

ACS Tools Presentation

Sebastien PEYNET – *Project Manager*

Airbus CyberSecurity

January, 23th 2025



This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101120779



Summary













a platform that can **simulate** highly **sophisticated** and realistic environments



Operational Tests and Validation



Reproduce realistic complex • • • systems (IT, OT and SCADA)

> **Content Library** provided • • •

Customised content

Hybrid capacity: interconnection with your existing HW&SW systems

Physical or SaaS • • •

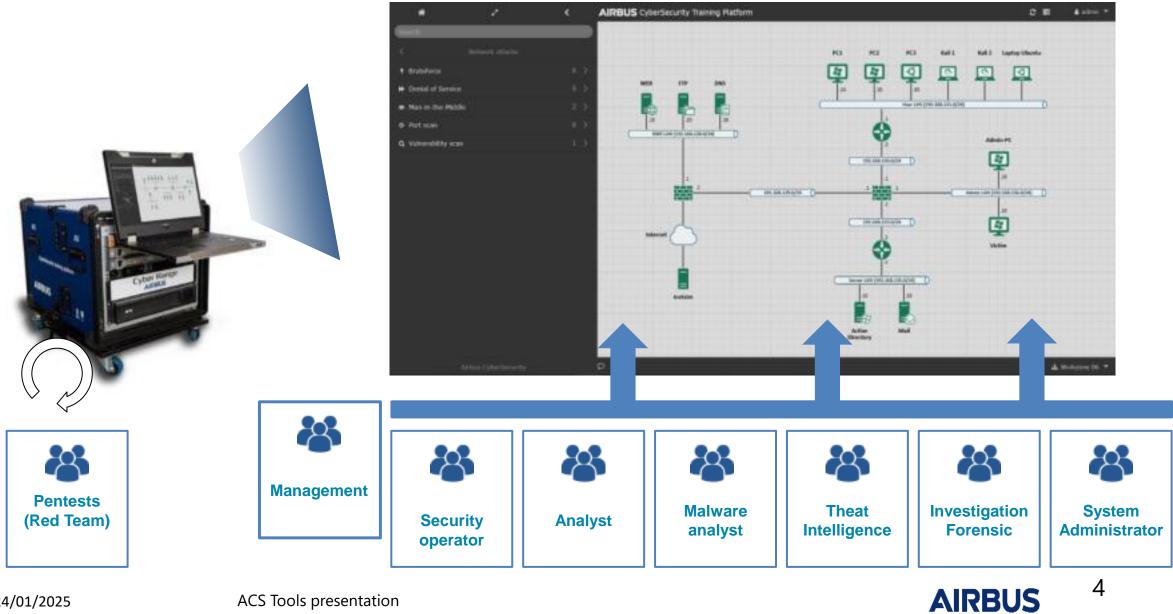
000



ACS Tools presentation

CyberSecDome

CyberRange Exercises





Log management

NIST summary helps to identify objectives and process to be put in place:

- "Organizations should establish policies and procedures for log management."
- "Organizations should establish standard log management operational processes:
- Monitoring the logging status of all log sources
- Monitoring log rotation and archival processes
- Checking for upgrades and patches to logging software, and acquiring, testing, and deploying them
- Ensuring that each logging host's clock is synched to a common time source
- Reconfiguring logging as needed based on policy changes, technology changes, and other factors
- Documenting and reporting anomalies in log settings, configurations, and processes.".





SIEM basics

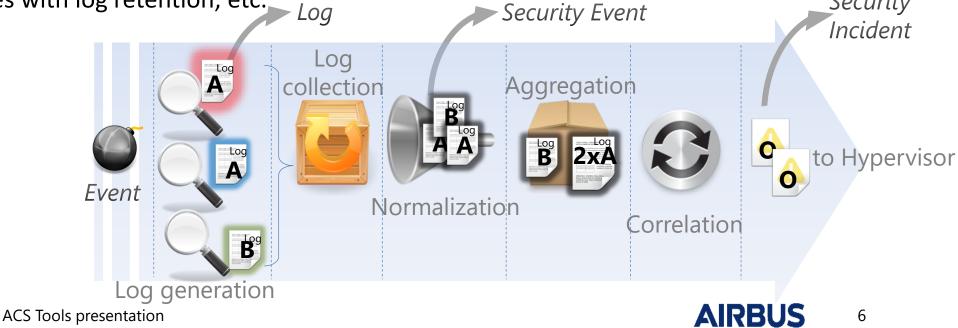
The SIEM product family is the core of events and information management. SIEM are providing security information management and also event management, by collecting information system logs from multiple assets and managing security event in real-time. Main commons features of SIEM products are:

Log collection and forward to Log manager

Log parsing, aggregation, normalization and correlation

Data indexing for query, reports visualization and analysis.

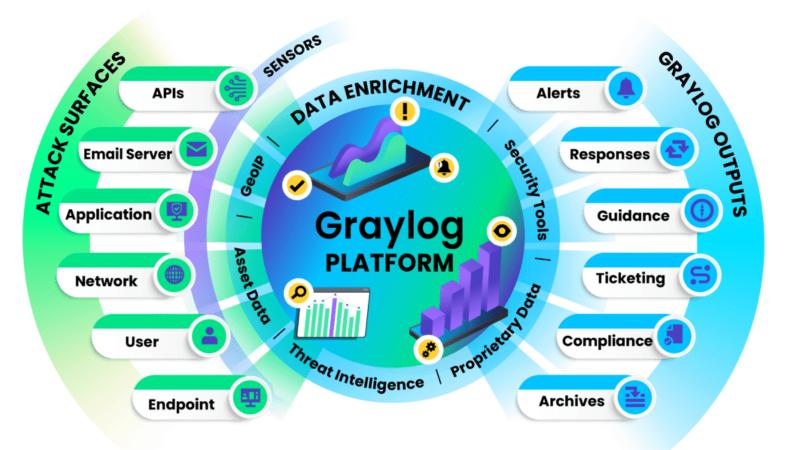
Depending of editor, SIEM products offers the toolbox for incident handling with real time alerting, forensic capabilities with log retention, etc.



SIEM - Graylog

Log management solution :

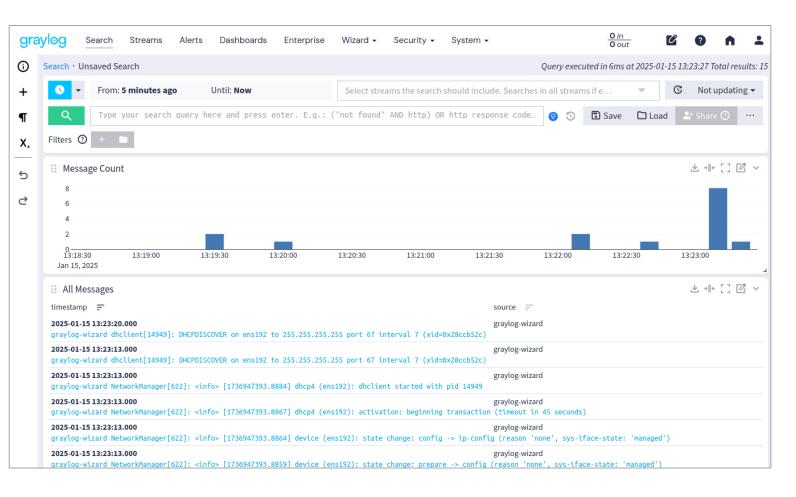
- Log data aggregation
- Log data analysis
- Log data management



SIEM - Graylog

- Unlimited log ingestion
- View log data in real-time
- Search through volume of log data
- Configure alerts for what matters

most



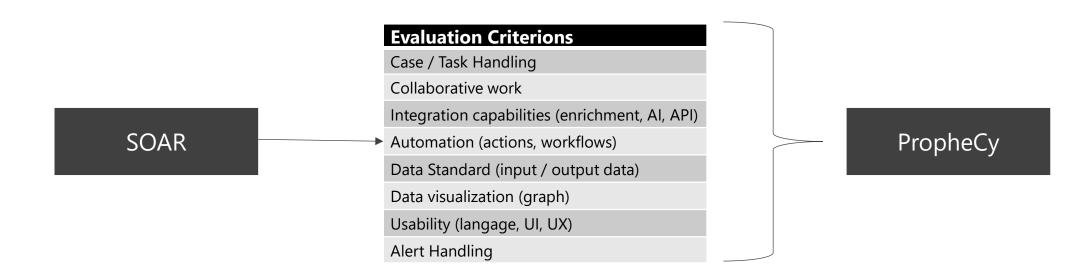
Grayog Wizard Alert creation Plugin to manage the alert rules Alert notification

🖻 😔 Graylog - Alert	Rules × +											\sim	×
$\leftarrow \rightarrow $ G	○ 192.16	8.134.60:9000/wizard	d/AlertRules							\$	\bigtriangledown	٩ ٢	≡
grayl⊙g Searc	h Streams Alert	s Dashboards	Enterprise	Wizard / Alert Rules -	Security -	System 🗸				0 in 0 out	C 0	n	÷
Alert Rules With the wizard, you ca	an manage the alert rule	s. An alert rule consists	s of one or mo	re streams with rules, an a	lert condition ar	nd an alert notification. Re	ad more about Wizard al	ert rules in the documentation (wizard ver	rsion : 6.1.0).	Cre	ate Impor	t Expo	ort
Filter alert rules													
Bulk actions 👻											Show	Column	s 💌
🗌 Title	Priority	Description		Creat	ted	Last Modified	User	Status				Acti	ons
🗆 aaa	High			2024-	12-24 09:09:58	2024-12-24 09:44:17	admin	Disabled	► Edit	Event definition	Notificatio	n Clor	ne
🗆 bbb	Low			2024-	12-24 09:30:41	2024-12-24 09:30:41	admin	Enabled	► Edit	Event definition	Notificatio	n Clor	ne
🗆 rrr	Low			2024-	12-24 10:08:09	2024-12-24 10:08:09	admin	Enabled	► Edit	Event definition	Notificatio	n Clor	ne
🗌 aaa2	High			2024-	12-24 10:12:20	2024-12-24 10:12:20	admin	Disabled	► Edit	Event definition	Notificatio	n Clor	ne
🗌 issue 101	Low			2025-	01-07 16:07:22	2025-01-07 16:07:22	admin	Enabled	► Edit	Event definition	Notificatio	n Clor	ne



Tools for Incident Response

Security Orchestration Automation and Response (SOAR) => a centralized and more efficient approach for incident response.





Introducing

PROPHECy Visualize - Understand - Automate

Cyber operations > Multiple **integrations** (bidirectional) 🕞 Tickets 1 🔥 Alertes 🎲 Artefacts 🕒 Tage > **REST API** for automation ▲ 1000 Q <u>ж</u> × I **г** Alertes / Ticketing 1 28 1 🖬 🕰 > Events enrichment & investigation 🛦 63 🖈 63 Trojan Notice and Take-down Intelligen Pull & push Dos Smut EDR / NDR Dos Smut SIEM Ajouter faux positif Emission & enrichment / Enrichment Security tools investigation Security Tools Information (CTI, ...) System 11

> Correlate events automatically

Visualize

Cybe ome

AIII DUS

> Materialize links between events

> Contextualize dynamically event

PROPHECy 🛱 Tickets 🔬 Alertes 🛞 Arte	efacts 🔖 Tags	Administration ⑦ し
Alertes	Q user:perez	× 🗛 15 Q
Trier par date 🗸 Tout 🗸	Tout 🗸	2 2 2 2 2
Nombre de noeuds 100 Ignorer les filtres temporels Alerte racine Artefact Ticket		Perez
		903 National Security State Affiliation Zero-Day Exploit Computer Network Attack
ACS Tools present:	ation	

ACS 1001s presentation

Understand

24/01/2025

> **Streamline** ticket handling and collaboration (Kanban)



> **Prioritize** and categorize with tags

> Cross analyze events through a modern UI

PROPHECy Fickets ⁴ Alertes	🕸 Artefacts 🛛 🗣 Tags			Administration ⑦ 🕛
E Tickets	Q Recherche		٩	🗄 🕂 Créer
Trier par numéro 🗸 🗸				1 28 1 28
Nouveau	En cours	• Fermé	. . 996 *	
Exvestropping (Password) (Phiching +2)	#996 Red Team Phishing Transparency Casus Belli Shoulder Surfing ▲ 5 Birthday Dos Eavesdropping +11 : Créé le 2022-01-25 08:25:15 PR	Privacy Law Hacktivist Data Mining Blacklist 1 Smuth Wom : Cree le 2022-01-25 08:25:15	996 Red Team Phishing Transparency Casus Surfing PR Birthday Dos Eavesdropping Macro Malware Mi	
Cree le 2022-01-25 08:25:15 PR PR PR Pr Pr Cree le 2022-01-25 08:25:14 PR PR PR PR PR PR PR PR PR P		Wegg7 Notice and Take-down Organized Crime Whitelist Best Practices Cyber Warfare Intelligence Infrastructure/Information Infrastructure 1 1 Bomets Dos 1 43	SQL +5 [™] Détails Analyse Paragraph ~ B I @ := ½= IP : ID INDUCTION match threat actor APT-1.	v
EINSTEIN Blacklist Computer Emergency Response Team Interdependencies Intelligence Infrastructure/Information Infrastructure Whitelist (1) Birthday (Macro (MrtM) (KSS) Creé le 2022-01-25 08:25:14			Information sent to team 2 for immediate response.	
ACS Tools pre-	sentation			12

> Automate each step of event analysis

Automate

> Orchestrate with workflow

> Provide intelligence out of the box : shared library of connectors and

ome

Cybe

PROPHECy F Tickets A Alertes	Artefacts Tags Admin	nistration ⑦ 🕛
Nom Malware type threat 2	Rang 🗘 1 Description	
Q Rechercher		÷
Évènements (2)		↔
Connecteurs (10)		€ Q
Custom (0)		€
Logiques (2)	escalate.py	
-C switch	Code 1	
]→ join		
Formulaire (1)	Code o	
	false_positive.py	
← Retour Terminé		
ACS Tools pre	sentation	1 4

24/01/2025

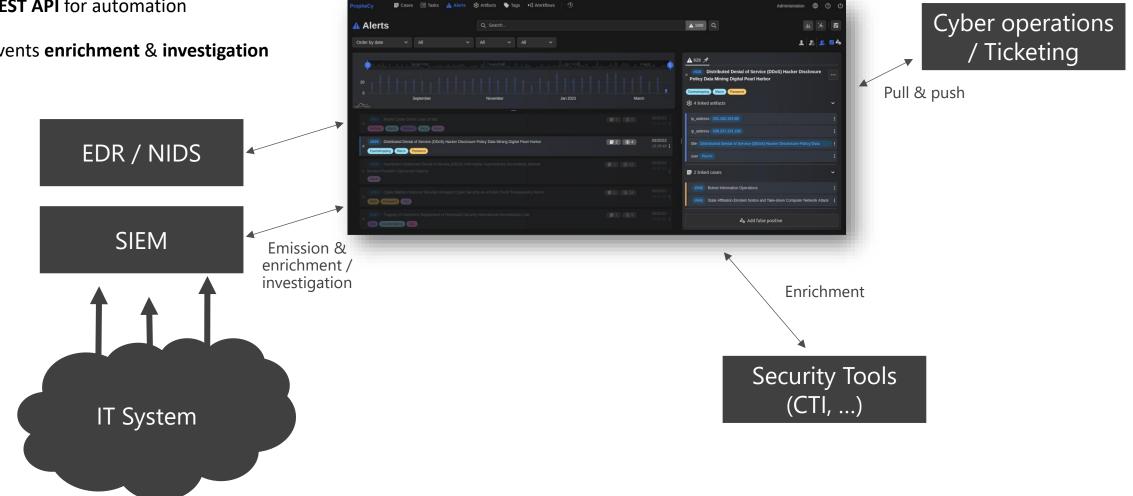


PropheCy

> Multiple integrations (bidirectional)

> **REST API** for automation

> Events enrichment & investigation





PropheCy

Visualise

- > Automatically **correlate** security events
- > Link artifacts between similiar events
- > Dynamic events contextualisation



PropheCy 🛱 Cases 🖅 Tasks 🛕 Alerts 🚯 Artifacts 🔖 Tags 📭 Workflows 🕚	Administration 🌐 ၇ 난
Alerts	× A 12 Q
Order by date V All V All V All V	L 28 L 🖬 🖉 🍫
Number of nodes 100 V C A A A A A A A A A A A A A A A A A A	Berez 🖈
□ Ignore time filters	user Perez
■ Root alert Passed Pero-Day C Pick Model	Birthday Botnets Eavesdropping Macro MitM Password Phishing Ransomware SQL +4
Neighbor alert Artifact Artifact Artifact	II Timeline
Attiliact Red Feam Product	2
Artifacts type to hide	1
Artifact to hide	
array doc to inde	October Jan 2023
Worm Script. Air Gapped	
	▲ 0 alert ✓
	There is no item to display
Tóra divar cityar Cara Milliet Inf	1 Properties
Collegidges plu jdepd ^{artere} 1711 Galage Galageude 394 Rever of War	Last reception date 2023-03-21 00:00:00
ears of two	Description



16

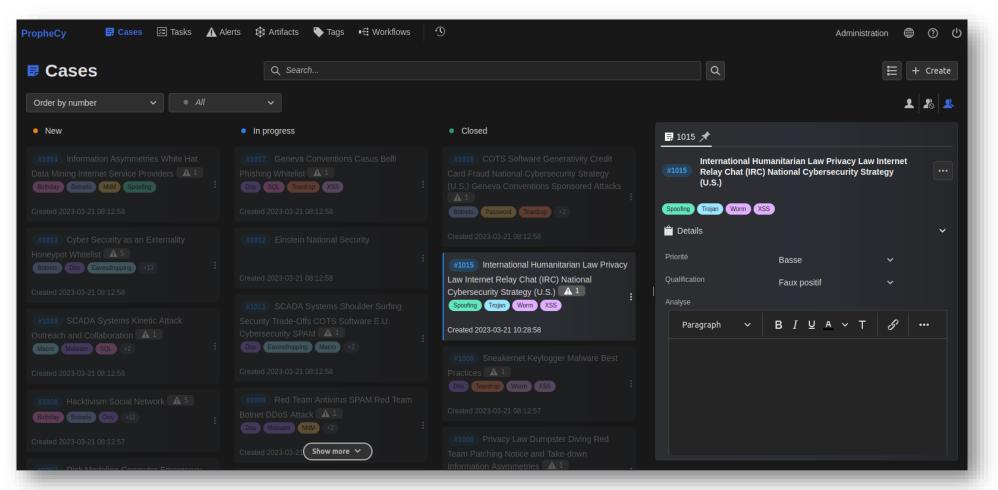


Understand

> Facilitate case handling & collaborative work (Kanban board)



> Easy-to-use & modern Web UI for in-depth event analysis





17

CyberSecDome

24/01/2025

PropheCy

> Automate investigations



18

> Workflows orchestration

> Triggered automatically or manually

PropheCy 🖬 Cases 🖻 Tasks	▲ Alerts 段 Artifacts 🎙 Tags • E Workflows 🕚	Administration 🌐 ⑦ 😃
Name Malware suspicion	Rank 🗘 1 Description	
Steps Extra		
Q Search Events (2) Incoming alert End Scripts (10)	 ► ► Control = 100 (model Cont	₽ ℃ ⊗ 0
Custom (0) Logicals (2) -C Switch Join	incoming alert	
Form (1) ← Back Submit	s Is presentation	AIRBUS

Automate

Contact

