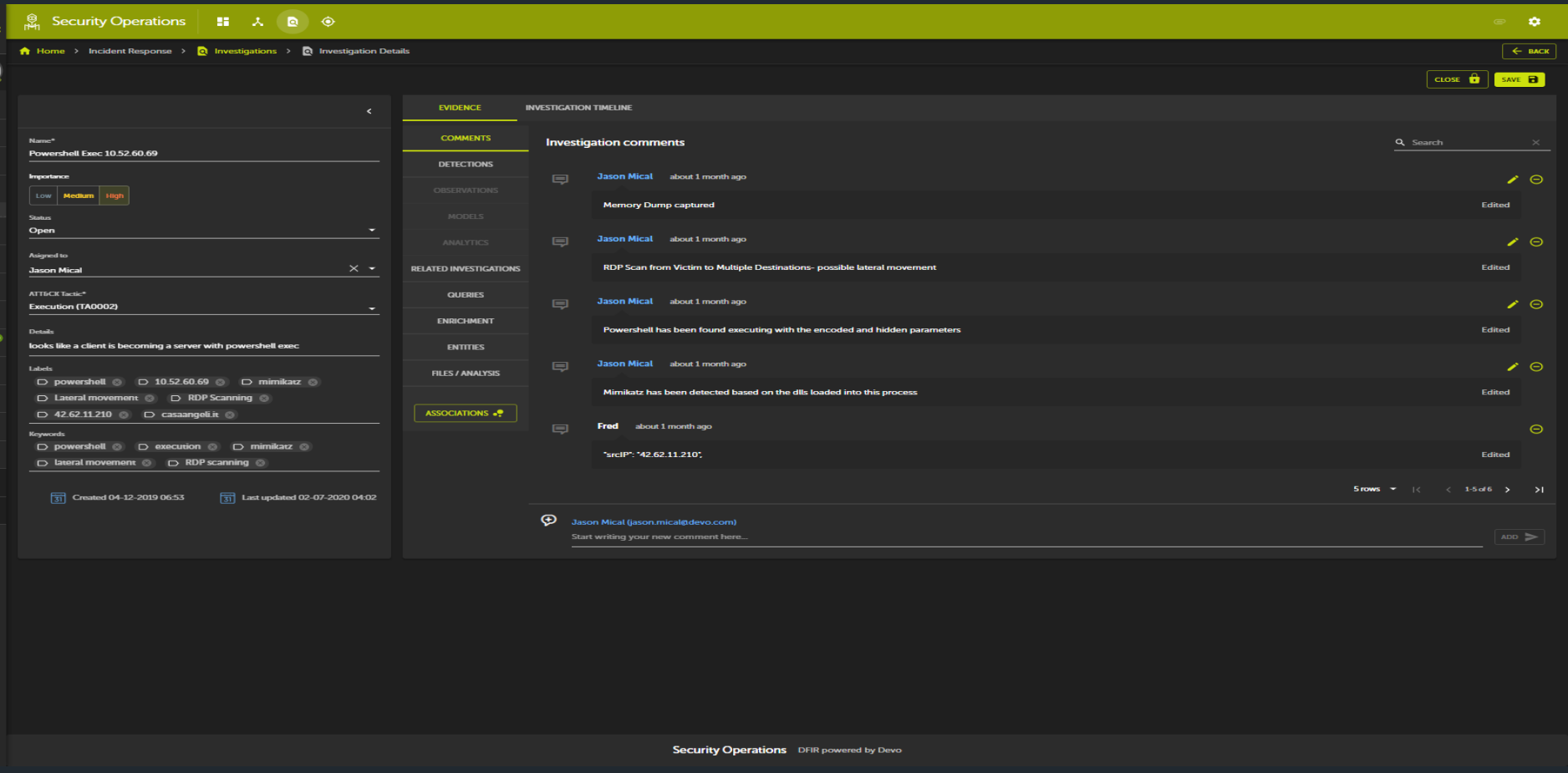
Tag artifacts for case creation



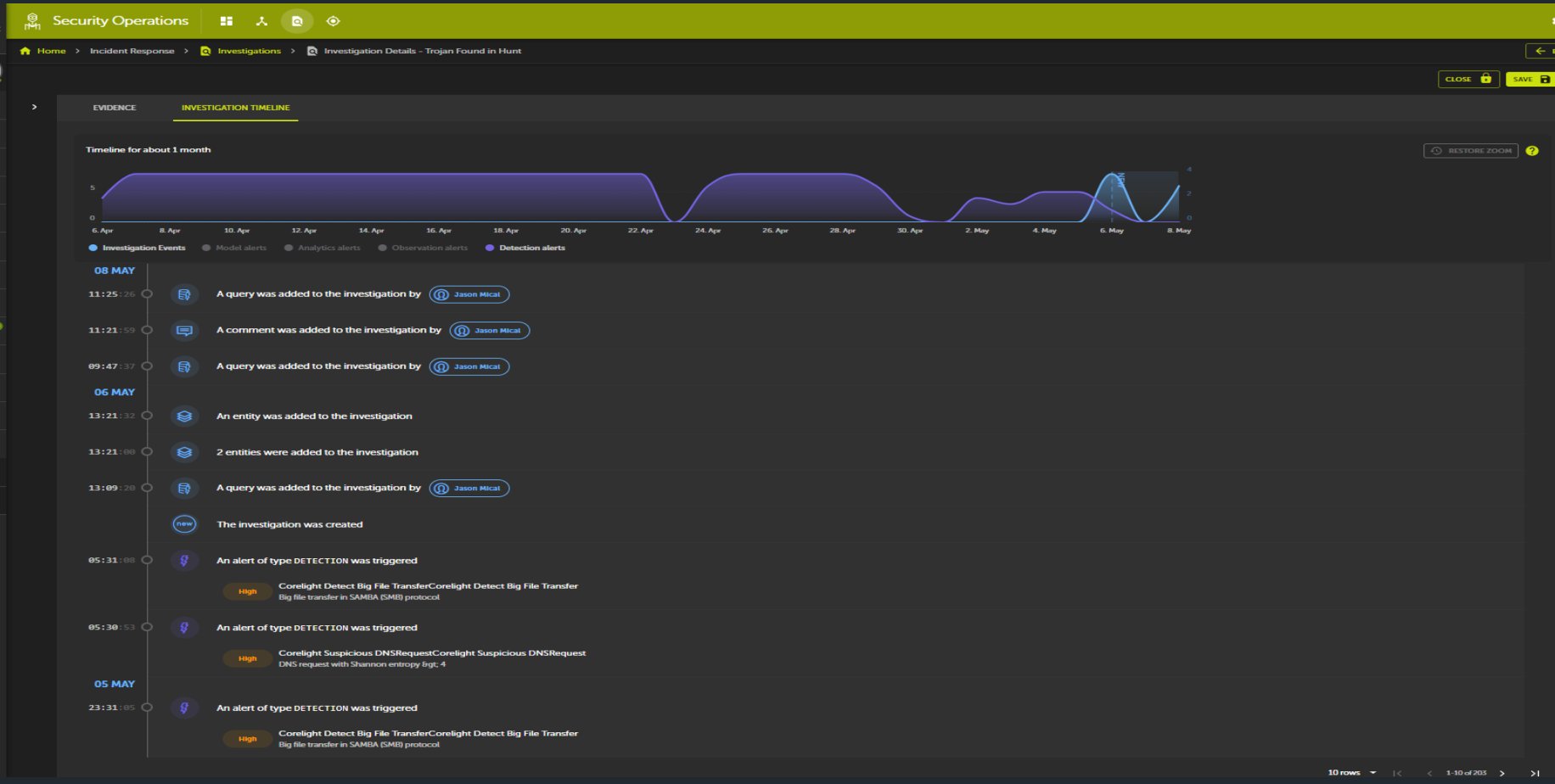
Case Management



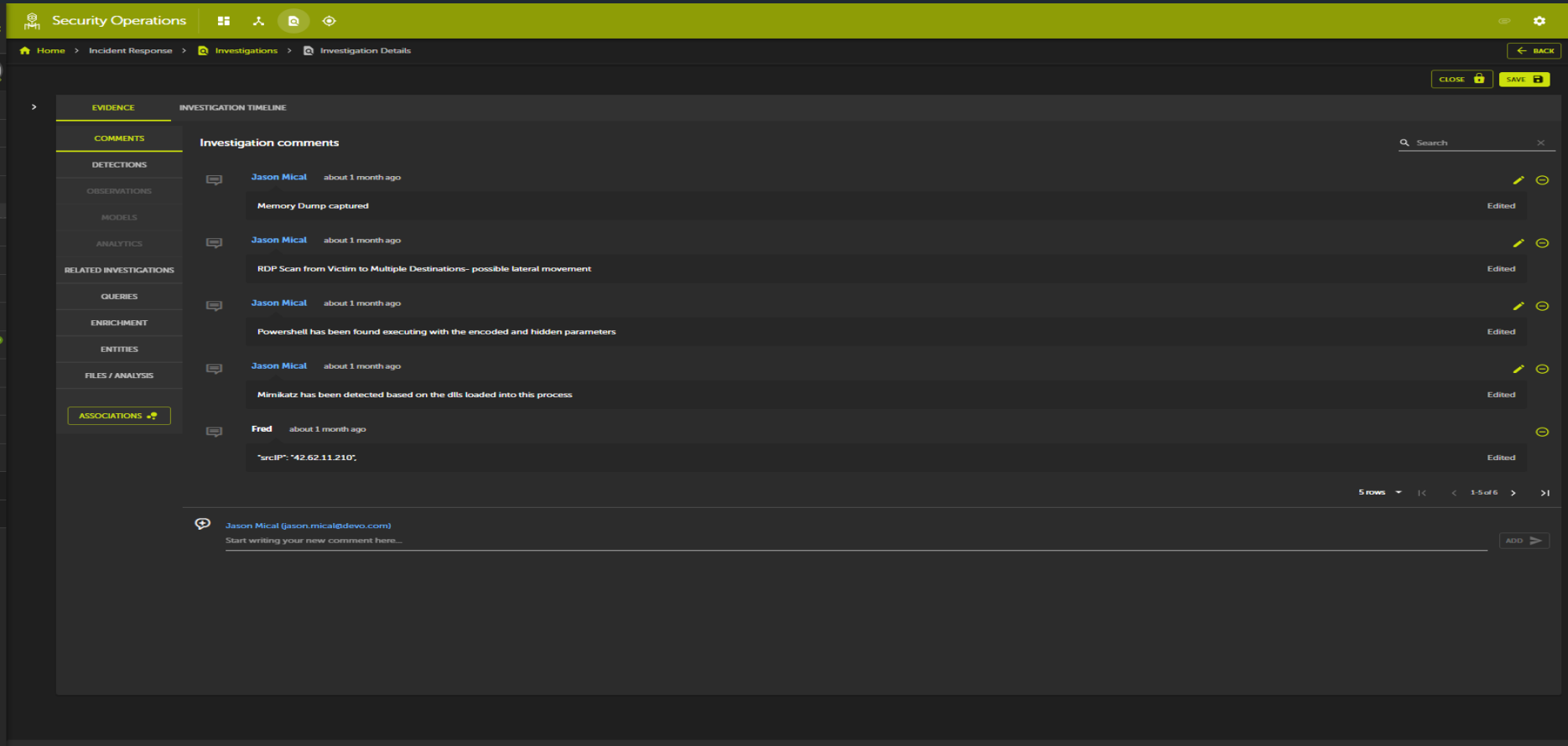
Investigation Workbench



