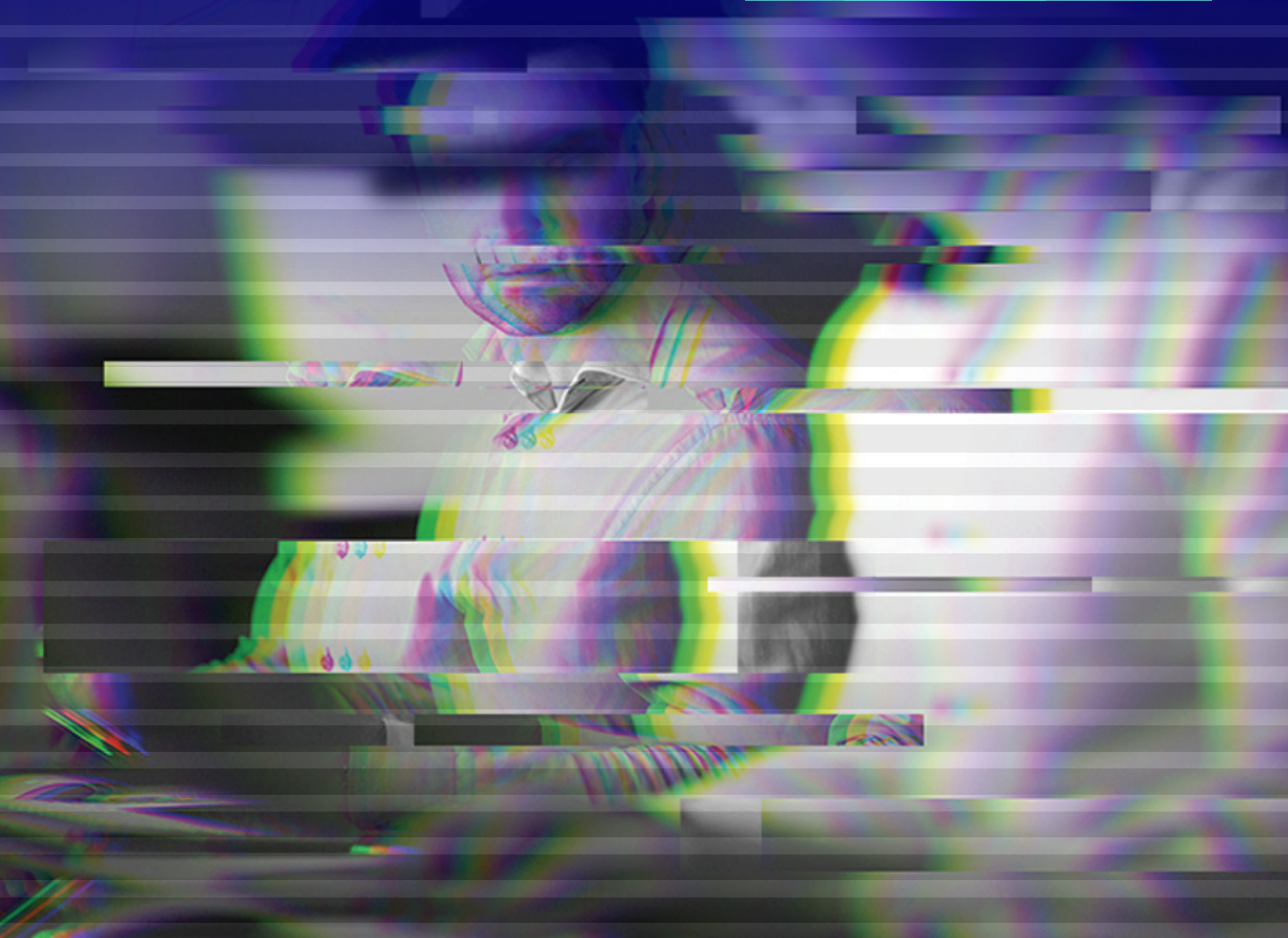
illusive

VAILLANCE GROUP

ULTIMATE GUIDE ON INSIDER THREATS

Their Changing Motives, Evolving Skills and How to Expose Them

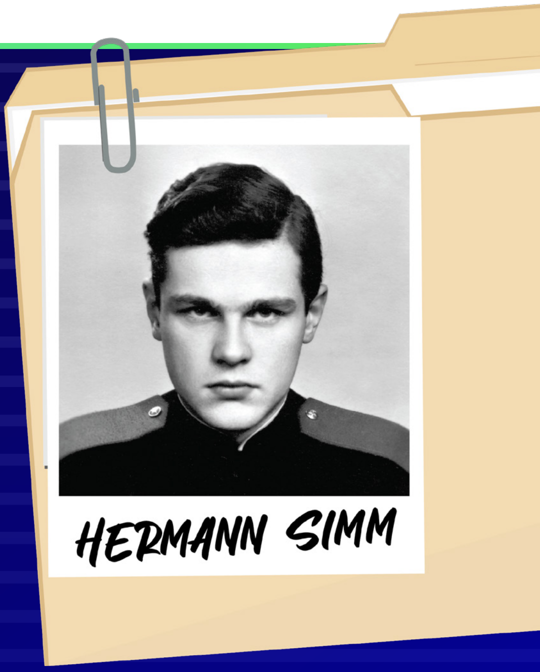
WHITE PAPER



INTRODUCTION

The Spy Game Goes Corporate

Insider threats have long been thought of as a crime that occurs when individual employees become disgruntled and seek revenge. These traditional insider attacks carried out by aggrieved, lone actors still happen. However, with nation-state attackers increasingly exploiting organizational dependence on the digital transformation and the data it generates, insider threats are beginning to resemble any other Advanced Persistent Threat (APT). The only real difference is that the new hyper-targeted and often government-funded insider threat will involve a recruitment and grooming process to convince the insider to give the adversaries the access they need to launch their attack. In fact, the latest evolution of insider threats is not all that different from the process governments use to recruit spies from other countries; the only difference is that the targets are now any large organization with money or valuable data.



Consider the following example. In September 2008, Estonian Ministry of Defense (MoD) official Hermann Simm was arrested for illegally collecting and passing state secrets to Russia. While serving as a police officer during the Soviet occupation of Estonia, Simm joined the Estonian resistance movement. Having joined the MoD after Estonia regained its independence in 1991, Simm served as Director of the Department responsible for protecting state secrets when Estonia was in the process of applying for NATO membership. In this role, Simm was responsible for working closely with Estonia's NATO and European Union member state partners, a critical area of interest to his Russian spy handlers.

