Authorized access: uncovering insider threats within oil and gas companies
Authorized access: uncovering insider threats within oil and gas companies

Over the past five years, the oil and gas sector has attracted public attention and generated high profile headlines around the world for being the victim of targeted attacks. These external threats have prompted IT security departments to invest in multi-million dollar technologies and transformation efforts.

Despite these efforts, the industry continues to experience data loss, market share impact and loss of competitive advantage. The reason for this is simple – insider threats. Insider threats pose one of the largest security threats to organizations. Yet, when asked about their risks related to internal exposure, companies often place reliance on their employees “doing the right thing” as sufficient risk mitigation. While companies continue to focus time and effort on combating external threats, insiders are able to see, steal, manipulate or share the company’s highly valued data. Additionally, external attackers often attempt to, and succeed, at taking on the identity of an authorized user in order to conceal their attack. This allows attackers to minimize the likelihood of being detected and prolong exfiltration of information from the corporate environment. Although less publicized, these threats are more common and equally as damaging to a company as an external threat.

Insider threats haven’t been a priority for IT security professionals for two key reasons. First, the implementation of processes to monitor against insider threats can cause friction between management and employees, especially in companies that have a work culture promoting trust and value in employees. In turn, companies and management can find it difficult to implement the processes and changes successfully. Second, many IT security strategies are focused more on keeping the company’s name out of the press than identifying the most relevant and impactful risks to the organization. Lack of understanding and external pressures on the business have impacted the effectiveness of companies’ ability to detect and respond to insider threats.

But with employees becoming more IT literate and companies linking their IT and operational technology (OT) infrastructure, the risk of reputational or collateral damage from insider threats is growing.
Defining an insider threat

What makes an insider threat so challenging is that the access or activity posing a threat may very well be authorized and appropriate for the end user. This can pose a threat to an organization in a variety of ways:

- **Malicious or inappropriate use of authorized credentials**: This can occur since the authorized user most likely is aware of the organization’s security control and the value of the data to which the user has access.

- **The authorized user may not be an employee of the organization**: As companies often have varying access management processes around contractors or other third-party personnel, there are less controls around maintaining and verifying accurate access.

- **Insider threats can appear in numerous forms**: This could include a disgruntled employee, a consultant/contractor looking for intellectual property which they could sell to competitors; compromised credentials which can pose as legitimate accounts.

- **Inappropriate use of access**: This could include an authorized user, such as an employee or a contractor who has inappropriately used their access (i.e., HR employee who emails employee records to their home email address to work on later); an authorized user with malicious intent that is trying to either escalate their privileges or misuse access they currently have (i.e., a sales rep who is planning on leaving tries to do a mass download of all customer data to use at their next job); an unauthorized user masking as an authorized user (i.e., hackers often will take control of an authorized user id and navigate the environment using a real credential).

Case in point

Senior management at an energy client received a series of disturbing messages from an internal email address. The issue escalated when board members started to receive similar messages, which were quickly brought to the attention of the organization. The messages were directed at key leaders in the organization, falsely accusing them of illegal and unethical behavior.

EY was asked to complete a penetration test to assist in determining the source of the emails as well as to identify other potential risks in the organization’s IT infrastructure. A disgruntled former IT employee had inappropriately set up concealed access accounts and used them to send out the messages.

The remediation included a complete review of current security configuration as well as the active and inactive user accounts. Also, as a result of the findings of the test, supporting processes were remediated, specifically to address risks related to segregation of duties.

Complexity to secure

The oil and gas industry has complex, integrated IT systems that control production, distribution and storage.

By its very nature, the industry requires IT systems for support across broad geographic areas, often in very remote and physically challenging conditions.

In our experience, the global nature of the oil and gas industry increases the risk of critical business data being inappropriately used or stolen by insider threats for several reasons:

- The competitive nature of the oil and gas industry means insiders can greatly benefit from the illegal information obtained through an insider exploit.

- There can be a significant cost to updating outdated and complex industrial systems, which were previously designed without IT security in mind.

- There is a large amount of business critical data, the majority of which is produced at geographically dispersed locations.

- There are various outsourcing and third-party agreements in place. Making it difficult to manage the number of third-party vendors with access to the company’s business critical data.

Timing is another complexity of insider threats. Accounts can go rogue at any time during their lifecycle, yielding point-in-time verification through audits insufficient for identifying insider threats. Further, due to changing roles and responsibilities within the organization, insider threats are difficult for organizations to predict, especially with the industry’s global mobility. However, the solution to combating insider threats is derived from the very factors that make it so complicated – employee behavior.
Turning the outward focus in

Many oil and gas companies have already made investments in security monitoring suites, such as a Security Information and Event Management (SIEM) technology, allowing them to aggregate security logs and data from across their environment into a central location for correlation and analysis. However, SIEM technology only allows security analysts visibility into the environments which they have integrated. Due to the damage caused by publicity from external attacks, oil and gas security departments have focused on integrating leading edge network monitoring and endpoint solutions into their SIEM in order to identify and contain commonly known external threats such as malware. This strategy relies on an “outward-in” approach. Over time, security analysts can become proficient in combating or containing these threats and reach a point of complacency. In these cases, only the foundational maturity around incident detection has been achieved.

Oil and gas companies have numerous business critical data sources. In order to strategically focus on the company’s internal critical applications, databases and host servers must be integrated into the SIEM for monitoring. However, security logs from these sources are not sufficient for identifying insider threats. Unlike many commonly known external threats, insider threats cannot be identified through file extensions, threat feeds or signatures. Therefore, an additional requirement must be added outside of the log correlation mix, and that is behavioral analytics.