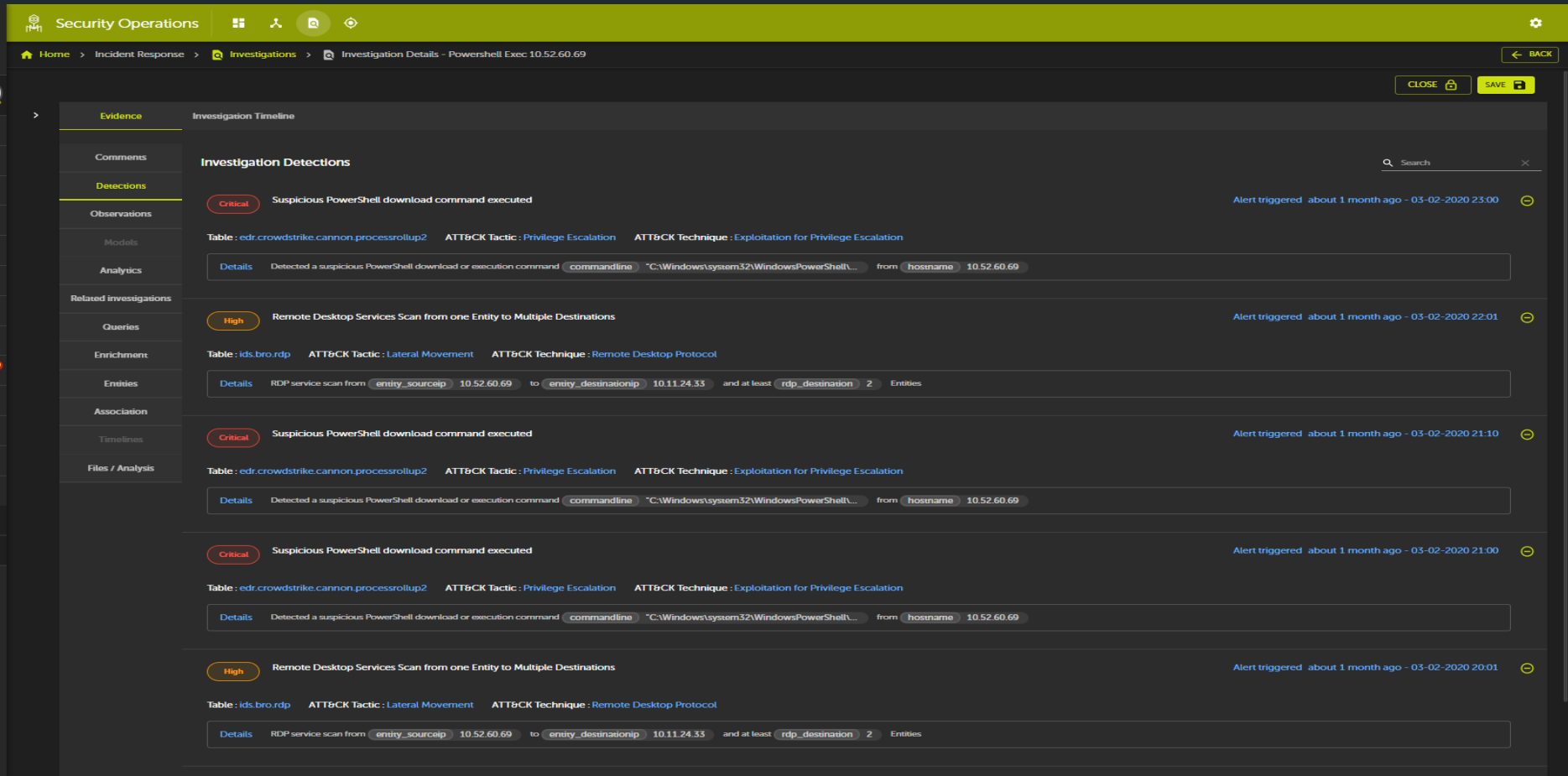
Investigation Timeline



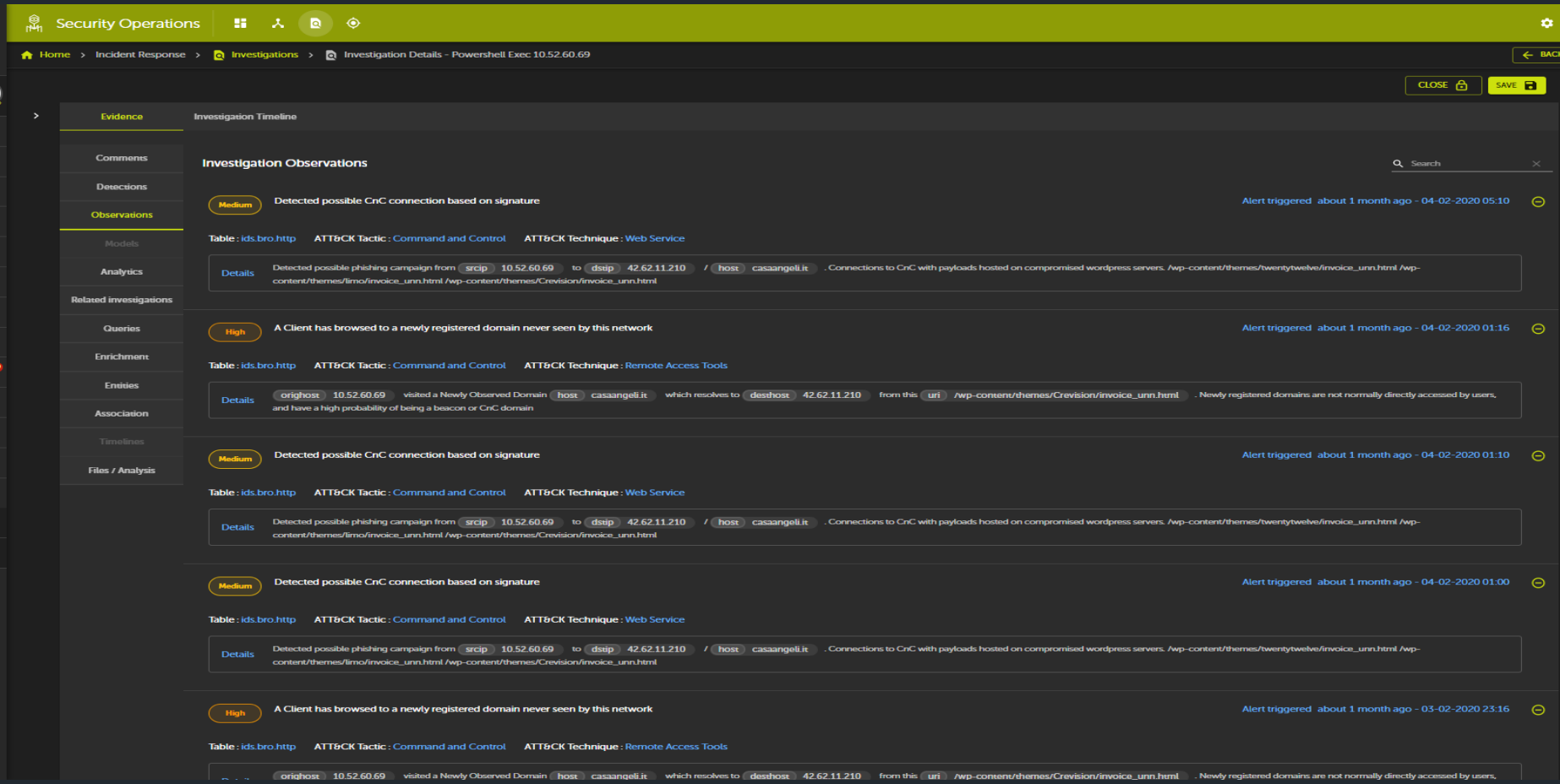
Investigation Workbench- case notes



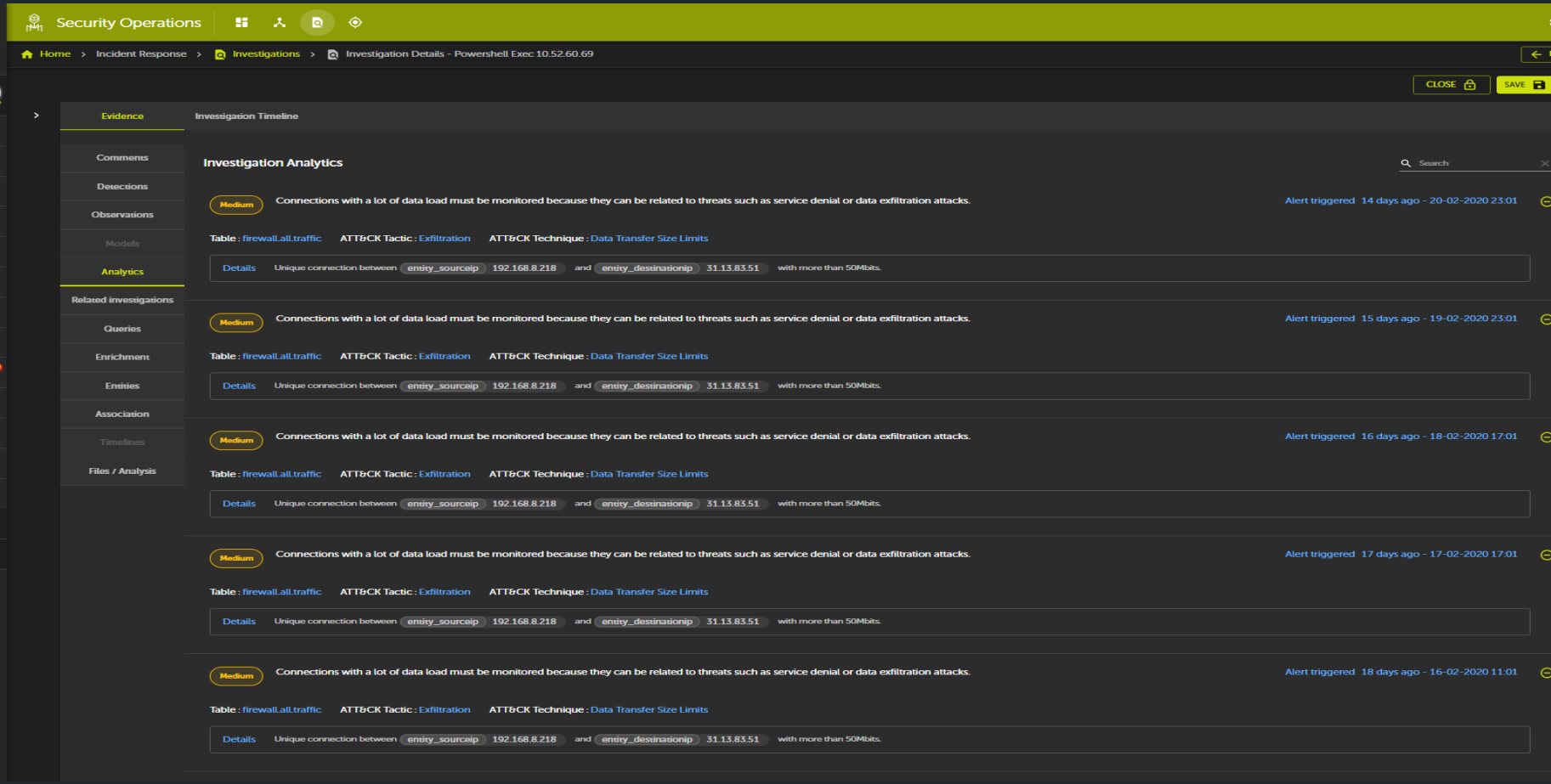