Simm's spying on behalf of Russian Intelligence has been described as the most significant espionage scandal in the history of NATO. Simm had access to volumes of classified NATO intelligence including tactical battle plans, which he passed to his Russian handlers. Aside from being a counterintelligence catastrophe, Simm risked damaging Estonia's reputation as an untrustworthy new NATO member. Already reserving its most sensitive intelligence for its so-called "Five Eyes" partners (United Kingdom, Australia, New Zealand, Canada, and the U.S.), the U.S. faced pressure further to limit intelligence sharing with Estonia.

According to the Estonian government, Russian Intelligence paid Simm at least $100,000 for spying. Simm was vulnerable to recruitment because he enjoyed a luxurious lifestyle, with significant property holdings and a collection of expensive artwork. Having lost his Soviet rank of colonel after Estonia regained its independence, Simm also experienced a deep psychological need for recognition.

Simm is only one of many high-profile insider threats which nation states have suffered in recent decades. Central Intelligence Agency (CIA) Officer Aldrich (Rick) Ames and FBI Special Agent Robert Hanssen are two of the most notorious Russian penetrations of the U.S. Intelligence Community. What is notable is that the CIA and Federal Bureau of Investigation (FBI) are well known for having the most sophisticated hiring, onboarding, and vetting of employees. They have scores of counterintelligence professionals dedicated to mole hunting; however, if these world class intelligence services can be penetrated, so can anyone else, including private sector businesses that typically spend much less time and resources on rooting out insiders. The Simm, Ames, and Hanssen cases are all analogous to what former FBI Assistant Director Donald Freese called the "skin behind the keyboard." This can refer to threats resulting from both unwitting employees who require training and malicious employees with ill intent.

