exabeam

WHITE PAPER

# A TECHNOLOGY SOLUTION FOR PROTECTING FEDERAL AGENCIES FROM INSIDER THREATS

## NITTF REQUIREMENTS MAPPING GUIDE

## SUMMARY


Insider threats pose major risks to every federal department and agency. All entities are directed to have a dynamic insider threat program to detect, respond, and mitigate risks posed by people who are supposed to have the government's trust. In scenarios modeled by Verizon,[1] insiders may be careless workers who misuse assets; inside agents who steal information on behalf of outsiders; disgruntled employees who destroy property or disrupt services; malicious insiders who steal information for personal gain; or feckless third parties who compromise security. This white paper describes risks posed by insiders and federal guidance for managing these risks. It also describes a modern technology approach to automate hundreds of use cases related to detecting and stopping insider threats. In particular, it maps insider threat solutions from Exabeam against maturity elements of the National Insider Threat Task Force's Insider Threat Program Maturity Framework. Security leaders in departments and agencies may use this information for planning and deployment of a robust Insider Threat Program.


### Why Insider Threats Pose Huge Federal Risks

Insider risks are a major growing threat vector. During 2018, 34 percent of all data breaches were caused by insiders, according to Verizon.[2] This percentage rose from 28 percent during 2017 and from 25 percent in 2016, according to Verizon.[3] Data breaches are often hard to detect, requiring an average of 197 days to identify and 69 days to contain one, according to Ponemon Institute.[4] Verizon says 40 percent of

[1] Verizon 2019 Insider Threat Report

[2] Verizon 2019 Data Breach Investigations Report, p. 5.

[3] See also, Verizon 2018 Data Breach Investigations Report, p. 5 and 2017 Data Breach Investigations Report, p. 3.

[4] Ponemon Institute, 2018 Cost of a Data Breach, p. 5.

insider-related breaches require years to detect; 30 percent require months, 15 percent weeks and 10 percent days.[5]

The federal focus on insider threats grew after major data breaches occurred early this century, such as diplomatic cables that were leaked by Chelsea Manning. Federal scrutiny intensified with leaks of sensitive information from the National Security Agency stolen by Edward Snowden. Incidents like these are typical of risks to the federal government, which are quite different from many of the risks facing commercial organizations. Examples of federal fallout by unauthorized disclosure of sensitive information held by departments and agencies may include disruption of diplomatic relationships, treaties and alliances; exposure of vulnerabilities affecting national security; disruption to critical infrastructure; wasted expenditures on infrastructure or personnel; and potentially grave personal risk to federal employees, contractors, international associates, and of course, U.S. citizens and guests.

## FEDERAL GUIDANCE FOR ADDRESSING INSIDER THREATS

Under the Office of the Director of National Intelligence, the National Insider Threat Task Force (NITTF) spearheads programmatic development and use of best practices for addressing insider threats. The concept of an Insider Threat Program (InTP) debuted by Executive Order 13587 in Nov. 2011.[6] In Nov. 2012, the new National Insider Threat Policy published "Minimum Standards for Executive Branch Insider Threat Programs."[7] They are the foundation of the insider threat program maturity process.

In Nov. 2018, the NITTF published the Insider Threat Program Maturity Framework.[8] The Framework's goal is to "help executive branch departments and agencies' insider threat programs advance beyond the Minimum Standards to become more proactive, comprehensive, and better postured to deter, detect, and mitigate insider threat risk."[9] The Framework includes six categories and 19 maturity elements (MEs) to help "enable departments and agencies to increase program functionality and garner greater benefits from insider threat program resources, procedures, and processes."

A major portion of the Framework presents themes aimed at strengthening InTP management, personnel and training. At a high conceptual level, the Framework also presents MEs for addressing the technological aspect for addressing insider threats but does not prescribe specific solutions. The balance of this white paper focuses on this technology: specifically the use of an insider threat solution approach that is successfully used globally by government organizations and commercial entities.

[5] Verizon 2019 Insider Threat Report, p. 6.