Investigation Workbench- Detections



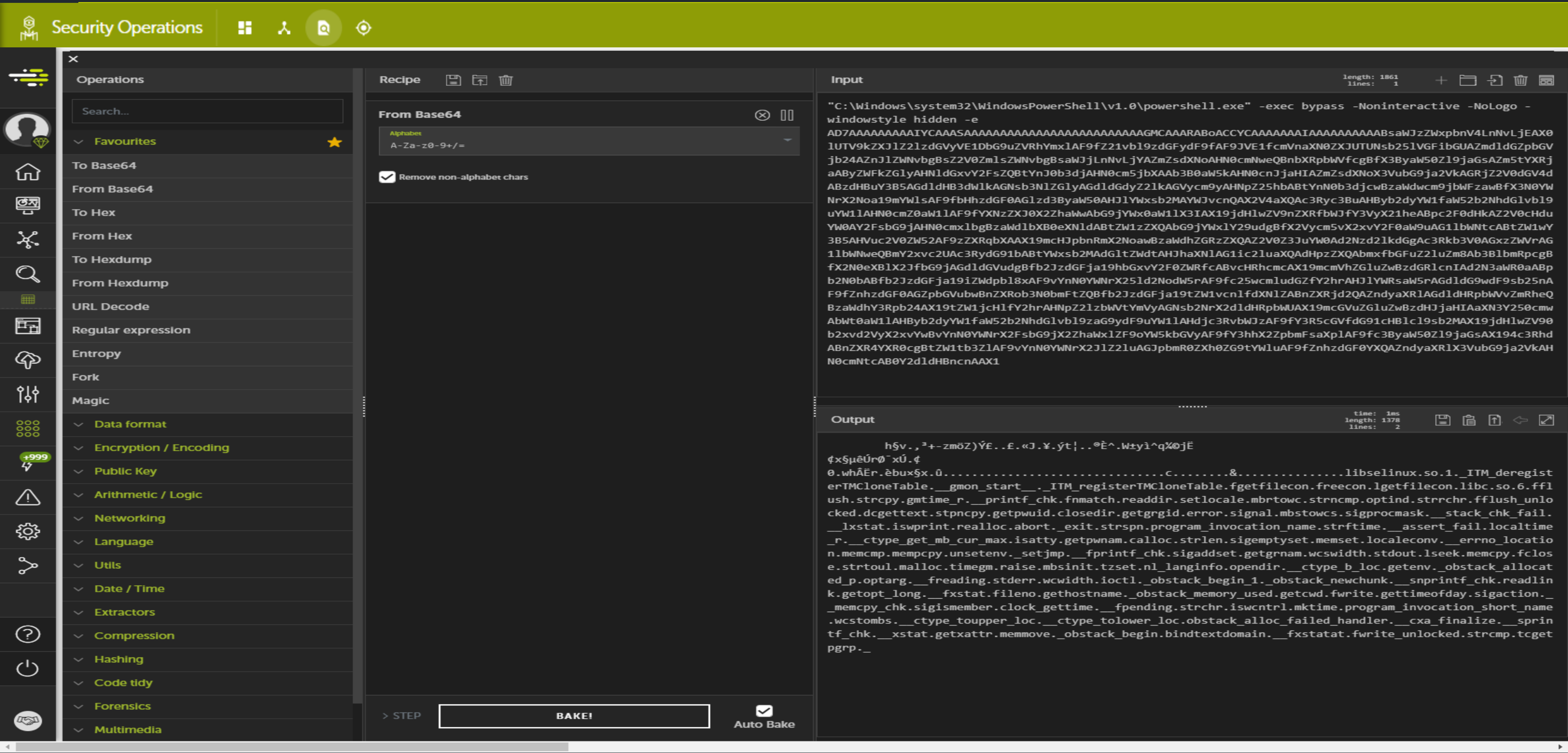
Investigation Workbench- Observations



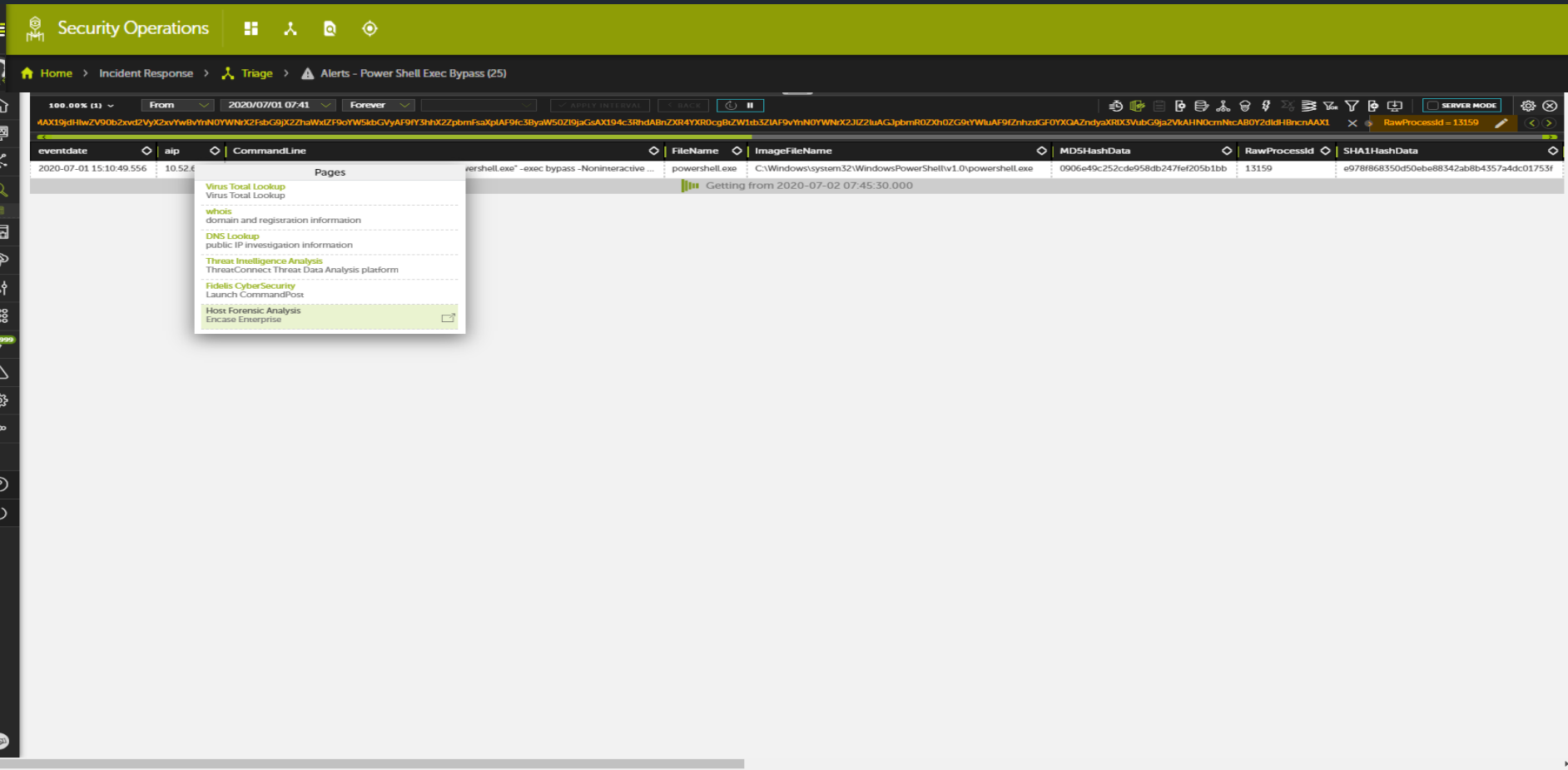
Investigation Workbench- Analytics



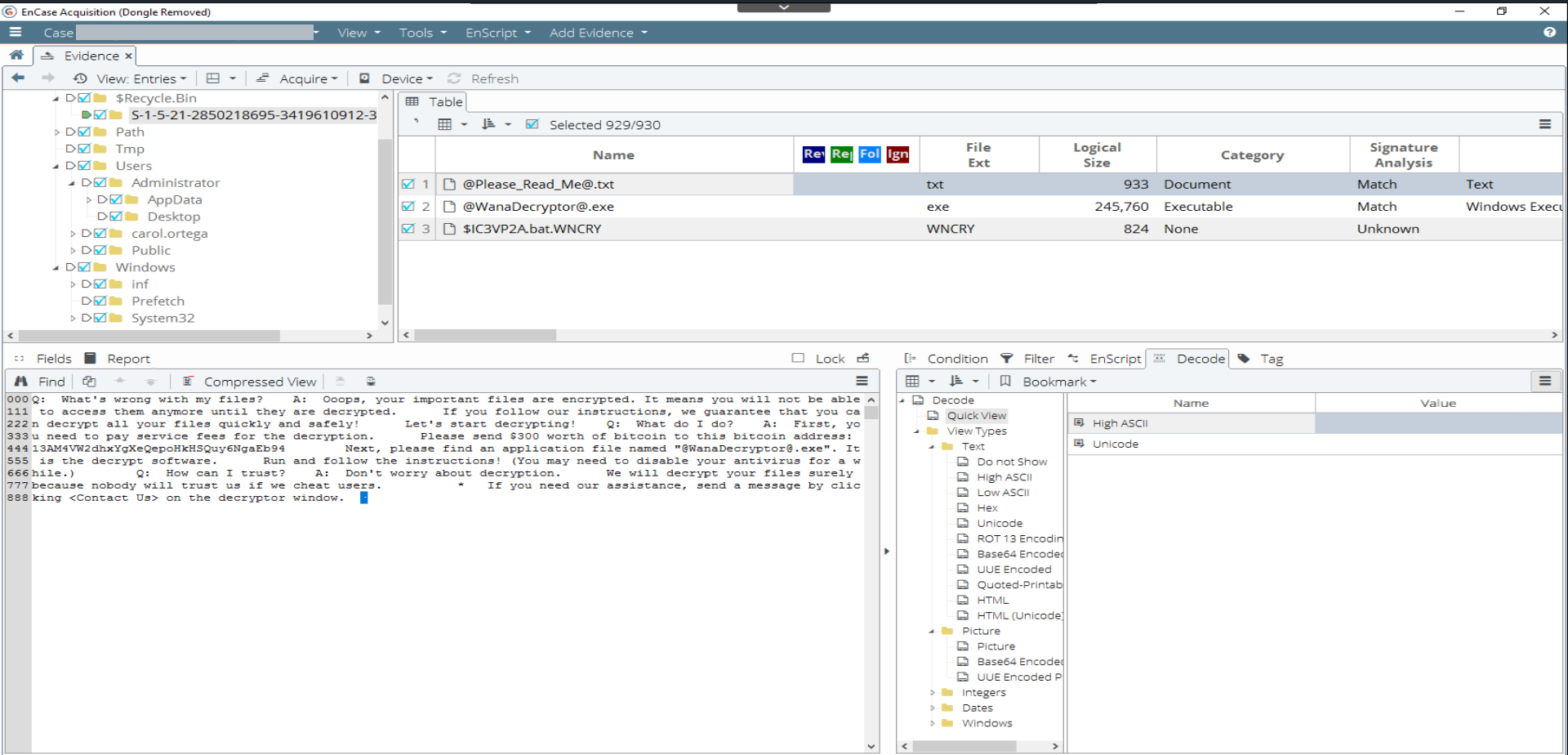