Hermann Simm was a spy, but he can also be considered a prototypical insider threat, defined as an individual or group with either current or former access to an organization's information, and/or facilities, who uses that access to cause harm either intentionally or unintentionally by abusing, misusing, or threatening an organization's confidentiality, integrity, availability, or resources.

Insider threats take many forms, with the vast majority falling in the category of unintentional acts such as unknowingly clicking on a phishing link or taking a selfie and posting it on social media with one's work laptop screen displaying sensitive internal data. A negligent employee might print company documents for a business trip by plane or train and then accidently forget them in the seat back pocket before disembarking. In fact, many people find shortcuts or workarounds thinking they are efficiently doing their job, but in fact are unknowingly creating vulnerabilities for their employer. Most employees are well intentioned; however, considering the nuances of human nature, even people with the best of intentions can commit grave errors. That is why unintentional acts fall in the most preventable category of insider threats.

Insiders with Malicious Intent

The category of intentional insider threats often involves the purposeful exfiltration of data. An insider threat might steal company information with the intent of leaking it to the media as a former Apple employee, Simon Lancaster, was accused of doing in 2021. Sued by Apple for "misappropriation of trade secrets" to the media as means to enhance his brand, Lancaster also wanted to use the information he stole to turbo boost his new employer's product line. Lancaster had worked for twelve years at Apple including as an Advanced Materials Lead and Product Design Architect, which enabled his access to Apple's intellectual property including company hardware.

In fact, since the start of the COVID-19 pandemic incidents of data exfiltration have dramatically increased. With the continual threat of job loss, employees have increasingly begun to steal intellectual property and trade secrets, which can be incredibly costly to the victim. Imagine a company's most sensitive data in the hands of a competitor who has gone on a hiring spree of the victim's current and/or former employees. This is why competitors often dangle inflated job titles and what might appear to be outsized financial benefits.

The ability for malicious actors to exfiltrate data is also substantially easier not just with personal devices and cameras, but the current work-from-home model to which many companies have been forced to shift during the coronavirus pandemic.

When he was hired, there was no evidence Lancaster was a threat, but he broke bad when something triggered his transformation into a malicious insider threat. The Lancaster case also demonstrated the importance of the "need to know" principle. He arguably had more access than he should have, and there was insufficient monitoring of how he was exploiting his access.

The Insider Grooming Complex

An insider threat might also steal data for use in starting his own company or selling it to hacktivists or nation state adversaries like China or Russia. According to Director FBI Christopher Wray, the FBI opens a new China investigation every 10 hours and has over 2000 investigations underway which lead back to the Chinese government. China is mounting full-throttled economic espionage attacks on the U.S. and its allies. China counterfeits U.S. products; steals trade secrets and intellectual property; and having hacked into the Office of Personnel Management to steal U.S. government employee data, ruthlessly targets anyone who has ever worked in the U.S. defense and national security sectors.

According to **Director FBI Christopher Wray**, the FBI opens a new China investigation **every 10 hours and has over 2000 investigations** underway which lead back to the Chinese government.

In 2020, a Tesla employee rejected a payment of $1 million from Russia to install a USB device with malware. This exemplifies how sophisticated intelligence services are mounting a full court press against the U.S. private sector, using bribery, espionage, and extortion to steal technology.

Espionage is extraordinarily prevalent, but the perpetrator is not always what we would consider an enemy state. According to former Director CIA and NSA General Michael Hayden, operating in cyber space is like "swimming in shark infested waters, where even the dolphins are a threat." If a businessperson travels to Europe and leaves his computer in his hotel for some time, he should expect his competitors, possibly with the assistance of the local government, to hack into his protected information.

