VITRIA®

Solution Overview >

Vitria Technology's Cyber Security Solution

Table of Contents

Executive Overview

There is an explosion from a Soviet gas pipeline. The cause is a malfunction in the computer-control system due to stolen information from an IT company in Canada. The Soviet government is unaware that the software has been hacked into by their own spies to reset pump speeds and valve settings to produce pressures far beyond those acceptable for pipeline joints. The result is the most enormous non-nuclear explosion in world history.

Although the above events may seem from a Hollywood movie, they actually occurred at the height of the Cold War in June of 1982. This was one of the earliest real-life examples outlining the importance of cyber security for smart grids.

Similarly, there can be little argument that today's smart grids also face serious threats from cyber attacks. In January of 2003, the Nuclear Regulatory Commission confirmed that the Microsoft SQL Server worm known as the "Slammer" infected the computer network at the Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours.

Current smart grid security defenses were not designed to thwart advanced cyber threats and must also advance to deal with future cyber conflicts

The combination of increased access points to traditional network or smart grid data and the increasing sophistication of cyber attacks are making the need for robust security measures even more apparent. Current defenses were not designed to thwart advanced cyber threats and must also advance to deal with future cyber conflicts. At the core of the issue is the fact that many Supervisory Control and Data Acquisition (SCADA) systems, which run everything from public transportation systems to air-traffic control networks, were often designed without Internet connectivity or security in mind.

Protecting smart grids from attack and maintaining the balance between supply and demand is critical. Get the balance wrong and there can be very serious safety and financial ramifications for utilities and their customers. As more and more SCADA network data and smart meter data are communicated across public networks, malicious attackers have more opportunity to alter and falsify that information. These cyber attacks can range from unauthorized access to simple theft (customers adjusting meter data to pay less for energy consumption) to blackouts, fires, and grid damage. In the famous New York City power outage in the summer of 1977, for example, damage from looting and arson alone totaled approximately $155 million – almost half of the total cost of damage repair.

Cyber security solutions must evolve to detect changes in user behavior

Unfortunately, cyber intruders are developing attack patterns faster than the current security solutions can detect. Most existing cyber security solutions simply look for "signature-based" threats that search for known malicious patterns. This approach, while sufficient in some cases, is ultimately inadequate for two key reasons: 1) cyber attackers are quickly evolving their methods to evade signature-based detection and 2) signature-based detection often flags as threats benign

Cyber Security Scenario – Phising Attack

Spearphising, or simply phishing, is the criminally fraudulent process of attempting to acquire sensitive information, such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity in an electronic communication. A phisher might pose as an actual manager and send an e-mail to an unsuspecting employee with a legitimate link to download some software updates. The employee clicks on the link and is redirected to a legitimate-looking website (with corporate logos) that is actually controlled by the phisher. Once the employee accepts the license agreement and downloads, a network-bot is installed as a phisher-controlled agent on the employee's machine. However, with Vitria's cyber security solution, the employee's network server would immediately send an application download event notification to Vitria, which would correlate the spearphish to the network-bot. A Vitria CEP-generated alert would then instantiate a business process that would communicate to the network and web servers to stop any access from the compromised list of machines. As a result, the phisher would not be able to access any other machine inside the company's firewall.

activities, generating a stream of false positives that only exacerbates the needle-in-the-haystack problem inherent in cyber security.

Instead of relying on known patterns, cyber security solutions must evolve to detect changes in user behavior. Behavior-based detection looks beyond "who" the user is to also include "what" that user is doing and "when" (in which context). For example, a signature-based solution would not detect an issue if an attacker were to impersonate a valid user and access servers or systems typically not accessed by that user. If that user had valid access it would not be a known malicious pattern. However, a behavior-based solution would detect a change in that user's behavior, flag the issue, and send notification for review and action. Thus, behavior-based solutions are much more likely to detect identity theft issues.

Vitria provides a comprehensive, fully integrated cyber security solution. Vitria's cyber security solution is the pioneer in assessing real-time behavior via data feeds, comparing that behavior to baseline reference data, determining appropriate action via a rules engine, and displaying results using role-based, graphical dashboards. It brings together the best of both worlds by extending existing solutions and taking signature-based output to find the signal-in-the-noise and filtering it to eliminate the false positives.

Value of Vitria's Real-Time Cyber Security Solution

Cyber attackers are increasingly becoming more sophisticated. They know the common ways of avoiding signature-based sensors and are employing new tactics to hack into systems. For instance, obtaining valid credentials for a system from a current user is a simple way to avoid detection. Once logged in, the attacker must be detected by his/her behavior, not by his/her signature. Inevitably, this is where most security systems fail.

