



Organisation mondiale
de la santé animale
Fondée en tant qu'OIE

Cyberthreats to animal production and agriculture

Date: March, 25th 2026

Pascaline BOSSARD



Dianetis
Cybersécurité au service du vivant



Cyber Threats



Ransomware

GOAL : financial

Opportunistic attacks

Easy-to-exploit
vulnerabilities usage



Destabilization espionage

**GOAL : collection of
information**

Mid / Long term goals

Competitors
(companies or states)



Activism hacktivisme

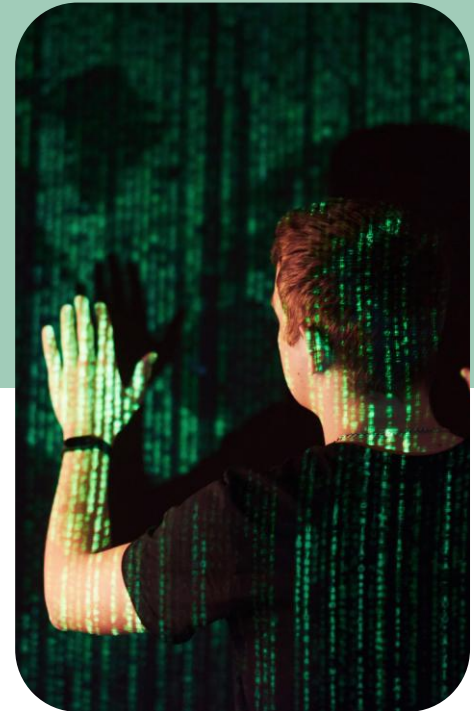
**GOAL : ideological
convictions**

Virtual attacks

Disinformation
or misinformation
campaigns

Some of the threats are about opportunities but
there are also intentional threats.

Question is not about if but when.



New trends



« Cybersecurity starts where there are data »

IA

Accelerator for attacks, increase complexity to detect
No technical knowledge (as a service)

Hybrid attacks

Connection to systems as part of a global attack (ex: lab entry), access to confidential datas...

Supply chain attacks

Link with One Health systems

Internet of Things (IoT)

Attack surface increasing a lot, lack of strong protection.

Impacts



CONFIDENTIALITY

- Data leak
- Confidential information shared



INTEGRITY

- Results are corrupted
- Wrong decisions taken

Economics · reputation · biosafety

AVAILABILITY

- Systems not available
- Tests cannot be performed or shared



TRACEABILITY

- Destruction of data
- Loss of historical information

These risks will be amplified in case failing to detect attacks when they occur but also being unprepared to respond to it.

Data manipulation threatens large-scale stability.



Examples



Crystal Valley Cooperative becomes latest agriculture business hit with ransomware

By The Cyber Post - September 22, 2021 1435 0

CYBERCRIME

Ransomware Attack Hits Production Facilities of Agricultural Equipment Giant AGCO

Agricultural equipment giant AGCO says its business operations have been impacted after falling victim to a ransomware attack last week. AGCO designs, makes, and distributes agricultural machinery and precision technology, offering equipment under brands such as Challenger, Fendt, Massey Ferguson, and Valtra.

In March 2022, for instance, Lynnfield, Mass.-based dairy supplier [HP Hood LLC](#) announced it was a victim of a “cyber security event” and had to temporarily take its plants offline as a precaution. This resulted in an inability to manufacture or receive raw materials, including milk.

In October 2021, Green Bay, Wis.-based [Schreiber Foods](#), manufacturer of cheese and other dairy products, halted operations at its plants and distribution centers following a cyberattack in which hackers reportedly demanded a rumored \$2.5 million to unlock its computer systems.

US-based medical technology giant Stryker admitted on Thursday that the recent [Iran-linked cyberattack](#) has caused significant disruption, as more evidence has come to light on the tactics and techniques used by the attackers.

Stryker said in its latest media [statement](#) that the hacker attack caused global disruption to the company’s Microsoft environment, but noted that the intrusion was limited to this environment.

**Hackmanac**
@H4ckmanac · Follow

Cyberattack Alert !!

USA - AskVet

Kill Security hacking group claims to have breached AskVet.

Allegedly, exfiltrated data include client names, contact numbers, addresses, email addresses, and detailed pet medical histories, including diagnoses, prescriptions, and [Show more](#)

ask.vet
70 174 129 555

Data
data contains, but is not limited to: Client names, contact numbers, addresses, email addresses, and detailed pet medical histories, including diagnoses, prescriptions, and treatments.

ask.vet provides virtual pet care services, offering 24/7 consultations through an AI-powered platform for pet owners. They are focused on delivering real-time support for pet health management.

9:49 AM · Oct 19, 2024

5 · Reply · Copy link

[Read more on X](#)

PREPARATION IS THE KEY



Power Up Your Cyber Defense



PEOPLE

- Awareness : train the entire ecosystem.
- Understand threats and risks
- Worked with already engaged stakeholders



PROCESS

- System interoperability to avoid data transfers
- Integrate cyber process into existing business workflow



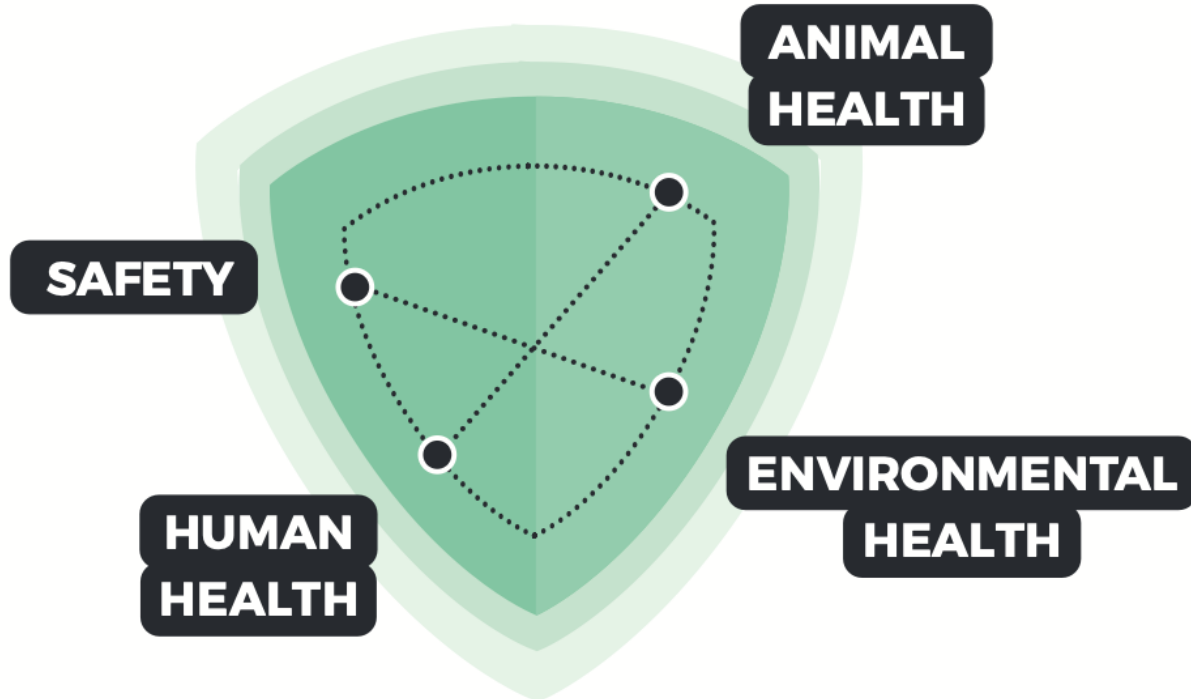
TECHNOLOGIE

- Put security basics in place
- Security by design for new system, tools...
- Use appropriated tools for systems monitoring and surveillance

ONE HEALTH



Starts with Teamwork



Collaboration is our strongest defense.
Cybersecurity needs a global, multi-sector approach.
Threats are global – our defense must be global.

CONCLUSION



Data's are now fully integrated in all process and bring depedencies

Hydride threats scenarios should consider virtual field

Cybersecurity is a governance topic