Fraud, defined as wrongful or criminal deception intended to result in financial or personal gain, is the most prevalent of all insider threat crimes. Especially during the coronavirus pandemic, which forced companies to cut employment, employees are deeply concerned about losing their jobs or looking for a new job if they have been fired. As financial instability grows, employees are increasingly committing acts of fraud to provide for their families. Criminal organizations are also playing upon the pandemic and recruiting trusted insiders to collude with them to commit financial crimes against companies. Human nature- - i.e., an existential need to care for one's family- - tends to rationalize these acts, which before the pandemic, would not have been as prevalent.

Insider Threats and Their Cost Are Both Increasing

We are in the midst of a perfect storm of pressures and/or incentives, coupled with opportunity or ability to commit crimes, which induce a change in normally law-abiding behavior.

Third parties, including venders and contractors who form a critical supply chain on which enterprises rely, are particularly vulnerable. They usually do not have the same level of training or awareness as the enterprise's permanent workforce and do not typically follow equally rigorous security practices. As the SolarWinds and other hacks have proven, no industry or organization is immune from this threat.

Those who are vulnerable to external stressors, which exacerbate existing issues, can become vulnerable to becoming an insider threat. A triggering event, which could be something as apparently benign as a new manager or not receiving an expected promotion, can transform a vulnerable person into a malicious insider.

The costs of this perfect insider storm are piling up. It includes loss of confidence among shareholders, customers, and employees at organizations where they occur. The specific dollar amounts vary, with industry experts estimating negligent insider threat cases cost $300,000 per incident while criminal cases cost roughly $750,000 per incident. We know definitively that morale, brand, and reputation are also consistent casualties.

One of the costliest malicious insider acts is IT sabotage, which can cause extraordinary harm to an organization. According to CERT, IT sabotage occurs when current or former employees, contractors, vendors or business partners intentionally exploit an authorized level of access to networks, systems, or data with the intention of harming a specific individual or organization. Privileged trusted users are the most at risk for committing this type of act. Some examples of just how simple an attack like this can be for a knowledgeable and motivated insider:

After quitting an Atlanta-based building products distributor, an IT administrator committed sabotage by changing router passwords and disabling the server.

In another case, a system administrator who had been fired sought to extort his former employer by refusing to reveal administrator passwords.

A system administrator at a financial institution who had been fired without any notice used his remote access connection to shut down the primary server for three days.

Insider threats are ubiquitous and dynamic. Mitigation of insider threats must therefore be a symbiotic combination of both technical and non-technical means.

NON-TECHNICAL METHODS

Training and Awareness

Training and awareness programs are critical for making it clear to all employees that the enterprise places the highest priority on protecting intellectual property and trade secrets. Education in cyber security should be rolled out with additional awareness campaigns focused on the need to protect intellectual property and trade secrets; if an organization does not do this, they are unable to pursue litigation against offenders. Further, insider threat/risk-specific policies or policy addendums should be advertised so employees cannot claim they did not know it was against the rules, for example, to email sensitive internal data to their personal account. A clear policy requiring use of data classification labels is another simple, yet critical means to protect intellectual property.

Employee Lifecycle Management

Companies should place an emphasis on proper employee lifecycle management. By being involved and aware throughout the entire lifecycle of each employee, organizations can significantly mitigate insider threats. Companies of course should start with hiring the right people with robust screening and selection for employees who are a good fit for the enterprise and, equally as important, its culture. The second step is proper and thorough onboarding, which should review the relevant policies with clear examples of what employees cannot do and should be aware of. The third step is to conduct and require ongoing training. Security, insider threat, and cyber hygiene training (at a minimum) should continue through the employment phase.

Managers and HR business partners should have additional specialized training in employee risk red flag indicators, what to do when a concern is raised, and details on the employee assistance program (EAP) support the company offers, when needed. Regarding identified high-risk users, human resources (HR), security and other company stakeholders must continually collaborate especially when concerning activity has been flagged.

