ITrust Cybersecurity as a service

Cybersecurity in space systems operations

cnes CENTRE NATIONAL D'ÉTUDES SPATIALES

comet

19/09/2019

SOC Security Operation Center

Agenda

- Itrust
- Cybersecurity in Space Program
- Artificial Intelligence
- Artificial Intelligence in Itrust Products

SOC
Security Operation Center

ITrust, European publisher of Cybersecurity solutions

ITrust Cybersecurity as a service

Shareholders and financial partners

100% French Company
Private and institutional investors (NewAlpha, Nestadio, Crédit Agricole, Caisse d'Epargne, Crédit Mutuel)
International development

Activities
❖Cyber security software edition :
- •Vulnerability scanner : **IKARE**
- •Malicious behavioral intelligence Engine: **REVEELIUM**
- •**SOC** Editor and Publisher – Security Operation Center

❖Counselling : PSSI, GDPR, Risk Assessment, Audit, Pentest, Training, Forensic.

11 years of cybersecurity experience
50 employees
More than 100 public and private clients,
Deloitte TOP 50 Fast Tech Company

Prizes & Associates

SOC Security Operation Center

ITrust, European publisher of Cybersecurity solutions

Expertise – Solutions – SOC as a Service

ITrust Cybersecurity as a service

EXPERTISE

This is the core business of ITrust. Our Security Consultants test the resistance of your architecture, be it externally or internally, and accompany you in order to help you secure your computer network in the long term.

- **Expertise**
- **Training**
- **Consulting**
- **Pentest**
- **Darknet**

SOLUTIONS

Our engineers are constantly developing new tools to facilitate the management, analysis and understanding of vulnerabilities and cyber attacks.

- IKare **vulnerability scanner**
- Revgelium **Malicious behavioral intelligence Engine**

SOC as a Service

ITrust manages the entire security process of companies that wish to outsource their cybersecurity.
Our Security Operations Center integrates advanced reporting and is based on our two leading products.

- **Managed** and/or
- **On Premise** and/or
- **SaaS** and/or
- **OEM** and/or

SOC Security Operation Center

Cybersecurity in Space Programs

ITrust Cybersecurity as a service

Space programs priorities

Historical Most Important Priorities
first Priorities was operational status and reliability

Identified New issues:
- Cyber security was evaluated after deployment and not well considered
- Data and ressource sizing
- Data protection process

Way to resolve them:
- Security Operational Center
- Security information management system
- Vulnerability scanner
- Virtualization
- General Data Protection Regulation

Be sure that there is NO operational impact

SOC Security Operation Center

Cybersecurity in Space Programs

ITrust Cybersecurity as a service

first feedback on the integration of cyber security

- Security Operational Center
  - demands specific skills and a lot of human resources
- Security information management system
  - Demands a lot of hardware resources for data collection
- Vulnerability scanner
  - A ground network is very segregated.
- Virtualization
  - Virtualization add additional logical layer…
  - … who can be vulnerable
- General Data Protection Regulation
  - Need process and human resource training
- No operational impact

SOC Security Operation Center

Cybersecurity in Space Programs

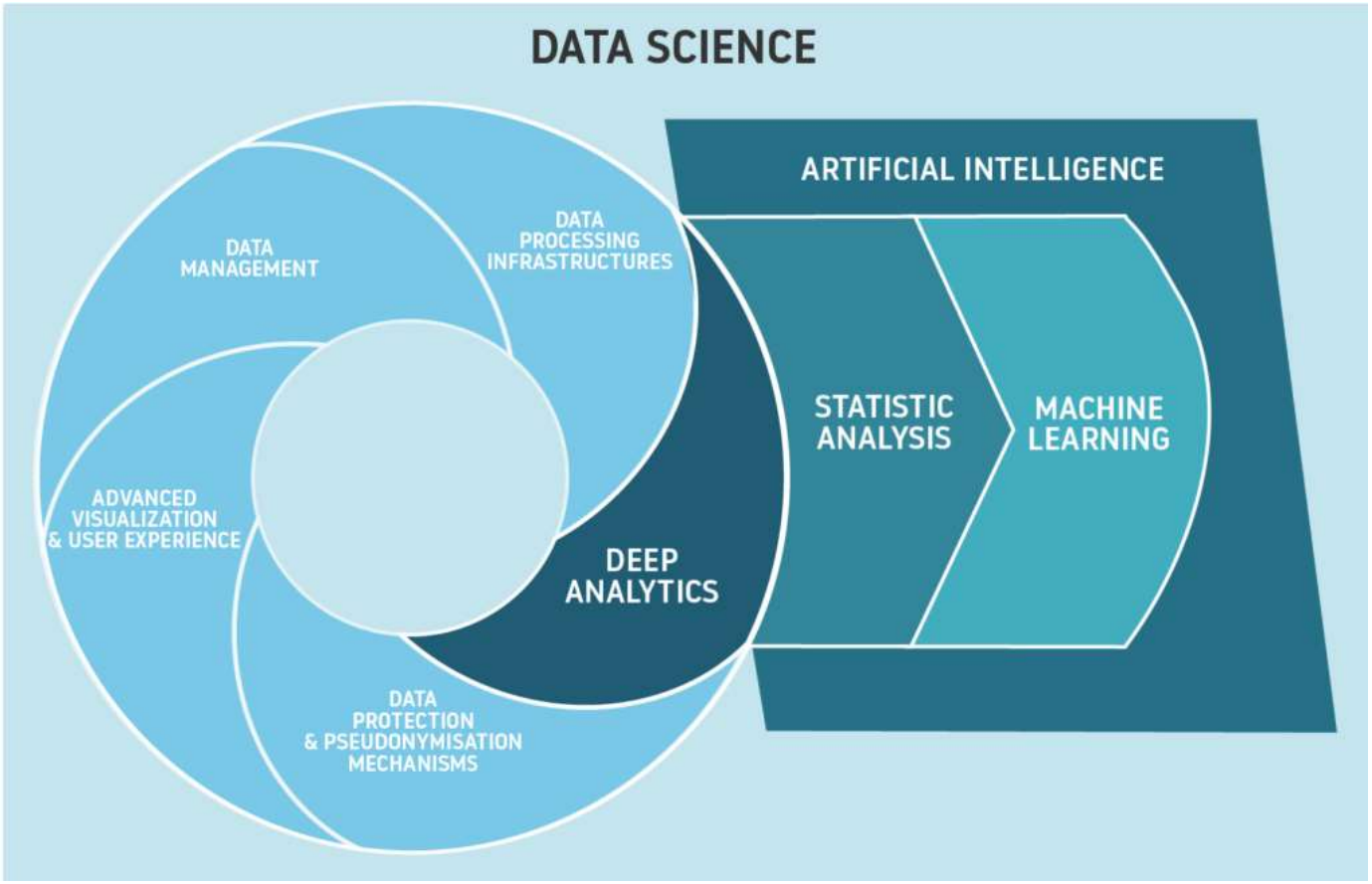
ITrust Cybersecurity as a service

What can we do?

- Specific training course
- Virtualization of the vulnerability scanner
- SIEM architecture based on the same virtualization concept for a full integration
- Normalization of event logs to reduce data storage issue
- Use of Machine learning to reduce event processing time and incident detection and response

