Coronado Group, Ltd.

A New Approach to Insider Threat
Proactive Cyber Defense

A Vector Approach To Identifying, Mitigating, and Securing Digital Assets from Insider Threat

A Coronado Group, Ltd. Innovation

Search The Way You Think

Proactive Cyber Defense - Mitigating Insider Threat

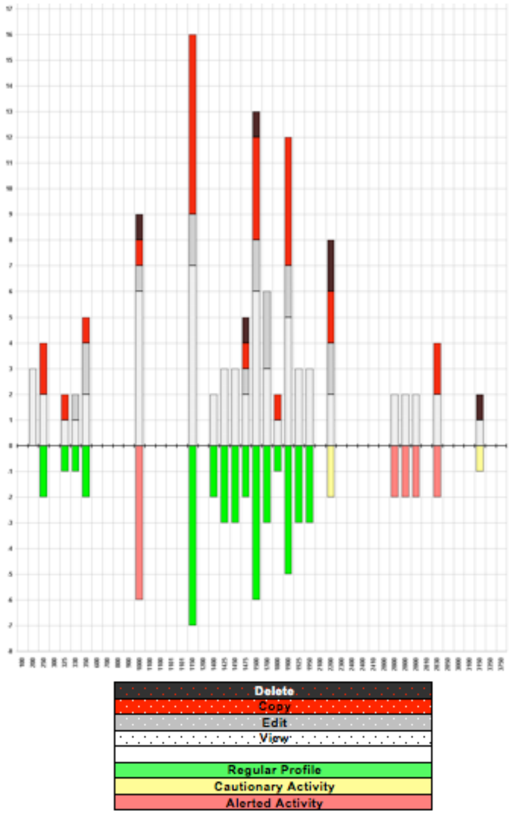
Coronado Group's Insider Threat uses new and innovative approaches to address one of the hardest problems in cyber security - how to detect, mitigate, and minimize the impact of malicious insiders and credential-holding virtual insiders. This effort offers a new method of understanding insider behavior and identifying behavior shifts that may become a threat. It provides cyber security professionals with:

- New tools to identify and analyze user behavior within their normal band of operation within their permissions across their total system presence;
- Methods to identify changes in "normal behavior" such as printing, searching, emailing, file manipulation that indicate potential malicious behavior;
- A comprehensive view of all of the insiders's behavior not just a view within individual applications and domains;
- Detection of "drift" in normal user behavior and methods to recognize differences between benign shifts based on changes in work assignments or seasonal changes in workload and malicious misuse behavior;
- Rapid identification of intruders and malicious behavior;
- Protection against highly credentialed insiders by providing unreadable mathematical representations of user behavior;
- Immediate identification of "virtual insiders" so that security personnel can block, track, or monitor attacker behavior;
- Integration with existing cyber security and FISMA/NIST compliant environments without change to those environments resulting in no implementation risk in deploying the new misuse detection tools into existing environments.

A Comprehensive Picture of Insider Behavior

Insiders have a very specific range of behavior within their privileges in each system and across all of the systems they interact with. They access parts of the system, email at certain times of day, print to specific printers, arrive through specific doors, and perform tasks based on their work assignments. Coronado's Insider Threat innovation provides a comprehensive picture of insider behavior.

Coronado Group is working on an innovative project to build a mathematical and contextual-based spatial security index of insider behavior using a comprehensive picture of real user's physical and digital presence in the systems. Using the vast array of digital information about the user - when they log in, how they work, how they come in and out of the building and the systems, we build a digital representation of how users and groups of users operate within their normal band of system presence and behavior. This approach leverages the extensive collections of audit logs, event logs, and access control and monitoring data found on enterprise systems to develop a multi-dimensional mathematical representation of user behavior within their defined permission set.

