WHITE PAPER

exabeam

SUPPORTING MAS-TRM GUIDELINES WITH EXABEAM

OVERVIEW

While the Monetary Authority of Singapore (MAS) has issued risk management guidelines for banks and FIs for many years, the Technology Risk Management (TRM) guidelines expand the breadth of impact and scope for these institutions:

- The TRM guidelines affect all systems within the IT environment
- FIs other than banks fall within the scope of TRM
- TRM has legal implications due to reporting notices

In short, TRM affects a broad set of firms, and a broad set of systems within those firms. Reporting requirements, both internally and to MAS, will drive significantly more powerful monitoring capabilities.

BEHAVIORAL MONITORING FOR MAS-TRM

While FIs have deployed multiple security and risk management solutions in recent years, many of those are unable to detect the modern threats that affect risk related to data security and protection. Specifically, modern threats are typically credential-based, but existing security products are not. As a result, firms are unable to detect risky activity, and even when threats are detected, these same firms are unable to respond quickly.

Exabeam has customers across the financial services industry, including leading firms within banking, insurance, and payroll processing. These customers use Exabeam behavioral analytics capabilities to monitor their IT environments for risks. Behavioral monitoring assesses IT risk and enables risk management personnel to investigate quickly and exhaustively. It is a leading-edge approach to IT security and risk management.

THE EXABEAM APPROACH

Exabeam provides a powerful software solution for detecting, prioritizing, investigating, and responding to security threats and risky user activity. The solution is built on a breakthrough data model that creates a new data object: the session. Sessions include all linked activity for each user, both normal and risk-elevated activity, as well as context and audit metadata. The result is a data analysis and reporting platform that enables auditors and risk analysts to find any users that are performing unusual and risky activity, even in a “dirty data” environment.

The effect is similar to the transformation in business intelligence brought about by the introduction of data cubes and star-schemas, i.e. a new data structure made new types of questions and analyses possible. Exabeam brings that same transformation to IT security and risk management. The solution consists of four data capabilities:

- ***Sessionize*** – Raw user data is processed into linked sessions, creating a data structure that can be queried in multiple high-level ways. For example, Exabeam can return “all user sessions where the employee used privileged credentials to access an executive system for the first time” – without requiring knowledge about the underlying raw data formats or system search languages.
- ***Analyze*** – Sessions are analyzed to determine which users are acting in a risky manner. Those users are presented to analysts for prioritized audit or investigation.
- ***Hunt*** – Analysts can also proactively hunt for users whose activity matches any combination of attributes. This is especially useful in cases where one FI has been attacked and shares the information with other FIs. Those other institutions can use Exabeam to search for any users that match the risk patterns.
- ***Investigate*** – Once users are identified as risk-elevated, Exabeam provides facilities for automating the the data collection and processing required for an investigation or audit.

APPLYING BEHAVIORAL MONITORING TO MAS-TRM GUIDELINES

Exabeam supports many of the key TRM guidelines, as described below.