Investigation Workbench- Forensic analysis of obfuscated commands



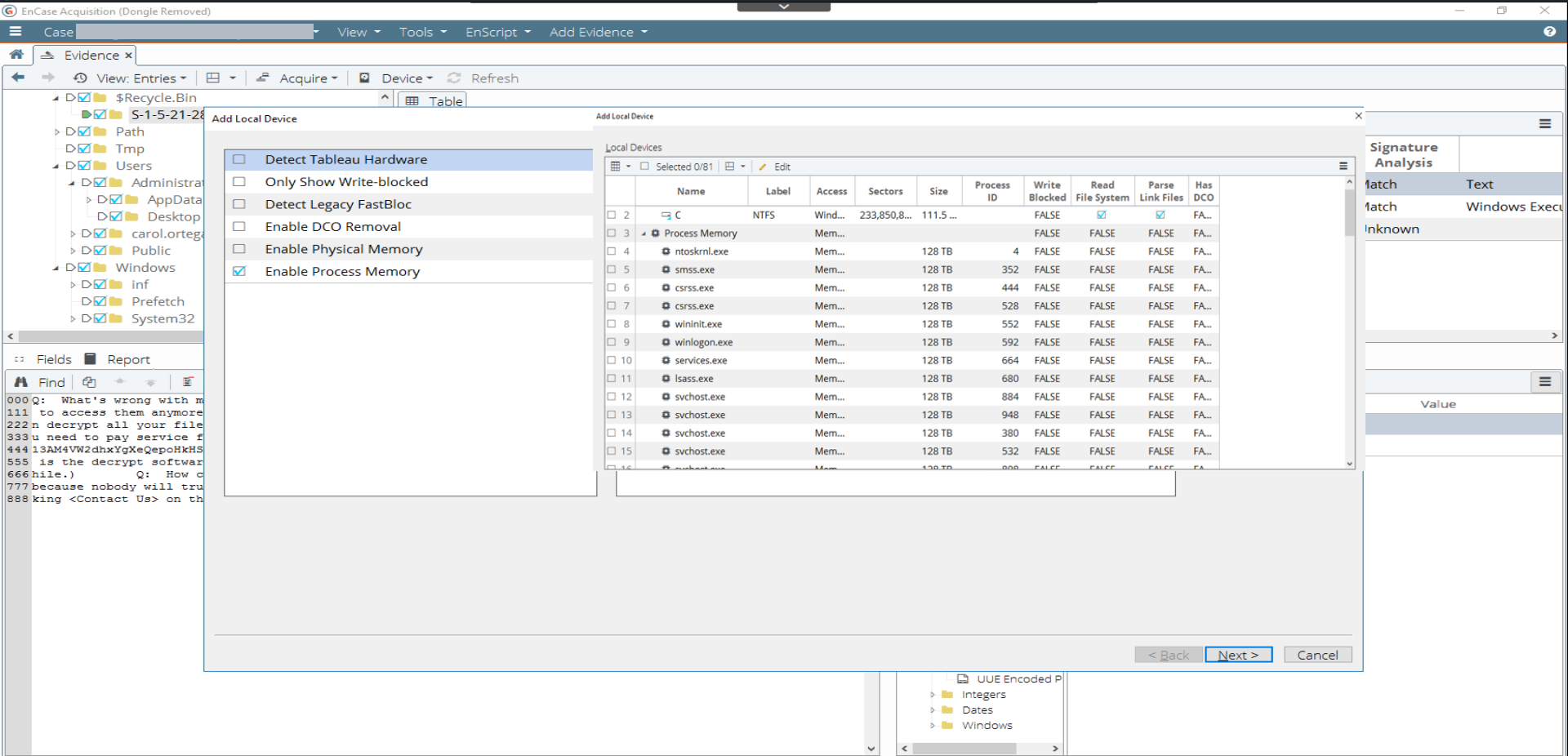
Investigation Workbench- Pivot to forensic utility to capture live artifacts



