

TIBCO Cyber Security Platform

Atif Chaughtai

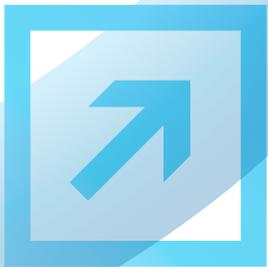


TABLE OF CONTENTS

1	INTRODUCTION/BACKGROUND	3
2	CURRENT CHALLENGES	3
3	SOLUTION	4
4	CONCLUSION	6
5	A CASE IN POINT: THE US INTELLIGENCE COMMUNITY	7

“A little bit of the right information, just a little bit beforehand- whether it is a couple of seconds, minutes or hours- is more valuable than all the information in the world six months later...”

- Vivek Ranadive, Founder & CEO

Introduction/Background

“A little bit of the right information, just a little bit beforehand – whether it is a couple of seconds, minutes or hours – is more valuable than all of the information in the world six months later...”. That is the 2-second advantage vision as described by our founder and CEO, Vivek Ranadive. One of the areas where it is most applicable is in the arena of Cyber Security. In most large organizations, there is an average of 40-50 security devices such as Firewall, IPS, IDS, etc providing perimeter defense. These devices are very good at what they do but are operating in silos creating disparate security alerts. In the case of a Cyber Threat, it is up to a human to piece together these alerts to identify a true threat. TIBCO applies the concept of the 2-second advantage to this challenge to provide a real-time multi-factor event correlation and prediction platform that is content and context aware.

Current Challenges

According to Gartner, a medium size organization consists of 750 employees. On average, a medium size organization collectively generates 20,000 security events per second. Over eight hours, this comes out to 576,000,000 events. If we are to take a 300 byte average size for each event, this amounts to 172.8 GB of data over eight hours that needs to be collected, moved and analyzed. This is an alarming fact and the amount of these alerts will only grow as users consume and produce more and more data. This shear amount of data along with the perimeter defense approach of point security devices used to protect the corporate digital assets creates several other challenges:

- **Compliance:** Unable to conduct real-time compliance analysis
- **Large Data Volumes:** How long does it take you to figure that some sensitive data was stolen or accessed wrongly?
- **Enterprise Security:** How do you balance the security concerns with usability concerns of your customers?
- **Identity Fraud:** How and when do you know when a trusted user goes rogue?
- **Data Loss:** How do you prove to your customers that they can trust you with their sensitive data?
- **Cyber Attacks:** How do you implement real time offensive/defensive mechanisms when a cyber attack occurs?

One key problem is that the current perimeter defense approach using point solutions offers no central point for Correlation and Analysis! The result is that the information is in disparate point systems. It is typically left up to a human to piece it together (correlate) and determine if it is a threat, determine how to react, and then to actually take the action. This manual task is slow and prone to errors. In some cases, customers have deployed Security Information and Event Management (SIEM) tools to collect these events from log files and use SIEM as the central point for correlation and analysis. However, the challenges with SIEM tools are that:

- a) The information is too much to process (Big Data)
- b) these tools create too many security alerts - Human's have to investigate these alerts & determine if it is a true threat. Most often these alerts turn out to be false positives and waste human resources - again slow and error prone. This is especially true when compared to the time frames and automated level of most attacks.

The attackers are faster, more nimble, and more automated; they are relying on exploits (computer programs) to identify weaknesses from a rich library of exploits. There is no Hollywood version of an attacker sitting in front of screens typing faster than your security professionals; it is in real time and dynamic. **TIBCO provides the same mechanism for fighting back: correlated; real time; dynamic; and capable of dealing with the data volumes of the 21st Century.**

Solution

TIBCO leverages its patented real time integration technology to relevant data sources, such as sensors, applications, LAC's/PAC's etc. to feed that information to the TIBCO Cyber Security Platform to provide comprehensive protection. The TIBCO Cyber Security Platform is a multi factor event collection, enrichment and prediction platform that is Content and Context Aware. All of this is done in real-time, in-memory, is automated, and scalable.

