Grant Thornton

Managed Cyber Analytics for Exabeam's Security Management Platform[1]

A team of specialists dedicated to driving consistent return out of your Exabeam investment, through user and entity event monitoring, system health monitoring, and incident response support at a flat monthly rate.

The Challenge Organizations Face with Maximizing Exabeam to Drive a Cyber Program

Organizations have been seeking to leverage Exabeam for enhanced cyber analytics capabilities to more efficiently detect and respond to both external and internal threats. Emerging use cases have typically included:

- User activity monitoring
- Insider threat monitoring
- Privileged user monitoring
- Advanced external threat cybersecurity analytics

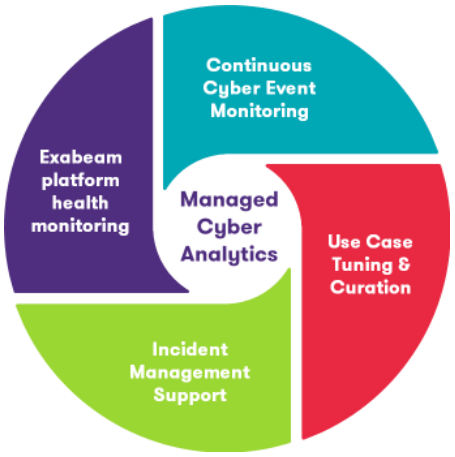
However many organizations underutilize the solution for a number of reasons:

- Limited understanding of the underlying technology to achieve actionable use cases. Leveraging Exabeam can require knowledge of a number of elements such as Hadoop, Elastic, Kibana, and Mongo.
- Limited resources to focus on monitoring and tuning the solution that does not function as their "core security incident and event management (SIEM) solution". Many organizations still leverage various components of legacy log management or SIEM solutions to support their cybersecurity programs, and therefore do not have the resources to invest in leveraging security analytics technologies.
- Limited focus on data curation and optimization within the solution to maximize use case results.
- Limited understanding of the underlying event data sources and their coverage for the organization.

Grant Thornton's Managed Cyber Analytics (MCA)

Grant Thornton's MCA is a tailored and transparent service powered by Grant Thornton's highly skilled Exabeam professional services specialists to monitor and address cyber threats in your environment. The solution encompasses:

- Daily cyber event monitoring leveraging Exabeam Advanced Analytics (AA), Entity Analytics (EA), Data Lake (DL), Incident Responder (IR), and Case Management (CM) with a 12 hour a day, 5 day a week support model[2]
- Cyber incident analysis and coordination to onsite customer cybersecurity staff
- Daily Exabeam platform health and fault monitoring
- Tuning and curating existing data sources and use cases
- Support and execution of Exabeam platform upgrades
- Professional services for additional data source integration, use cases, automations, and report development available at a flat hourly rate



[1] www.Exabeam.com

[2] Custom support models available upon request

Our MCA Program

Planning & Health Checks

- Initiate platform onboarding (system access, platform health check, current state data sources and use case configuration review)
- Designate roles and responsibilities between Grant Thornton and client staff
- Confirm processes for:
  - Change control
  - Security event notification
  - Incident response support

Key Outputs:

- System health-check summary
- MCA process document

System Monitoring

- Conduct 12x5 event monitoring for Exabeam AA, EA, DL, and IR/CM
- Provide incident management support in accordance with documented processes:
  - Review activity in comparison to peer activity
  - Collaborate with stakeholders to correlate events with other client telemetry
- Support remote response actions with client stakeholders for escalated events

Key Outputs:

- Weekly event summary reports and metrics
- Quarterly project reviews

Upgrades & Enhancements

- Integrate additional data sources and use cases
- Integrate additional user context data
- Support change control requests
- Conduct requested upgrades
- Monitor Exabeam platform for tuning and performance

Key Outputs:

- Updated data sources integrated
- Requested upgrades completed

Why Grant Thornton?

- Dedicated alliance partner with direct access to Exabeam's engineering, product development and customer support teams
- Experience and expertise with the implementation and operation of Exabeam technologies for numerous clients including, AA, EA, DL, and IR/CM
- Our deep understanding of the Exabeam platform combined with our depth and breadth of experience in cybersecurity, privacy, and incident management allows us to bring this experience to bear for your greatest cyber challenges
- Backed by a national team of cybersecurity and privacy professionals to meet the needs of your cyber program

Contact

John Pearce
Principal,
Cyber Risk
T +1 703 637 4071
E john.pearce@us.gt.com

Grant Thornton