PROMIS

Professional Master in Information Security
Online Courses for Professionals in Security

BLEKINGE INSTITUTE OF TECHNOLOGY

"Using SIEM for Anomaly Detection" –
By Volodymyr Tkach

Upcoming Security Seminars and Events
Send an email to **Nina Wennberg** **niw@bth.se** to subscribe to our mailing list and stay up to date for PROMIS talks and events!

PRO.M.IS
security built in

Visit PROMIS promisedu.se

PROMIS

Senior Lecturer here at DIDA, BTH
Associate Professor at Igor Sikorsky Kyiv Polytechnic Institute (Ukraine), Department of Cybersecurity
Senior Project Manager at EBRD & Advisor to the Cybersecurity Department of the National Bank of Ukraine
More than 15 years in education
Over 8 years in cybersecurity

BLEKINGE INSTITUTE OF TECHNOLOGY

I teach in these courses :

Machine Learning and Security 6 credits

Data-Driven Security 3 credits

Introduction to Secure Software Development 7,5 credits

PRO.M.IS
security built in

agenda

- What is SIEM?
- How to choose the right one
- SPL and its magic
- Anomaly detection DEMO
- IDS/IPS vs ADS/SIEM
- Upcoming PROMIS courses

What is SIEM?

Security **I**nformation and **E**vents **M**anagement

SIEM = SIM + SEM

Security Information Management

Security Event Management

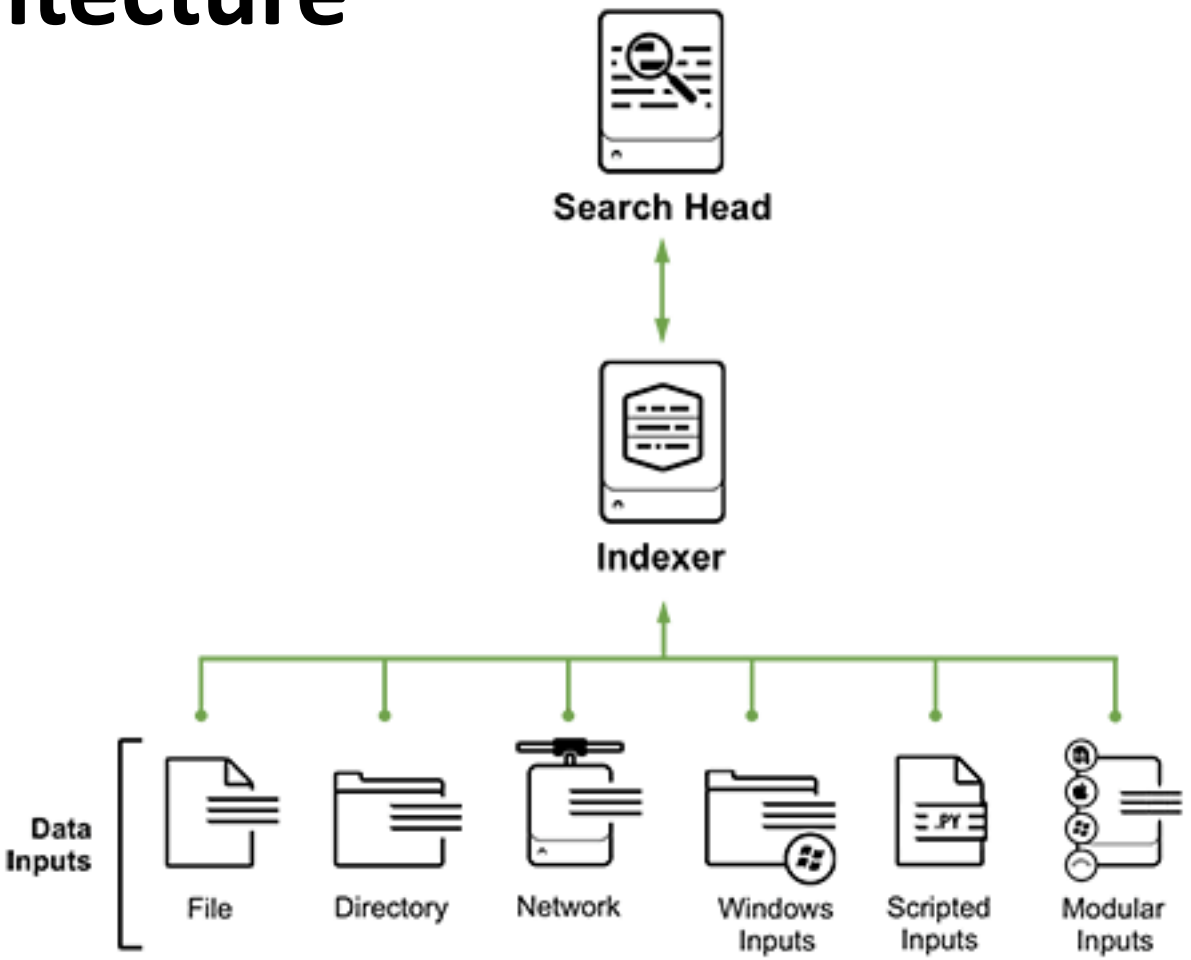
Security Information Management (SIM) - retrieves and analyses log data and generates a report