SOC Security Operation Center

Artificial Intelligence

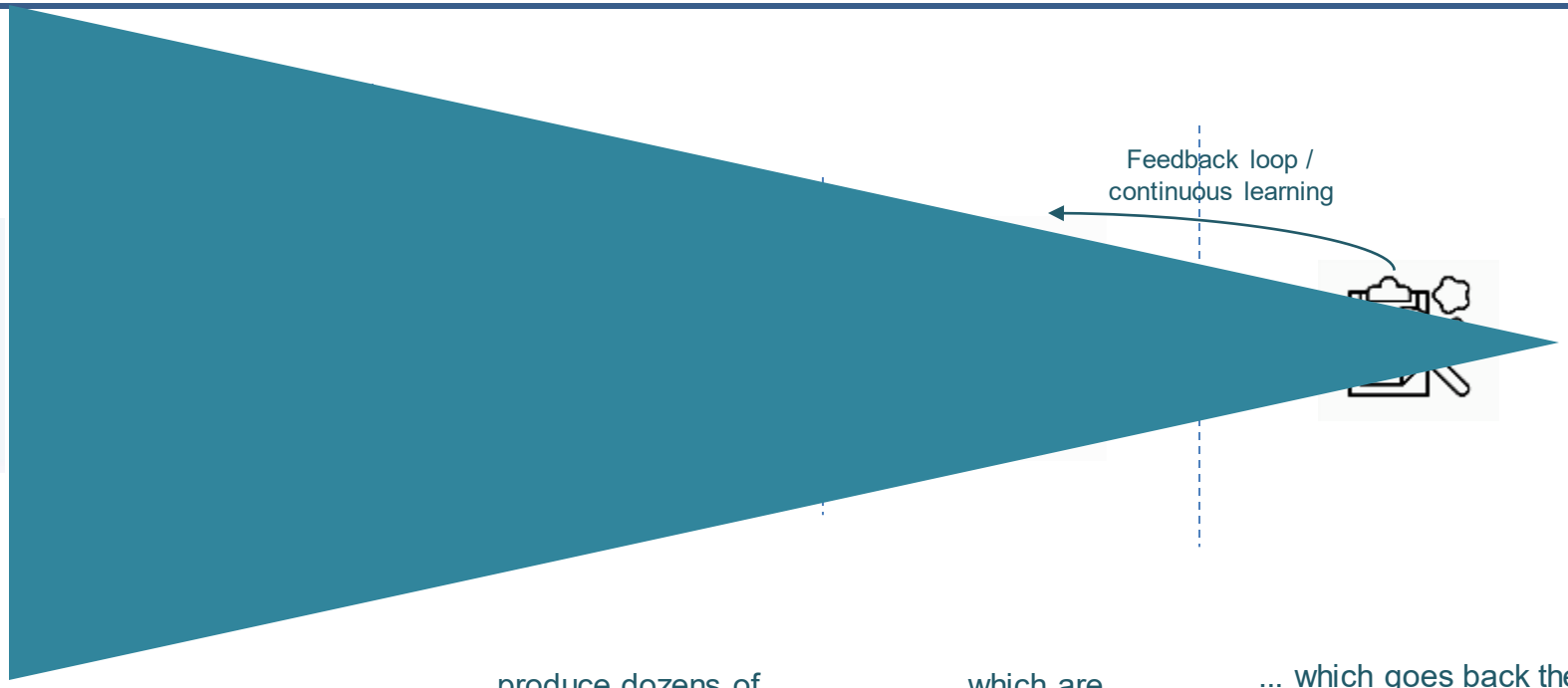


- Data mining for large collection
- Statistics for analysis
- Machine Learning for evolution
- Artificial Intelligence for behavior definition

AI – How to use in Cybersecurity?

ITrust Cybersecurity as a service

- AI and data science are a set of techniques for efficiently handling large volumes of data
- These techniques make it possible to learn complex "patterns" in the structured or non-structured data and to detect them automatically when the algorithms are in production.



Users…

… produce dozens of GB of logs a day …

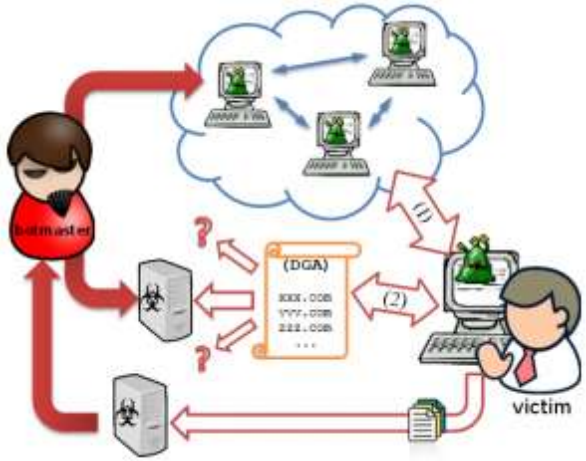
… which are processed thanks to machine learning …

… which goes back the most relevant anomalies only

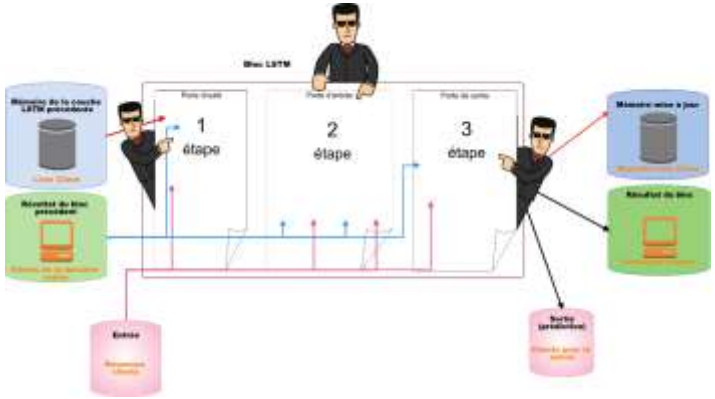
SOC Security Operation Center

AI – scenario integration

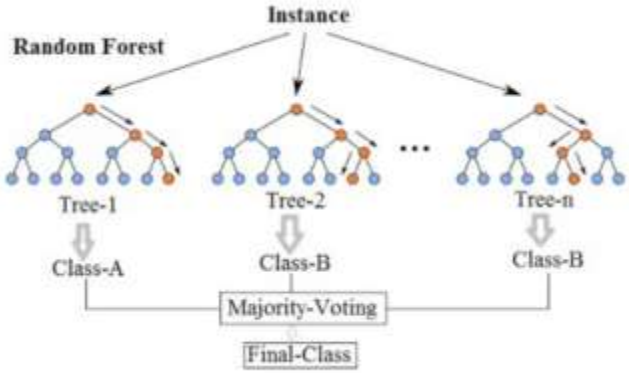
ITrust Cybersecurity as a service



LSTM



Random Forest



BiGram

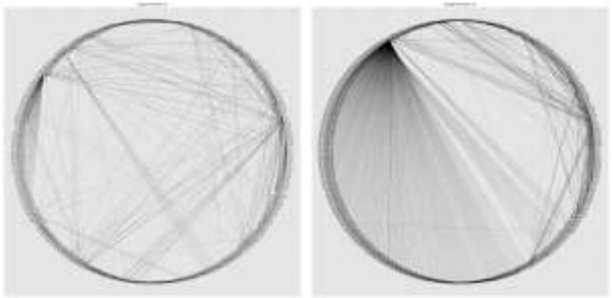
SOC Security Operation Center

AI – UEBA integration

ITrust Cybersecurity as a service

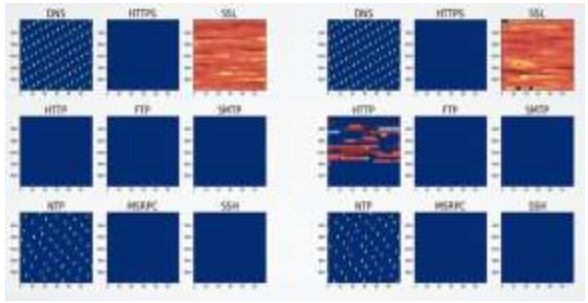
- UEBA is an area of cybersecurity AI application that detects changes and anomalies in the behavior of entities (users or machines) that make up the company's network.
- Algorithms detect changes in the overall behavior of the network or at the individual level (machines / users)

Machine learning and graph theory to detect changes in the structure of communications



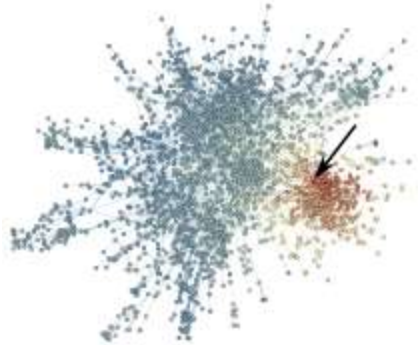
On the left, a "healthy" network. On the right, an internal machine tries to "ping scan" on a set of machines belonging to a subnet

Supervised learning algorithms to determine users' "network signature"



On the left, the usual network signature of a user. On the right, the network signature during a day during which an attack took place (increase of HTTPS connections)

Embeddings and dimensionality reduction to detect abnormal relationships between network machines



After reducing the dimensionality, it is possible to identify areas in which the density of communications is abnormally high, and which differ from normal.

SOC Security Operation Center

AI – dashboards

ITrust Cybersecurity as a service

Tableau de bord

Monitored user	Current Logged user since 2h	Current High Risk User	Nb de menaces levées
34609	37	9768	164

Overview of Security Activity for all users

Day | Week

Users with the highest risk score

RealTime | 48h | View all >

User ID	IP	Score	
John Doe	176.54.32.14	+10%	2205
Obi-Wan Kenobi	176.54.32.18	+10%	2154
Jane Doe	176.54.32.06	+10%	1765
Jane Doe	176.54.32.06	+10%	1765
Jane Doe	176.54.32.06	+10%	1765
Jane Doe	176.54.32.06	+10%	1765

SOC Security Operation Center

Itrust SOC : Advanced threat Detection

APT Kill Chain

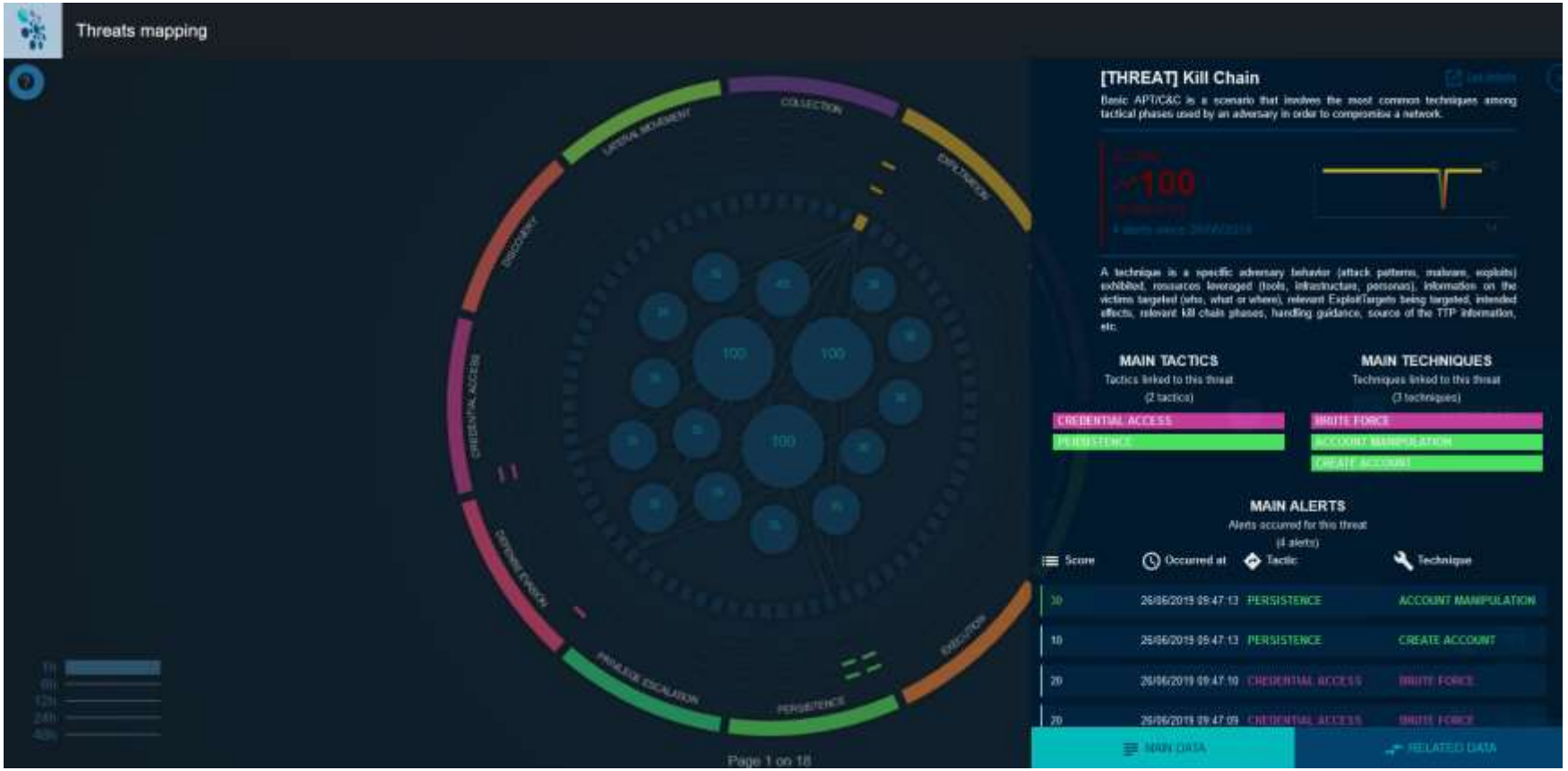
- Reconnaissance
- Infiltration
  - Phishing
- Persistence
  - Malware installation
  - C&C communication
- Internal intelligence
  - Information gathering & mapping
- Lateral movement
  - Spreading (credential use)
  - Target access
- Exfiltration

Reconnaissance | Infiltration | Persistence | Internal Intelligence | Lateral Movement | Exfiltration

SOC Security Operation Center

IA – REVEELIUM

ITrust Cybersecurity as a service



SOC Security Operation Center

Contact

ITrust Headquarters
55 Avenue l'Occitane, BP 67303
31673 Labège Cedex
+33 (0)5 67 34 67 80

Thank you!

International Office
6 rue 4 Septembre
Issy-les-Moulineaux, France
www.itrust.fr

SOC
Security Operation Center