

Enhancing Academic Cyber Resilience – Integrating TGuard into ACAD CSIRT Services



Dr. Ir. Charles Lim, Msc., Bsc., CSAP, Security+, CySA+, CND, CCSE, CTIA, CHFI, EDRP, ECSA, ECSP, ECIH, CEH, CEI

Swiss German University

Da Nang, 10th September 2025

About Me

Dr. Ir. Charles Lim, Msc., Bsc., CSAP, Security+, CySA+, CND, CCSE, CTIA, CHFI, EDRP, ECSA, ECSP, ECIH, CEH, CEI

Deputy Head Master IT Program

Head of Cyber Security Laboratory (now Security Operation Center)

Swiss German University

Charles.lims [at] gmail.com and charles.lim [at] sgu.ac.id

http://people.sgu.ac.id/charleslim

Research Interest

- *Malware*
- *Intrusion Detection*
- *Vulnerability Analysis*
- *Digital Forensics*
- *Cloud Security*

Community

Indonesia Honeynet Project - Founder

Academy CSIRT – Chief Operation

Asosiasi Forensik Digital Indonesia - member



Indonesia Honeynet Project

ACADCSIRT



Agenda

- Academic Cyber Threat Landscape
- About ACAD CSIRT
- Key Achievement ACAD CSIRT Summit 2025
- Why TGuard?
- What ACAD CSIRT will provide
- Integration & Onboarding Workflow
- Use Cases
- Early Adopters
- Key Takeaways

Academic Cyber Threat Landscape



Indonesia University's Landscape

- 4500 Universities in Indonesia, 1500 of them teach IT
- Only about 20 have CSIRTs
- Now, that Indonesia has UU PDP (Data Privacy Law)
- It is a law NOW, to protect students' data privacy

About ACAD CSIRT

- ACAD-CSIRT stands for **Academic Computer Security Incident Response Team**—a *non-profit, non-governmental national CSIRT in Indonesia*.
- **Core mission**
 - Unites university-related incident response teams to enhance the country's cybersecurity posture.
 - Promotes security training and research, forging public-private partnerships across academia, government, and industry.
 - Engages with global CSIRT organizations to share knowledge and strengthen international cybersecurity collaboration.

About ACAD CSIRT

ACADCSIRT



ACADCSIRT



ACAD CSIRT Summit 2025 – Program Highlights



The poster for the ACAD CSIRT Summit 2025 features a red and white color scheme. At the top, it lists sponsors including Aptinor, Universitas Kristen Maranatha, and PUSDATIN. The main title 'ACAD CSIRT SUMMIT 2025' is in large red letters, followed by the tagline 'Building a National Cyber Resilience Ecosystem through Industry, Government, and Academia Collaboration'. The program is divided into three days: Day 1 (Wed, 9 July 2025) includes Cyber Security Incident Response Training and a Cyber Competition Final Announcement; Day 2 (Thu, 10 July 2025) includes a Conference, Technical Workshop, and ACAD CSIRT & Campus Registry Initiation; Day 3 (Fri, 11 July 2025) includes a Site Visit and MOU Signing. A 'PROMO KHUSUS' box lists special prices for Summit + Training: 1-8 July 2025 for 550 K and 9 July 2025 for 700 K. A QR code for registration is provided, along with contact information for Adriani and Aristia. The bottom of the poster shows logos for sponsors like Huawei, CompTIA, and Google Cloud, and mentions co-managers.

ACAD CSIRT SUMMIT 2025
"Building a National Cyber Resilience Ecosystem through Industry, Government, and Academia Collaboration"

DAY 1 | WED, 9 JULY 2025

- Cyber Security Incident Response Training (09:00 - 17:00 WIB)
Empowering Cyber Security Professionals with Advanced Incident Response Skills
- Cyber Competition Final Announcement

DAY 2 | THU, 10 JULY 2025

- Conference (10:00-12:00 WIB)
Shape the Future of Cybersecurity: Connect, Inspire, and Lead
- Technical Workshop (13:00-16:00 WIB)
Empower Innovation & Cyber Resilience Through Expert Workshops (7 parallel tracks)
- ACAD CSIRT & Campus Registry Initiation (16:00-17:00 WIB)