[6] President Barack Obama, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information"

[7] National Insider Threat Task Force, National Insider Threat Policy

[8, 9] National Insider Threat Task Force, Insider Threat Program Maturity Framework

## A TECHNOLOGY APPROACH FOR STOPPING INTERNAL THREATS

While insider risks for departments and agencies are different from risks for business entities, the risks of both share similarities in their manners of execution. These shared malicious insider behaviors include illicit use of credentials for systems access, logging into sensitive data with a privileged user's identity, downloading or transferring sensitive data for exfiltration, and so forth. Fortunately, federal entities can use an established technology approach for efficient user activity monitoring (UAM), analytics and response prescribed by the Framework. This approach, called user and entity behavior analytics (UEBA)[10] is typically deployed as an integrated capability of a modern security information and event management (SIEM) system.

User and entity behavior analytics is one of the fastest-growing areas within enterprise security, growing at a compound annual growth rate of 48 percent per year, according to Gartner.[11] Modern enterprise IT security solutions use this technology to detect and remediate advanced threats that cannot be addressed by legacy solutions. UEBA solutions ingest operational and security data from many sources, and use analytics such as machine learning and behavior analysis to determine what is "normal" behavior by users and entities on an enterprise network. Entities may include IT assets such as hosts, applications, network traffic and data repositories. The solution builds standard profiles of behavior across peer groups over time in order to create a baseline. As anomalous activity is identified, it is assigned a risk score.

### INSIDER USE CASE: COMPROMISED USER CREDENTIALS

User account credentials are keys to legitimate access, and stolen credentials is the primary vector for data breaches achieved by hacking, according to the Verizon 2019 Data Breach Investigations Report (p.10).

When a hacker uses stolen credentials, legacy security tools cannot identify unauthorized access. This scenario allows the attacker to proceed at will to access sensitive data or internal resources. Clearly, the result of compromised user credentials can be devastating, which makes this use case mandatory for a UEBA solution. It's irrelevant how the attacker obtained the credentials – UEBA must be able to detect unauthorized access across the combination of a user's account credentials, devices or IP addresses.

The capability to easily detect compromised credentials of any employee or contractor within the organization is a foundational requirement for UEBA.

The score rises with increasing amounts of anomalous behavior until it crosses a predefined threshold. Upon this escalation, UEBA sends an alert to security operations center analysts who use the data for appropriate remediation of threats.

[10] For more background, see Exabeam, "Top 10 UEBA Security Use Cases"

[11] See https://www.gartner.com/reviews/market/user-and-entity-behavior-analytics

UEBA is important because legacy tools are often unable to detect insider threats, swamping analysts with alerts that are difficult to understand and are often useless for rapid detection and remediation. UEBA solutions employ a different approach by using variations of artificial intelligence and machine learning, advanced analytics, data enrichment, and data science to effectively detect and thwart insider threats. The UEBA solution combines all the data sources together for analysis and automatically synthesizes results. Analysts get a lower volume but higher fidelity feed instead of drowning in alerts. The result is faster, more effective detection and response to active insider threats. Exabeam provides hundreds of out-of-the-box behavior models and auto-generated Smart Timelines[12], which are machine built incident timelines that easily illustrate attack chains, for each user and entity to help departments and agencies automate detection, response and mitigation of insider threats. The next section maps specific insider threat capabilities of Exabeam solutions to relevant maturity elements in the Framework.

**INSIDER USE CASE: INSIDER ACCESS ABUSE**

Insider threat detection is challenging because "trusted" behavior doesn't set off alerts in most security tools; the threat actor appears to be a legitimate user. In this case, the UEBA solution must be able to detect when a user (privileged or not) is performing risky activities that are outside of their normal baseline.

The UEBA solution can help discover insider threat indicators via behavioral analysis, which helps security teams identify and mitigate attacks. Some of the techniques used by UEBA include:

- Detecting logins at unusual hours, at unusual frequency, or accessing unusual data or systems
- Changes or escalation of privileges for critical systems
- Correlating network traffic with threat intelligence to discover malware communicating with external attackers
- Discovering data exfiltration by correlating seemingly unrelated events such as insertion of a USB thumb drive, use of a personal email service, or unauthorized cloud storage or excessive printing.

Other discoveries of insider abuse may include detecting and stopping encryption of large amounts of data or lateral movement.

[12] Learn about Exabeam Smart Timelines, https://www.exabeam.com/library/exabeam-smart-timelines/

# MAPPING EXABEAM TO THE INSIDER THREAT MATURITY FRAMEWORK

The matrix below presents the Framework's technology-focused Maturity Elements and maps how Exabeam solutions help with relevant MEs. Implementation of all the MEs will require the use of multiple technology solutions. Many of the best practices described by these MEs are addressed by Exabeam insider threat solutions. The legend describes the Exabeam solutions noted throughout the matrix.

## Exabeam Solution Legend

**Advanced Analytics** – Modern UEBA-based threat detection using behavioral modeling and machine learning.

**Data Lake** – Unlimited data collection, storage and search without volume-based pricing.

**Entity Analytics** – Behavioral analytics for internet-connected devices providing end-to-end network visibility, establishing baseline behavior, and automatically identifying anomalous insider activity.

**Incident Responder** – Security automation and orchestration (SAO or SOAR) to make a security operations team more productive in response.

**Threat Hunter** – Proactive threat hunting using a point-and-click interface that enables analysts to easily launch complex search queries without the need to learn any proprietary query language.

## NITTF Insider Threat Program Maturity Framework and Exabeam Solutions

| SENIOR OFFICIAL / INSIDER THREAT PROGRAM LEADERSHIP | |
|---|---|
| **MATURITY ELEMENT** | **HOW EXABEAM HELPS** |
| **ME2 –** Employs metrics to determine progress in achieving program objectives and to identify areas requiring improvement. | Exabeam provides security analysts with dashboards and metrics to track the notable users and entities deemed risky in an environment. These dashboards also contain metrics around the frequency of abnormal occurrences and user behavior trends, which senior leadership can use to identify and quantify insider threat issues.<br><br>Exabeam also provides SOC productivity metrics that help quantify the type of cases handled, number of incidents faced, mean time to detection, mean time to response, and dwell time. This can be used to benchmark the efficacy of an insider threat program and measure the impact of process improvements. |
| **ME4 –** Employs risk management principles tailored to address the evolving threat environment and mission needs. | Exabeam monitors user and entity behavior to look for anomalous, high-risk activity, and prioritizes threats based on risk so analysts can focus action on where it is needed most. This information helps agencies leverage a risk-based approach to detect threats and employ or change processes, procedures, and tools to curb the emerging threats. Furthermore, dashboards and reporting can be used to illustrate risk posture and demonstrate it to regulatory bodies. |

| ACCESS TO INFORMATION | |
|---|---|
| **MATURITY ELEMENT** | **HOW EXABEAM HELPS** |
| **ME8 –** Develop automated or scheduled processes for regular and timely receipt and integration of information from all relevant agency stakeholders. | Exabeam integrates with hundreds of disparate data sources to gather information and analyze the data. Centralizing security relevant data facilitates regular processes and distribution of information to stakeholders.<br>Using Exabeam, insider threat programs can increase the effectiveness of their agency's security posture by detecting insider threats and proactively providing reports and metrics on notable events to relevant stakeholders. These reports can be ad hoc, upon discovery of a threat, or scheduled as part of a regular information sharing process. |
| **ME9 –** Establish procedures to receive notification with predictable frequency of information relevant to insider threat from other US Government and federal partner data holders. | Exabeam helps security teams and insider threat programs by constantly assessing the relevancy of insider threat information and analytics data. Department and agency stakeholders and security program personnel are notified about potential threats and any indicators related to insider threats. Exabeam can also inform stakeholders if any automated response is triggered as a result of any security incident. |
| **ME10 –** Employ documented processes to validate information sources and identify and assess the use of new information sources. | Exabeam has a modular and flexible platform capable of ingesting data from various sources and has documented processes to identify and validate new data sources. This helps security teams easily add the data needed to detect insider threats, data exfiltration, compromised credentials, privilege escalation and other relevant threat indicators—using behavioral analysis. |

