Anomalous Behavior Detection

Anomaly detection techniques and tools

PRO.M.IS
security built in

Professional Master in Information Security

Dr. Volodymyr Tkach
volodymyr.tkach@bth.se

introduction

Dr. Volodymyr Tkach
volodymyr.tkach@bth.se

- Senior Lecturer here at BTH (within PROMIS project)
- 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
- Fields of interest:
  - Data-Driven Security
  - Anomaly detection
  - Behavioral Analysis
  - Machine Learning

agenda

- Behavior analysis
- Anomaly definition and samples
- Anomaly detection (pattern based vs non-pattern based)
- Tools, methods
- Conclusions & some tricks

- PROMIS general information
- Courses
- How to apply

behavior analysis

Anomalous Behavior Detection

behavior analysis

Anomalous Behavior Detection

Cambridge Dictionary

the way that a person, an animal, a substance, etc. behaves in a particular situation or under particular conditions

to show particular behavior in a particular situation or under particular conditions

behavior analysis

Anomalous Behavior Detection

WIKIPEDIA
The Free Encyclopedia

Behavior is the range of actions and mannerisms made by individuals, organisms, systems or artificial entities in conjunction with themselves or their environment…

behavior analysis

Anomalous Behavior Detection

- Can be observed and measured
- Changing over time
- May be represented as vector of state in time
- Vector components can have either numerical or categorical values
- For most of categorical values we can find their numerical representations*
- **Simplest way to start learning behavior is one-dimensional time series**

123.123.123.123 - jsmith [17/Dec/2016:18:55:05 +0800] "**GET /index.html HTTP/1.0**" **200** 2046 "http://referer.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.17.3) AppleWebKit/536.27.14 (KHTML, like Gecko) Chrome/55.0.2734.24 Safari/536.27.14"

behavior analysis

5W + H

- What?
- Where?
- When?
- Who?
- Why?
- How?

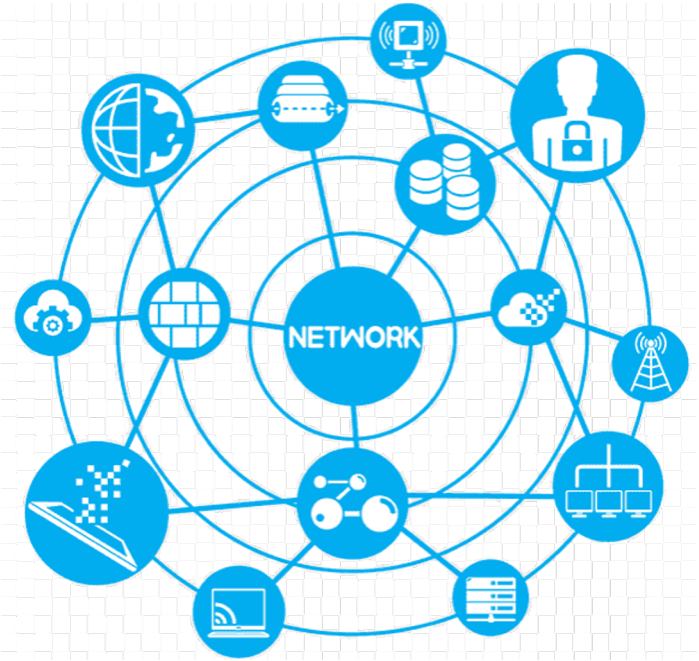
behavior analysis

UBA

User Behavior Analysis is basically a permanent analysis of user behavior that is normally related to the User inside of some specific system, e.g. Operation System, CRM, specific Application etc.

NBA

Network Behavior Analysis (NBA), also known as "**Behavior Monitoring**" is the collection and analysis of internal network data to identify malicious or unusual activity. Behavioral monitoring tools analyse information from a wide range of sources and use machine learning to identify patterns that could suggest an attack is taking place. Network analysis tools provide valuable insight to help businesses defend against the latest cyber threats.



anomaly

Anomalous Behavior Detection

Cambridge Dictionary

anomaly

a person or thing that is different from what is usual, or not in agreement with something else and therefore not satisfactory

anomaly

Anomalous Behavior Detection

WIKIPEDIA
The Free Encyclopedia

Anomaly

From Wikipedia, the free encyclopedia

Not to be confused with Abnormality (behavior).

Anomaly may refer to:

Science [edit]

Natural [edit]

- Anomaly (natural sciences)
  - Atmospheric anomaly
  - Geophysical anomaly

Medical [edit]

- Congenital anomaly (birth defect), a disorder present at birth
  - Physical anomaly, a deformation of an anatomical structure
    - Congenital vertebral anomaly, any of several malformations of the spine
  - Collie eye anomaly, eye disease of dogs
    - Coronary artery anomaly, a congenital abnormality in the heart
    - Ebstein's anomaly, a congenital heart defect in which the opening of the tricuspid valve is displaced
    - Uhl anomaly, a congenital heart disease affecting the myocardial muscle
    - Vaginal anomalies

Biology [edit]

See also: List of congenital disorders and List of genetic disorders

- Anomalous, a species of moth in the Noctuid family
- Chromosome anomaly, a disorder caused by a structural error in a chromosome or an atypical number of chromosomes
- Genetic anomaly, a disorder caused by mutation
- Teratology, the study of developmental anomalies

Physics [edit]

- Anomalous diffusion is the movement of molecules from a region of lower concentration to a region of higher concentration
- Anomalous dispersion (optics), when the speed of an electromagnetic wave increases with increasing frequency
- Anomalon, a hypothetical type of nuclear matter that shows an anomalously large reactive cross section
- Anomaly (physics), a failure of a symmetry of a theory's classical action
- Conformal anomaly, a quantum phenomenon that breaks the conformal symmetry of the classical theory
- Chiral anomaly, an anomalous nonconservation of a chiral current
- Gauge anomaly, the effect of quantum mechanics that invalidates the gauge symmetry of a quantum field theory
- Global anomaly, an anomaly in quantum physics
- Gravitational anomaly, an effect in quantum mechanics that invalidates the general covariance of some theories of general relativity
- Konishi anomaly, the violation of the conservation of the Noether current associated with certain transformations
- Mixed anomaly, an effect in quantum mechanics
- Parity anomaly, an anomaly associated with parity

anomaly

Anomalous Behavior Detection

WIKIPEDIA
The Free Encyclopedia

Anomaly

From Wikipedia, the free encyclopedia

Not to be confused with Abnormality (behavior).

Anomaly may refer to:

Science [edit]

Natural [edit]

- Anomaly (natural sciences)
  - Atmospheric anomaly
  - Geophysical anomaly

Medical [edit]

- Congenital anomaly (birth defect), a disorder present at birth
  - Physical anomaly, a deformation of an anatomical structure
    - Congenital vertebral anomaly, any of several malformations of the spine
  - Collie eye anomaly, eye disease of dogs
    - Coronary artery anomaly, a congenital abnormality in the heart
    - Ebstein's anomaly, a congenital heart defect in which the opening of the tricuspid valve is displaced
    - Uhl anomaly, a congenital heart disease affecting the myocardial muscle
    - Vaginal anomalies

Biology [edit]

See also: List of congenital disorders and List of genetic disorders

- Anomalous, a species of moth in the Noctuid family
- Chromosome anomaly, a disorder caused by a structural error in a chromosome or an atypical number of chromosomes
- Genetic anomaly, a disorder caused by mutation
- Teratology, the study of developmental anomalies

a **significant deviation** from **expected** value

anomaly

Anomalous Behavior Detection

normally?

anomaly

Anomalous Behavior Detection

normally

abnormally (anomaly)!