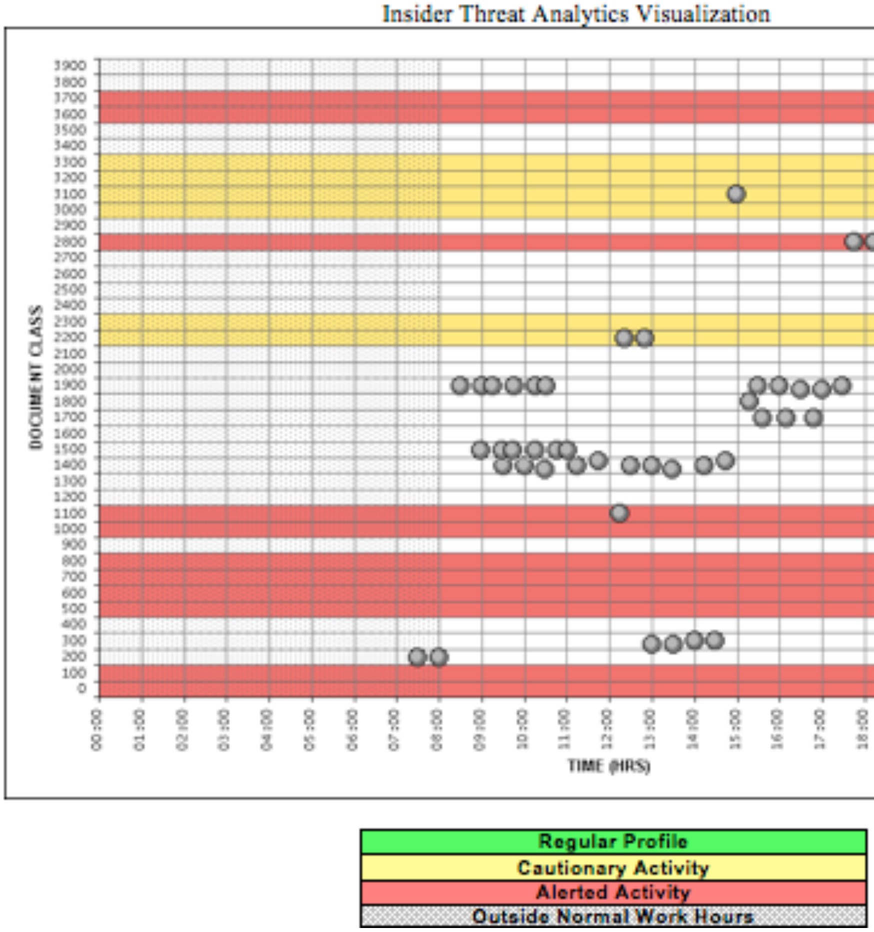


Where Do Insiders Go?

User presence data is used to create vectors that represent user behavior and categories of insider behavior defining an insider's "normal band" of behavior within their permissions. This high performance spatial security index is used for on-going analysis of user behavior to identify "drift" in behavior within their permission set and to determine when shifts in user behavior may indicate malicious behavior.

This approach enables a wide range of disparate user activity and access data to be used to create a highly nuanced, vector representation of user behavior making it extremely difficult for intruders or disgruntled employees to fully replicate user behavior. The proposed project uses established commercially available technology in an innovative way to create this user misuse detection tool. Our insider threat software can be integrated with existing security programs, protocols, and security tools without disruption to those models providing enhanced capabilities in identifying, analyzing and monitoring authorized user behavior and malicious intruder behavior at a relatively low cost of operation.

Insider Threat Analytics Visualization



Protection Against Insider Threat by Highly Credentialed Insiders

This approach has the potential to minimize threat from computer experts as the spatial index and processing techniques use complex configurable algorithms, are extremely difficult to replicate and provide data that is not human readable unlike conventional security software and techniques.

Protection from Virtual Insiders
The spatial index and vector-based representation of user behavior significantly complicates the ability of intruders to create “virtual insiders” or for users with access to user IDs and passwords to fully replicate the nuanced “normal behavior” of the user. This provides new rapid detection of intruders providing security administrators with improved insight and detection into intruder behavior and targets.

Rapid Integration of New Technology Platforms

Because Coronado's insider threat approach uses all of the available data about user behavior, its insider threat management capabilities can be integrated quickly as new digital assets and new technology is introduced into the user environment. Security personnel can DHS can rapidly introduce insider misuse detection when new technology platforms are introduced in the department regardless of the nuances of the audit/event information and security monitoring techniques of the new platform.   Our approach uses existing audit/event logs, access control data and other security files as they exist on the system making this tool complementary to existing cyber security protocols and programs. Any type of alphanumeric audit/event or other security monitoring data can be incorporated into this framework making it compatible with a wide range of systems no normally supported by traditional IDS/IPS environments.

A Look Under the Hood - The Science and Technology

The Insider Misuse/Threat Analysis and automated evaluation tool is being developed using a combination of latent semantic indexing (LSI), advanced categorization analytics, and metadata and user profiling informatics.

The system consists of four components:

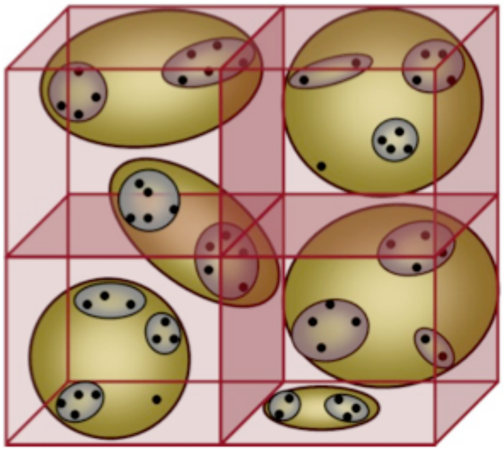
1) The spatial security index- a multi-dimensional array that represents user behavior and categories of behavior based on user roles, permissions, time, physical and application access data;
2) Tools to automate the on-going capture and evaluation of users to assess insider behavior against models of expected "normal behavior" and scoring mechanisms to create warnings and alerts as user behavior drifts or fails to meet the expected behavior parameters;
3) A meta data and user profile repository to store longitudinal user behavior; and
4) Visualization tools to enable security experts to interpret, react, and reconfigure the tool to address suspect user behavior. Following is a high level overview of the design and concepts of operations of the solution.