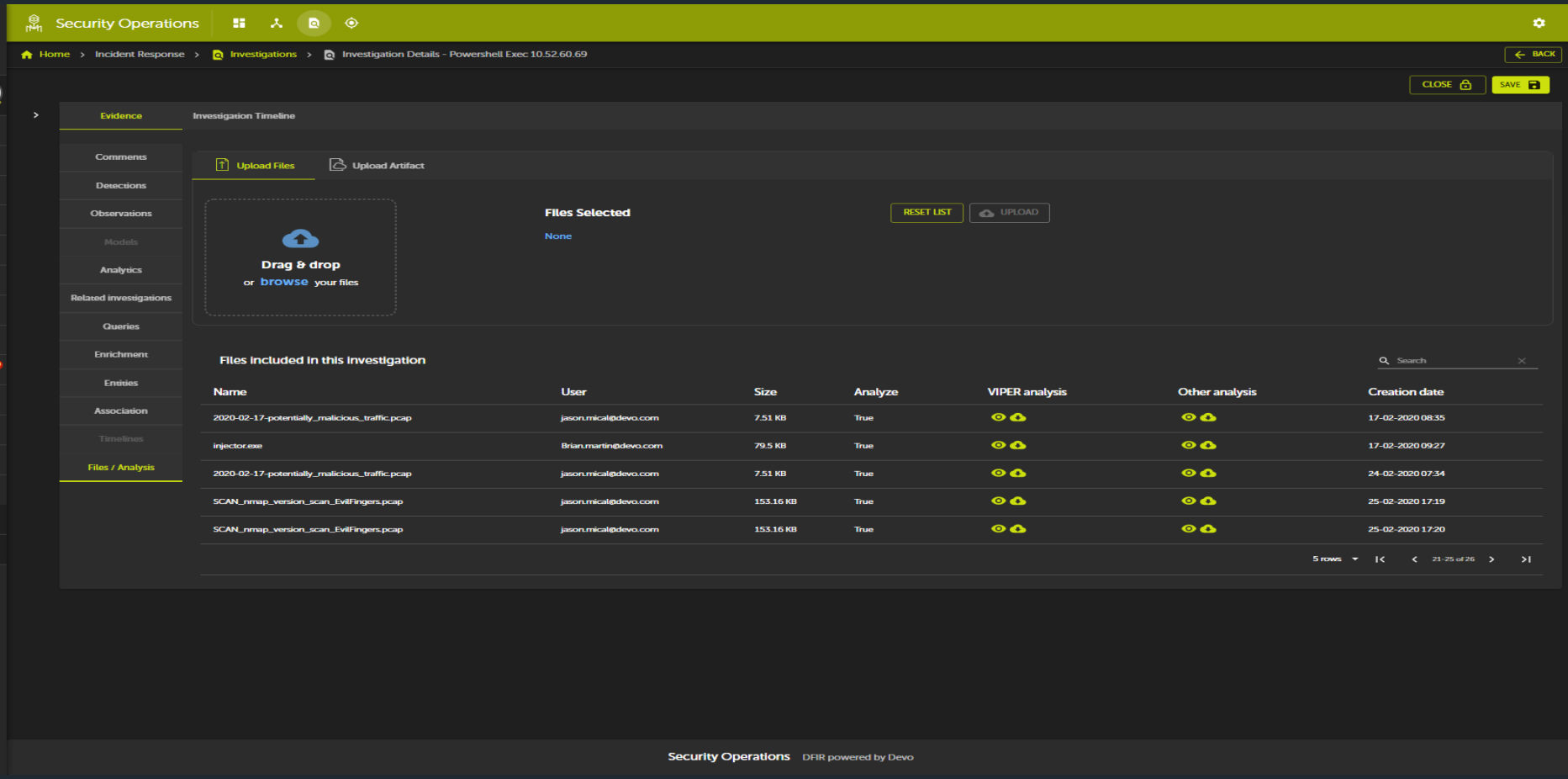
Acquire forensic Image from identified victim