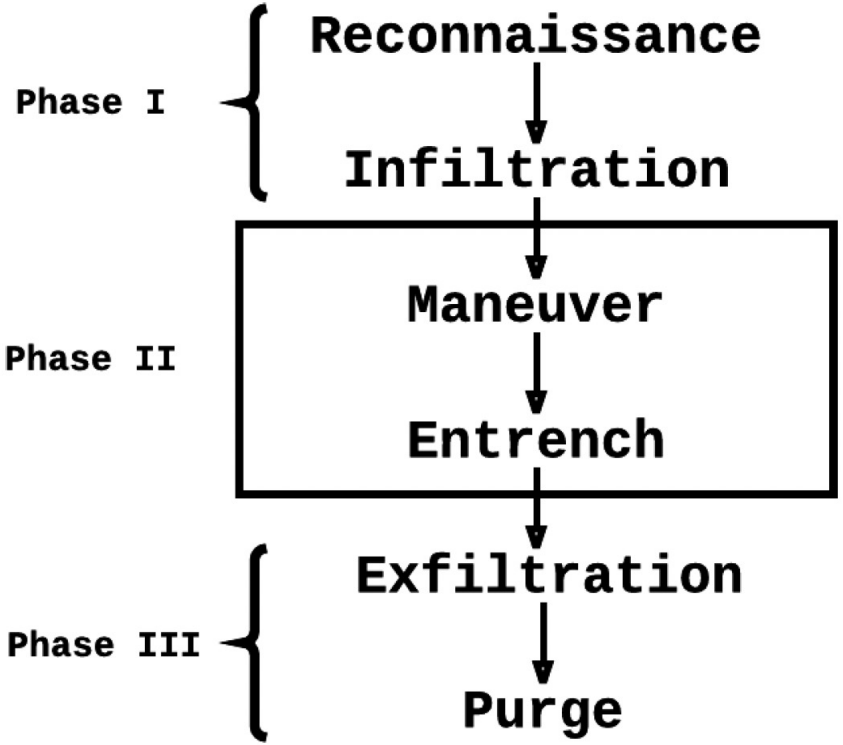
anomaly detection

Anomalous Behavior Detection

anomaly detection

Main stages:

- Preparation (generates anomalies)
- Execution (generates anomalies)
- Covering up the tracks (generates anomalies)

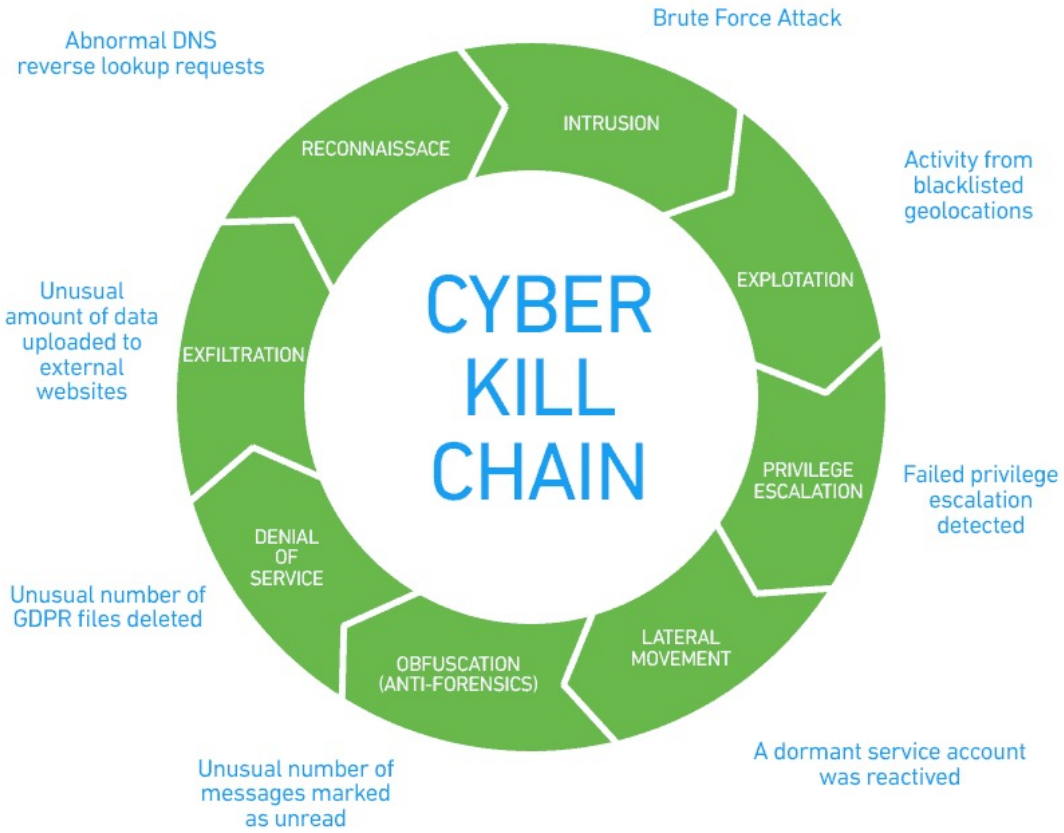


anomaly detection

anomaly may be found on the every single stage of cyber kill chain

anomaly is not something you may immediately understand looking at some small piece of data or a very narrow time range