Companies must recognize when an employee is out-processing to exit the organization, whether voluntarily or involuntarily, this is a risky time when a disgruntled employee can be triggered into committing a malicious act. Monitoring end of employment actions assumes the highest importance. When a high-risk employee leaves the organization, enterprises should have clear end of employment policies. Seeking to ensure outgoing employees cause no harm, HR should create and update an out- processing checklist which includes reminders of non-compete and confidentiality agreements as well as direct questions about whether the employee ever violated data access policies, such as using unapproved external cloud storage or USB devices to exfiltrate company data. IT managers, anyone with access to sensitive information such as competitive strategies, and persons involved in research and development, should be subjected to the most stringent vetting and monitoring. There should be security tracking for those who have system side access for monitoring purposes.

Know Your Crown Jewels

Leadership must know where the company crown jewels are located, who has access to them, who should have access to them, and what they would be worth to adversaries or competitors if they were compromised. Educating the workforce on what constitutes a crown jewel and how employees can better protect them is important, and ideally rolled into the general insider threat training and awareness platform. With this, if done well, companies should be able to shift company culture to apply more stringent data protection. For example, enforcing a need-to-know policy can help employees understand that the projects they touch daily are worth protecting. This can also help increase anonymous and protected internal employee reporting on suspected malicious or negligent acts they witness.

Clearly Define WFH Policies

Enterprises should institute clearly defined work from home (WFH) policies. Even post-coronavirus pandemic, work from home will likely remain at elevated levels. Companies must refine relevant policies and train the workforce in how to practice cyber security hygiene. Too often, security practices are ignored in the interest of keeping business operating. As a result, insider threat activity such as fraud and data exfiltration has risen significantly over the last year. At home, employees are more likely to take photos of sensitive data on computer screens, snap selfies, print hard copy documents, or leave devices unsecured. Without training employees on how securely to conduct business from their homes, businesses cannot enforce consequences against negligent or malicious acts.

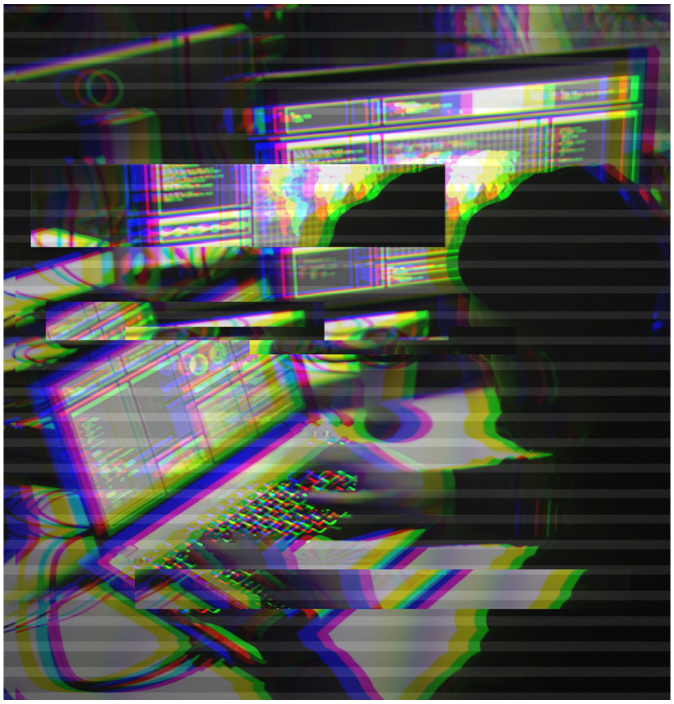
Assume Compromise

Cyber-savvy enterprises must continuously strive to detect the insider threat in the prevention and detection "left of boom" pre-attack phase before the enemy secures a beachhead. They need to harden defenses with a variety of tools by reducing vulnerable attack space with secure routers and servers, using firewalls and sophisticated web codes, rigorously applying both patches and back-up protocols, encrypting data both a rest and in motion, and monitoring alerts for changes in users' patterns of behavior or red flag actions. Enterprises should also have a platform in place to detect shared credential usage as well as anomalous, out of pattern database activity, which raises red flags.