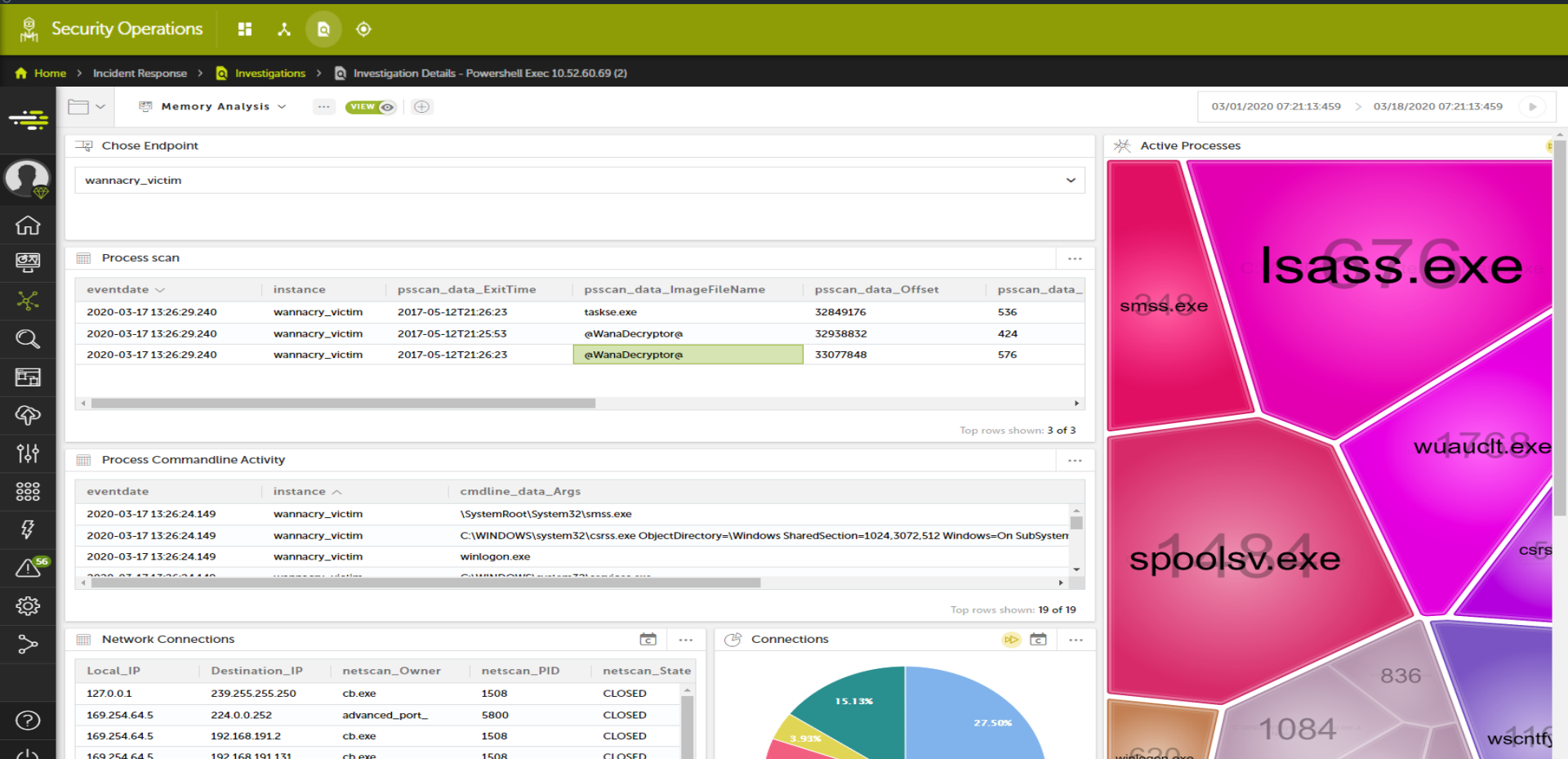
Capture Live memory from victim



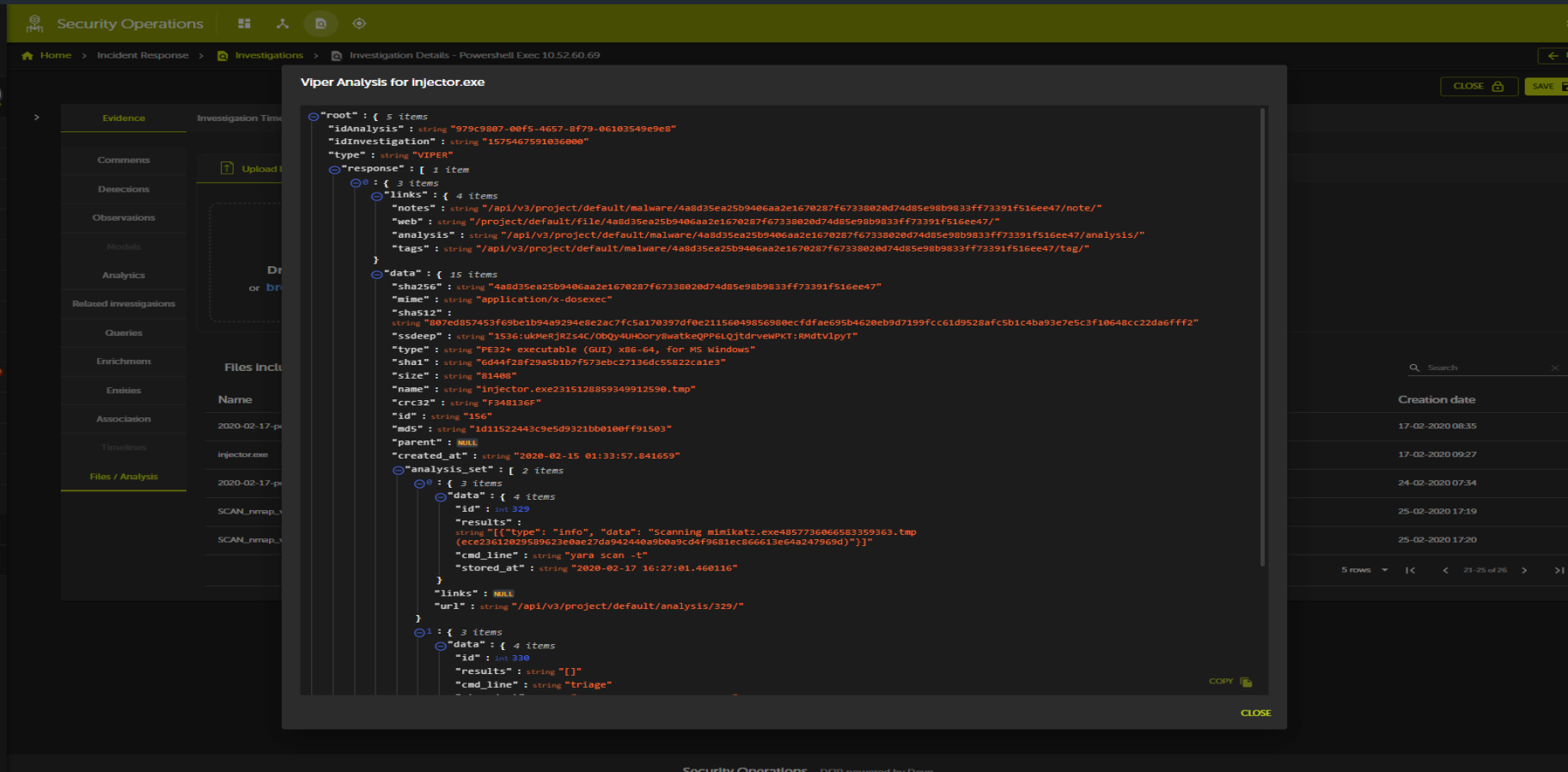
Centralized Evidence Locker



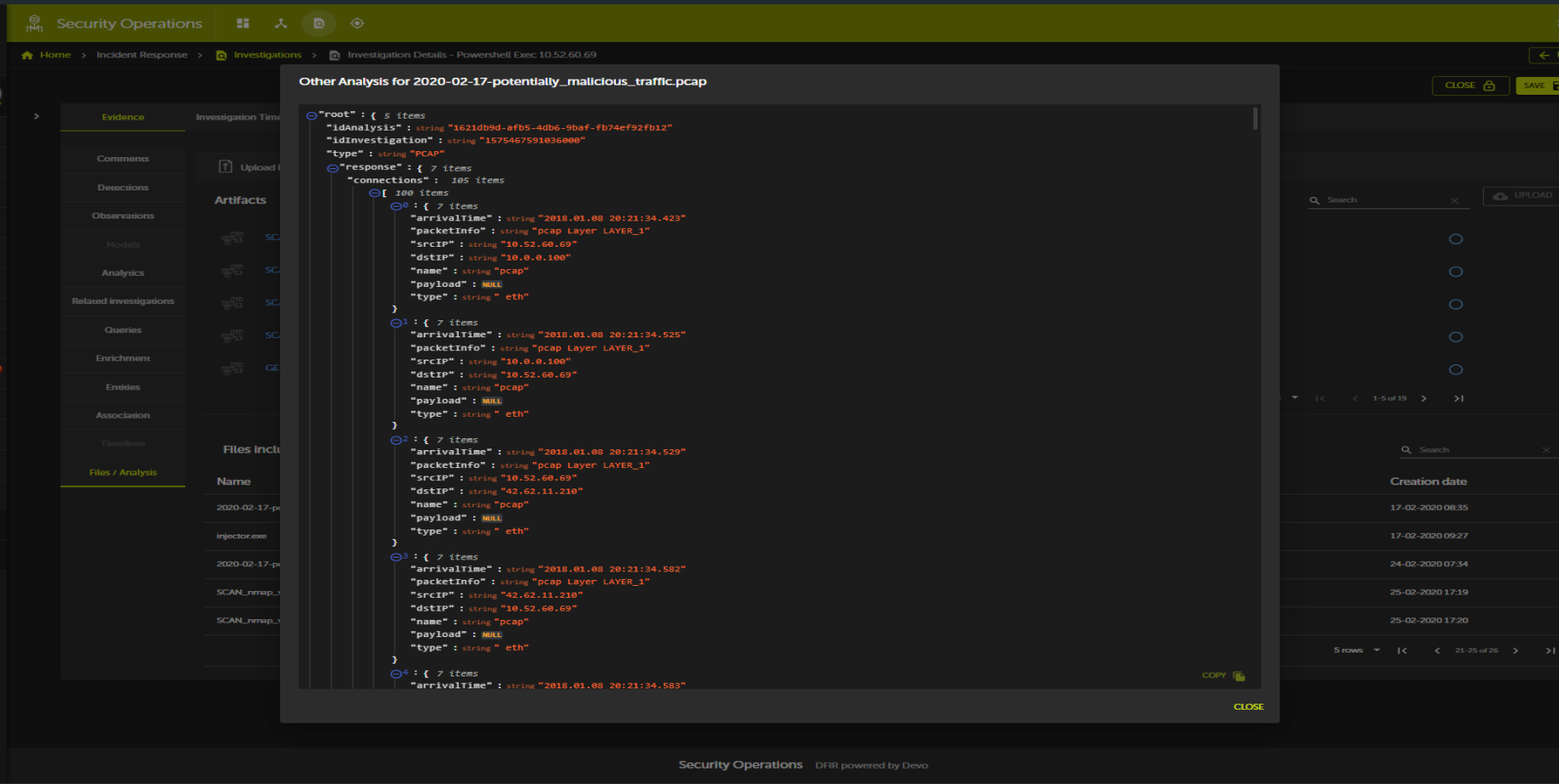
Evidence Locker- memory analysis



