Balbix®

Tackling the Toughest Cyber-Security Challenges Using AI

Contents

Introduction

In the eBook *Executive Guide to AI and Machine Learning* , we explored the differences between *human intelligence and AI*, specifically what we mean when we talk about artificial intelligence, machine learning, expert systems, and deep learning.

We considered a definition of intelligence and its three components: *a store of knowledge, mechanisms to acquire knowledge, and the ability to use knowledge for problem solving*. We differentiated between the notions of *general AI* (which does not exist today) and *narrow AI* (which does). We also reviewed the relationship between the terms AI, machine learning, expert systems, and deep learning, and we looked at several narrow AI systems in domains outside of cyber-security.

In this eBook, we will focus specifically on how we can tackle the cyber-security challenges using AI and Machine Learning.

- What is the state of this technology today?
- What does the future hold?
- How can AI/human partnerships address our most pressing cyber-security challenges?

Balbix

Chapter 1:

The Cyber-Security Challenge

The cyber-security challenge can be defined as maintaining the confidentiality, availability, and integrity of our computer systems. There are three major focus areas involved in cyber-defense:

1. **Vulnerability assessment**
2. **Setup and management of effective security controls**
3. **Security incident handling and response**

In recent years, cyber-security has become *a hyper-dimensional problem of extreme scale*. With the "computerization" of our businesses, the number and variety of vulnerabilities has exploded. New and novel ways of compromising computer systems are discovered every day by security professionals as well as adversaries. Despite best efforts and robust technology investment, breaches are occurring with alarming frequency, oftentimes resulting in significant damage.

In security circles, we talk about the importance of getting basic security hygiene right before deploying exotic security tools. The term security hygiene (or *cyber hygiene*) refers to the practices and steps that users of computers and other devices take to maintain system health and improve online security. *At Balbix, we consider basic security hygiene to be the first goal of AI in cyber-security*.

Balbix

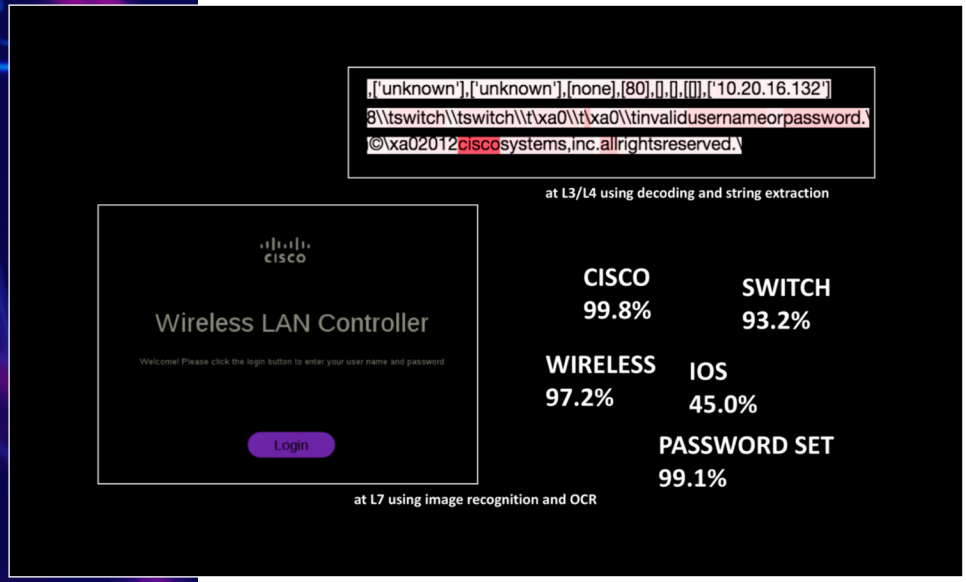

Figure 1: Asset inventory using intelligent analysis

A deeper dive into Asset Inventory

Let's take the problem of asset inventory. We know that the best human experts can put together an accurate picture of the type and category of a device on your network by manually looking at a broad variety of data sources. For example, from Layer 3 packet analysis, an expert might be able to extract media access control (MAC) organizational unit (OU) information that indicates that a device is a Cisco device. At Layer 4, they might see transport headers and protocol behavior that are consistent with the device being a switch with a management portal available at ports 80 and 443. From Layer 7 analysis of protocol behavior and a study of artifacts rendered in the web browser, we might be able to say that port 80 does not automatically redirect to port 443, and that the device is a wireless LAN controller made by Cisco.

Balbix

Chapter 2:

AI in Cyber-Security

At Balbix, we use AI to mimic this type of intelligent analysis by throwing L3, L4, and L7 data from different vantage points on your network into a sequence-to-sequence *deep neural network* which discovers, inventories, and categorizes all devices, users, and applications. The system is near real time, with entities analyzed the second they show up on your extended network. Once the confidence level of the algorithms is above a threshold, we surface an analyzed device in the appropriate part of the model, indexed with all of its relevant attributes.

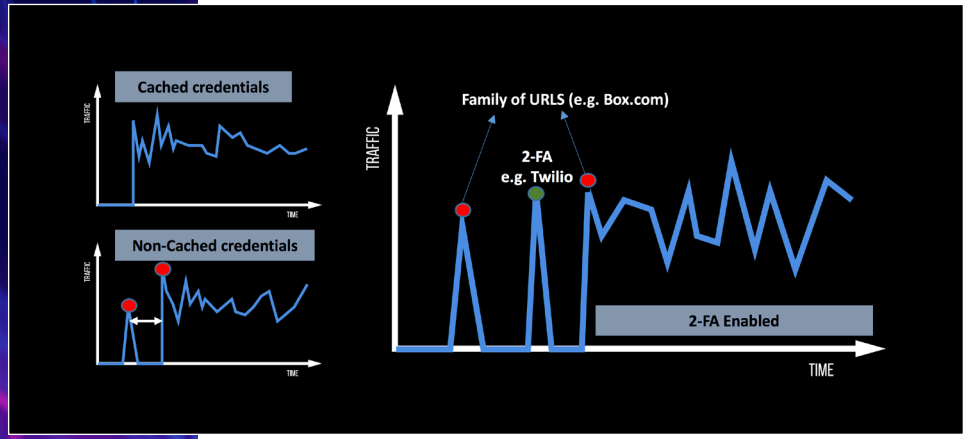

Figure 2: Time-domain correlation analysis

Hyper-Dimensional Machine Learning

One great example of hyper-dimensional machine learning is the algorithm Balbix uses to figure out users associated with certain types of unmanaged devices. Typically, you can identify users associated with laptops and desktops either by linking them with Kerberos authentication or domain logon sessions. But as you can imagine, you might walk into the office with your laptop and smartphone together, and then start doing things on the network in a somewhat time-correlated fashion. One day, you might walk in with a colleague with their own laptop and smartphone, confusing the correlation, but after a few days a clear picture of linkage between your devices should emerge. The Balbix system uses the time-domain correlation of Dynamic Host Configuration Protocol (DHCP) lease renewals, beginning-of-day traffic time, on-off times, and timing of Gmail push notifications to different devices to figure out if a smartphone and a laptop/desktop have the same owner. The effectiveness of this model is quite amazing.

Balbix®

Security and Risk Insights

Balbix uses other advanced machine learning models to figure out tiny and yet important details that impact risk, such as whether 2-factor authentication is turned on and active for a particular device, or if a user's device is caching login credentials. An ensemble of such models is chained together to build an overall picture of security posture and breach risk, device by device, group by group, and site by site.

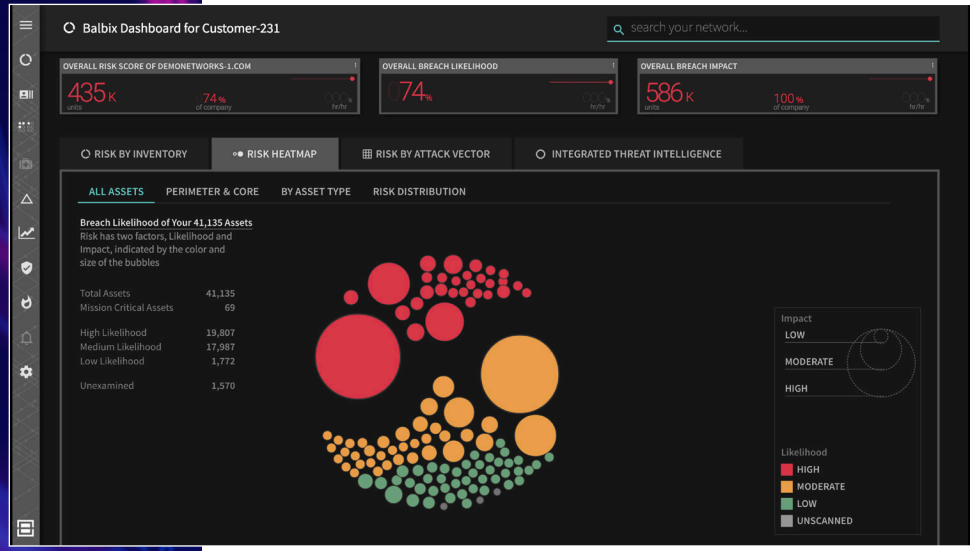

Figure 3: Balbix risk heat map

To access this corpus of security and risk insights, Balbix provides a searchable and clickable risk heat map. You can search your inventory using simple terms such as "smartphones," "DNS servers," "source code," "PCI data," or more complex queries such as "all unpatched OSX devices in Mountain View on the HR team." You can also ask risk-focused questions like "where will attacks start," "what will they go after," or "where is my data."

The Balbix dashboard provides various drill-down screens that let you "see" the detailed attributes and attack surface drivers of an individual system area. Balbix also lets you see various trends and create custom reports and notifications. And perhaps most important, it plugs into your enterprise workflows and systems with APIs and connectors.

The Balbix dashboard provides various drill-down screens that let you "see" the detailed attributes and attack surface drivers of an individual system area.

Balbix®

Chapter 3:

Balbix BreachControl

Imagine a properly trained, self-learning system capable of autonomously and continuously gathering data from a wide variety of sources about your enterprise and performing correlation of patterns across hundreds of dimensions. BreachControl does all this and more in order to surface the following categories of intelligence:

1. Deep understanding of every relevant detail (configuration, usage, etc.) of your **extended enterprise inventory** – all devices, users, and applications, on-premises and off.
2. Deep context around **business criticality** of each asset and user.
3. Up-to-date knowledge of **global and industry-specific threats** – aka what is fashionable with the adversary on a daily and weekly basis.
4. Intimate understanding of the various security products and processes you have deployed as part of your overall **breach risk mitigation** plan.
5. Calculation of your effective risk that takes into account all the information in items 1-4 above and **predicts** how and where you are most likely to be breached.
6. **Prescriptive insights** into how you might best configure and enhance your security controls and processes to improve your cyber-resilience, without negatively impacting business operations.
7. Maximal context for **prioritized and efficient handling of security alarms** and incidents with impact minimization; inform **tactical response** to incidents, but also surface root causes and **prescribe strategic mitigations** for the underlying vulnerability.
8. **Visualizations and reports** that explain calculations and recommendations and contain relevant information for all stakeholders involved – users, business unit owners, security operations, CISO, auditors, CIO, CEO, and board members.

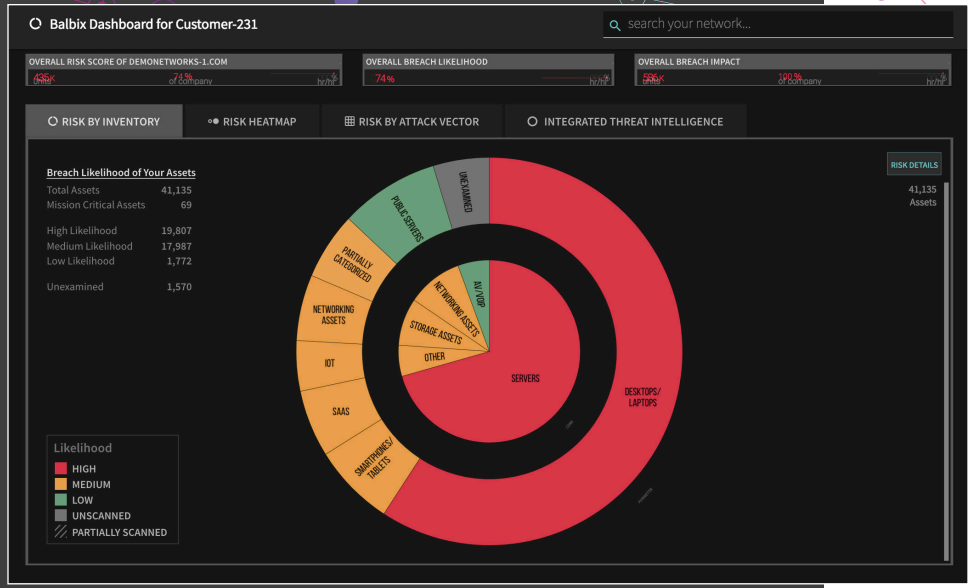

Figure 4: Balbix risk dashboard

Conclusion

BreachControl platform uses some of the world's most advanced AI algorithms, and has already been trained with lots of data. BreachControl is in production in many networks, and it is helping our customers leverage the power of AI to enhance business outcomes. If you had such a system, it would be a force multiplier and central enabler for your team, improving visibility and effectiveness by several orders of magnitude, and changing the meaning of what you can do at human scale.

Balbix®