Predictive Cyber Defense
A Strategic Thought Paper

Don Adams
Vice President, Chief Technology Officer, Worldwide Government
TIBCO Software Federal, Inc.

TIBCO®
The Power of Now®

Summary

The art and science of multi-sensor data fusion has emerged as the underlying foundation for Predictive Business®, including applications in telecommunications, finance, transportation, defense intelligence, and law enforcement. All of these have common threads requiring complex inference processing solutions and require the management of real-time events from distributed sensors, agents and other processing components, including historical data-at-rest repositories.

Distributed coordination-based architectures such as TIBCO Enterprise Message Service™ or TIBCO Rendezvous® and large-scale distributed memory systems like TIBCO ActiveSpaces® provide the underlying communications infrastructure that enables complex event and high performance rule-based processing services.

In this paper, we discuss Predictive Business in the context of a pressing need to remove a perpetrator's decision loop in a predictive cyber defense environment, with a focus on the distributed processing architecture. The focus: how complex event processing solutions like TIBCO BusinessEvents® can be applied to developing new cyber defense strategies.

KEYWORDS: COMPLEX EVENT PROCESSING, EVENT-DRIVEN ARCHITECTURE, EVENT STREAM PROCESSING, JDL DATA FUSION MODEL, MULTISENSOR DATA FUSION, PREDICTIVE BUSINESS, RULES-ENGINE, RULES-BASED SYSTEM, PREDICTIVE CYBER DEFENSE

Getting Ahead of Cyber Warfare

The sharp rise in cyber warfare threats on military infrastructures, government communications systems, and financial markets has amplified the need for a new generation of cyber defense weapons.

As new attack methods become more sophisticated and persistent, traditional detection and remediation efforts not only put the security of critical assets in danger, they also threaten the security of critical infrastructures – including the power grid, oil and gas distribution, and transportation models. Rigid and inflexible, classic-defense solutions – such as firewalls, intrusion detection and preventative decoys (a.k.a. honeypots) – can easily be identified, thwarted, and bypassed.

In order for defense, homeland security, and critical infrastructure protection organizations to effectively defend systems and infrastructures from cyber attacks, they must stay ahead of cyber warfare techniques.

This paper addresses how event-driven infrastructures and complex event processing (CEP) solutions enable this capability by allowing highly intelligent, flexible monitoring and response systems to proactively detect when security is being breached and in automated fashion, defend critical infrastructures before damages have occurred. It also discusses how Predictive Business can minimize infrastructure risk through turning historical data into actionable knowledge.

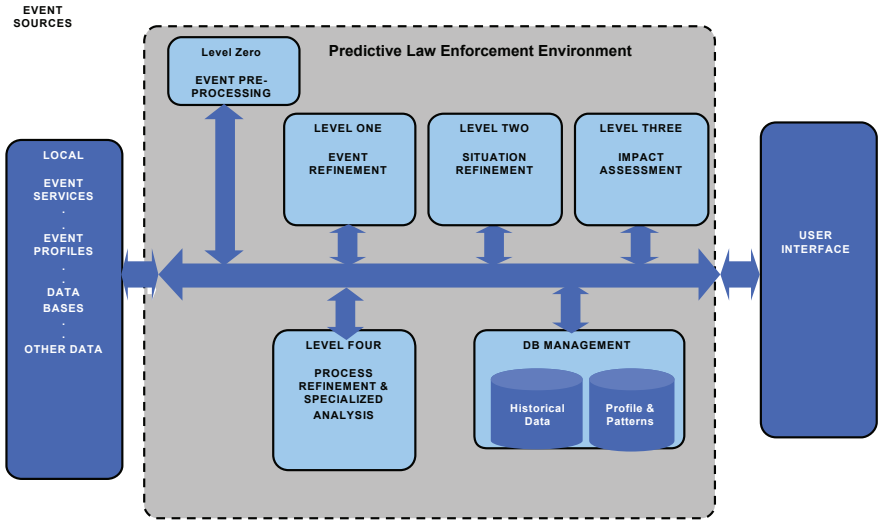
Predictive Cyber Defense

In his latest book, founder and CEO of TIBCO Software Inc. Vivek Ranadivé discussed how the fusion of historical knowledge with real-time information can ignite Predictive Business. This powerful combination – one that lives at the heart of TIBCO's event-driven technologies – enables organizations to take action the moment an event occurs. No matter the business domain, the right information reaches the right place just a little ahead of when it's needed to seize opportunities before they vanish and avoid disruptions before they occur.

In the world of governmental affairs, Predictive Business has very much been part of the evolution in cyber defense strategies. The detection theory of the Joint Directors of Laboratories (JDL) data fusion model, for example, has been deployed utilizing complex event processing for autonomous monitoring and alarming, as well as a passive command and control platform for cyber defense.

Demonstrated to be directly applicable to detection theory – where patterns and signatures are discovered by abductive and inductive reasoning processing (e.g. data mining) is fused with real-time events, the JDL model has survived the test of time as the dominant fusion model for decades. Vivek Ranadivé indirectly refers to this model when he discusses how real-time operational visibility, in context with knowledge from historical data, is the foundation for predictive business.

