2022-11-08

CYBERWAL

Journée des doctorants – Security Orchestration and Observability

Sebastien Dupont (CETIC), Guillaume Ginis (CETIC)

https://cyberwal.be
https://cyberexcellence.be

Observability

SIEM, IDS

01

SOAR

Security Orchestration
Automation and Response

02

Vacsine

Training and evaluating digital
immune systems

03

04

Case Study - SecuRover

Supply chain attack protection

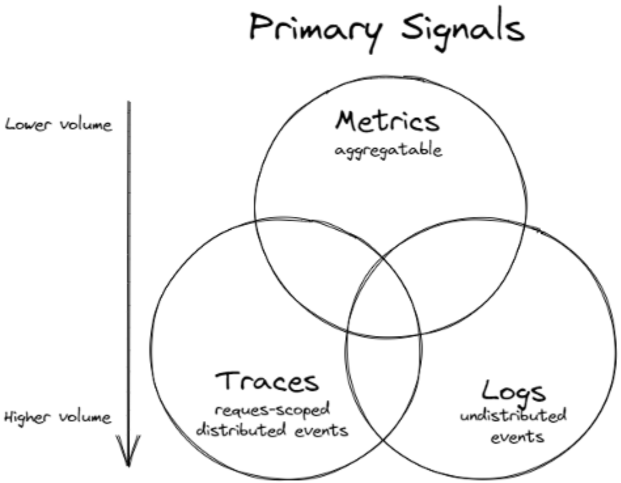
05

Conclusion and Roadmap

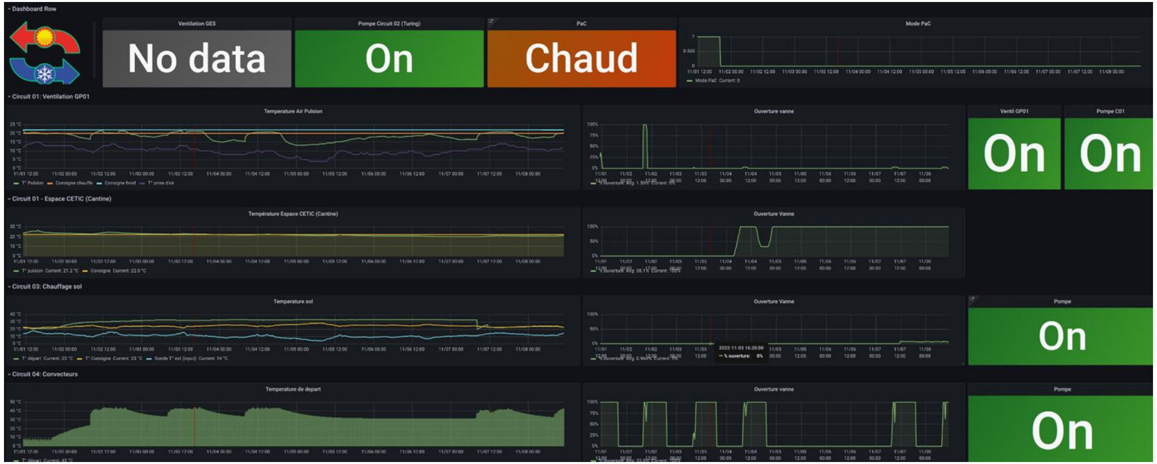
01

Security Observability

Observability



Fournir une visibilité sur les systèmes distribués pour permettre l'identification et la résolution de problèmes, de manière rapide et automatisée.
(ref IBM)

