Case study

UNDER DEFENSE

Threat & Fraud detection
How Splunk can catch and stop it

Version 2 www.version-2.com 二版

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

splunk> CERTIFIED ADMIN V.6
splunk> CERTIFIED ARCHITECT V.6
splunk> CERTIFIED KNOWLEDGE MANAGER V.6
splunk> CERTIFIED CONSULTANT I V.6
splunk> CERTIFIED SALES ENGINEER I V.6
splunk> CERTIFIED SALES REP I V.6
splunk> CERTIFIED SALES ENGINEER II V.6
splunk> CERTIFIED CONSULTANT II V.6

Project Background

Client

#1 National Telecommunications and Internet Technologies provider

Technical Challenge

Employee fraud is hard to detect as employees have an access to the company environment. No perimeter defense or rules-based system can be effective in detecting, let alone preventing, their malicious activity. With the help of Splunk we were able to monitor 600,000,000 historical unstructured old data and 2,000,000 events per day

Business Challenge

Provide assurance to telecom's clients on security and controls protecting the privacy and confidentiality of users' data. Processing integrity of the systems that generate their customers ability to connect to the global world

Team

SOC team

UNDER
DEFENSE

Problem detected: Asset misappropriation

Asset misappropriation fraud happens when people who are entrusted to manage the assets of an organisation steal from it. This use-case shows how employees of Telecom accessed data they had no obligation to use, spied on clients and exploited their Personal Information

We used Splunk as a tool to investigate the situation in order to detect deceivers and avoid company fraud

Splunk vs. Traditional anti-fraud tools

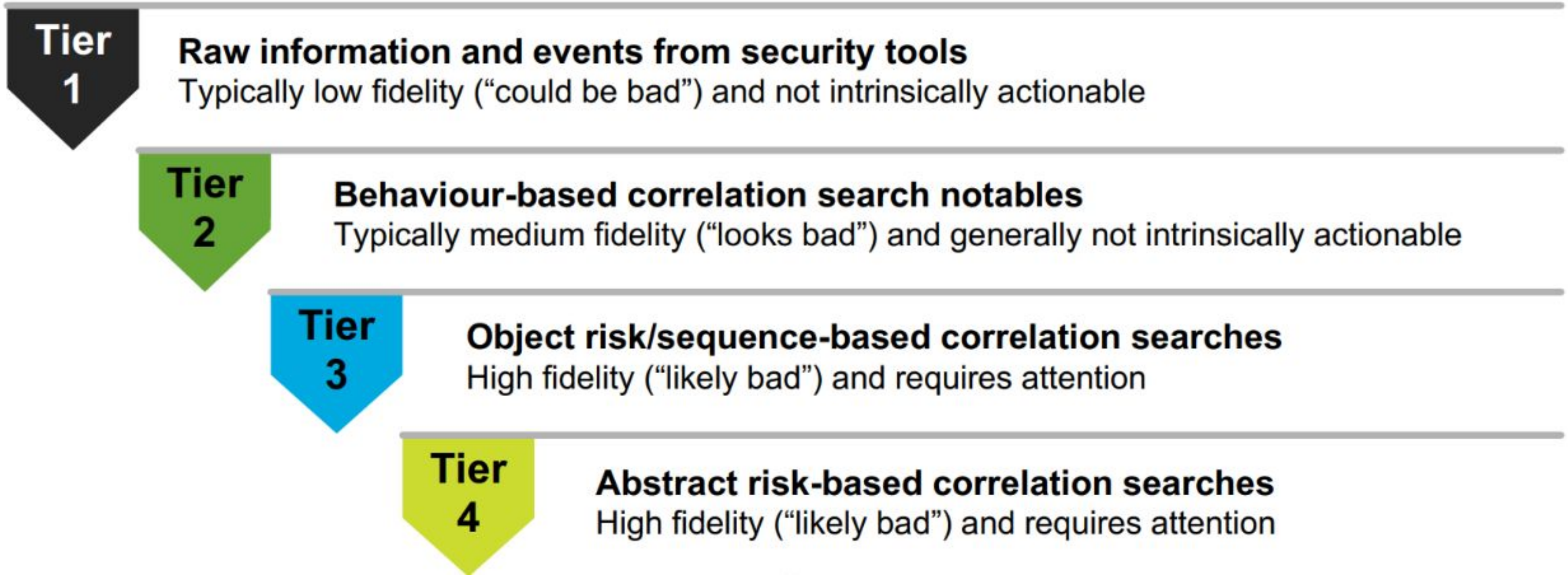
Splunk Enterprise:

1. has features of investigation, analytics and reporting to enhance your existing fraud tools
2. is flexible to index relevant machine data across all data sources
3. helps to identify fraudulent patterns in order **to alert on fraud in real time** and act to prevent it

Traditional anti-fraud tools:

1. aren’t able to scale and give a narrow view that leaves gaps
2. struggle with flexibility around machine data and large volumes of data
3. hardly correlate massive amounts of unstructured machine data

Process of data correlation with Splunk



Tier 1

Raw information and events from security tools
Typically low fidelity (“could be bad”) and not intrinsically actionable

Tier 2

Behaviour-based correlation search notables
Typically medium fidelity (“looks bad”) and generally not intrinsically actionable

Tier 3

Object risk/sequence-based correlation searches
High fidelity (“likely bad”) and requires attention

Tier 4

Abstract risk-based correlation searches
High fidelity (“likely bad”) and requires attention

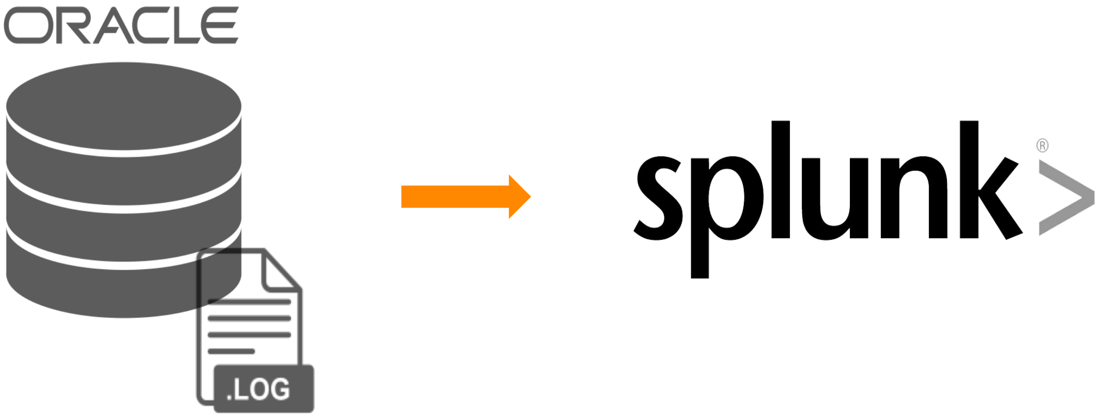
Inception point

Target:

- Oracle DB
- “Some” logs
- 600 000 000 events of users (employees) activity

Goals:

- Connect (indexed data) to Splunk
- Produce graphic analytics of data



Initial Data Fields for Analysis

Our analysts have used the following fields in the dataset to detect anomalies:

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

➕ Additionally we’ve created a customized field in Splunk to track the amount of time the user spends on a specific page in order to detect abnormal activities:

7. DURATION(END DATE- START DATE)

UNDER
DEFENSE

Writing correlation rules to detect fraud

1. Correlation/ Patterns

   (Ex. of a correlation rule: A and B and C not D = FRAUD)

2. Anomalies/outliners off baseline

3. Risk Scoring for users profiles

4. Data Enrichment with external information

Data enrichment process

Our client has defined their biggest asset -“VIP users”- as the main target for fraudsters. We suggested establishing a precise target monitoring on activities related to these accounts. The data enrichment process was essential to improve the data and add more value to them

As the client didn’t have the list of all possible unique user identifiers, that’s why we have created 2 069 646 of them according to predefined masks and tagged all the data with “regular”, and “VIP user” labels

tag: “regular users”

Example: NSJE-HND-ERU-GSTE

tag: “VIP user”

Example: XXXX-AAA-CCC-XXXX

Outcomes of Data Enrichment process

Default splunk fields:

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

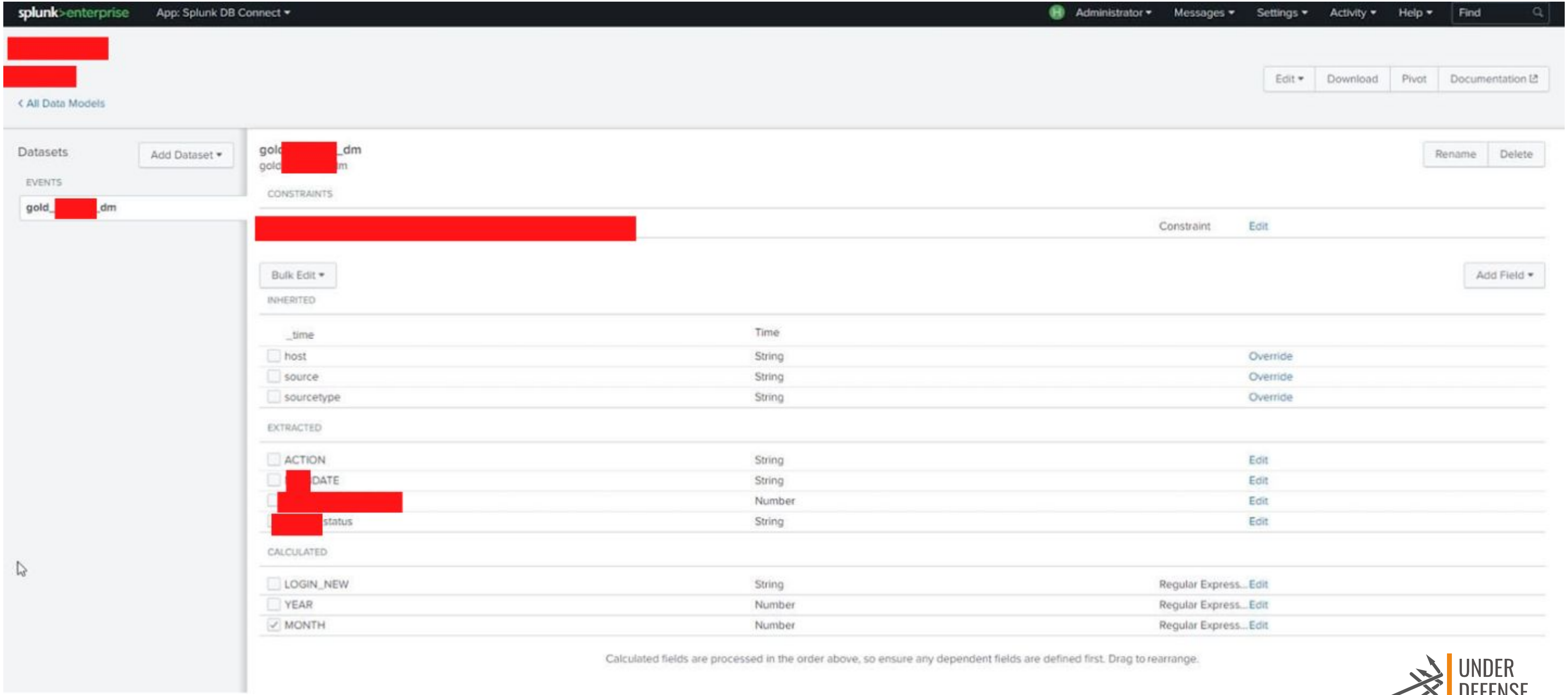
Clients dataset:

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

Enrichment:

- Client_status (Regular, VIP)

Project artifact: VIP Users Data Model



[redacted]

‹ All Data Models

EVENTS

gold_[redacted]_dm

gol[redacted]_dm
gol m

CONSTRAINTS

[redacted]	Constraint	Edit

INHERITED

	_time	Time	
□	host	String	Override
□	source	String	Override
□	sourcetype	String	Override

EXTRACTED

□	ACTION	String	Edit
□	[redacted]DATE	String	Edit
□	[redacted]	Number	Edit
□	[redacted]status	String	Edit

CALCULATED

□	LOGIN_NEW	String	Regular Express... Edit
□	YEAR	Number	Regular Express... Edit
☑	MONTH	Number	Regular Express... Edit

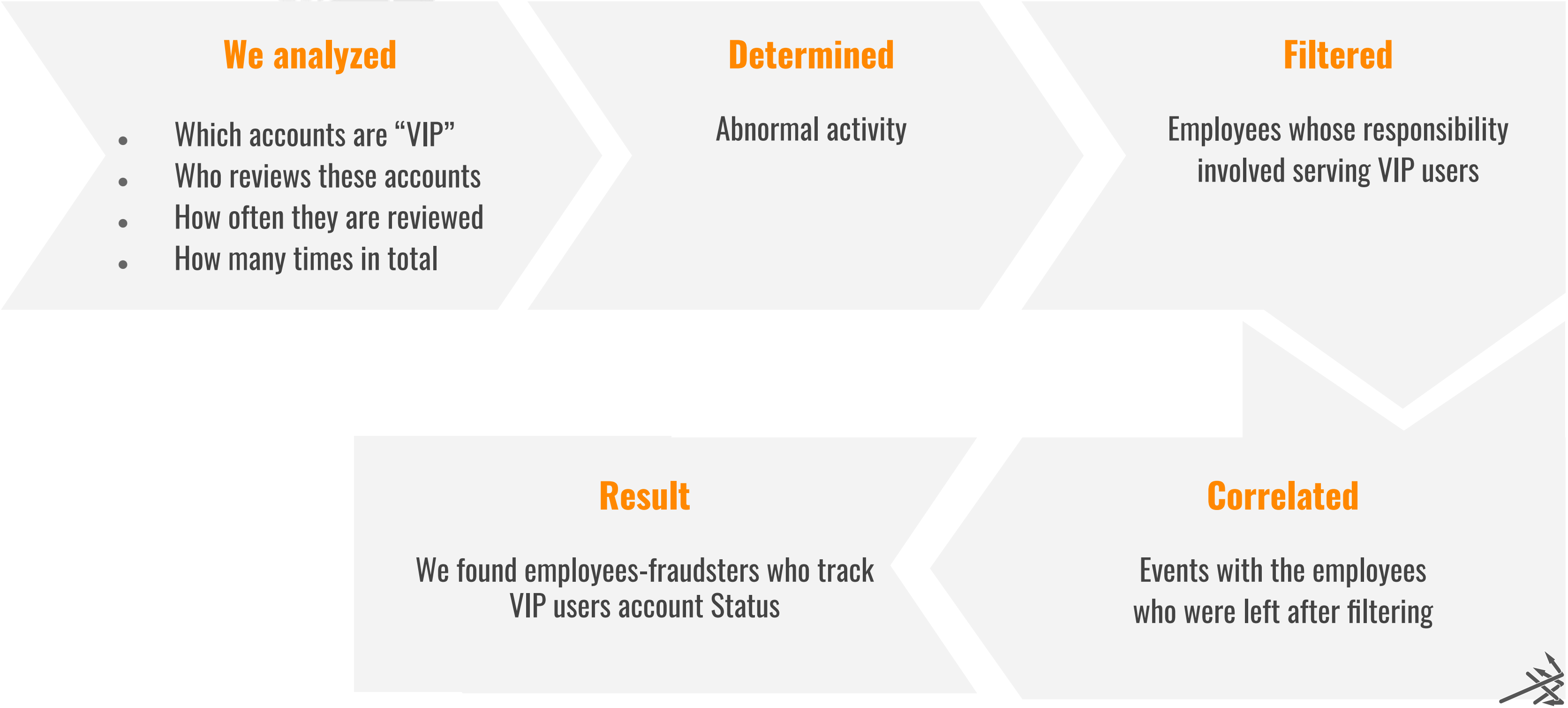
Calculated fields are processed in the order above, so ensure any dependent fields are defined first. Drag to rearrange.

Splunk monitoring - Use Cases

Detecting the employee-fraudsters who:

1. Track the Status of VIP User accounts
2. Suspiciously observe User accounts
3. Review the history of all Users' Actions

Use Case 1 - VIP Users’ Accounts Status Monitoring



We analyzed

- Which accounts are “VIP”
- Who reviews these accounts
- How often they are reviewed
- How many times in total

Determined

Abnormal activity

Filtered

Employees whose responsibility involved serving VIP users

Correlated

Events with the employees who were left after filtering

Result

We found employees-fraudsters who track VIP users account Status

Use Case 2 - Abnormal continuous users’ accounts monitoring

We analysed

How many times an employee reviews an account Status in total:

1. During how many weeks at least 1 event/week
2. During how many months at least 1 event/week (or several weeks)

Filtered

Results higher than the normal numbers

Analysed

Which accounts have been monitored by fraudsters

Determined

Abnormal high activity

Filtered

The employees whose responsibility involved this actions

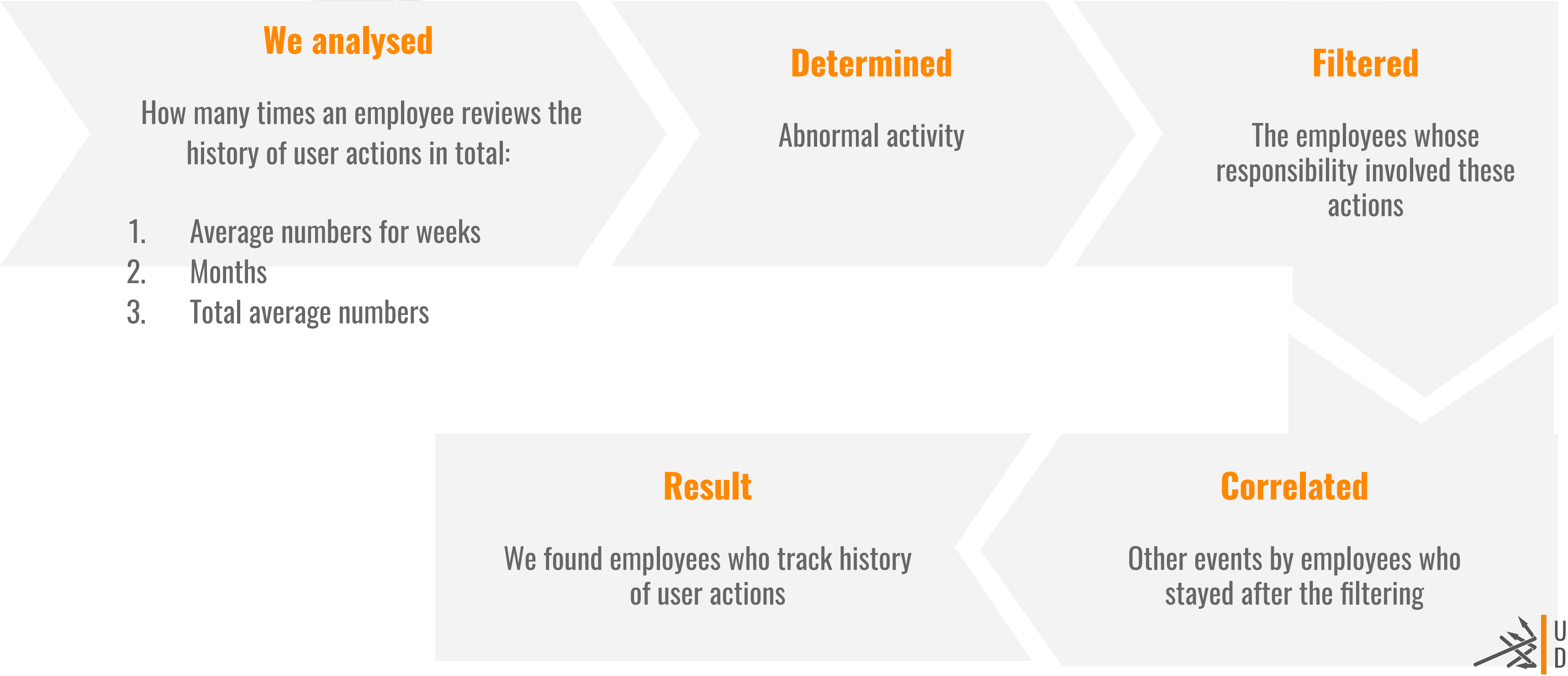
Correlated

With other contextual data

Result

We found employees-fraudsters who track activity of all users

Use Case 3 - Users' Actions History review



We analysed

How many times an employee reviews the history of user actions in total:

1. Average numbers for weeks
2. Months
3. Total average numbers

Determined

Abnormal activity

Filtered

The employees whose responsibility involved these actions

Correlated

Other events by employees who stayed after the filtering

Result

We found employees who track history of user actions

UNDER
DEFENSE

Strategic recommendations

To prevent possible relapse of fraud activities we've advised our client to:

- 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 reporting wrongdoing

UNDER
DEFENSE

Solution/Service Title	Fraud and Insider Threat Detection
Client Industry	Telecommunications
Client Overview	#1 Nationwide telecommunications company that provides communication and Internet services globally, and data transmission based on mobile technologies, including 3G and 4G (LTE)
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 to identify fraud threats and prevent fraud behavior in future. Around 300 fraudsters were quit as an outcome of asset misappropriation
Results	Detecting fraudulent activity with Splunk the company saved $1,08M in loses. Around 300 insider fraudsters were fired and corporate data leakage was prevented saving clients’ data and privacy.

UNDER
DEFENSE

Business goals reached

Insider Fraud detection

Money loss prevention

+

Data exploration

Automatization

- Detected internal fraud and dismissed 300 people
- Money saving around 1 080 000$ preventing repetition of the situation
- Reduced operating costs using Splunk
- Possibility to understand machine data and make it meaningful
- Detect and prevent insider threats and fraud

UNDER
DEFENSE

Thank you for your trust!

Version 2 二版
www.version-2.com
Hong Kong | Taiwan | Singapore | Macau | Mainland China

Hong Kong & Macau
Tel : (852) 2893 8860
Email : sales@version-2.com.hk

Taiwan
Tel : (886) 02 7722 6899
Email : sales@version-2.com.tw

Singapore, Malaysia & SEA
Tel : (65) 6296 4268
Email : sales@version-2.com.sg