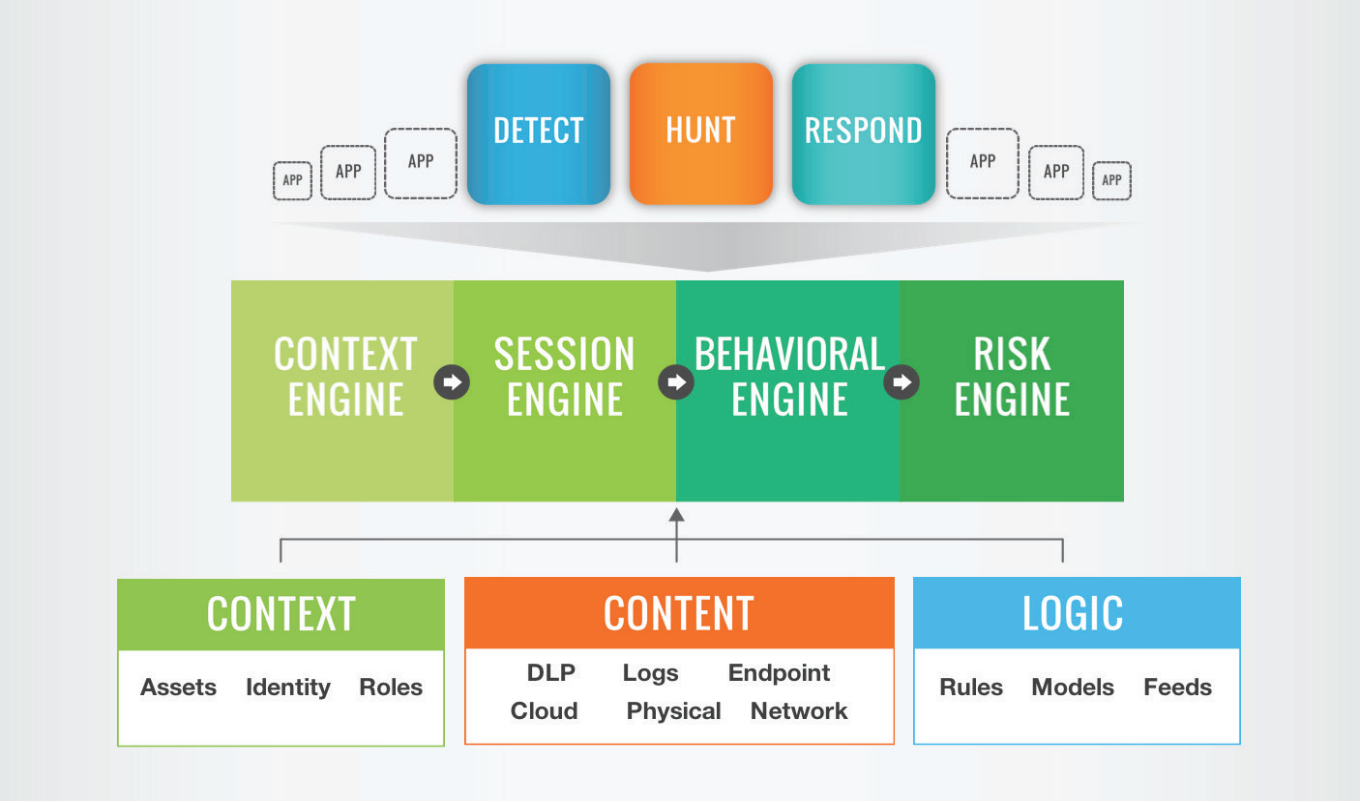
SECTION	GUIDELINE	EXABEAM SUPPORT
4.1.1	*For each type of risk identified, the FI should develop and implement risk mitigation and control strategies that are consistent with the value of the information system assets and the level of risk tolerance.*	Exabeam security intelligence solutions enhance risk mitigation and control strategies by providing a complete picture of activity-based risk, at the account, user, and department levels. Based on asset value and risk level, Exabeam can also invoke actions within third-party controls, such as freezing a transaction or account, or requiring higher levels of authentication.
5.1.4	*IT outsourcing should not result in any weakening or degradation of the FI's internal controls. The FI should require the service provider to employ a high standard of care and diligence in its security policies, procedures and controls to protect the confidentiality and security of its sensitive or confidential information, such as customer data, computer files, records, object programs and source codes.*	Exabeam monitors external access to the corporate assets and can be especially useful in IT outsourcing scenarios, where account credentials might be shared across outsourcer staff. Exabeam can tie specific activity to specific machines and IP addresses, and then to identities, making audits easier and more accurate.
7.1.5	*All changes to the production environment should be approved by personnel delegated with the authority to approve change requests.*	By integrating with change-control systems and ingesting configuration logs, Exabeam can notify security analysts any time that a system is changed without a corresponding approval.
7.1.7	*Audit and security logs are useful information which facilitates investigations and trouble shooting. The FI should ensure that the logging facility is enabled to record activities that are performed during the migration process.*	Exabeam solutions ensure that all activity can be monitored. Auditors can proactively drill into risky activity of users or departments to understand exactly how a problem unfolded and how to mitigate it.
9.0.1	*The IT landscape is vulnerable to various forms of cyber-attacks, and the frequency and malignancy of attacks are increasing. It is imperative that FIs implement security solutions at the data, application, database, operating systems and network layers to adequately address and contain these threats.*	Exabeam's intelligence solutions operate at all levels: network, cloud, application, database, OS, as well as physical badge reader and USB-port levels. Essentially, Exabeam's monitoring can integrate useful data from any level in the IT infrastructure. Unlike endpoint or privileged user security products, Exabeam operates everywhere and applies to every user of every level.