Behavioral analytics allow a company to understand the behaviour of users, within their environment, to quickly identify anomalies. This approach can be explained through the following principles:

1. Baselining

The baselining process is referred to as building a behavioral profile. This process looks at 6 to 12 months of access and activity logs compiled from across the organization’s environment to form a profile of normal behavior based on strategically extracted access and activity attributes from the system’s logs. Baselining is built on the premise that a user should have similar behavior on a day-to-day basis barring any recent job function, role or geographic re-location change. For instance, an oil and gas company would assume that their gas pipes application administrator would access the same gas pipes applications and perform the same types of activities within these applications on a daily basis, as it is related to their job function. The trends in access and activity in which this administrator performs these daily operations would make-up their behavioral profile. To be most effective, companies should leverage their existing centralized security log system, such as a SIEM solution or log warehouse to perform the baselining process. Once established, the behavioral profile can be integrated into the SIEM to assist security analysts in identifying outliers, or indicators of a potential insider threat within their environment.

2. Anomalies

Instead of identifying threats based on signatures or correlation rules, behavioral analytics allows security analysts to detect threats through anomalous behavior. Anomalous behavior can be identified in two ways:

a. Peer anomalies

A peer group can be formed by any attribute derived from the human resource data obtained. For instance, data, such as job role or title, business unit and location, can all be factors in determining a user’s peer. This analytical capability is derived from the principle that users within the same peer group will behave similarly (i.e., have the same system access and perform the same types of activities in the systems to which they have access). If a user has access to systems outside of their
b. Behavior-based anomalies
Activity outliers are more basic in nature in that they are derived solely from user's behavior—specifically their activity and access. Regardless of any other factors, a user can be expected to access similar systems and perform similar activities on a day-to-day basis. A behavioral anomaly occurs when a user's access of activity varies from his or her baseline activity. For example, if a process control engineer has behaved in a consistent way within a company's environment for the past six months but suddenly varies from his or her typical behavior, this would result in a behavioral anomaly. This type of anomaly is useful in identifying compromised credentials, rogue accounts, disgruntled employees or malicious use.

Peer Group Baseline

Note: Each dot represents an access or activity instance.

3. Detection and response
Once an anomaly is identified through behavior analytics, immediate alerts can be triggered within the SIEM for security analyst investigation and response. For best results, the anomalous behavior should be associated with specific access or activity. This anomalous activity or access is referred to as an outlier. For example, if the gas pipes application administrator previously mentioned suddenly begins to perform activities within the application that they have never performed before, this specific activity would be flagged as an outlier.
Both activity and access outliers can aid in the detection of insider threats as follows:

<table>
<thead>
<tr>
<th>Description</th>
<th>Objective</th>
<th>Risk addressed</th>
</tr>
</thead>
</table>
| **Access outliers**              | Identify users whose access does not match their peers, job role/function or historical access behavior | • Lack of visibility into anomalous user access within the environment  
• Inability to identify or determine that inappropriate access or privileges exist or have been exploited by users  
• Inability to baseline user access with their environment leading to an inability to identify anomalies |
|                                  | • Identify access permissions that may exist from previous job roles/functions and may need to be cleaned-up  
• Identify access that was inappropriately granted  
• Identify access that may be inappropriate for their job role/function  
• Identify inappropriate access to sensitive data without a business reason  
• Identify accounts that may need to be investigated/monitored to profile an attack |
| **Activity outliers**            | Identify users whose activity does not match their peers, job role/function or historical activity behavior | • Lack of visibility into anomalous user behavior within the environment  
• Inability to detect the loss of intellectual property, the occurrence of a privacy breach or fraud within the environment  
• Inability to determine inappropriate or malicious use by insiders or external threats |
|                                  | • Identify inappropriate activity within the organization’s environment  
• Identify malicious use or activity within the organization’s environment  
• Identify a privacy breach, stealing of IP, fraud, etc.  
• Identify accounts that may need to be investigated/monitored to profile an attack |

Specific correlation rules, dashboards and alerts should be built-out within the SIEM to highlight access and activity outliers across the organization’s environment. Tuning the SIEM to flag outliers will increase the security analyst’s ability in identifying a potential insider threat, allowing for prompt initiation of the incident response process. This enhanced capability can significantly minimize or prevent the financial, reputational or competitive advantage loss an insider threat can cause to an organization.
Results within reach

The identification of potential threats using behavior analytics increases an analyst’s visibility, allowing for more precise and targeted threat detection and greatly reducing the potential impact of an insider threat.

Threats facing the oil and gas industry continue to adapt and change. We have helped our clients globally implement behavioral analytics techniques alongside their existing IT and OT security frameworks, to help reduce their insider threat risk.

Our experience will enable you to detect and respond to the various threats quickly, giving confidence to your board, stakeholders and the market.
For more information, contact:

Kent Kaufield  
+1 403 206 5100  
Kent.d.kaufield@ca.ey.com

Jose Granado  
+1 713 750 8671  
jose.granado@ey.com

Tom Pruszkowski  
+1 713 750 5226  
tom.pruszkowski@ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

How EY's Global Oil & Gas Center can help your business
The oil and gas sector is constantly changing. Increasingly uncertain energy policies, geopolitical complexities, cost management and climate change all present significant challenges. EY’s Global Oil & Gas Center supports a global network of more than 9,600 oil and gas professionals with extensive experience in providing assurance, tax, transaction and advisory services across the upstream, midstream, downstream and oilfield service sub-sectors. The Center works to anticipate market trends, execute the mobility of our global resources and articulate points of view on relevant key sector issues. With our deep sector focus, we can help your organization drive down costs and compete more effectively.

© 2013 EYGM Limited.  
All Rights Reserved.

EYG no. DW0311  
CSG/GSC2013/1182166  
ED 0114

In line with EY’s commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/oilandgas

You can also connect with us using social media: