Detect Employee Fraud using Splunk

splunk> partner+

UnderDefense is Splunk partner and our team is holding the following Splunk certifications:

- Splunk Certified Consultant I
- Splunk Administrator
- Splunk Power User
- Splunk Sales engineer 1
- Splunk User
- Splunk Sales Rep 1
- Splunk Sales Rep 2
- Splunk Sales IT & App
- Splunk UBA User

UnderDefense is also a developer of Splunk apps and plugins like:

- App for Eset Remote Administrator | Splunkbase
- TA for Eset Remote Administrator | Splunkbase

TAERA APPERA

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Solution/Service Title	Fraud and Insider Threat Detection
Client Industry	Telecommunications
Client Overview	National-wide telecommunications company, provides communication services and data transmission based on a broad range of fixed and mobile technologies, including 3G and 4G (LTE). As of the year 2018, the largest mobile operator, as well as one of the largest internet providers of broadband access
Client Challenge	Implementing a process and actions that protect customers and enterprise information, assets, accounts and transactions through the real-time, near-real-time or batch analysis of activities by users and other defined entities.
Technologies	Splunk, Splunk DB Connect, Oracle DB, Splunk CIM
Key Benefits	Understand employee and entity behavior—and its context—is the key to determining fraud threats. In order to detect suspicious and fraud behavior.
Results	We created a continuously self-learning baseline of each worker, device, application, privileged account and shared service account, based on which it derives deviations from the normal.

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Client Info

Industry:

Telecommunication

Client overview:

One of the biggest National Telecommunications and Internet Technologies provider, established in early 1990. With a wide Service offering including fixed line and digital radio and satellite communications, as well as wideband Internet access, data transmission, and international transit of traffic.

Technical details:
600,000,000 - historical unstructured old data

2,000,000 events per day

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Clients info: problems encountered

Problem:
Given the nature of its service offering, national reach and large volume, high-profile customers, our client identified a problem it needed to solve in order to maintain and grow its business:

“ How can it provide assurance to its users regarding the controls it implements to protect the privacy and confidentiality of users’ data as well as the security, availability, and processing integrity of the systems that generate their customers ability to connect to a global world. ”

Use case:

Employee Fraud Detection

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Clients info: business challenges

Employees Fraud have an advantage—they are within an organization and have access to the environment. No perimeter defense or rules-based system can be effective in detecting, let alone preventing, their malicious activity.

As a result, fraud threats are amongst the hardest to catch and most successful in exfiltrating valuable corporate and customer data.

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Asset Misappropriation

Asset misappropriation fraud happens when people who are entrusted to manage the assets of an organisation steal from it.

Why Splunk?

Patterns of fraud are often found across different silos of both structured and unstructured data

Traditional anti-fraud tools can`t scale, give a narrow view that leaves gaps, struggle with flexibility around machine data

Splunk Enterprise helps with many needs of anti- fraud teams from anti-fraud and monitoring, investigations, analytics and reporting, to enhancing your existing fraud tools

Gain Insight into transaction and behavioral red flags over disjointed data sources

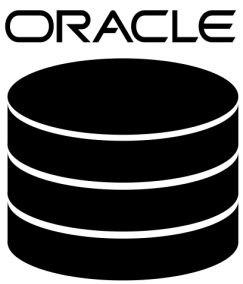
Flexibility to index relevant machine data across all data sources to search and correlate, making it easier to identify fraudulent patterns, so an organization can detect and alert on fraud in real time and act to prevent it before it adversely impacts the bottom line

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Start point

splunk>

ORACLE



Target:

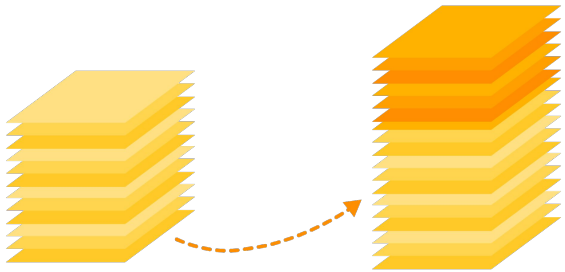
- Oracle DB
- “Some” logs
- 600 000 000 log lines
- Events About users(employees) activity

Goals:

- Connect (indexed data) to Splunk
- Basic charts

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Dataset



6 Fields:

1. USER
2. CLIENT
3. DATE (date of event)
4. ACTION
5. START DATE
6. END DATE

* Created

7. DURATION(END DATE- START DATE)

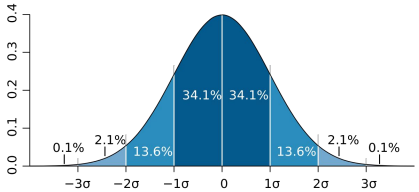
UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Correlation rules: create them without difficulties

1. Correlation/ Patterns

A and B and C not D = FRAUD

2. Anomalies/ outliners off baseline

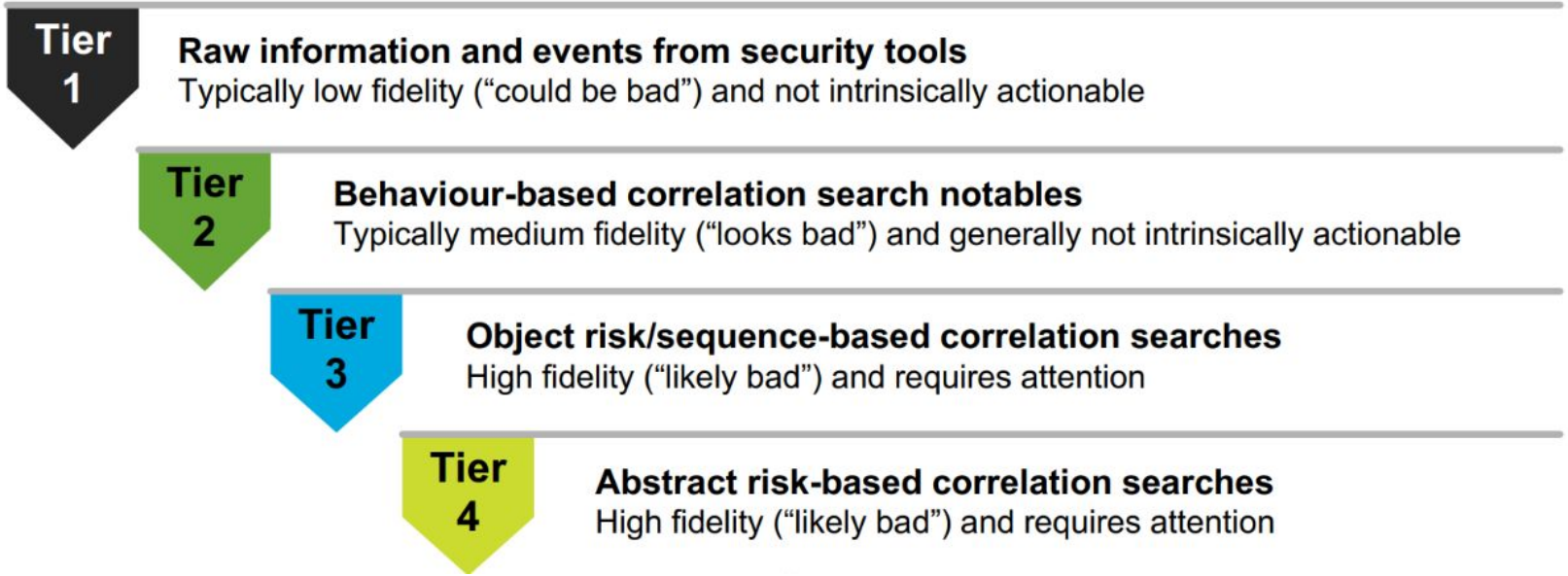


3. Risk Scoring

***Correlation with external feed of data in KV- Store for scale

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

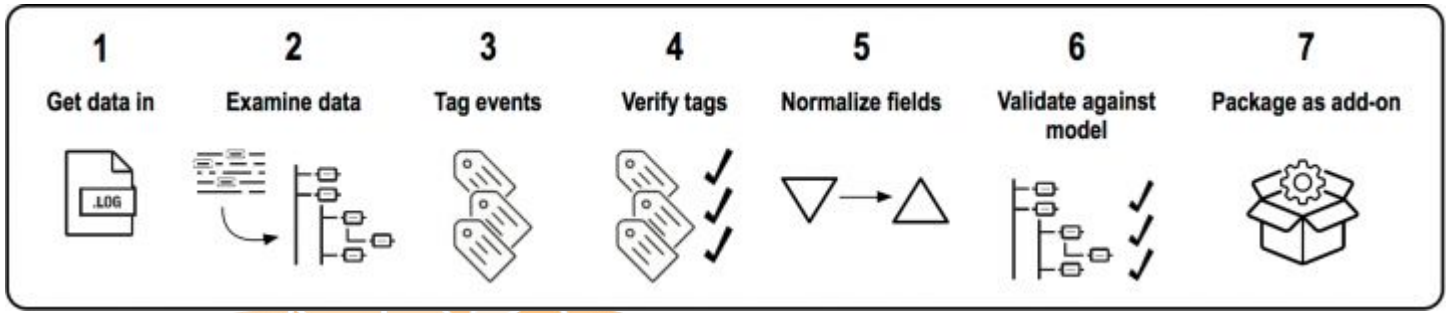
Process of data correlation



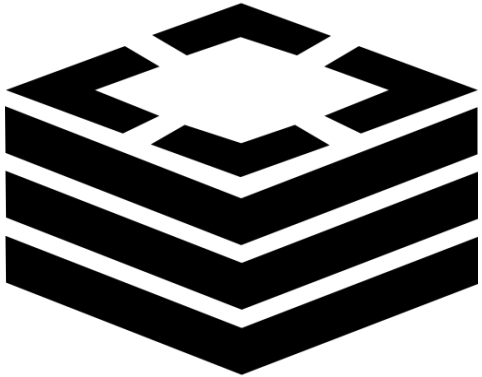
UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Data Wrangling

Data wrangling, sometimes referred to as data munging, is the process of transforming and mapping data from one "raw" data form into another format with the intent of making it more appropriate and valuable for a variety of downstream purposes such as analytics. A data wrangler is a person who performs these transformation operations.



Enrich your data



- 2 069 646 of “golden” clients
- Main target of Dishonest employees

Data Wrangling result

Default splunk fields:

- _time (extracted from date)
- host
- source
- sourcetype

Dataset from DB:

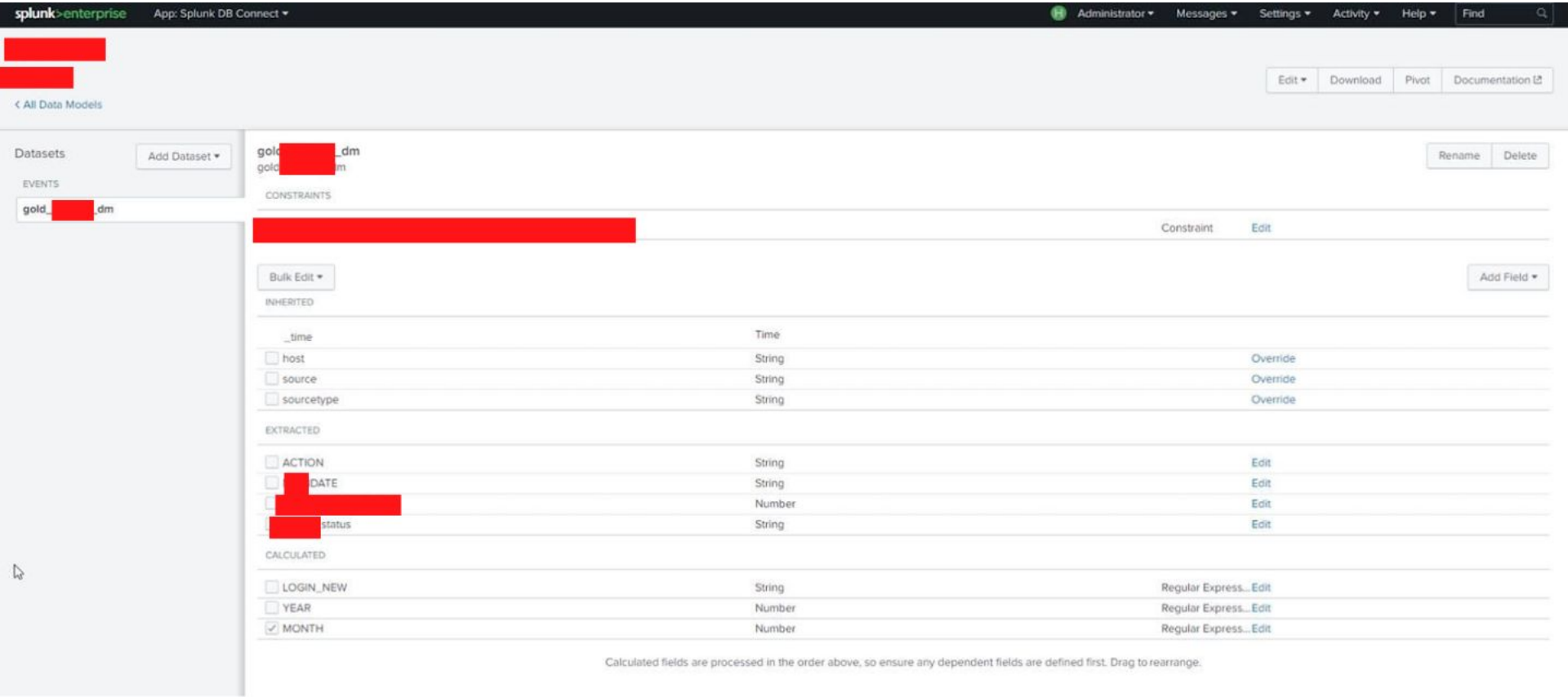
- action
- date
- client
- User
- End Date
- Start Date

Data Model:

- User_new (changed username in readable format)
- Year
- Month
- Client_status (Prem 1, Prem 2, Prem 3 ....)

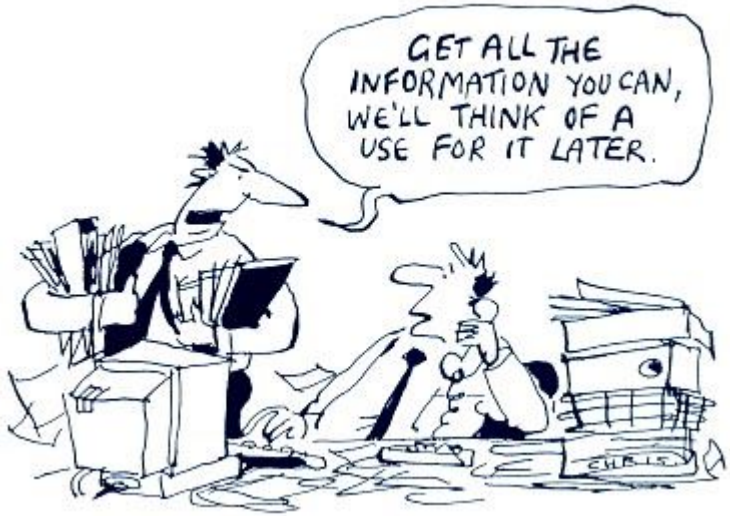
UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Data Model with Correlation of premium clients



Use Cases

- Golden Clients' Accounts Status monitoring
- Abnormal continuous clients monitoring by employees
- Clients' Actions history review



UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

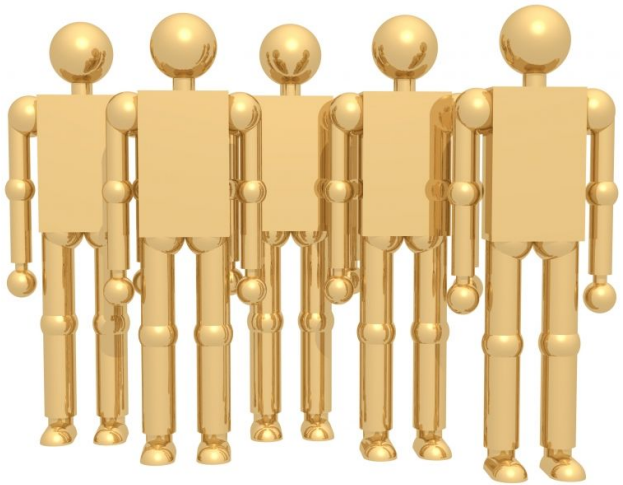
Clients' Actions History review

1. Analyse:
    - Statistical data for in total
    - Average values for weeks, months and total average values
2. Determine abnormal high activity
3. Filter the employee whose responsibility involves this actions
4. Correlate another events by employees who stay after the filtering

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Golden Clients' Accounts Status Monitoring

- Analyse :
  - Who reviews this accounts
  - How often
  - How many times in total
  - Which accounts
- Filter employees whose responsibility involves this activity
- Correlate another events by employees whose stay after filtering



The more clients pay, the more attractive they become to offenders and malices!

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Abnormal continuous clients' accounts monitoring by employees

1. Analyse:
    a. How many times an employee reviews the account in total:
        - During how many weeks with at least 1 event per week the employee monitors the account
        - During how many months with at least 1 event per month (or several weeks) employee monitors the account
        - Filter results more than the normal values
    b. Which accounts have been monitored
2. Determine abnormal high activity
3. Filter the employees whose responsibility involves this actions
4. Correlate with other contextual data

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Strategic recommendations

Conduct thorough background checks on each new employee

Implement checks and balances

Separate the functions of check preparer and check signer

Rotate duties of employees in accounts

Conduct random audits of company accounts

Implement an anonymous ethics hotline to encourage employees to report wrongdoing

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Business goals reached

Cost efficiency

Customer satisfaction

Data exploration

Automatization

- Reduced operating costs using Splunk
- Possibility to understand machine data and make it meaningful
- Detect and prevent insider threats and fraud
- Money saving

Thank you!

Call us now at +1 929 999 5101