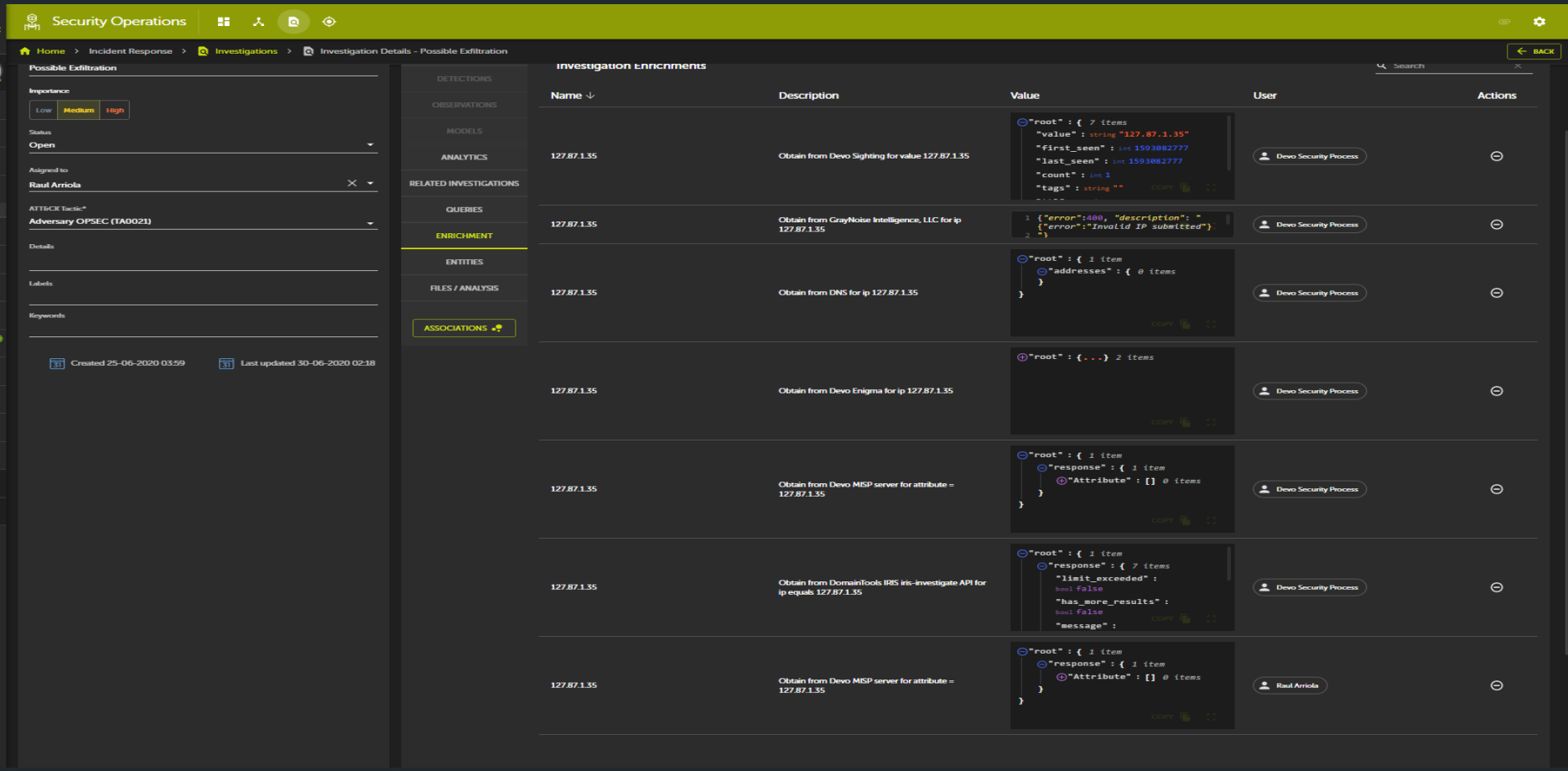
Evidence Locker- Binary Analysis



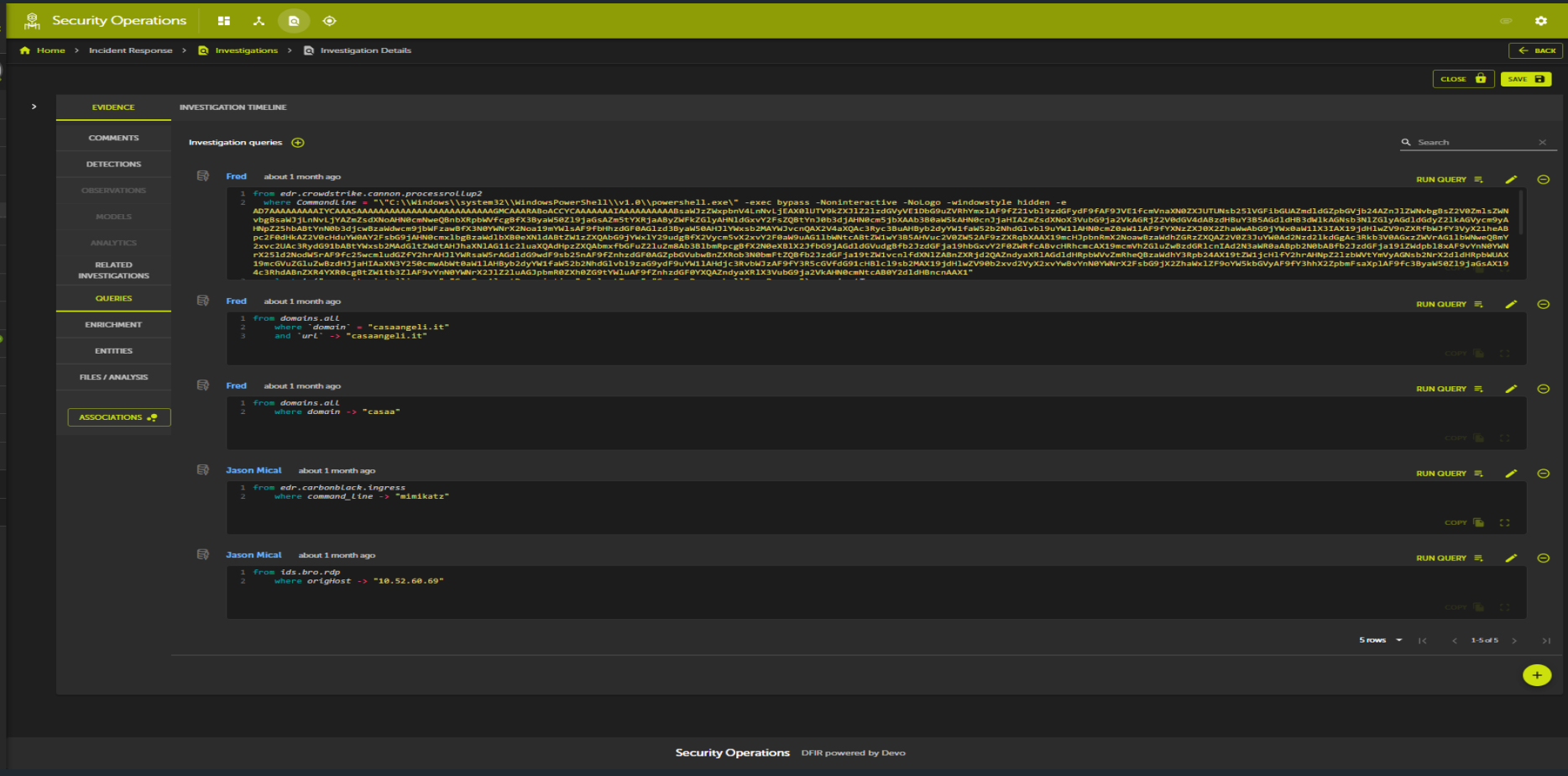
Evidence Locker- Pcap analysis



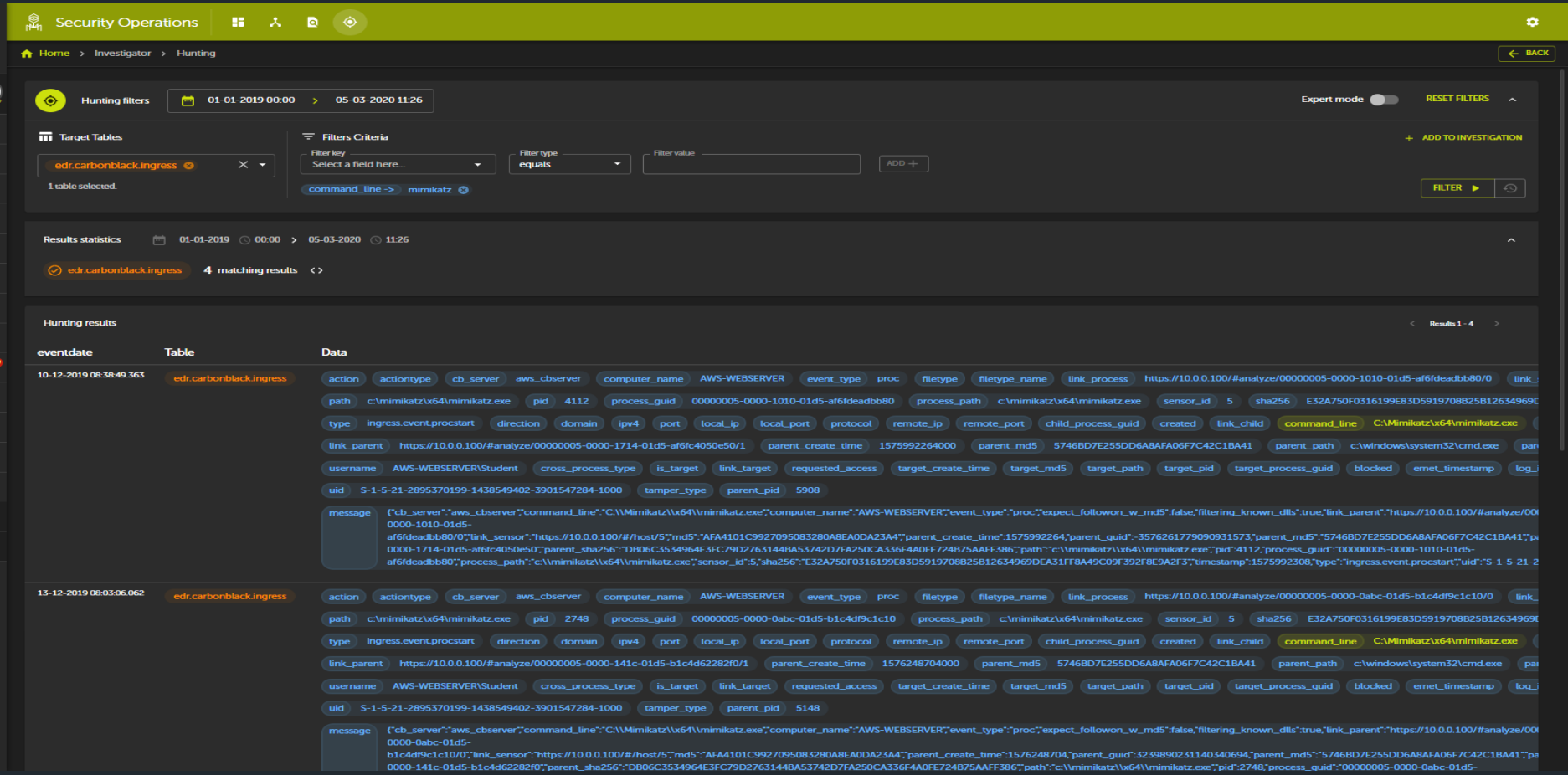
Investigation Workbench- Automated Entity Enrichment



