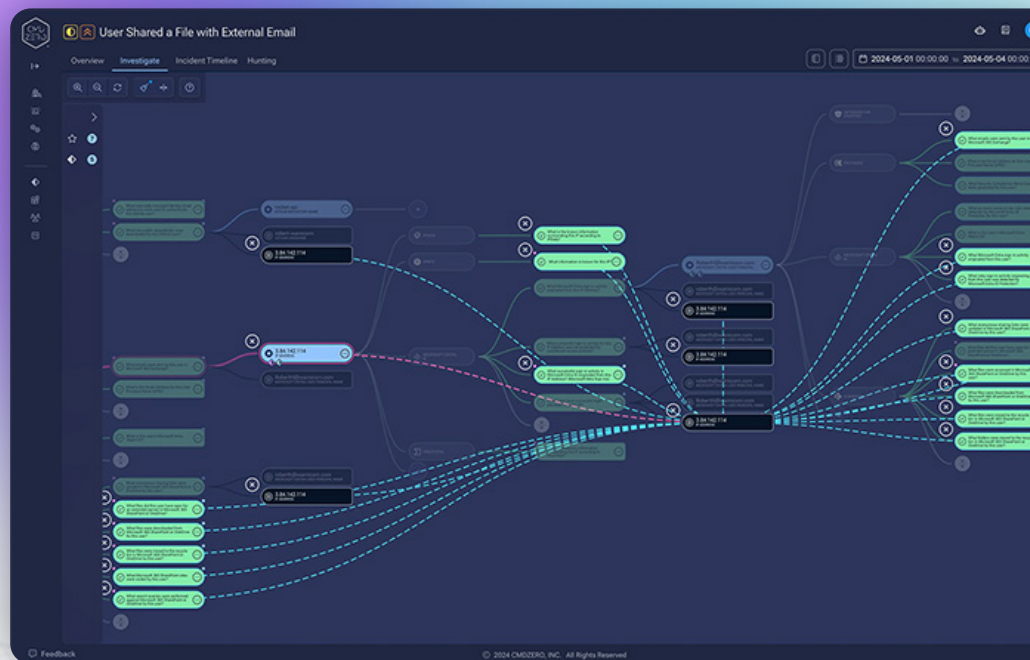# Autonomous & AI-assisted Cyber Investigations

Supercharge tier-2+ analysis

- Resolve complex cases in minutes
- Remove the grunt work
- Speed up analyst onboarding
- Continuously build knowledge
- Coach, collaborate, hand over

Cyber Investigations

Identity-based investigations

BEC & Email investigations

Threat Hunting

Learn more at cmdzero.io

Complex investigations are the most significant bottleneck for security operations today.

94%
of organizations report a lack of standardized processes for cyber investigations.

88%
of security leaders express concerns about operational issues related to lack of skilled staff and high attrition rates.

72%
or respondents admit to having blind spots for non-security data sources.

ⓘ **Read the Top Challenges in Cyber Investigations & Recommendations for SecOps Leaders to learn more.**

Maximize value from existing SecOps investments

DATAOPS
SIEM

INGEST
Data Ops

Data collection
Normalization
Detection/Alerting
Storage/Index

IN-HOUSE TIER-1
MDR/MSSP
SOAR/HYPERAUTOMATION

TRIAGE
Tier-1

Triage
Prioritization
Resolve/Escalate

CMD ZERO

INVESTIGATE
Complex
(Tier-2+) Analysis

Investigation
Threat Hunting
Building Institutional
Knowledge

MANUAL PROCESSES
SOAR/HYPERAUTOMATION

RESPOND
Take Remedial Action

Benefits

- Reduce time to understand and respond
- Deliver consistent outcomes
- Enable collaboration and learning
- Build institutional knowledge

Supercharge tier-2+ analysis

- **Tier-3 analysts** overcome administrative drag with automated data collection, timelines and repor.
- **Tier-2 analysts** can now investigate complex cases across all data sources.
- **All users** benefit from autonomous investigations and AI-assisted flows.

CMD ZERO

Visit cmdzero.io to learn more →