Improve Exabeam Output Through Watchlists & Dynamic Tagging

SCENARIO:

Customer is looking to improve incident detection and response capabilities by enriching Exabeam output with contextual data.

SOLUTION:

Identropy developed a framework for “Watchlist Automation” and “Dynamic Tagging & Rules Amplification” for Exabeam that can withstand product upgrades.

WHAT PAST CUSTOMERS HAVE ACHIEVED:

- Improved threat hunting and incident response capabilities by deploying watchlists and dynamic tagging.
- Operationalized Exabeam output for conducting investigations by generating usable data.
- Replaced manual updates of watchlists with automated procedures which leveraged active directory attributes.
- Improved risk scoring by combining adjusted scores with the tagging of higher risk individuals to amplify risk scores as needed.

IDENTROPY’S CONTEXT DEVELOPMENT SERVICES

- **REVIEW** Exabeam rules, the quality of log data ingested, and applicable context data.
- **IDENTIFY** Exabeam content where watchlists and dynamic tagging can improve incident detection and escalation processes.
- **IMPLEMENT** watchlists for areas with known risks which require continuous monitoring, and tagging for areas where aggregate risks could elevate risk level of an individual.
- **AUTOMATE** processes by allowing watchlists to dynamically update based on attributes in Active Directory.

ESTIMATED LEVEL OF EFFORT

- Duration of 4 weeks
- 1 PS engineer and 1 part-time manager for oversight
- Customer SOC manager and SOC analysts contribute 15-20% of their time