Security Event Management (SEM) - carries out analysis of event and log data in real-time to provide event correlation, threat monitoring an incident response

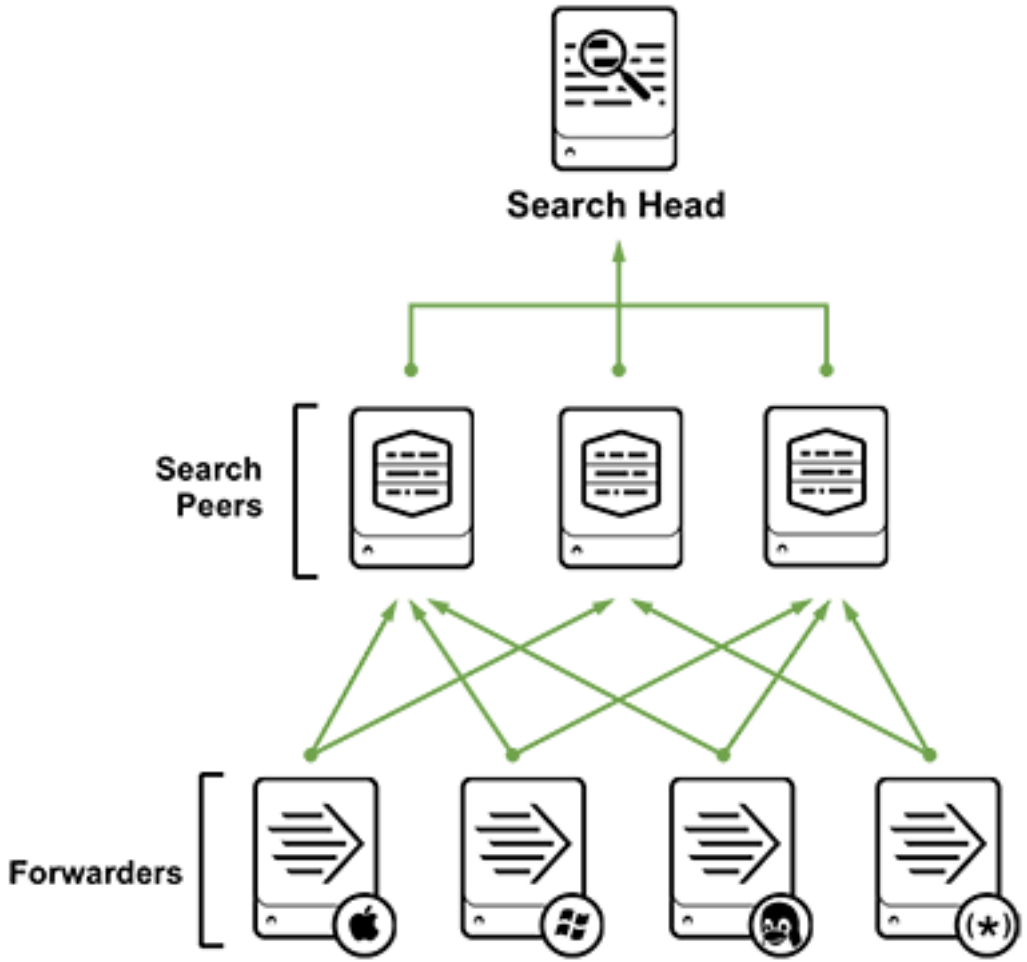
How to choose the right one

- Price (normally using any cybersecurity tool is a matter of investments)
- Functionality
- Flexibility
- Scalability
- Maintenance and Support
- Other

SPLUNK :: Sample Architecture



SPLUNK :: Real one



SPLUNK :: SPL Search Processing Language

- 140+ search commands
- Syntax similar to Unix pipeline and SQL (structured query language used in database management) and optimized for timestamped data
- SPL allows you to search, filter, modify, enrich, combine and remove
- SPL includes machine learning and anomaly detection functionality

SPLUNK :: SPL Search Processing Language

search and filter | munge | report | cleanup

```
suorcetype=access*
| eval KB=bytes/1024
| stats sum(KB) dc(clientip)
| rename sum(KB) AS «Total KB» dc(clientip) AS «Unique Clients»
```

pictures are taken from https://habr.com/ru/company/tssolution/blog/324136/

SPLUNK :: SPL Search Processing Language

```
index="INDEXNAME" sourcetype="access*"
| eval _time=strptime (StartTime,"%b %d, %Y, %H:%M:%S %p")
| timechart span=20s count(host) as "requests", dc (SourceIP) as "size"
| where requests > 0
| eval k = round(requests/size,3)
| head 1000
| streamstats window=100 current=true median(k) as median
| eval absDev = (abs(k-median))
| streamstats window=100 current=true median(absDev) as medianAbsDev
| eval lowerBound = (median-median), upperBound=(median + medianAbsDev*exact(5))
| eval isOutlier= if(k < lowerBound OR k > upperBound, 1, 0)
| table _time, k, lowerBound, upperBound
```

pictures are taken from https://habr.com/ru/company/tssolution/blog/324136/

Anomaly detection

- brief reminder on what anomaly is

deviation from the normal or usual order, type, etc.; irregularity (BRITISH DICTIONARY SAYS…)

deviation from the normal or **EXPECTED** order, type or **BEHAVIOR**; irregularity of any kind (WE SAY…)

ANOMALY of STATE vs **ANOMALY in BEHAVIOR**

Essential features for ADS

- Anomaly Detection
- Real-time Alerts
- Dashboards
- Integration

Anomaly detection

DEMO

Upcoming Courses

BLEKINGE INSTITUTE OF TECHNOLOGY

Application Open for Autumn 2022 Courses – visit promisedu.se

[Development Security Applications (DevSecOps) 7,5 credits]

[Security Inventory for Software Development 3 credits]

[Applied Cryptography 5 credits]

[Security for Critical Infrastructure (Operational Technology) 7,5 credits]

[Web System Security, 7,5 credits]

All courses are:
- Designed for professionals
- Given Online and flexible
- App 25% Study Pace
- Free of charge, University credits

Questions about Application?

Contact Nina Wennberg niw@bth.se or Anna Eriksson aes@bth.se

PRO.M.IS
security built in


AXIS
COMMUNICATIONS


advenica


addalot


factor10


IBM


SWEDSOFT


BALLOU


Handelsbanken


Nordea


sast
SWEDISH ASSOCIATION FOR SOFTWARE TESTING


BILSweden


DXC.technology


Orange Cyberdefense


TRUESEC


BorgWarner


CYBERCOM
GROUP


BLEKINGE TEKNISKA HÖGSKOLA
BTH

Polisen


ERICSSON


FKG

MaxKompetens


citynetwork


telenor


2Secure

Thank you!


SAAB
TECHNOLOGIES
SAAB

IT&Telekomföretagen


IKEA


SIREN
Swedish Requirements Engineering Research Network


TOLPAGORNI
product management


Knowledge Foundation


PRO.M.IS
security built in