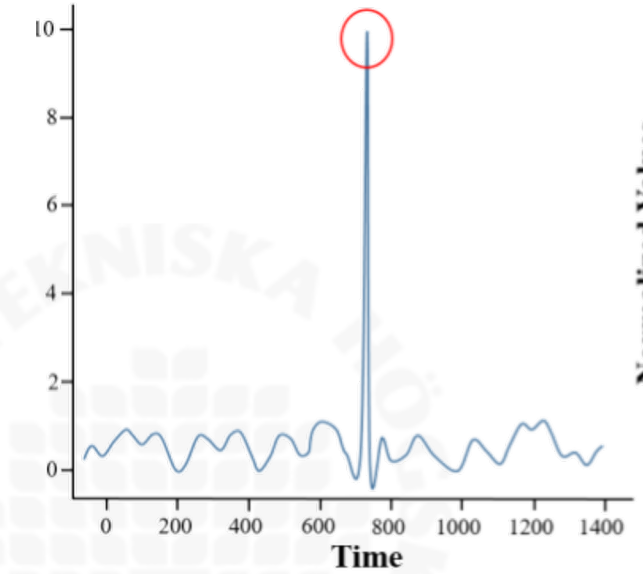
to detect anomaly you have to monitor the system state including its behavior as actions and as re-actions (response)

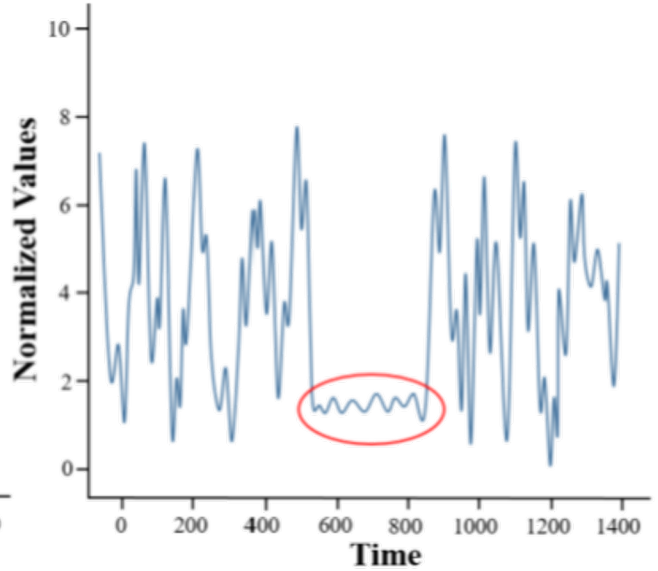


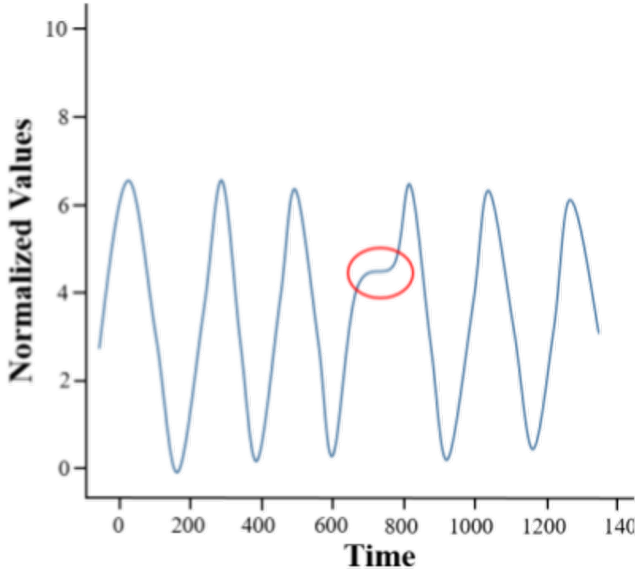
anomaly detection

time-series anomaly types:

- point (outlier)
- contextual
- collective

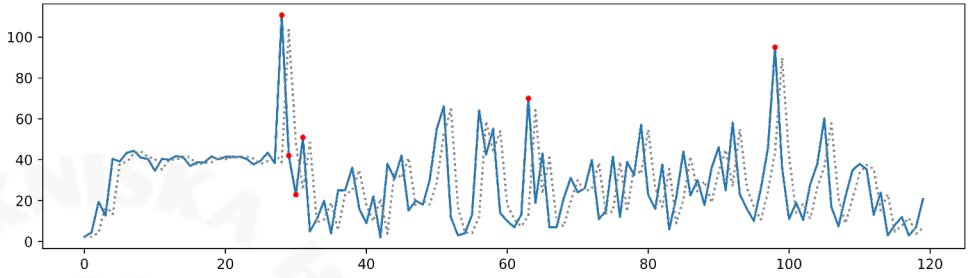


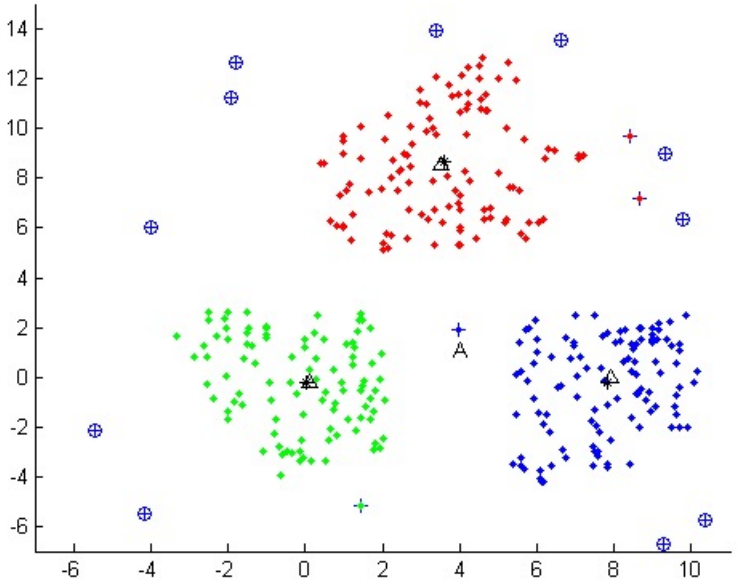




anomaly detection

- static anomaly (density based, mainly used to understand whether the value belongs to particular cluster)
- dynamic anomaly (time-value based)





anomaly detection

123.123.123.123 - jsmith [17/Dec/2016:18:55:05 +0800] "**GET /index.html HTTP/1.0**" **200** 2046 "http://referer.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.17.3) AppleWebKit/536.27.14 (KHTML, like Gecko) Chrome/55.0.2734.24 Safari/536.27.14"

data:

- Request IP (categorical)
- Username (categorical)
- HTTP-referrer (string)
- HTTP request (string)
- User-Agent (string)
- HTTP-response (categorical)
- Bytes sent
- etc.

NCSA Common log format

anomaly detection

123.123.123.123 - jsmith [17/Dec/2016:18:55:05 +0800] "**GET /index.html HTTP/1.0**" **200** 2046 "http://referer.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.17.3) AppleWebKit/536.27.14 (KHTML, like Gecko) Chrome/55.0.2734.24 Safari/536.27.14"

data:

- Request IP (categorical)
- Username (categorical)
- HTTP-referrer (string)
- HTTP request (string)
- User-Agent (string)
- HTTP-response (categorical)
- Bytes sent
- etc.

information (extracted):

- average requests amount from this IP per time range (numerical)
- average amount of requests from this user (numerical)
- HTTP-referrer string length (numerical)
- HTTP request string length (numerical)
- HTTP request parameters amount (numerical)
- etc.

anomaly detection

123.123.123.123 - jsmith [17/Dec/2016:18:55:05 +0800] "**GET /index.html HTTP/1.0**" **200** 2046 "http://referer.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.17.3) AppleWebKit/536.27.14 (KHTML, like Gecko) Chrome/55.0.2734.24 Safari/536.27.14"

data:

- Request IP (categorical)
- Username (categorical)
- HTTP-referrer (string)
- HTTP request (string)
- User-Agent (string)
- HTTP-response (categorical)
- Bytes sent
- etc.

information (extracted):

- average requests from this IP per time range (numerical)
- average amount of requests from this user (numerical)
- HTTP-referrer string length (numerical)
- HTTP request string length (numerical)
- HTTP request parameters amount (numerical)
- etc.

Normalization is normal!

methods

outliers detection:

statistical method (standard deviations)
machine learning (supervised, unsupervised)
artificial neural networks
prediction-based models

context anomaly detection:

machine learning
artificial neural networks
prediction-based models

collective anomalies:

machine learning
artificial neural networks
prediction-based models

tools

Essential features for ADS

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

Numenta, AVORA, **Splunk Enterprise**, **Loom Systems**, **Elastic X-Pack**, Anodot, Crunch Metrics

are some of the Top* Anomaly Detection Software

Also, take a look into **Sentinel One** and **Darktrace**

* **https://www.predictiveanalyticstoday.com/top-anomaly-detection-software/**

conclusions & tricks

Behavior is actions and re-action we can measure and expect
Behavior is always put into context
Anomaly is the behavior we do not expect
Anomaly can be found by patterns of behavior expectations (more precise, less alerts)
Anomaly can be found pattern-less (more alerts but more FP)
Anomaly may exist even you're not aware of it, so keep watching and extend your monitoring area (normalization is normal)

Anomalous Behavior Detection

Anomaly detection techniques and tools

PRO.M.IS
security built in

Professional Master in Information Security

Any questions?

Dr. Volodymyr Tkach
volodymyr.tkach@bth.se