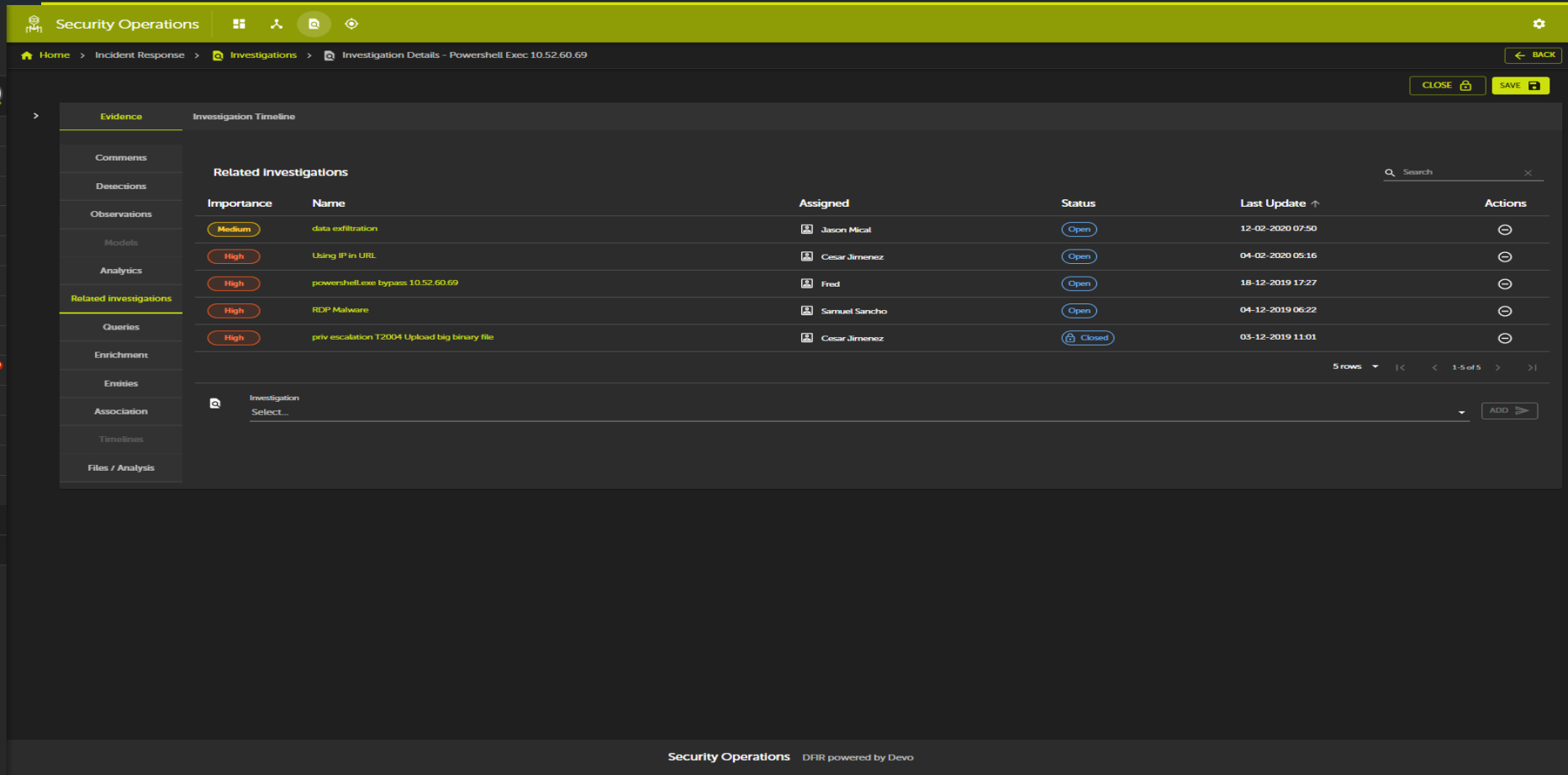
Investigation Workbench- investigative searches



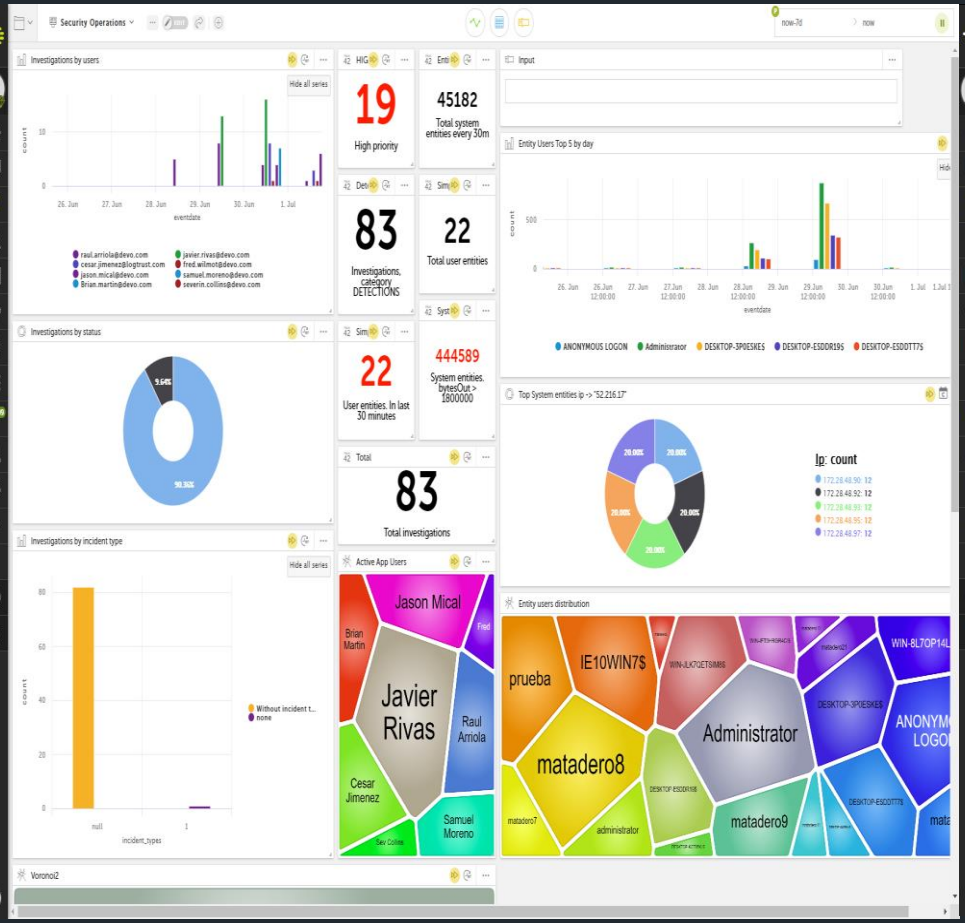
Hunting workbench

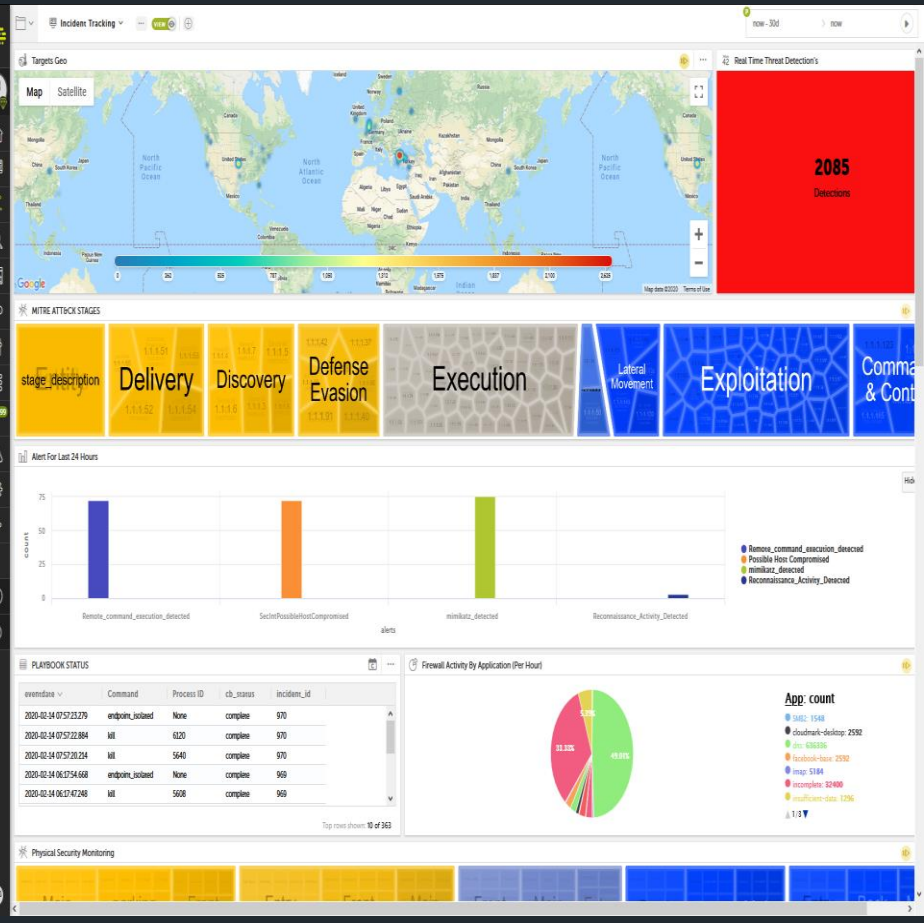


Investigation Workbench- Related investigations



Live Interactive Reporting/Dashboards





Questions?

Learn more at devo.com or email us at sales@devo.com


DEVO
THANK YOU