Using our real-time event enabled adapters to applications, we are able to correlate information across applications and security sensors to provide deeper contextual and content awareness. These adapters are integrated at the API level and are able to pick up state changes at the events level before a transaction is committed. A transaction is typically comprised of several steps (events). All of

these events are transported on our secure, reliable and scalable information bus. This approach has a clear advantage over just reading log files which capture information after the fact. This deeper contextual knowledge allows us to automatically enrich security events and reduce false positives. One of the additional key features of the platform is its in-memory capability. We are able to model and keep knowledge of the asset behavior based life cycle in memory and are able to do complex multi factor event correlation in real time. We call this “enrichment of raw events with Content and Context”. This event based analysis allows us to deliver the vision of the 2-Second Advantage in Cyber Security. For-example:

Typical Event Correlation Rule:

An abnormal number of activities are being conducted on a sensitive application by a privileged user.

Content Rule: (TIBCO added value)

Privileged user is not an Administrator and is updating historical records in the sensitive application.

Context Rule: (TIBCO added value)

Privileged user has badged out for the day – Raise Critical Alert

Additionally, our advanced “in memory” capabilities, in conjunction with our ability to provide continuous queries and firing of rules as new events take place, provides a solution to the increasing amounts of data. This is very different from SQL and log based solutions where query times increase dramatically as the amount of information increases. If there is one thing that is definite, data volumes are going to continue to increase.

The TIBCO Cyber Security Platform enables fast response, taking into account changing business conditions and new Cyber threats to provide effective real time cyber security – This is known as the **TIBCO Two-Second Advantage**.

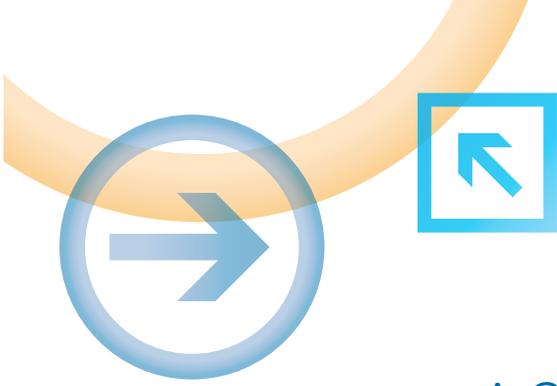
Conclusion:

Cyber Security is the biggest challenge of our decade and you need a 21st century technology and approach to address this challenge. TIBCO Cyber Security Platform leverages 21st century technology to provide a real time, in-memory, scalable and automated platform. TIBCO knows correlation of log files is just not enough to have confidence in the cyber surveillance. With TIBCO Cyber Security Platform you can now:

- Get a big picture of the attack in real time: the actors, the asset, time, content & context
- Sense malicious actors and automatically refine evidence
- Reject requests that do not fit the profile of good behavior
- Focus efforts on true threats – filter out low priority noise
- Provide Interoperability - Get a “backbone” able to move the data quickly & reliably

Using these techniques, we help organizations such as yours to:

- meet the challenge of real time compliance
- help deal with identity fraud
- handle large amounts of data for real time analysis
- provide enterprise security including insider threats
- automate reaction to cyber attacks in real time.



A Case in Point: The US Intelligence Community

- Spent 2+ years evaluating solutions before deciding on TIBCO
- Standardized on TIBCO technology for all internal organizational messaging
- Standardized on TIBCO messaging technology for Cyber Security - Einstein 3
- DHS is tasked with deploying the Einstein 3/TIBCO to protect the .gov domain

TIBCO Software Inc. (NASDAQ: TIBX) is a provider of infrastructure software for companies to use on- premise or as part of cloud computing environments. Whether it's optimizing claims, processing trades, cross-selling products based on real-time customer behavior, or averting a crisis before it happens, TIBCO provides companies the two-second advantage™ – the ability to capture the right information at the right time and act on it preemptively for a competitive advantage. More than 4,000 customers worldwide rely on TIBCO to manage information, decisions, processes and applications in real time. Learn more at www.tibco.com.



Global Headquarters
3307 Hillview Avenue
Palo Alto, CA 94304

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

www.tibco.com