| MONITORING USER ACTIVITY | |
|---|---|
| **MATURITY ELEMENT** | **HOW EXABEAM HELPS** |
| **ME11 –** Establishes a user activity monitoring (UAM) capability on all USG end points/devices and government-owned IT resources connected to USG computer networks accessible by cleared D/A (department and agency) personnel. | Exabeam's UAM is powered by user and entity behavior analytics (UEBA). Exabeam ingests and analyzes data from disparate data sources to detect high-risk users and devices. Exabeam is able to identify and detect risks and assign notable users and devices a risk score based on this abnormal activity. Threats are automatically prioritized by risk so that analysts can easily focus their efforts on affected users and machines. Analysts can automatically monitor executive users and assets, service accounts, vulnerable assets, critical assets and they can add departing employees as well via watchlists to keep a close watch on their activities. |

| MONITORING USER ACTIVITY | |
|---|---|
| **MATURITY ELEMENT** | **HOW EXABEAM HELPS** |
| **ME13 –** Establishes capability to monitor the activity and conduct independent audits of InTP personnel with access to insider threat information and tools. | Exabeam monitors users including security personnel who are part of the Insider Threat Program (InTP) for any anomalous behavior using UEBA. Exabeam has roles defined by role-based access control (RBAC) to grant different levels of permissions like admin operations, view-only access, searching and viewing masked data. Security personnel can perform actions based on the role or group to which they belong, and set permissions that are assigned to that role or group. For example, a Tier 1 analyst may not be able to approve or accept user sessions with the default configuration, but they can review sessions for signs of insider threats. This helps department and agency administrators control sensitive information and even enables InTP to investigate or monitor members of the InTP team if needed. |

| INFORMATION INTEGRATION, ANALYSIS, & RESPONSE | |
|---|---|
| **MATURITY ELEMENT** | **HOW EXABEAM HELPS** |
| **ME14 –** Employs data integration methodologies and advanced analytics to help detect anomalous activity and potential insider threats. | Exabeam can be used as a scalable data repository to store relevant information to help detect potential insider threat indicators. Exabeam has collectors and integrations with hundreds of security, employee data, and IT infrastructure sources to gather information into a centralized location.<br><br>Exabeam uses this data to detect anomalous activity and potential insider threats via UEBA. Once anomalous activity is detected, Exabeam provides analysts with machine-built incident timelines that flag anomalies, follow lateral movement, and display the entire scope of the incident.<br><br>Exabeam also includes a security orchestration and automation solution that has dozens of pre-built integrations with third party services to help department personnel collect evidence and perform corrective actions to remediate incidents. |

| INFORMATION INTEGRATION, ANALYSIS, & RESPONSE | |
|---|---|
| **MATURITY ELEMENT** | **HOW EXABEAM HELPS** |
| **ME15 –** Employs behavioral science methodologies to help identify indicators of potential insider threat. | Exabeam leverages user and entity behavior analytics (UEBA) for tracking, collecting, and analyzing user and machine data as part of its threat detection methodology. Using various analytical techniques, UEBA learns normal behavior and automatically identifies anomalous behavior that may indicate potential insider threats. This is done by collecting data from hundreds of data sources and using them to baseline normal user and machine behavior and then detect behavior that deviates from normal activity.<br><br>For example, Exabeam employs various machine-learning algorithms to monitor daily user activity patterns, determine personal email accounts and abnormal data exfiltration to those accounts, identify privilege escalation, find account switching activity, and detect other activity that may indicate insider threats. |
| **ME16 –** Employs risk scoring capability based on behavioral and workplace factors to assist with detection of anomalous activity and potential insider threats and in the application of tailored mitigation strategies. | With Exabeam, behavior models assign risk scores for those whose observed event patterns sufficiently differ from their own past patterns and learned behavioral baselines. Exabeam uses Bayesian statistics to further highlight unusual anomalies and de-emphasize those that occur more commonly.<br><br>There are various factors that determine risk scores. Users and machines that exhibit a higher degree of abnormal behavior, larger deviations from their baseline, or higher-risk activity will have higher risk scores. Users and machines are then automatically sorted by risk score, such that higher risk users are sorted to the top and escalated to analysts for review. |
| **ME17 –** Documents procedures and agreements with other USG InTPs to request or refer information on insider threats of mutual concern. | Within Exabeam, departments and agencies can easily export the rules and models they have used as part of their insider threat detection efforts, and share that with their counterparts. They can also create reports and dashboards to document threats detected, rules in place, or adherence with compliance requirements.<br><br>Exabeam incidents include a full audit log of activity performed against the case as well as embedded commenting to facilitate collaboration and transfer knowledge between analysts. |