All enterprises should assume that they will be successfully hacked and prepare for such a scenario. This should encompass a robust business continuity plan as well as a holistic enterprise risk management program. In the words of General Hayden, cyber defense is about "defense in depth, situational awareness, response, recovery, and resiliency."

Effective Incident Response

The most effective incident response for any enterprise enables Hayden's five elements of cyber defense, and a dynamic workflow accounting for the event so that leadership can effectively integrate the evolving event with previously identified data. Incident response is a four-step process. First, a security incident management tool "ingests" the threat. Second, a security module "escalates" the notification by characterizing the incident, assessing the threat, and directing the workflow response. Third, the workflow response creates additional notifications, while complying with legal requirements related to any data loss which might have occurred. Fourth, the entire process adheres to privacy notification laws and manages both internal triage as well as notification of those who were breached.



An effective incident response reduces response time and enrichment notification to seconds and serves as an analytic tool, which enables the most effective and efficient executive decisions. A single command and control center, sometimes referred to as a "hub," should provide immediate updates on cyber security posture including historical statistics on indicators of compromise; integrate all existing security protocols with intelligence reporting to enables an adaptive response to threats; and ensure basic triage steps are immediately taken even before an analyst becomes directly involved. The gold standard would integrate these technical capabilities to detect cyber-attacks with an insider threat-specific tool that can detect anomalous behaviors in users. Most tend to assign users a risk score that investigators or insider threat team can then look into to determine if there is a legitimate issue.

The best incident response creates the clearest situational awareness so that the analyst can make the right decisions. The process is dynamic and inductive. As they collect, collate, and analyze more information, enterprises enhance their incident response capability.

Layered Insider Defense

Many organizations rightly question the return on investment (ROI) in a robust insider threat program. Preventing losses can be less enticing than realizing profit. But without such a program, companies risk great damage to their reputation and financial solvency.

Companies should aim to add a layered defense system, which integrates both technical and non-technical tools. There is a wide array of detection tools available including User and Entity Behavior Analytics (UEBA), User Activity Monitoring (UAM), Data Loss Prevention (DLP), Security Information and Event Management (SIEM), digital forensic tools for investigations, and other analytical systems such as deception technology, which we'll discuss in more detail below.

MITRE, a nonprofit dedicated to creating engineering and technical guidance for the U.S. government, recently created an active defense-focused knowledge base it calls Shield. MITRE Shield is a set of best-practice recommendations for basic cybersecurity hygiene, as well as advanced defensive techniques covering deception and adversary engagement.

The goal, wrote MITRE in its introductory blog post about Shield, is to allow "an organization to not only counter current attacks but also to learn more about that adversary and better prepare for new attacks in the future." At its core, active defense seeks to proactively create an antagonistic environment for the attacker instead of simply reacting to something the attacker has already done, raising the cost of hacking to a level where it becomes unattractive to the threat actor.

Deceptive files, data, and credentials create work for attackers that is difficult to automate away. When attackers trip a deception, security teams have a detected incident that is deterministic and based on genuine attack behavior, certain not to be a false positive. With such detection it is possible for an organization to gather valuable real time telemetry to understand their target, remediate, and adjust security strategy and tactics to safeguard against similar attacks in the future no matter how they are carried out.

Defenders deserve to win the battle against insider threats, and active defense through deception is a key part of that noble effort. If done right, insider threat mitigation improves the health and functioning of the enterprise. A commitment among all employees to work together on behalf of a common mission should raise the level of camaraderie as much as profit margins. Key to success is being transparent with the workforce about the combined system of technical and non-technical methods designed to detect, counter, and prevent insider threats and most importantly the enterprise's commitment to care for the wellbeing of its employees.

