CLEARFORCE Case Study

Mitigating Human Risk in the Defense Sector

Introduction

Together, the Defense Industrial Base Sector and the vast private defense industry span worldwide and are integral in protecting our national security. Over 100,000 companies contribute to the research, development, and advancement of the most complex technologies and weaponry in the world, and the millions of defense employees within these companies require security clearances to handle highly sensitive information.

The arduous and in-depth background investigation and clearance process, despite its thoroughness, can still be susceptible to employee insider risk. Having a real-time automation system can enhance visibility to pinpoint employee risks in defense organizations before they occur, especially when it comes to fulfilling self-reporting requirements.

As part of standard risk detection practice, security clearance holders are expected to self-report incidents or issues that may affect their clearance or as required by company policy. This is one of the nonautomated aspects of the clearance process which creates a risk gap, making it a metric of personal integrity as well. However, it is best to self-report proactively to preserve the security of sensitive information and prevent the incident from being retroactively discovered, which often leads to greater consequences.

Security Executive Agent Directive (SEAD) 4 and Adjudicative Guidelines in 5 CFR 731 202 are two of the guides that outline initial and continued eligibility requirements for access to classified information and lists the types of incidents that need to be self-reported. These incidents include foreign travel and interactions, loss or compromise of information, financial problems, and arrests. Disclosing reportable security incidents before they are discovered by a clearance investigator can serve as a potential mitigating factor upon

adjudication proceedings:

“2(e) When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:
(1) voluntarily reported the information
(2) was truthful and complete in responding to questions
(3) sought assistance and followed professional guidance, where appropriate”

Nonautomated self-reporting can support the adjudication process, however the employer should be equipped with information in real time so that HR and security managers have the opportunity to intervene sooner. It is always best for managers to address these risks with the employee as soon as possible to avoid compromising the integrity of the organization or threatening classified information. Employee retention can also be preserved through a proactive approach depending on the event at hand.

This case study focuses on ClearForce’s Resolve implementation in a U.S. government defense company in summer 2022, illustrating the importance of mitigating employee-related risk by augmenting automated measures to stay on top of the self-reporting process.

Findings

ClearForce is working with a defense company that has employees with access to Top Secret projects, weapons, and surveillance systems. The company deploys ClearForce’s Resolve platform to augment their insider threat capability and pinpoint employee risk by providing essential information like real-time arrest records, criminal watchlists, sex offender registries, and financial monitoring, all while ensuring full employee privacy and legal compliance.

ClearForce further supports the company’s insider threat capability by incorporating real-time push-based trigger alerts. This gives the company early indicators of risky behaviors or clear violation of the following six Adjudicative Guidelines for determining eligibility for access to classified information:

GUIDELINE D: Sexual Behavior
GUIDELINE E: Personal Conduct
GUIDELINE F: Financial Considerations
GUIDELINE G: Alcohol Consumption
GUIDELINE H: Drug Involvement
GUIDELINE J: Criminal Conduct

Upon the deployment of the ClearForce Resolve platform, it was discovered that one employee was arrested for driving under the influence of alcohol while on authorized time off out of the local area of employment. Unless the employee self-reported, the defense company would have had no visibility into the arrest, subsequent court proceedings, or final adjudicated outcome without ClearForce's Resolve platform.

DUIs are often underreported because those who are arrested for DUIs will wait until the final ruling in hopes that it will be reduced to something that does not mandate reporting. However, this approach goes against the self-reporting clearance policies. Withholding this information, even before a final ruling, is prohibited and, in the interest of defense security, cannot be left undetected. Lack of awareness about violating behaviors introduces risk to the company if the government discovers the arrest via their continual vetting program.

The defense company employee was enrolled in the ClearForce Resolve platform and reached out to the company's security team within 72 hours of the incident to fulfill the U.S. government self-reporting requirements. When the government acknowledged the arrest, the company and employee had already initiated an internal mitigation strategy and shared all the information in a timely manner, and as a result, were not penalized. The company was able to keep the employee on contract and keep them on their team.

Because the defense company utilized ClearForce in its insider threat architecture, the arrest was quickly addressed and the employee and company were able to handle the reportable life event ahead of government notification and potential job loss..

Key Takeaways

Employees who occupy positions of trust within the defense sector, and the defense companies who initiate and track their clearances, are required to self-report certain life events and changes to the U.S. government to proactively safeguard sensitive or classified information. Any misstep in the self-reporting process can compromise the reputation of the company and potentially compromise U.S. national security.

By augmenting a behavioral monitoring system that tracks the legally-binding eligibility requirements in real time, defense companies can bolster their insider threat capabilities to stay ahead of reporting requirements and ensure that all staff are following clearance guidelines. Having these measures in place can result in a smoother adjudication process, higher retention of staff, and the preservation of organizational and employee integrity.