| INFORMATION INTEGRATION, ANALYSIS, & RESPONSE | |
|---|---|
| **MATURITY ELEMENT** | **HOW EXABEAM HELPS** |
| **ME18 –** Employs case management tools to ensure the integrity and effectiveness of the insider threat inquiry and response processes. | Exabeam includes a feature rich case management system, directly embedded into all detection, investigation, and response workflows. Analysts can view open cases and those that are in the queue. Analysts are able to easily determine what they should be working on, the status of their investigations, and what has been done with other incidents. It allows them to directly view the timelines and are able to figure out the severity of the incident to respond manually or via automated workflows. |
| **ME19 –** Conducts routine exercises to improve integration, analysis, and response procedures and processes. | Exabeam can be used to test the effectiveness of regularly conducted exercises that emulate cybercriminals' behavior and tactics, for example pen testing or red team activities. This can help security teams gauge the effectiveness of their security posture and insider threat programs. When doing so, department and agency security personnel can use Exabeam to detect threat indicators relevant to insider threats which were successful in bypassing security controls. This information can help improve insider threat programs and processes by identifying gaps and weaknesses which need to be overcome. |

The following chart shows which Exabeam solutions help support each maturity element in the NITTF:

| EXABEAM SOLUTION MAPPING | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **MATURITY ELEMENT** | **DATA LAKE** | **ADVANCED ANALYTICS** | **ENTITY ANALYTICS** | **THREAT HUNTER** | **CASE MANAGER** | **INCIDENT RESPONDER** |
| **ME2** | Employ metrics to determine Insider Threat Program improvements | x | x | x | | x | x |
| **ME4** | Employ risk management principles | x | x | x | x | | |
| **ME8** | Automating information transfer from relevant agencies | x | | | | | |
| **ME9** | Establish notification procedures relevant to Insider Threat Program | x | x | x | | x | x |
| **ME10** | Employ documented validation processes | x | x | x | | | |
| **ME11** | Establish User Activity Monitoring (UAM) | x | x | x | x | | |
| **ME13** | Establish Insider Threat Program auditing capability | | x | x | x | | |
| **ME14** | Employ data integration | x | x | x | | x | x |
| **ME15** | Employ behavioral science methodologies | | x | x | | | |
| **ME16** | Employ risk scoring capabilities | | x | x | | | |
| **ME17** | Document procedure for information transfer between USG Insider Threat Program teams | x | x | x | | | |
| **ME18** | Employ Case Management | | | | | x | |
| **ME19** | Conduct exercises to emulate detection and response processes as part of Insider Program | x | x | x | x | x | x |

exabeam

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.

## CONCLUSION

The risks to federal departments and agencies from insider threats are a "new normal" situation that will not go away by itself. Detecting, responding to, and mitigating insider threats should be top of mind for federal security and risk managers. Their actions must rise above "paper compliance" with Insider Threat Program guidelines by the National Insider Threat Task Force. In addition to addressing personnel and programmatic elements, security and risk leaders must also choose and deploy technologies tailored for rapid detection, response and mitigation of insider threats. This white paper described a widely-used technology solution approach using user and entity behavior analytics (UEBA). Exabeam's UEBA solutions provide more than 400 use case models that your organization can stand up and deploy within a few months or sooner. Exabeam urges you to consider this option in moving your department's or agency's Insider Threat Program forward to meet new and evolving insider threats. For more information on how we can help or to arrange a demo of our solutions, please visit us at exabeam.com.

## ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premise or in the cloud. Exabeam Smart Timelines, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures. For more information, visit https://www.exabeam.com.