Behavior-based threats are characterized by suspicious behavior that is associated with a type of attack. Behavior-based analysis is inherently probabilistic and typically rule-based. When network interactions mirror malicious behavior or fall outside the normal behavior, the session can be flagged as a potential attack and appropriate action can be taken. This type of detection can also be anomaly-based, where normal activity is characterized and behavior that deviates from normal interaction is identified as a potential threat. For example, if a valid user enters the system and performs some type of device discovery action, such as pinging or porting scans, and if this user was either logged in on multiple systems or onto an unused system, then this would raise a red flag.

There are many other challenges, such as:

- The flood of real-time data from routers, firewalls, and Intrusion Detection and Prevention Systems (IDPS)
- Determining which of the above alerts are important
- Generating timely responses to these predetermined alerts

- Post-event inspection across multiple domains, hosts, and Intrusion Detection Systems (IDS)

What is needed to meet these challenges is a powerful, complete system that is user-friendly and role-based to ensure the right people get the right information at the right time. Powerful data feed services, advanced analytics, query-based complex event processing (CEP) for correlation, an automated response mechanism, and advanced visualization capabilities are needed in order to deliver a complete real-time data surveillance and analysis solution. Although there are commercial off-the-shelf (COTS) tools available in some of these functional areas, integrating them is a challenge.

A widespread signal-in-the-noise and filtering problem is that of spearphishing, as highlighted by the scenario in the box to the left. Phishing became so prevalent on AOL in the mid-1990s that they added a line on all instant messages stating: "No one working at AOL will ask for your password or billing information." Not only can Vitria's cyber security solution alleviate this problem by filtering out the false positives generated by traditional cyber security solutions, but also deliver a behavior-based solution that can identify the more sophisticated attacker.

Vitria's Cyber Security Solution Software Components

Vitria delivers groundbreaking real-time data surveillance and analysis with the M3O Operational Intelligence platform. This fully integrated software suite provides the following benefits:

- Access to a wide variety of data sources in real-time, including business transactional systems, operational systems, and external sources (i.e., Web feeds)
- Continuous monitoring and analysis of information in real-time
- Ability to access and correlate information
- Rich visualization of the raw and analytical data organized easily from the user's perspective
- Ability to quickly expand the field of inquiry through a patented Dynamic Rules API, which allows IT analysts to quickly model new targeted queries to further track and mitigate a potential threat
- Ability to respond to an alert using a variety of automated and human workflow processes

Vitria's M3O Operational Intelligence suite fosters development productivity and collaboration by delivering model-driven, fully integrated products, including a CEP engine, dashboarding and visualization tools, and policy and process management. The M3O components can be deployed in traditional enterprise computing environments or via the Cloud as-a-Service.

M3O components can be deployed in traditional enterprise computing environments or via the Cloud as-a-Service

Vitria's M3O Operational Intelligence product components are as follows:

M3O® Analytic Server

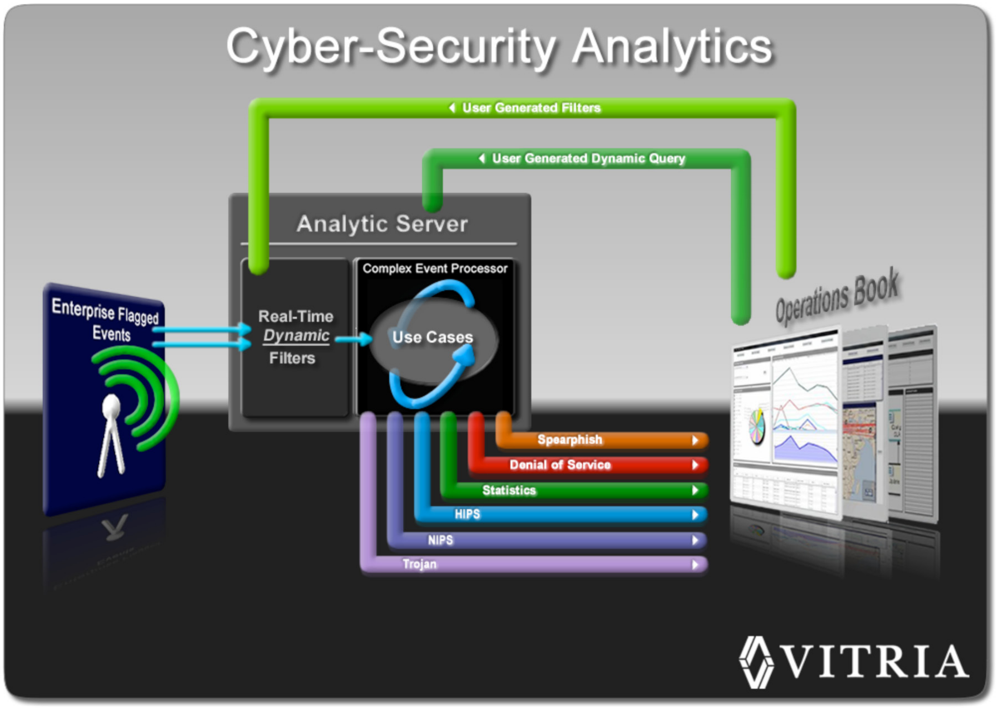
The core of Vitria's cyber security solution is the powerful M3O Analytic Sever equipped with a complex event processing (CEP) engine that performs multi-dimensional analysis, correlation, event filtering, aggregation, trending, and pattern analysis of continuous real-time feeds. This powerful CEP engine is designed for elevated performance in highly scalable, distributed environments.