Create User and Time Specific Audit Text Objects and Convert Into Vectors

An Audit Text Object (ATO) is created from the contents of all of the significant/important audit log file contents (events) that represent a user's behavior in the system. The ATO represents the user's system behavior "personality," an integrated and comprehensive view of a user's behavior rather than how a user's behavior is represented by individual audit logs created by the systems/applications. Files are created for users in the time granularity defined for monitoring - an hour, 24 hours, files for 30 days, seasonal files, etc.   A collection of vectorized ATOs is created representing historical behavior of users and groups of users.[1] Individual daily user vectors can contain over 4 million characters providing support for even the most complex systems and access event management systems. The vector is associated with a small set of user defining metadata that is stored in the insider threat system. The content of the ATO is format-independent; any alphanumeric audit log data from any system can be configured as part of the ATO. This includes system access control data, physical control data, and application specific audit data.

Create a Multi-Dimensional Spatial Security Index

The spatial security index is a mathematical representation of collected of ATOs for all of the users in the system. It is created by clustering/categorizing the vectors. Clustering techniques create vector placement that corresponds to related subsets of user and role-based ATOs within the array. This is a multi-dimensional array is created using single value decomposition and dimensional reduction to establish the grouping of ATOs. Similar vectors are close to each other in the array. The clusters help define user behavior within their permission sets. Clusters present a hierarchical view of the groups of user behavior representing the user "personality" - the integrated view of all of a user's relevant system behavior. In the exhibit below, the larger circle indicate boundaries of permission sets and where individual users sit within those permission sets. Users that have similar behavior are closer together as indicated by the smaller circles within the boundaries.



Establish Behavior Boundary Scores

Cluster data is used to define upper and lower closeness ranges for user permission sets represented by the ATOs to determine the baseline used to assess on-going user behavior. This is used to establish the "continuum of good insider behavior" and closeness scores. A specific user assignment called a User Personality Score -- a baseline "score" or range of "scores" that reflect where the user operates within their assigned permissions is established. This data along with other relevant metadata that define the user are stored and associated with the index. The scores indicate how close a user's behavior is to their expected behavior.

[1] Coronado's system currently supports vectors exceeding 3.9M characters with millions of individual vectors available in seconds.

Create New Temporary Vectors and Assess Insider Threat

At scheduled intervals the tool will automatically assemble and translate the new audit files for users into new temporary vectors.
The vector processing engine will receive the vector representing the new audit log object; map the vector into the spatial security index and return closeness score for the user and other relevant identifying information about the user's current behavior as represented by the respective similarities between the representation of the new object and the representation of the baseline objects. The insider misuse detection tool will use the results to determine how the user's current behavior matches against the expected behavior for this user.

What You Need To Make It Work

The proposed technology platform used is commercially available and widely used. This facilitates rapid development and ramp up of the environment for new clients so that the effort can focus on the misuse detection effort. The first step is defining the optimal audit log/event data on which to build the spatial index and the content of the ATOs and best approaches to extract and capture it. The next step is defining optimal timeframes for assessing user drift and the frequency of behavior monitoring. This is usually driven by the value of the assets the insider's access and the security concerns of the organization. Different users will require different time parameters and granularity of the behavior being evaluated by the system. If you already have a large repository of historical use audit logs across the enterprise, these files can be used to build the insider threat monitoring and control environment.

About Coronado Group

Coronado Group has 20 years of experience introducing new and emerging technology into existing enterprise environments. It works with leading inventors, technology transfer professionals, licensing agents, and information technology product manufactures and product developers to develop and implement complex market strategies to commercialize and integrate new products into the platforms offered by software providers. Coronado Group has extensive intellectual property commercialization experience focused on reducing time to market by funding and accelerating new product introductions.

Coronado Group has implemented conceptual, contextual spatial indices, and vector-based analysis tools to support to solve complex scientific and technical problems. Its experience covers projects with the same characteristics as the technical solution proposed here - long strings of alphanumeric data - chemical strings, DNA sequences, formulas, log files, biometric and bibliographic data, mathematical representation of complex data - with varying patterns, content, granularity and longitudinal analysis challenges, and the need for rapid analysis across a multi-dimensional problem spectrum to develop new insight into information relationships, user profiling, and advanced scientific informatics. Coronado has extensive experience with the information security aspects of implementing nascent technology into large scale, data intense environments. The firm has deployed large scale systems in secure federal and commercial locations requiring ATO, FISMA, NIST 800-53, Information Assurance compliance, implementing the vary types of audit logs and security features and security procedures defined by these standards. Its principals are experienced Solutions Architects responsible for attaining IATO and ATO for secure systems

Coronado Group's interdisciplinary team of computer scientists and software engineers has deep experience in the design, development, and deployment of cyber security information technology; complex enterprise-wide solutions supporting thousands of users with diverse information access and security requirements; biometrics; development of products specifically designed to be deployed to support e-commerce, online transaction systems, and internet based deployment of medical devices requiring the highest level of HIPAA and privacy management. Our systems engineers have acted as both Solutions Engineers and Security Officers for secure and classified systems.

Please contact Arleen Zank at azank@coronadogroup.com or 703-909-7722 to learn more about this Coronado Group innovation.