
# DTECT: Customer Value Proposition

Alan Chen, Weiyuan (Carl) Che, Or Aharoni,
Rutwa Engineer, Xi Huang


Dtect The Undetected

# Customer Personas

NAME

Javier Lorenzo

NAME

Larry Powell

# Customer Profile

## Javier Lorenzo

**Important Jobs:**

- Functional jobs

**Important Pains:**

- Insider threats may already exist undetected
- Time and effort to create and maintain their own solution
- It is hard to tell whether a solution is effective

**Important Gains:**

- Expectations of detection and avoidance of insider threats are satisfied
- Saves time and effort
- Failure and success are measured (false positives/negatives, avoidance of incidents)

# Customer Profile

## Larry Powell

**Important Jobs:**

- Social jobs and basic needs

**Important Pains:**

- Requires money and effort to purchase and integrate a third-party solution
- Too many false positives
- Lack of feature to further investigate the alert raised by the product

**Important Gains:**

- Saves money and effort
- Bein able to identify anomalous patterns of behaviour
- Being able to validate alerts raised by the product before taking actions

# Products & Services

Activity log ingestion

Behavioural data visualization

User behaviour analysis with machine learning

Security system onboarding

Regular system updates

Recurring billing

# Value Proposition

## Pain Relievers

- Flexibility & Scalability
- Recurring updates
- Insider threat alert system

## Gain Creators

- Identify subtle and pattern-based behavioural anomalies
- Overall visualization for behaviour monitoring
- Elevate decision maker’s image with a satisfying product

# Competitive Landscape

## Direct competitors




# Competitive Landscape

## Indirect competitors



# Differentiation

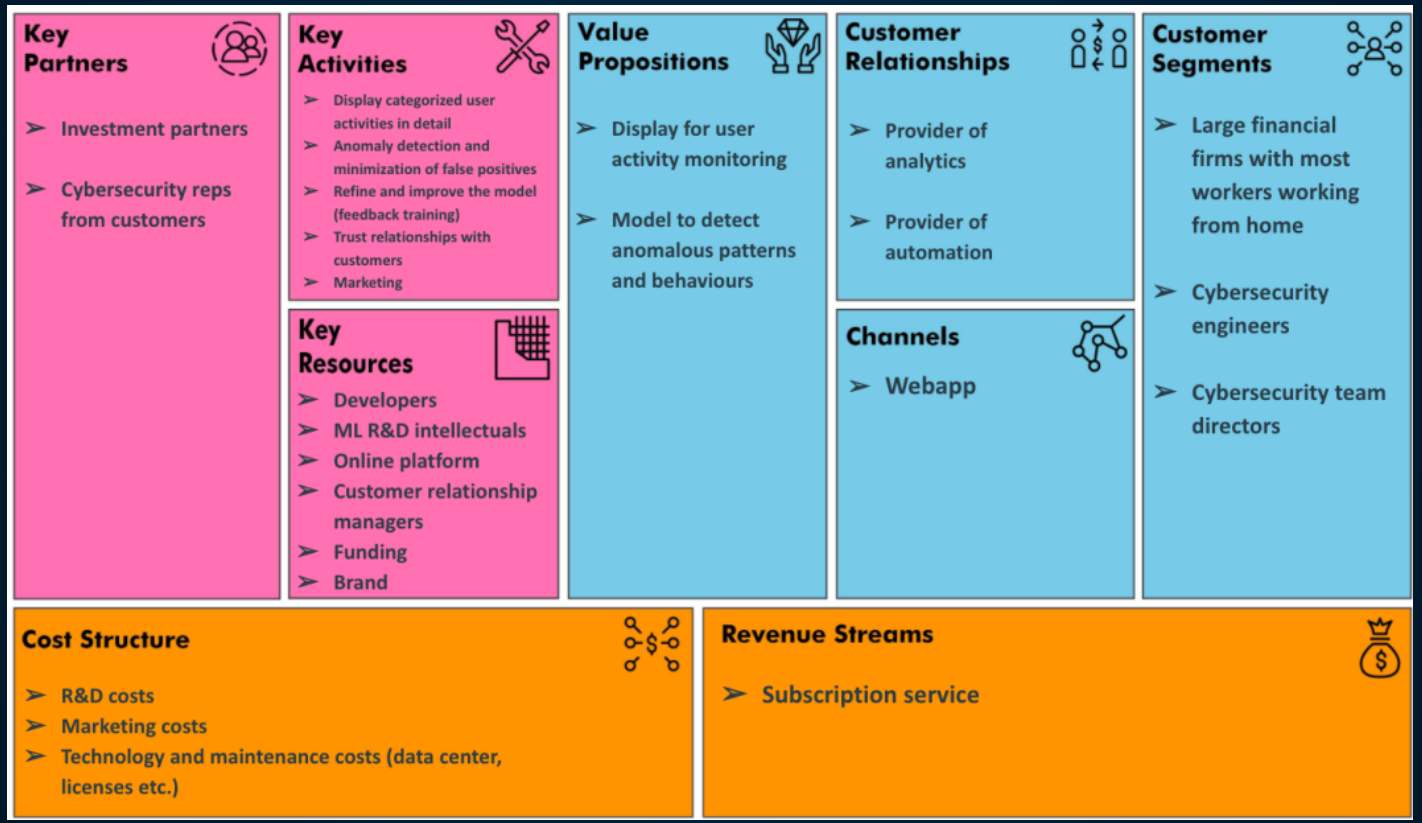
Infrastructure

- Data ingestion
- Data analysis
- Data representation

Financial model

- Free Trial
- Low pricing

# Business Model Canvas



# Technology

- Machine Learning

Insider threat detection: Where and how data science applies

Derek Lin

is chief data scientist at Exabeam, building data science-driven defence against cyberthreats. His research interests and experiences include anomaly detection, insider threat detection and behaviour analytics. Derek's prior machine learning works from Pivotal Software include the consultation and building of data science-based solutions for custom security use cases for large enterprises. Before Pivotal Software, Derek was with RSA Security developing analytic systems for risk-based online banking fraud detection, data loss prevention, voice-based biometrics security and speech and language processing. Derek holds numerous patents and publications in the areas of IT operations and security. He graduated with a Bachelor's and a Master's degree in electrical engineering from the University of Southern California.

Exabeam Inc., 3 Waters Park, #200, San Mateo, CA 94403, USA
Tel: (844)392-2326; E-mail: derek@exabeam.com

**Abstract** Insider threats are one of the top concerns of enterprise security. Traditional means of addressing general security threats, such as the use of signature matching and correlation rules, fall short when detecting insider threats. New possibilities for detecting insider threats have emerged as a result of the data-driven approach to security problems. Insider threat activities are multifaceted and require that security teams address the problem on multiple fronts. This paper introduces four areas where data science can be applied when building a system that detects threats. These four areas include the use of statistical analysis for anomaly detection, contextual information derivation for network intelligence, specific threat detection use cases, and meta learning for false positive control. Example use cases within each category are described, as well as how data science is used to approach them. The goal of this paper is to provide the general security audience with an overview of data science applications for insider threat detection.

KEYWORDS: insider threat, data science, machine learning, SIEM, user and entity behaviour analytics

**INTRODUCTION**

An insider threat is a threat to an organisation that comes from users who have access to the corporate network. The threat may be coming from external adversaries who have compromised internal user accounts to conduct illicit activities, or from legitimate employees and contractors who have accessed network resources with malicious intent, or even from employees who have used the network resources carelessly in ways result in compromised intellectual properties, leaked sensitive data and a tarnished company reputation.

While security policies, procedures and controls' are the essential first line of defence against insider threats, preventative measures do not detect threats. Conventional means of detection that rely on signatures do not apply, as insider activities have no factual signatures. The traditional use of correlation rules in security information and event

Machine learning based Insider Threat Modelling and Detection

Duc C. Le and A. Nur Zincir-Heywood

*Faculty of Computer Science, Dalhousie University, Halifax, Nova Scotia, Canada*



**Abstract**

Recently, malicious insider attacks represent one of the most damaging threats to companies and government agencies. This paper proposes a new framework in constructing a user-centered machine learning based insider threat detection system on multiple data granularity levels. System evaluations and analysis are performed not only on individual data instances but also on normal and malicious insiders, where insider scenario specific results and delay in detection are reported and discussed. Our results show that the machine learning based detection system can learn from limited ground truth and detect new malicious insiders with a high accuracy.

**Index Terms**

insider threat, cyber-security, machine learning

I. Introduction

Some of the most damaging security threats that companies and government agencies are facing is insider threat, where the malicious acts are performed by authorized personnel in the organizations. Recent reports show that 53% of organizations and 42% of U.S. federal agencies are suffering from insider threats every year [1], [2].

Insider threat related activities can be carried out both intentionally, such as information system sabotage, intellectual property theft and disclosure of classified information, as well as unintentionally, such as careless use of computing resources. One of the challenges of insider threat related research is that a malicious insider is authorized to access the organization's computer systems and has knowledge about the organization's security procedures. Moreover, in organizational environments, malicious insiders' activities may only make up a small portion of user activities in a wide range of domains that are recorded, from web and file access, to email history. Any proposed system for insider threat detection needs to overcome the challenges in learning from highly skewed data of heterogeneous sources in order to distinguish malicious activities from the legitimate ones, where all are from authorized users.

This research presents a system that focuses on user-centered analysis for insider threat detection. Proposed and evaluated on publicly available CERT dataset of corporate data for insider threat detection [3], our system seeks to learn from only a small number of normal / malicious insider actions for identifying threats in unknown data. In this context, we assume the point of view of cybersecurity analysts, where the amount of work is proportional not only to the amount of alerts but also to the number of users flagged, where a range of user's actions need to be taken into account for adequate decisions on alerts [4]. Hence system results are reported per user as well as per data point.

A novel embedding-based framework improving the User and Entity Behavior Analysis

Thomas Anglade [1] and Christophe Denis [2] and Thierry Berthier [3]

[1] Data Scientist, iTrust, tanglade@itrust.fr
[2] Sorbonne University, LIP6, Paris, France, christophe.denis@lip6.fr
[3] CREC Saint-Cyr & Université de Limoges, thier.berthier@orange.fr

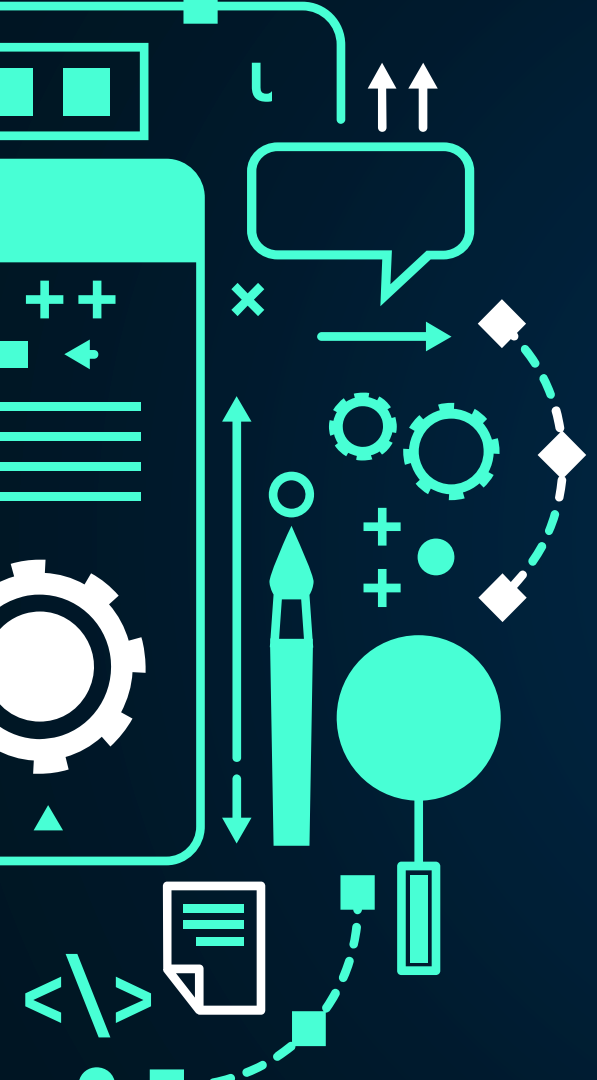
**Abstract.** Over the last few years, the number and the variety of cyber-attacks have been constantly growing. The landscape of cyber-attacks has become extremely large (DoS, DDoS, phishing, C&C, botnets, malwares, ransomwares, etc.). Today, UEBA (User and Entity Behavior Analysis[1]) is the best solution that companies need to use to adapt to these changes. Using UEBA, companies do not track security events or monitor devices; instead they track all the users and entities in the system. They use machine learning algorithms and statistical analyses to know when there is a deviation from established patterns.
This paper offers a novel embedding-based framework that facilitate UEBA by projecting sparse and unstructured log data into a new mathematical space in which numerous behavior trends and changes can be analyzed in a simpler and more visual way than using typical deep learning algorithms. We show that in this space, advanced cyber-attacks can be detected through a variation analysis of the fitted 2D-kernel density. The last part of the paper deals with the validation and the explanation of prediction obtained by black box Machine Learning methods. Indeed, the operational benefit of using Machine Learning methods is recognized but is hampered by the lack of understanding of their mechanisms, at the origin of operational, legal and ethical operational problems. This is largely dependent on the ability of engineers, decision-makers and users to understand the meaning and the properties of the results produced by these tools.

**Keywords:** cybersecurity, UEBA, Machine Learning, Explainable AI.

1 Introduction

Over the last few years, the number and the variety of cyber-attacks have been constantly growing [1]. The landscape of cyber-attacks has become extremely large (DoS, DDoS, phishing, C&C, botnets, malwares, ransomwares, etc.). In the same time, information systems have been quickly evolving IT perimeters used to be well-defined and they changed to become very porous and difficult to manage and oversee [2]. This is due to structural changes in the workplace, like remote work, BYOD, extensive use of leasing contracts for IT hardware, or even shared workplaces. As a result, it is now impossible to block all the cyber-attacks using old tools (web gateways, firewall, intrusion prevention tools, etc.). *Attackers will manage to penetrate the networks sooner or*

- Data Visualization



# THANK YOU

Questions?

# REFERENCES


Advantages and disadvantages of open source intelligence. (2017). Retrieved from https://expertsystem.com/advantages-disadvantages-open-source-intelligence/

Aruba Introspect Trial | Bridgeway. Retrieved from https://www.bridgeway.co.uk/aruba-introspect-trial

Azure Advanced Threat Protection | Microsoft 365. (2020). Retrieved from https://www.microsoft.com/en/microsoft-365/identity/advance-threat-protection

Belkasoft Offers Free Licenses to Evidence Center 2012 to Eligible Forensic and Educational Organizations. (2020). Retrieved from https://belkasoft.com/bec/en/free_evidence_center_for_le.asp#:~:text=Pricing%20and%20Availability&text=Pricing%20for%20Forensic%20IM%20Analyzer,edition%20is%20available%20from%20%249999.95.

Bennett, J., & Hopper, R. (2014). Automated and Manual Forensic Examinations. Encyclopedia Of Criminology And Criminal Justice, 100-108. doi: 10.1007/978-1-4614-5690-2_613

Burstein, D. (2012). Market Competition 101: The 3 types of competitors to keep an eye on | MarketingSherpa Blog. Retrieved 26 October 2020, from https://sherpablog.marketingsherpa.com/marketing/competition-types-to-watch/
Cortex XSOAR Community Edition. (2020). Retrieved from https://start.paloaltonetworks.com/sign-up-for-community-edition.html

Forensic Examination of Digital Evidence: A Guide for Law Enforcement (2020). Retrieved from https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Guercio, K. (2020). Best User and Entity Behavior Analytics (UEBA) Tools. Retrieved from https://www.esecurityplanet.com/products/top-ueba-vendors.html

Iqbal, S., & Abed Alharbi, S. (2020). Advancing Automation in Digital Forensic Investigations Using Machine Learning Forensics. *Digital Forensic Science*. doi: 10.5772/intechopen.90233

Magnet AXIOM Reviews and Pricing - 2020. (2020). Retrieved from https://www.capterra.com/p/149088/Magnet-IEF/

Top Digital Forensics Solution Companies. (2020). Retrieved from https://digital-forensics.enterprisesecuritymag.com/vendors/top-digital-forensics-solution-companies-2019.html

Snusbase Database Search Engine. (2020). Retrieved from https://snusbase.com/

Splunk Enterprise and Cloud | Pricing. (2020). Retrieved from https://www.splunk.com/en_us/software/pricing/enterprise-and-cloud.html