The JDL model shares similar structural components to TIBCO's enterprise service bus. For details on how these compare, please reference "Predictive Business Architecture: Using RETE and the JDL Knowledge Building Models."



Changing the Game with a New Set of Cyber Defense Players

The opportunity for cyber defense organizations lies in these similarities – surveying and monitoring a pattern of an intruder's behavior and based on historical movement, proactive combating attacks. This idea is at the heart of what TIBCO specifically calls the two-second advantage™: the ability to capture the right information, at the right time, and act on it preemptively for a competitive advantage.

Specifically, organizations can leverage CEP technology and the JDL model to:

1. Identify the threats that resemble attack vectors or patterns of probing that have the potential to precursor an impactful attack

2. Analyze patterns to predict system and network vulnerabilities that are most attractive to attackers

3. Stage decoy systems as bait (a.k.a. honeypots) to capture attention and movement, further adding to the depth in which behavioral patterns are understood

4. Harvest events on a massive scale happening within the threat event cloud to identify previously unseen internal and external multi-vector threat profiles (which are becoming more common threats in critical networks)

5. Deliver false information on vulnerabilities and threat responses from replicas of systems under threat

6. Protect "real" systems while undermining attacker's credibility

What might this cyber defense strategy look like in the real world?

In a remote network center, Jin is on a mission: find and archive vulnerable locations and systems. This is not an attack or a precursor to an attack; he is simply keeping a log in case he needs to disable the systems he is watching. By performing random patterns of door knocking, he will slip in and out of critical infrastructures around the globe to determine changes in protective and preventative solutions.

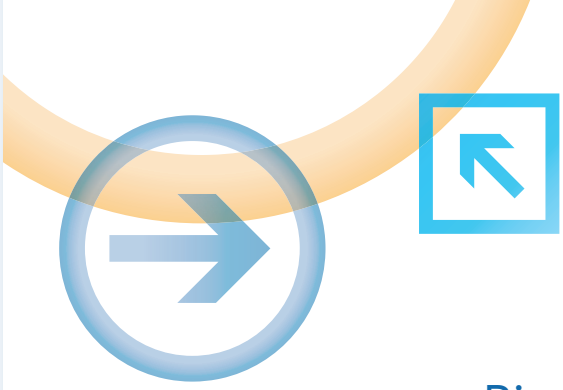
Little does he know that he is not the hunter, but rather the hunted. Drawn into a trap, Jin's actions have been located, patterned, and modeled by a new set of players in the cyber defense arena.

Within seconds, Jerry, a senior cyber defense officer was alerted to Jin's presence based on a pattern of probing that matched Jin's past approaches. In defense, Jerry launches a CEP model that will distract Jin and lead him to believe he had found a new system that is highly vulnerable.

After carefully characterizing the potential value inside the decoy system, Jin files this away in his priority list of systems to frequently update.

In reality, the complex event-driven predictive cyber defense would provide Jin with an invalid set of attack vectors that would not only be false, but would also undermine the faith of his attack team – eroding credibility from within.

Whether it's Domain Name System (DNS) poisoning, BotNet exploitation, random latch rattling, or complex multi-vector data exfiltration protections, a new series of predictive cyber defense strategies and tools are finding their way into the arsenals of national defense organizations and cyber warrior – delivering the ability to fuse historical data and real-time events into actionable knowledge and a secure means to proactively defend against cyber warfare.



Biography

Don Adams (dadams@tibco.com) is currently the vice president, chief security officer and chief technology officer, worldwide government, at TIBCO Software Federal, Inc. In this position he provides expertise in security, government strategy and emerging technologies related to the TIBCO family of software solutions and service offerings.

Prior to TIBCO, Mr. Adams was the chief technology officer of TriStrata Inc. where he set the overall security philosophy, design and systems architecture for the revolutionary TriStrata Secure Information Management System. Prior to TriStrata, Mr. Adams spent six years at Sun Microsystems, where his last position was principal architect, security and networks. While at Sun Don participated as architect or chief architect on over four and a half billion dollars worth of government contracts won.

Prior to Sun Microsystems, Mr. Adams spent a highly decorated 23-year career in the United States Air Force. Mr. Adams started his career teaching at the Air Force Cryptographic Systems School in San Antonio, Texas, and spent the majority of his career in design, architecture, operations and maintenance of command, control, communications, computer and intelligence (C4I) systems.

Mr. Adams was recently published as one of the contributing authors of the McGraw Hill Homeland Security Handbook. His chapter on critical concepts for IT in homeland security covers both Sense and Respond and Predictive Response for enterprise, counterterrorism and healthcare emergency response.

TIBCO®
The Power of Now®

Global Headquarters
3303 Hillview Avenue
Palo Alto, CA 94304

Tel: +1 650-846-1000
+1 800-420-8450
Fax: +1 650-846-1005

www.tibco.com