Deception is also a vital part of a diversified insider detection strategy, filling an important lateral movement detection gap in existing defenses and accelerating the time to detection for an insider that has gone rogue. It carries this strategy out in three steps:

1 Attack surface management continuously analyzes and removes unnecessary credentials and pathways on the network, reducing the insider's potential to carry out an attack.

2 These unnecessary credentials and pathways are then replaced by agentless deceptive versions on every endpoint, designed to attract threat actors to targets that appear real but are not and make it impossible for insiders to move laterally without being detected.

3 As soon as an insider interacts with a deception, human readable on-demand telemetry is delivered to the organization about all current insider threat activities to speed investigation and remediation.

About Illusive

Illusive's active defense stops the lateral movement that ransomware and nation-state attackers use to access critical assets. Despite significant investments, it's still difficult to see and stop attackers moving inside your environment. The Illusive Active Defense Suite enables organizations to create a hostile environment for attackers by reducing the attack surface, forcing detection through deception, and delivering on-demand visibility into attacker activity.

Illusive was founded by nation-state attackers who developed a solution to beat attackers. We help Fortune 100 companies protect their critical assets, including the largest global financials and global pharmaceuticals. Illusive has participated in over 130+ red team exercises and has never lost one!

To learn more, visit us at **https://illusive.com/solutions/by-use-case/insider-threats/** or write us at **info@illusive.com.**

About Vaillance Group

With exceptional and unique experience, Vaillance Group is a leader in the Insider Threat arena providing uncompromised delivery of services. Vaillance Group helps its clients protect their company assets, people, and intellectual property from Insider Threats through expert training and organizational design. We provide bespoke Insider Threat program development, vulnerability assessments, and awareness training to organizations who recognize that protecting their assets means protecting their people. Vaillance Group is a licensed partner with Carnegie Mellon's Software Engineering Institute (SEI) to conduct Insider Threat vulnerability assessments utilizing the CERT Vulnerability Assessment Tool.

To learn more, visit us at **www.vaillancegroup.com** or write us at **info@vaillancegroup.com.**

About the Authors

Daniel N. Hoffman

Retired CIA Senior Clandestine Services Officer,
Three-Time Station Chief

Daniel N. Hoffman had a distinguished career with the Central Intelligence Agency, where he was a three-time station chief and a senior executive Clandestine Services officer.

Hoffman also led large-scale HUMINT (human intelligence gathering) and technical programs and his assignments included tours of duty in the former Soviet Union, Europe, and war zones in the Middle East and South Asia. In addition, Hoffman served as director of the CIA Middle East and North Africa Division.

During his 30 years of government service, Hoffman also served with the U.S. military including as an associate professor at the Army Command General Staff College.

Hoffman graduated from Bates College with a B.A. in History. He has a Master of Science from the London School of Economics and a Master of Public Administration from Harvard's Kennedy School of Government (2006).

Hoffman is the proud father of two children.

Shawnee Delaney

CEO, Vaillance Group and
Former DIA Detachment Chief

Shawnee Delaney, a decorated Intelligence Officer, and licensed private investigator, is the founder and CEO of Vaillance Group. Shawnee spent nearly a decade with the Defense Intelligence Agency (DIA) as a Clandestine Officer conducting Human Intelligence (HUMINT) operations all over the world. She served four combat zone tours in Iraq and Afghanistan as a Case Officer and Detachment Chief and served as a Supervisory Branch Chief in Europe.

After leaving DIA, Shawnee supported the Department of Homeland Security (DHS) in the protection of U.S. critical infrastructure and industrial control systems for the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Shawnee has built Insider Threat programs for major Fortune 500 companies such as Uber and Merck. She holds an M.A. in International Policy Studies with a Specialization in Counter-Terrorism and Counter-Proliferation, and a M.S. in Cyber Security. She is a doting mother of three very talkative and strong-willed children.

Illusive Inc
488 Madison Avenue
11th Floor
New York, NY 10022

Visit us: www.illusive.com
Email us: info@illusive.com
Call us:: US: +1 844.455.8748
EMEA / AsiaPac: +972 73.272.4006
Find us: