Managed Threat Mitigation Services

Overview

As the risks of the insider threat take a more predominant place in media attention, U.S. Government policies are emerging that place a greater focus on the Defense Industrial Base (DIB) and Corporate responsibilities for detecting, preventing, and reporting insider threats. In many cases, leakage of U.S. Government secrets, proprietary government program data, and theft of corporate intellectual property can be traced to contractor staff who have legitimate access to that data. Recent insider threat cases in the government contractor and corporate communities demonstrate the need for effective enterprise-wide cyber-audit solutions that can withstand the scrutiny of government policy oversight, yet are familiar to the broad range of government investigative staff that a company might interface with as part of a security-related inquiry. But where does one begin in establishing an insider threat audit program? What tools are available that are best for the job, and how does one use them effectively?

Corporate Insider Threat Cases*

Wen Chyu Liu, a retired research scientist was convicted in February 2011 of stealing trade secrets from his former employer and selling them to companies in China. Mr. Liu conspired with at least four current and former employees, traveled throughout China to market the stolen information, paid current and former employees for material and information, and bribed a then -employee with $50,000 in cash to provide a process manual and other information.

Yuan Li, a former research chemist with a global pharmaceutical company, Ms. Li accessed her employer's internal databases, downloaded information to her personal home computer, and made them for sale.

Elliot Doxer sent an e-mail to the Israeli Consulate stating that he was willing to provide information from his employer that might help Israel. Mr. Doxer provided customer and employee lists, contract information, and other trade secrets.

Sergey Aleynikov worked as a computer programmer for a Wall Street company. During his last few days at that company, Mr. Aleynikov transferred 32 megabytes of proprietary computer codes — a theft that could have cost his employer millions of dollars.

Michael Mitchell became disgruntled and was fired from his job due to poor performance. Mr. Mitchell kept numerous computer files with his employer's trade secrets; he entered into a consulting agreement with a rival Korean company and gave them the stolen trade secrets.

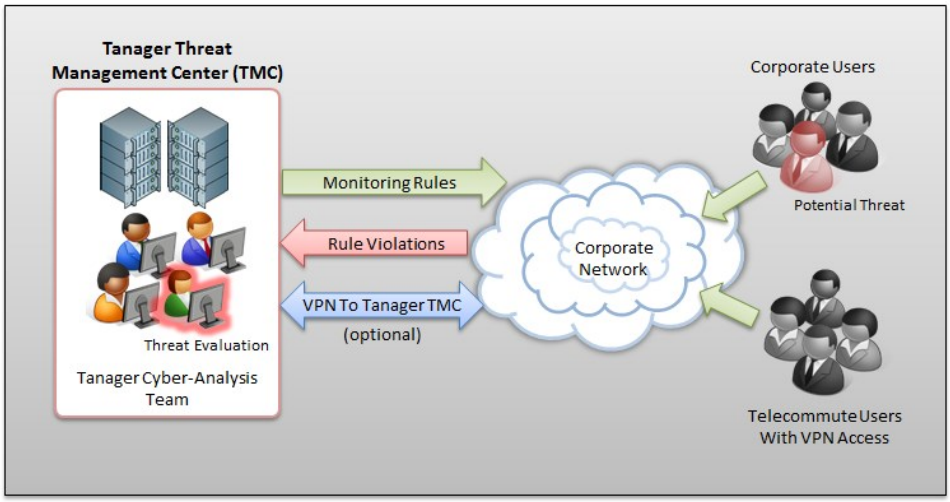
Do You Know What's Happening In Your Enterprise?

*FBI Counterintelligence - Insider Threat webpage

What is the cost of an insider threat incident to your organization compared to the price of establishing a threat mitigation program?

Introducing Tanager Managed Threat Mitigation Services

Tanager Inc., a leading small business in U.S. Government insider threat program execution, is pleased to present our Managed Threat Mitigation Services providing businesses in the Defense Industrial Base and related markets with a turn-key solution for robust insider threat audit and inquiry. Tanager implements tools, rule sets, and analysis techniques drawn straight from our extensive experience in federal government insider threat audit. Our customers can have confidence that their insider threat protections utilize the same technologies and techniques in use throughout government today, without the high cost of designing, implementing, licensing, and staffing "yet another" new IT or Security project from within the organization. There are many potential concerns that a company may have with regard to an internal audit program. Whether a fully outsourced "audit as a service" option works for you, or corporate policy requires a capability 100% within the corporate network borders, Tanager provides a number of options to allow for maximum flexibility in helping an organization implement an insider threat audit capability.



High-level diagram of Tanager's Threat Mitigation Service

An Experienced Partner in Threat Mitigation

Tanager has been an active participant in insider threat mitigation, including audit and investigation for the US Government, performing a full range of technical and investigative services, since 2010.

The Tanager team builds upon that experience as a provider of managed cyber-audit solutions for US Government corporate partners and concerned commercial companies. Our Managed Threat Mitigation Service employs a programmatic, technical and services approach that has proven successful within the U.S. Government.

Robust Protections for Corporate Data

Tanager employs a number of safeguards to ensure Managed Threat Mitigation Services customers' data is protected and secure.

- Encrypted VPN from the Threat Management Center (TMC) to customer the network
- Encrypted data stores
- FIPS 140-2 validated software
- Non-Disclosure Agreements for analysis personnel – "firewalled" from Tanager corporate.
- A "watch the watchers" approach to ensure analyst integrity
- Two-party authentication

FLEXIBLE OPTIONS

TIER 1 "Audit As A Service" – A cyber audit solution completely hosted, managed, and monitored by the Tanager Threat Mitigation Center (TMC) team.

TIER 2 Partially Managed Option 1 – Hardware solution installed within the client network, and managed and monitored by the Tanager TMC team.

TIER 3 Partially Managed Option 2 – Hosted technical solution provided by the Tanager TMC team. Audit monitoring and analysis performed by your corporate security staff.

Tanager's Managed Threat Mitigation Services offer the flexibility enterprises need to match their security requirements

Tanager Expertise

- Use "U.S. Government-grade" Insider Threat audit and investigation solutions.
- Leverage rule sets and subject matter expertise consistent with US Government best-practices for insider threat audit and investigation.
- Assistance with navigating the legal and ethical hurdles often associated with employee insider threat mitigation.
- Provide tangible Fraud, Waste, and Abuse (FWA) detection results as an additional benefit .

Leverage Tanagers Insider Threat mitigation expertise to create your own internal threat mitigation program

Added Potential Benefits Of Insider Threat Audit

There are several additional benefits that can be realized from implementing Tanagers Managed Threat Mitigation Service.

Among them are:

- Better DSS facility accreditation – Defense Security Services (DSS) recognizes the value of cyber-audit and insider threat mitigation practices when contractors employ those measures.
- Proposal Discriminator – Demonstrate an active approach to the US Governments insider threat concerns that other potentially bidders may not have. Being at the forefront of insider threat mitigation in your industry sets you apart from the competition.
- Fraud, Waste, and Abuse (FWA) return on investment – While detection, and mitigation of the insider threat is the primary goal, there are substantial opportunities to reduce FWA within the corporate network through an active insider threat mitigation program.

Tanager®

Cyber Security ·Information Technology· Insider Threat ·Fraud, Waste and Abuse

Tanager was founded in the State of Maryland in August 1996, and is a Woman Owned Small Business, self-certified with the Small Business Administration, under 25.5 million in revenue. The corporate headquarters is in Annapolis Junction, Maryland. This facility possesses a top secret facility clearance with a federal government agency and is audited annually by the Defense Security Service (DSS). We currently have a Government approved accounting system, audited by the Defense Contract Audit Agency (DCAA).

For more information on any of our services please visit us on the Web or email us at **insiderthreat@tanagerinc.com**

www.tanagerinc.com