DAY 3 | FRI, 11 JULY 2025

- Site Visit
Experience Real-World Cyber Security in Action
- MOU Signing
Strengthen Future Collaborations

WED-FRI, 9-11 JULY 2025
08.00-17.00 WIB

Building & Floor 2*
Maranatha Christian University
Surya Sumantri 65, Bandung
West Java, Indonesia

Info: Adriani (0812-2380-614)
Aristia (0818-0921-5545)
acad.csirt@maranatha.ac.id

PROMO KHUSUS!
Kode Promo: SUMMIT_PROMOT2025TS
SPECIAL PRICE Summit + Training
1 - 8 Juli 2025
550 K
9 Juli 2025
700 K

REGISTRATION

Sponsored by: HUAWEI, APNIC, ISG, IIS, ISO, and others. Co-Managed by: and others.

- **Cyber Competition Final** – showcase of student and professional cybersecurity skills.
- **Incident Response Training** – hands-on simulations using NIST, SANS, and ISO frameworks.
- **Technical Workshops** – deep dives on CSIRT setup, SOC ops, research funding, and honeypots.
- **Cybersecurity Expo** – live demos of tools, solutions, and academic-industry innovations.
- **Networking Sessions** – cross-sector collaboration and knowledge sharing.
- **Field Visits / Industry Tours** – command center, IXPs, universities, and vendor facilities.
- **MoU Signing Ceremony** – formalizing partnerships among academia, industry, and government.
- **Closing & Awards** – reflections, competition winners, and VIP networking.

ACAD CSIRT Summit 2025 – The Event Gallery



ACAD CSIRT Summit 2025 – The Event Gallery



ACAD CSIRT Summit 2025 – The Winners

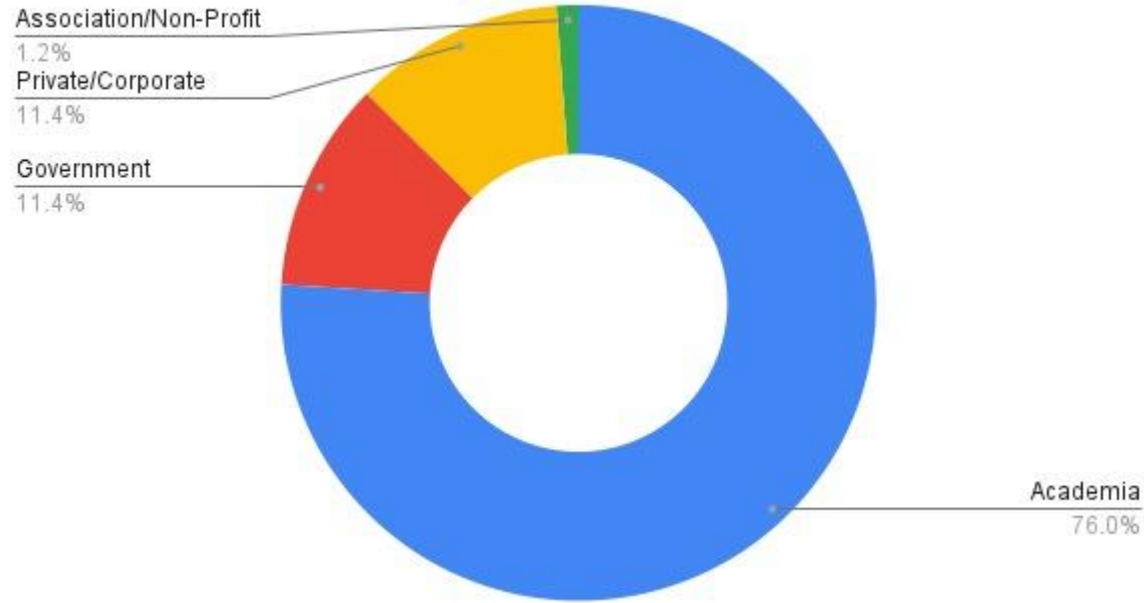


ACAD CSIRT Summit 2025 – Key Achievements

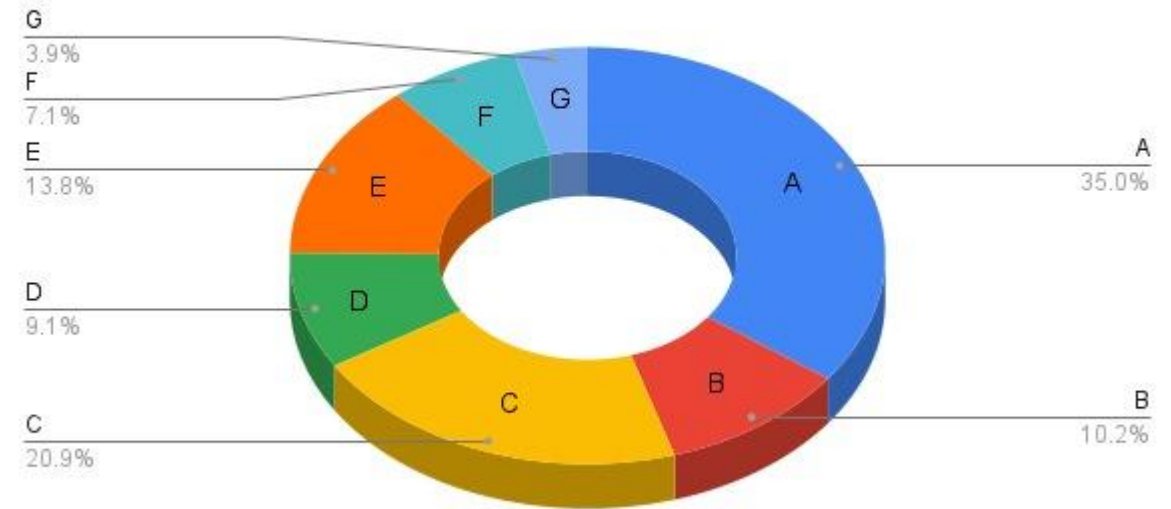
- **Incident Handling Training Impact:** Trained about 100 academics & professionals in incident handling (more than 300% than expected #s).
- **High Engagement IH Competition:** ACADefence 2025 drew 111 teams (247 individuals) - more than double the expected 50.
- **Diverse Winners:** Top 5 competition winners spanned military, government, academia, and cybersecurity services.
- **University Commitment:** 162 campuses committed to CSIRT formation, far surpassing the 50% participation goal.
- **Collaboration Highlight:** Summit reinforced public–private partnerships as vital for national cyber resilience.
- **People-Centric Focus:** Stressed academia’s role in empowering people as the core of sustainable cyber capacity.

ACAD CSIRT Summit 2025 – Some Stats

Summit & Workshop Participants (By Sectors)

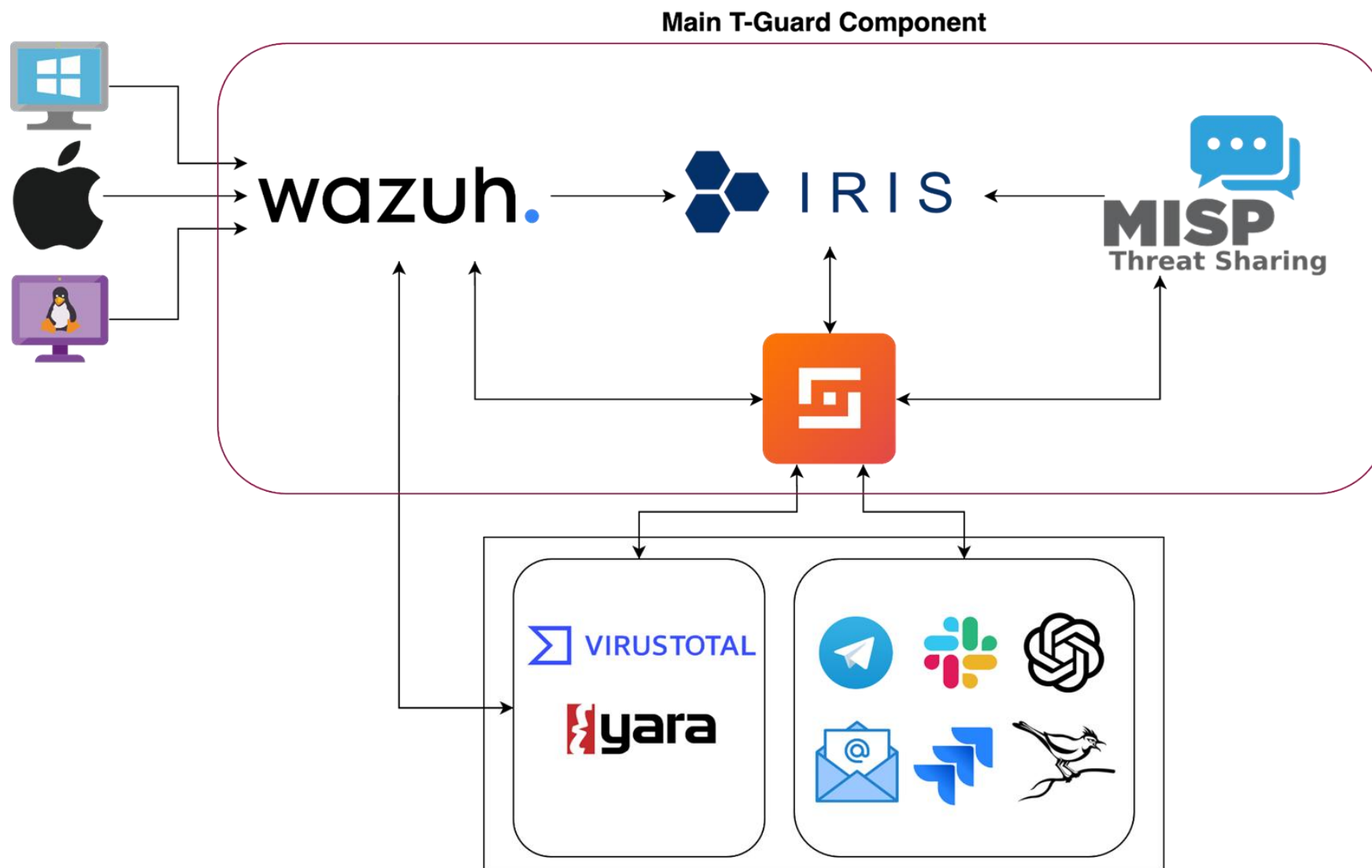


Workshop Participants By Track No. (%)



Why T-Guard?

Why T-Guard



Why T-Guard

- **Open & Cost-Efficient**
Built on open standards → avoids vendor lock-in & reduces license costs.
- **Unified Security Hub**
Collects logs & alerts from Windows, Linux, macOS into one SOC platform.
- **Threat Intelligence Built-In**
Integrated with **MISP**, **VirusTotal**, **YARA** for instant enrichment & detection.
- **Automated Response (SOAR-Lite)**
Connects with **Slack**, **Telegram**, **Email**, **Jira**, **AI-assistants** to cut response times.
- **Scalable Multi-Tenant Model**
Easily onboard multiple customers without heavy infra.
- **Streamline Installation**
With proper Internet connection, Installation can be done within an hour.

What ACAD CSIRT provides

- Low-cost yearly subscription for all universities (4500 universities in Indonesia)
- Start with Basic Notification Services
 - 5 endpoint (Starter package)
 - 1 month log retention (longer retention is possible when required)
- Threat Sharing among higher education



Simple Onboarding Workflow

Managed SOC for Education

University Registration & Service Agreement

1

University Details -

2

Technical Assessment -

3

Service Agreement -

4

Confirmation

Step 1: University & Contact Information

University Name

Full Address

Use Cases: Ransomware

Detection - RDP Brute-Force

1. The RDP brute force command triggered
2. Alert will be show up as follows:

Security Alerts						
	Time ↕	Technique(s)	Tactic(s)	Description	Level	Rule ID
3	Aug 28, 2024 @ 08:34:33.956	T1110	Credential Access	Multiple Windows logon failures.	10	60204
3	Aug 28, 2024 @ 08:34:30.253	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
3	Aug 28, 2024 @ 08:34:30.238	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
3	Aug 28, 2024 @ 08:34:28.662	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
3	Aug 28, 2024 @ 08:34:26.625	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
3	Aug 28, 2024 @ 08:34:22.906	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
3	Aug 28, 2024 @ 08:34:19.284	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
3	Aug 28, 2024 @ 08:34:15.630	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
3	Aug 28, 2024 @ 08:34:14.571	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
3	Aug 28, 2024 @ 08:34:11.928	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122

Detection - Script & File Creation

1. The Lockbit file executed
2. Alert will be show up as follows:

Security Alerts						
Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID	
> Aug 28, 2024 @ 11:12:13.834	T1059 T1105	Execution, Command and Control	Scripting file created under Windows Temp or User folder	6	92200	
> Aug 28, 2024 @ 11:12:13.786	T1059 T1105	Execution, Command and Control	Scripting file created under Windows Temp or User folder	6	92200	
> Aug 28, 2024 @ 11:12:13.462	T1059 T1105	Execution, Command and Control	Scripting file created under Windows Temp or User folder	6	92200	
> Aug 28, 2024 @ 11:12:13.379	T1059 T1105	Execution, Command and Control	Scripting file created under Windows Temp or User folder	6	92200	
> Aug 28, 2024 @ 11:15:56.334	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032	
> Aug 28, 2024 @ 11:15:55.645	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032	
> Aug 28, 2024 @ 11:15:55.574	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032	
> Aug 28, 2024 @ 11:15:55.495	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032	
> Aug 28, 2024 @ 11:15:55.437	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032	
> Aug 28, 2024 @ 11:15:55.378	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032	

Detection - Command & Control

1. With the Lockbit file executed
2. Alert will be show up as follows:

Security Alerts						
Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID	
> Aug 28, 2024 @ 11:19:19.056	T1070.001	Defense Evasion	Multiple Registry Keys created in Event Viewer on WIN-F6NF7R6I6PJ. Possible Ransomware Activity.	10	100032	
> Aug 28, 2024 @ 11:19:09.011	T1070.001	Defense Evasion	Multiple Registry Keys created in Event Viewer on WIN-F6NF7R6I6PJ. Possible Ransomware Activity.	10	100032	
> Aug 28, 2024 @ 11:18:59.030	T1070.001	Defense Evasion	Multiple Registry Keys created in Event Viewer on WIN-F6NF7R6I6PJ. Possible Ransomware Activity.	10	100032	
> Aug 28, 2024 @ 11:18:49.029	T1070.001	Defense Evasion	Multiple Registry Keys created in Event Viewer on WIN-F6NF7R6I6PJ. Possible Ransomware Activity.	10	100032	
> Aug 28, 2024 @ 11:18:39.081	T1070.001	Defense Evasion	Multiple Registry Keys created in Event Viewer on WIN-F6NF7R6I6PJ. Possible Ransomware Activity.	10	100032	
> Aug 28, 2024 @ 11:18:29.016	T1070.001	Defense Evasion	Multiple Registry Keys created in Event Viewer on WIN-F6NF7R6I6PJ. Possible Ransomware Activity.	10	100032	
> Aug 28, 2024 @ 11:18:19.037	T1070.001	Defense Evasion	Multiple Registry Keys created in Event Viewer on WIN-F6NF7R6I6PJ. Possible Ransomware Activity.	10	100032	

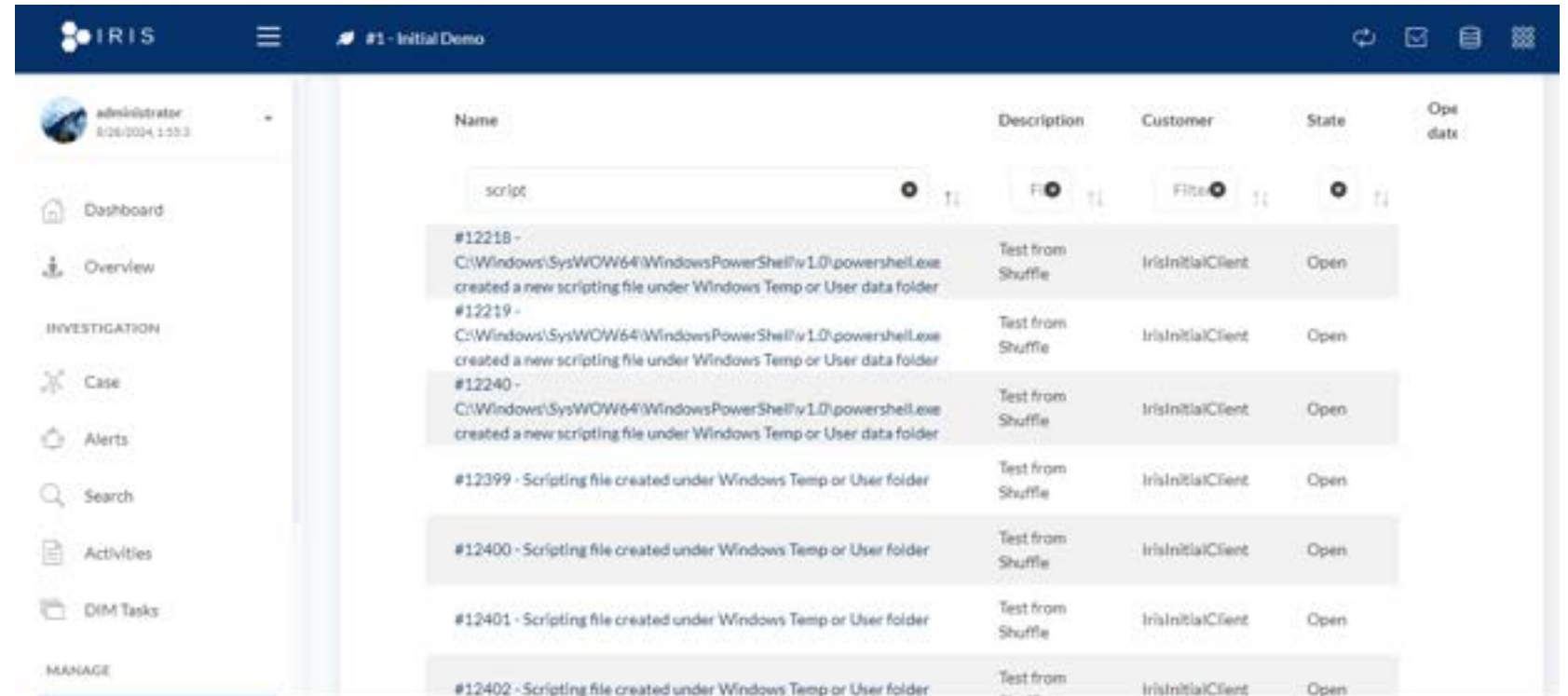
Auto-Ticketing

1. Open IRIS:
[https://\[IP_Address\]:8443](https://[IP_Address]:8443)

1. Click **Manage Cases** in the left panel

1. Choose **Cases List**

1. Ticket already created automatically



The screenshot shows the IRIS web interface. The top navigation bar is dark blue with the IRIS logo, a menu icon, and the text "#1 - Initial Demo". On the left, a sidebar contains a user profile for "administrator" and a list of navigation items: Dashboard, Overview, INVESTIGATION (with sub-items Case, Alerts, Search, Activities, DIM Tasks), and MANAGE. The main content area displays a table of cases. The table has columns for Name, Description, Customer, State, and Open date. A search bar with the text "script" is visible above the table. The table contains several rows of case data, all with a state of "Open".

Name	Description	Customer	State	Open date
#12218 - C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe created a new scripting file under Windows Temp or User data folder	Test from Shuffle	IrisInitialClient	Open	
#12219 - C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe created a new scripting file under Windows Temp or User data folder	Test from Shuffle	IrisInitialClient	Open	
#12240 - C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe created a new scripting file under Windows Temp or User data folder	Test from Shuffle	IrisInitialClient	Open	
#12399 - Scripting file created under Windows Temp or User folder	Test from Shuffle	IrisInitialClient	Open	
#12400 - Scripting file created under Windows Temp or User folder	Test from Shuffle	IrisInitialClient	Open	
#12401 - Scripting file created under Windows Temp or User folder	Test from Shuffle	IrisInitialClient	Open	
#12402 - Scripting file created under Windows Temp or User folder	Test from Shuffle	IrisInitialClient	Open	

Use Cases: Web Defacement

Wazuh Alert & Detection

When SQL Injection is performed

On the **Security Monitoring**

Wazuh detects the action

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Aug 27, 2024 @ 00:42:45.951	002	vm-demo	T1190	Initial Access	SQL injection attempt.	7	31103
Table	JSON	Rule					
@timestamp	2024-08-26T17:42:45.951Z						
GeoLocation.country_name	United States						
GeoLocation.location.lat	37.751						
GeoLocation.location.lon	-97.822						
_id	IA6j5EBEvO7gcDnmbf7						
agent.id	002						
agent.ip	159.223.68.187						
agent.name	vm-demo						
data.id	404						
data.protocol	GET						
data.srcip	159.223.68.187						
data.url	/users/?id=SELECT+++FROM+users						
decoder.name	web-accesslog						
full_log	159.223.68.187 - - [26/Aug/2024:17:42:44 +0000] "GET /users/?id=SELECT+++FROM+users HTTP/1.1" 404 437 "-" "curl/7.81.0"						
_id	1724694185.11033692						

Wazuh Alert & Detection

When there is modification
on Apache Directory

On the **Security Monitoring**

Wazuh detects the action

Aug 27, 2024 @ 10:17:33.763	002	VM-Research	T1105	T1505	Command and Control, Persistence	[File creation]: Possible web shell scripting file (/var/www/html/webshell-script2.php) created	12	100500
Table	JSON	Rule						
@timestamp	2024-08-27T03:17:33.763Z							
_id	ROLWkZEBUxoeAUCPzJOB							
agent.id	002							
agent.ip	192.168.1.4							
agent.name	VM-Research							
decoder.name	syscheck_new_entry							
full_log	File '/var/www/html/webshell-script2.php' added Mode: whodata							
id	1724728653.16245							
input.type	log							
location	syscheck							
manager.name	wazuh.manager							
rule.description	[File creation]: Possible web shell scripting file (/var/www/html/webshell-script2.php) created							

Web Defacement – Auto-Ticketing

On IRIS:

[https://\[IP_Address\]:8443](https://[IP_Address]:8443)

On the **Manage Cases** in the left panel

Cases List shows all the cases automatically created during the detection

This includes: Malware detection ticket automatically created

The screenshot shows the IRIS web interface. The top navigation bar includes the IRIS logo, a menu icon, and the text '#1 - Initial Demo'. The left sidebar contains a user profile for 'administrator' and a list of navigation items: Dashboard, Overview, INVESTIGATION (Case, Alerts, Search, Activities, DIM Tasks), and MANAGE (Manage cases). The main content area is titled 'Cases management' and features a 'New' button and a 'Cases list' button. Below these is a 'Refresh' button and a search bar. A table displays a list of cases with the following columns: Name, Description, Customer, State, Open date, Close date, SOC Ticket, and Opening user. The table shows two cases, both with the description 'File modified in /root directory.' and the state 'Open'. The first case has the name '#1001 - File modified in /root directory.', the customer 'IrisInitialClient', the open date '05/18/2024', the SOC ticket '123', and the opening user 'administrator'. The second case has the name '#113 - File modified in /root directory.', the customer 'IrisInitialClient', the open date '05/18/2024', the SOC ticket '123', and the opening user 'administrator'. A third case is partially visible at the bottom with the name '#117 - File modified in /root directory.'.

Name	Description	Customer	State	Open date	Close date	SOC Ticket	Opening user
#1001 - File modified in /root directory.	File modified in /root directory.	IrisInitialClient	Open	05/18/2024		123	administrator
#113 - File modified in /root directory.	File modified in /root directory.	IrisInitialClient	Open	05/18/2024		123	administrator
#117 - File modified in /root directory.	File modified in /root directory.						

Early Adopters

Early Adopters

ACADCSIRT



Key Takeaways

- 162 campuses signed up to initiate CSIRT programs, with a target of 500 new sign-ups annually.
- 5 early adopters engaged as the first institutions to begin active asset monitoring.
- Launched with basic service, incident notifications as the entry point.
- Campus visits organized in clusters to accelerate onboarding and implementation across regions.

Questions & Answers (Q&A)