SECTION	GUIDELINE	EXABEAM SUPPORT
9.1.1	*Internal sabotage, clandestine espionage or furtive attacks by trusted staff, contractors and vendors are potentially among the most serious risks that FIs could face in an increasingly complex and dynamic IT environment. Current and past staff, contractors, vendors and those who have knowledge of the inner workings of the FI's systems, operations and internal controls have a significant advantage over external attackers. A successful attack not only jeopardises customer confidence in the FI's internal control systems and processes but also causes real financial loss when trade secrets and proprietary information are divulged. FIs should identify important data and adopt adequate measures to detect and prevent unauthorised access, copying or transmission of confidential information.*	Exabeam automatically classifies executive and sensitive assets, classifies accounts as privileged, system, or standard user, and creates baseline profiles of normal behavior for every user and machine on the network. As a result, if either a compromised insider or malicious insider account begins performing unusual and risky activity, Exabeam flags it in real time and links the activity to what came before and after, i.e. a complete investigative chain.
9.6.1	*Security monitoring is an important function within the IT environment to detect malicious attacks on IT systems. To facilitate prompt detection of unauthorised or malicious activities by internal and external parties, the FI should establish appropriate security monitoring systems and processes.*	Exabeam performs this function, as a top-level security monitoring solution that monitors all activity of internal and external users. The solution comes with pre-built monitoring processes and use cases, to facilitate best practices for security operations centers.
9.6.3	*The FI should implement security monitoring tools which enable the detection of changes to critical IT resources such as databases, system or data files and programs, to facilitate the identification of unauthorised changes.*	Exabeam links all activity, both security violations, normal activities, and other management actions, into a risk-scored timeline for every user, for every day. This timeline can show how a system was re-configured, how there is no accompanying approval, and also any downstream risky actions that occurred after the change. As a result, Exabeam not only detects unauthorized changes, but can automatically link those to risky activities, to facilitate investigations and audits.
9.6.4	*The FI should perform real-time monitoring of security events for critical systems and applications, to facilitate the prompt detection of malicious activities on these systems and applications.*	Exabeam solutions apply behavioral analysis of user and machine behavior to detect malicious activities occurring either via compromised or misused credentials.
11.1.1	*The FI should only grant user access to IT systems and networks on a need to-use basis and within the period when the access is required. The FI should ensure that the resource owner duly authorises and approves all requests to access IT resources.*	A common issue for financial organizations is that, over time, users accumulate multiple levels of privileged access (i.e. multiple accounts or tokens) but never relinquish them. As a result, these firms find that many users currently hold and use access rights that are unrelated to their jobs. Exabeam solutions enable detection and remediation of privileged account use, to "shrink the threat surface" by reducing privileged access.

SECTION	GUIDELINE	EXABEAM SUPPORT
11.1.3	*For accountability and identification of unauthorised access, the FI should ensure that records of user access are uniquely identified and logged for audit and review purposes.*	Exabeam is unique in its ability to link security alerts to machines and most importantly, back to specific identities, even if the data is "dirty" or missing. This is especially useful for audit, where shared administrative credentials might make attribution difficult. Exabeam is able to attribute activity to users, regardless of the state of the data itself.
11.1.6	*The FI should ensure that no one has concurrent access to both production systems and backup systems, particularly data files and computer facilities. The FI should also ensure that any person who needs to access backup files or system recovery resources is duly authorised for a specific reason and a specified time only. The FI should only grant access for a specific purpose and for a defined period.*	Exabeam solutions link activity across a user's multiple accounts, machines, networks, and IP addresses, making it easy to determine if a user has concurrent access to production and backup systems.
11.2.3	*The FI should closely supervise staff with elevated system access entitlements and have all their systems activities logged and reviewed as they have the knowledge and resources to circumvent systems controls and security procedures. The FI should adopt the following controls and security practices:* *a. Implement strong authentication mechanisms such as two-factor authentication for privileged users;* *b. Institute strong controls over remote access by privileged users;* *c. Restrict the number of privileged users;* *d. Grant privileged access on a "need-to-have" basis;* *e. Maintain audit logging of system activities performed by privileged users;* *f. Disallow privileged users from accessing systems logs in which their activities are being captured;* *g. Review privileged users' activities on a timely basis;* *h. Prohibit sharing of privileged accounts;* *i. Disallow vendors and contractors from gaining privileged access to systems without close supervision and monitoring; and* *j. Protect backup data from unauthorised access.*	Exabeam solutions monitor the actual use of authentication mechanisms and privileged accounts, making it easy to detect unusual or out-of-policy activity. Proactive query and reporting also enables on-demand detection of all users who currently match any combination of activity and attributes that are deemed risky. The Exabeam solutions are often used by auditors to confirm security control operations.

EXABEAM IN DEPTH

The Exabeam platform consists of multiple engines that a) ingest contextual information about a FI's assets and IT environment, b) create session data structures that link all raw user activity into a coherent structure, c) build baselines of normal behavior for every user (and/or machine) on the network, and d) apply new activities to the baselines to determine which users are acting in a risk-elevated manner.



ABOUT EXABEAM

Exabeam's security intelligence solution leverages existing log, endpoint, and other data to quickly detect advanced attacks, prioritize incidents and guide effective response. The company's Stateful User Tracking™ automates the work of security analysts by resolving individual security events and behavioral anomalies into a complete attack chain. This dramatically reduces response times and uncovers attack impacts that would otherwise go unseen. Built by seasoned security experts and enterprise IT veterans from Imperva, ArcSight and Sumo Logic, Exabeam is headquartered in San Mateo, California.

For more information, please visit the Exabeam website, or send an email to **info@exabeam.com.**