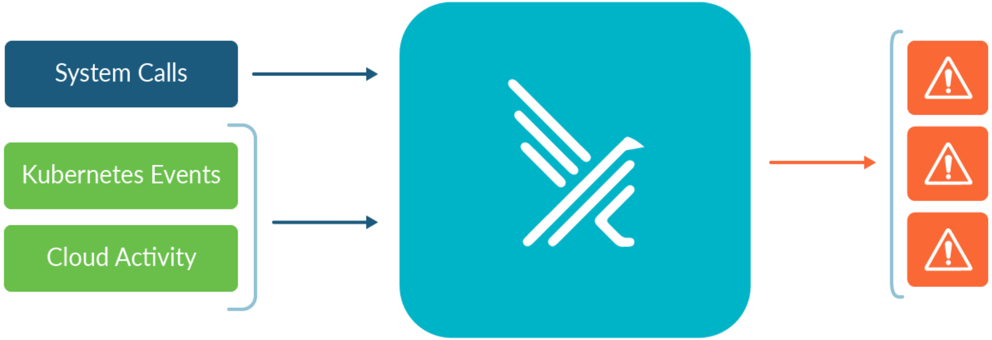


https://microsoft.github.io/code-with-engineering-playbook/observability/log-vs-metric-vs-trace/

Observability for Security - IDS - Intrusion Detection System

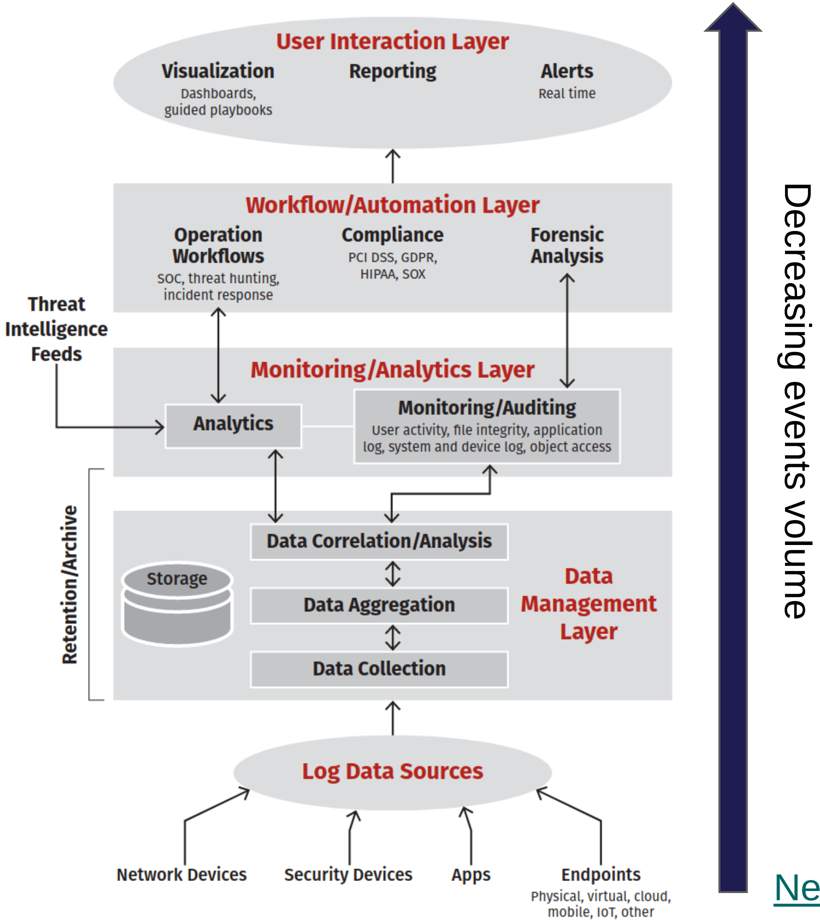
System allowing the detection of abnormal or suspicious activities on a target to be analyzed (a network or a host).

- network intrusion detection (NIDS), host intrusion detection (HIDS), ...
- architecture:
    - Sensors - generate events
    - Console - monitor events and alerts, control sensors
    - Detection Engine - signature detections (malware recognition) vs anomaly detections (deviations from a model representing good behavior).



https://falco.org/

Observability for Security - SIEM


User Interaction Layer
Visualization
Dashboards, guided playbooks
Reporting
Alerts
Real time
Workflow/Automation Layer
Operation Workflows
SOC, threat hunting, incident response
Compliance
PCI DSS, GDPR, HIPAA, SOX
Forensic Analysis
Threat Intelligence Feeds
Monitoring/Analytics Layer
Analytics
Monitoring/Auditing
User activity, file integrity, application log, system and device log, object access
Retention/Archive
Data Correlation/Analysis
Storage
Data Aggregation
Data Collection
Data Management Layer
Log Data Sources
Network Devices
Security Devices
Apps
Endpoints
Physical, virtual, cloud, mobile, IoT, other
Decreasing events volume

“Security information and event management (SIEM) technology supports **threat detection, compliance and security incident management** through the **collection and analysis** (both near real time and historical) of **security events**, as well as a wide variety of other event and contextual data sources.”

-- Gartner

NextGen SIEM Reference Architecture Visualization - SANS

02

Security Orchestration

SOAR - WHY

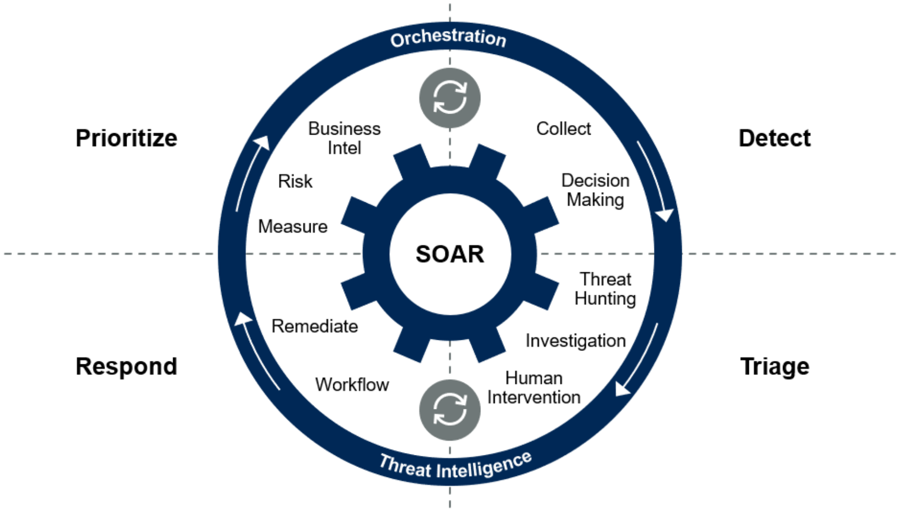
Security orchestration, automation, and response (SOAR)

3 key software capabilities that security teams use:

1. case and workflow management,
2. task automation,
3. centralized means of accessing, querying, and sharing threat intelligence.

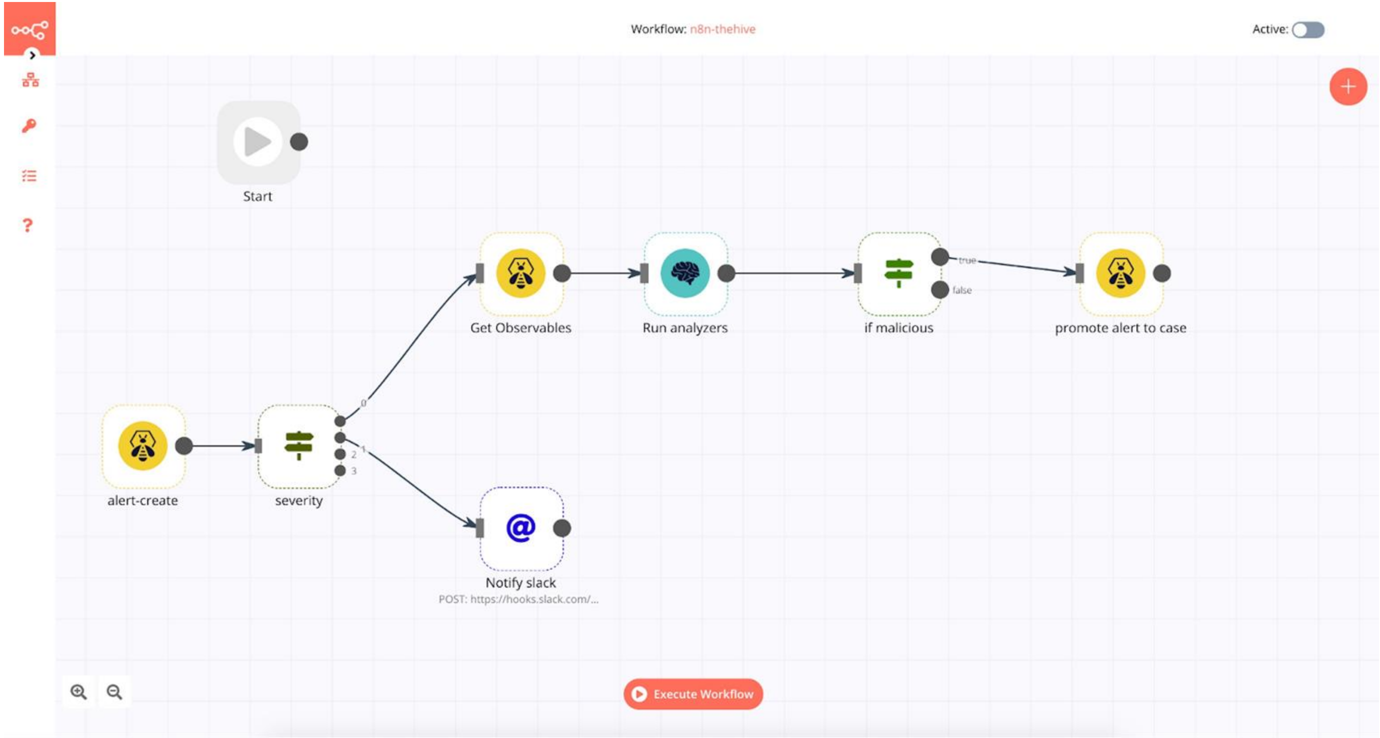
https://www.redhat.com/en/topics/security/what-is-soar

Security Orchestration, Automation and Response: An Overview



Source: Gartner
ID: 389446

SOAR - The Hive + TIP (MISP, MITRE)



https://thehive-project.org/ Exemple de workflow: notification Slack et case creation

03

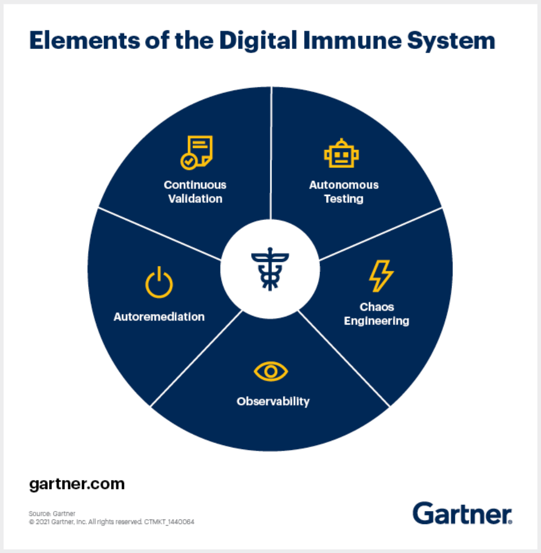
Vacsine - Training and evaluating security response efficiency

Vacsine - Digital Immune systems in the Cloud/Edge

security cloud continuous-integration orchestration edge certification soar

Vacsine is an open-source tool that helps building Digital Immune Systems:

- It relies on **continuous monitoring** of **Cloud and Edge** systems to define, evaluate and apply automated countermeasures such as firewalls, intrusion detection systems, honeypots or quarantining.
- The **automated response** is triggered by changes to security requirements, indicators of compromise, incidents and vulnerabilities.
- The **efficiency and speed of countermeasures** deployment is evaluated in automatically provisioned sandbox environments that shadow the target Cloud/Edge systems. Those sandboxes provide observability and scalability for the training and maintenance of security response strategies.



Elements of the Digital Immune System

gartner.com

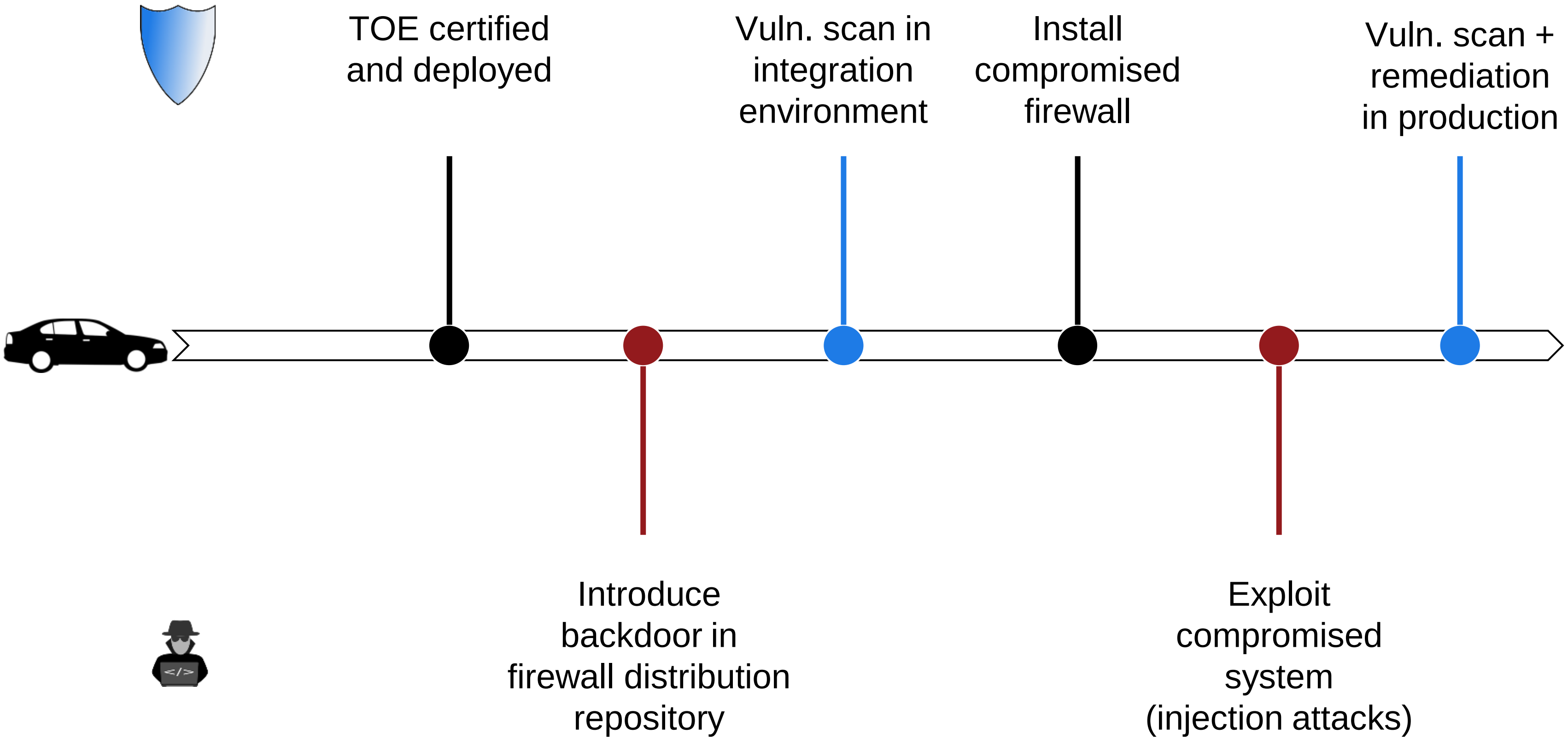
Source: Gartner
© 2021 Gartner, Inc. All rights reserved. CTMKT_1440064

https://github.com/cetic/vacsine

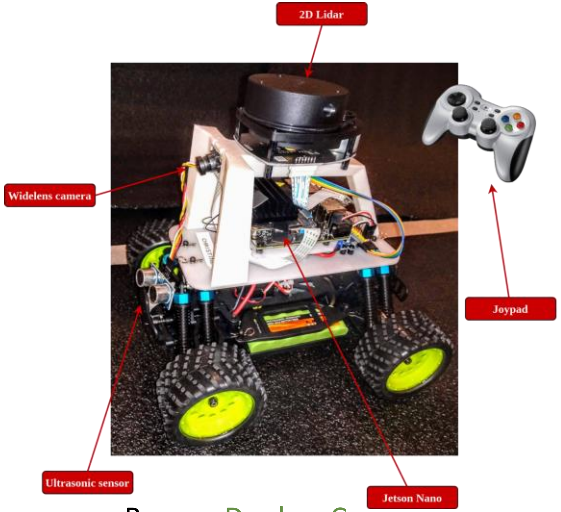
04

Case study - Securover: Supply chain attack protection

Case Study - Securover: Supply chain attack protection

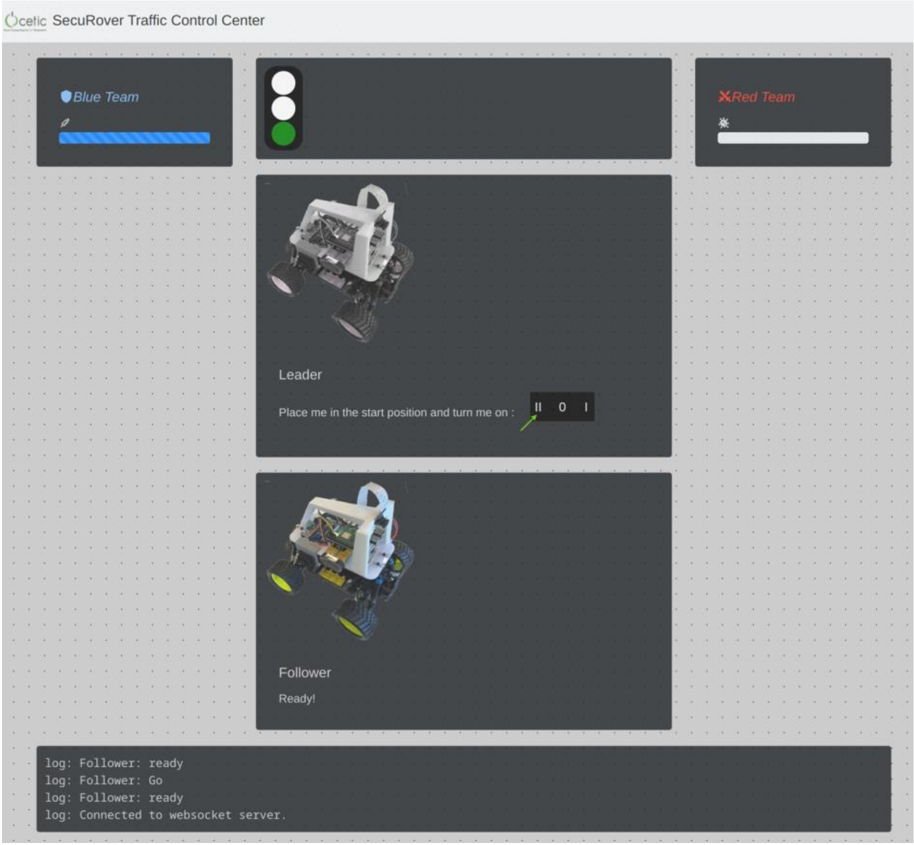

TOE certified and deployed
Vuln. scan in integration environment
Install compromised firewall
Vuln. scan + remediation in production
Introduce backdoor in firewall distribution repository
Exploit compromised system (injection attacks)
</>

Case Study - Securover - Supply chain attack protection



Rover - Donkey Car

ROS industrial



SecuRover Traffic Control Center

Blue Team

Red Team

Leader

Place me in the start position and turn me on : II 0 I

Follower

Ready!

```
log: Follower: ready
log: Follower: Go
log: Follower: ready
log: Connected to websocket server.
```

Case Study - Securover - Supply chain attack protection

metasploit

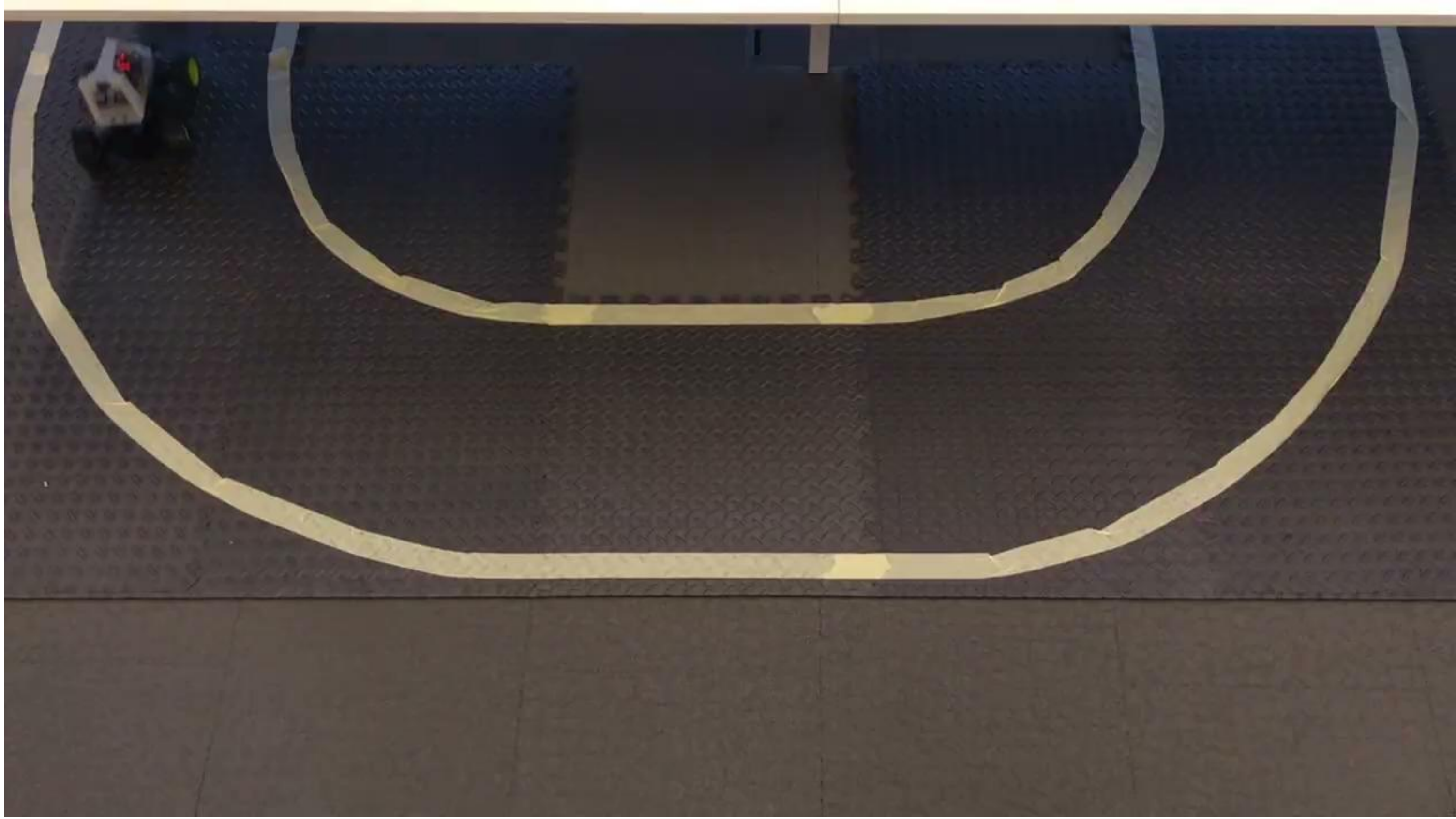
The attacker uses this access to modify the car behavior and create an accident

GAZEBO

*Evaluation of attack and defense in a **virtual environment**.*

Case Study - Securover - Supply chain attack protection

The attacker uses this access to modify the car behavior and create an accident



Conclusion and next steps

- Publication de la brique logicielle sur la software factory
  - Expérimentations
  - Démonstrateur
  - Montée en TRL
- Integration IDS (Falco) et HoneyPot dans Kubernetes/OpenShift comme service de sécurité

Merci de votre attention

Fonts & colors used

Viga
(https://fonts.google.com/specimen/Viga)

DM Sans
(https://fonts.google.com/specimen/DM+Sans)

#aedbdd

#1f1c51

#eb7e33