How The God Particle will Help Securing Your Assets

Roger Bollhalder

Thomas Punz
Agenda

• Challenges
• Lessons Learned from LHC
• Big Picture
• Conclusion
Large Hadron Collider

CHALLENGES
Data Collection LHC

- The LHC is producing about a billion proton-proton collision events per second
- Only 100 to 200 carefully selected events per second can be captured
- “Use cases” define which data is required for analysis and analytics
- The big challenge is to create a rejection filter (trigger) which will remove about $10^7$ events and keep only the most important and relevant events
- With a typical event size of 1.5 MB this results in an annual data volume of approximately 10 PB
Data Collection IT Sec

• Amount of data is significantly smaller but all of it must be captured and logged (stored)

• Use cases define which data is required for monitoring

• Challenges are:
  – Smart selection of collectors so that they can collect all relevant data in good quality and that their restrictions are acceptable based on risk appetite
  – Sensible placement of collectors
  – Measure and ensure continuous coverage of collectors
  – Maintenance of collectors
Large Hadron Collider – IT Security

DATA ANALYSIS & ANALYTICS
The removal of false positives (good events) can result in missing true positive (bad events).

The acceptance is defined by the risk appetite of the company.
In this perfect example one has:

• No False Positive
• No Missed True Positive

• The separation of the good and bad events can be improved by adding an additional dimension.
Data Analysis Rules LHC

Signal (Bad Event)

Unknown Event

2 Leptons

Kinematic Properties

2 Neutrinos

Jet Veto

Higgs Candidate

Background (Good Event)

Event Fraction After Applied Cuts

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Signal (Bad Event)</th>
<th>Background (Good Event)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Leptons</td>
<td>21.0 %</td>
<td>17.0 %</td>
</tr>
<tr>
<td>Kinematic Properties</td>
<td>18.0 %</td>
<td>7.0 %</td>
</tr>
<tr>
<td>2 Neutrinos</td>
<td>8.0 %</td>
<td>0.1 %</td>
</tr>
<tr>
<td>Jet Veto</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1.24 pb

62.0 pb

IT Security

LESSONS LEARNED FROM LHC
Data Collection

• High data volume
  – SIEM (logging) infrastructure must be capable to store all received data as dumping irrelevant (for security monitoring) data is usually not an option

• Ensure completeness of data:
  – Know assets in scope (CMDB)
  – Alert (and react) if data streams should be interrupted ⇒ this might be done by operations monitoring or SIEM
  – Ensure data completeness and integrity

• Process data
  – Normalize data to make it understandable and ready for selection and further processing
  – Categorize events for better selection and more efficient analysis
Jan 01 01:00:01 tux kcheckpass[5603]: pam_unix(kdm:auth): authentication failure; logname=roger uid=1000 euid=1000 tty=:0 ruser= rhost= user=roger

Server: tux
Time: 2015/01/02 01:00:01 (UTC)
User: roger
Message: kcheckpass[5603]: pam_unix(kdm:auth): authentication failure; logname=roger uid=1000 euid=1000 tty=:0 ruser= rhost= user=roger

Category 1: Authentication
Category 2: Fail
Category n: Linux, Ubuntu, Kubuntu, 14.04, KDE, PAM, …
Monitoring Rules

Unix
- Unix Rule: Failed Login
  - Unix Alert: Failed Login
- Unix Rule: Concurrent Login
  - Unix Alert: Concurrent Login

Windows
- Windows Rule: Failed Login
  - Windows Alert: Failed Login
- Windows Rule: Concurrent Login
  - Windows Alert: Concurrent Login
Monitoring Rules

Filter: Internet Facing

Filter: Authentication

Filter: Failed

Rule: Failed Login

Alert: Failed Login

Unix

Windows

Rule: Concurrent Login

Alert: Concurrent Login

Unix

Windows
Analysis IT Security

• The LHC approach to minimize both false positives and false negatives can work for IT Security

• One way is to enhance the added value of the SIEM by further enriching data:
  – Include further (not so readily available) reference data like workflow or ticketing systems
    • Is the employee using root access based on a valid incident ticket or as part of a planned change?
  – Map information from external sources like vulnerability information (external feeds or collected by other tools like compliance checking)
    • Is the targeted system vulnerable for this specific attack?
  – Calculate and store trending information to identify unusual behavior
    • Is a person downloading or accessing sensitive data to an extent not common for her or her peers?
Another way to improve efficiency of the SIEM is to let SOC L2 and L3 (Analytics team) use and analyze, ‘slice and dice’ the enriched data.

This will allow identification of threats not easily detectable near real-time (e.g. APT or advanced scenarios).

Lessons learned will be incorporated into the real-time alerting rules and improve effectivity and efficiency of the SIEM as a whole.
Accountability

• Define accountabilities but allow space for excellence:
  – Separate the analytics team from SOC
  – Make analytics team accountable for the real-time alerting rules
  – Let analytics perform quality assurance controls over incident handling by SOC L1 and L2
  – Make sure the team is skilled and can allocate time to tasks they consider important
Large Hadron Collider – IT Security

BIG PICTURE
Big Picture LHC
Big Picture IT Security

Threat Model

Alerts

SOC

Real Time Monitoring

Historic Monitoring

Analytics

All Logs

Collection

Collected Logs

Processing & Enrichment

Processed & Enriched Logs

Real Time Processing

Offline Processing

2015/11/11
Conclusion

• Experimental particle physics and IT security have more in common as one would think at first glance
• Well established and understood methods used at the LHC can be adapted for IT security and help us doing our job better and more efficient
• Added value of a SIEM implementation requires sustainable and efficient implementation of:
  • the technical implementation
  • threat and security event management
• It’s sensible to start with high-risk infrastructure and only iteratively expand as soon as one stage of expansion was successfully and sustainably completed