M3O® Feed Server

The M3O Feed Server is an advanced event stream management system and is the underlying source of data for the M3O Analytic Server. It is a new type of data management system that allows continuous handling of data streams in a real-time and incremental fashion. The M3O Feed Server provides seamless connectivity to traditional and non-traditional information sources, such as JMS, RSS, web services, and databases, enabling what-if analysis, event archiving, and recovering of feed histories. The M3O Feed Server also allows managing and balancing large volumes of real-time events across multiple M3O Analytic Servers as necessary.

Dynamic Rules API

The Dynamic Rules API allows partners and customers to use custom-built or commercial off-the-shelf (COTS) Flex or Java-based applications to interface with and push queries into the M3O Analytic Server. The API enables non-Vitria Flex and Java clients to access the M3O Analytic Server to programmatically create new queries or modify existing queries, define result destinations, and so on. This dynamism is a key capability as situations change and threats develop.



Cyber Security Dynamic Forensics using the Dynamic Rules API

M3O® Business Process Server

The M3O Business Process Server is the runtime environment to perform model-driven execution of policies and processes defined as BPMN models via the M3O Modeler. The M3O Business Process Server also provides the capability to define and manage policies across the enterprise, apply the policies to events, and then take action according to these predefined policies.

M3O® Operations Book

The M3O Operations Book is a powerful Web 2.0-rich Internet application that easily defines dashboards to monitor Key Performance Indicators (KPIs) and Service Level Agreements (SLAs). The M3O Operations Book has an extensive library of widgets providing rich visualization of data in a variety of ways. Users can mash-up and display analytics that visually model the relationship between information and events, leveraging the CEP engine in the M3O Analytic Server. With easy-to-use dashboards that combine real-time information sources with historical data, the M3O Operations Book delivers real-time information, reducing time-to-visibility when it matters most.

Conclusion: Benefits & Experience

Secure and reliable operation of the electrical grid is fundamental to a nation's economy, security, and quality of life. An electrical grid's interconnectedness makes it increasingly vulnerable to disruptions initiated by intentional attacks.

You cannot have a smart grid without equally "smart security" protecting it

Smart grid deployments result in SCADA networks that are more integrated, leading to increased vulnerability to cyber attacks. It is important to realize that the current electrical grid is being transformed into a smart grid, and that you cannot have a smart grid without equally "smart security" protecting it.

Vitria's cyber security solution combines CEP capabilities with business process management (BPM), analytics, intelligent decision aids, and database enrichment to provide this "smart" security solution. It has therefore been the basis for multiple applications from defense intelligence to financial services to the healthcare industry to communications/media to energy/utilities.

About Vitria

Vitria Technology, Inc. is the industry's leading Operational Intelligence company. Our innovative Operational Intelligence solutions empower customers to analyze business activities in process and take real-time action. The result is better decisions when they matter most—before opportunities have faded or problems have escalated. With a rich heritage as a pioneer of BPMS, Vitria's award-winning solutions provide the backbone for many Global 2000 companies' mission-critical business processes. Vitria has customers in North America, South America, Europe, Asia, and Australia.

VITRIA®

945 Stewart Drive, Sunnyvale, CA 94085
Tel: +1 (877) 365-5935
Email: moreinfo@vitria.com
www.vitria.com