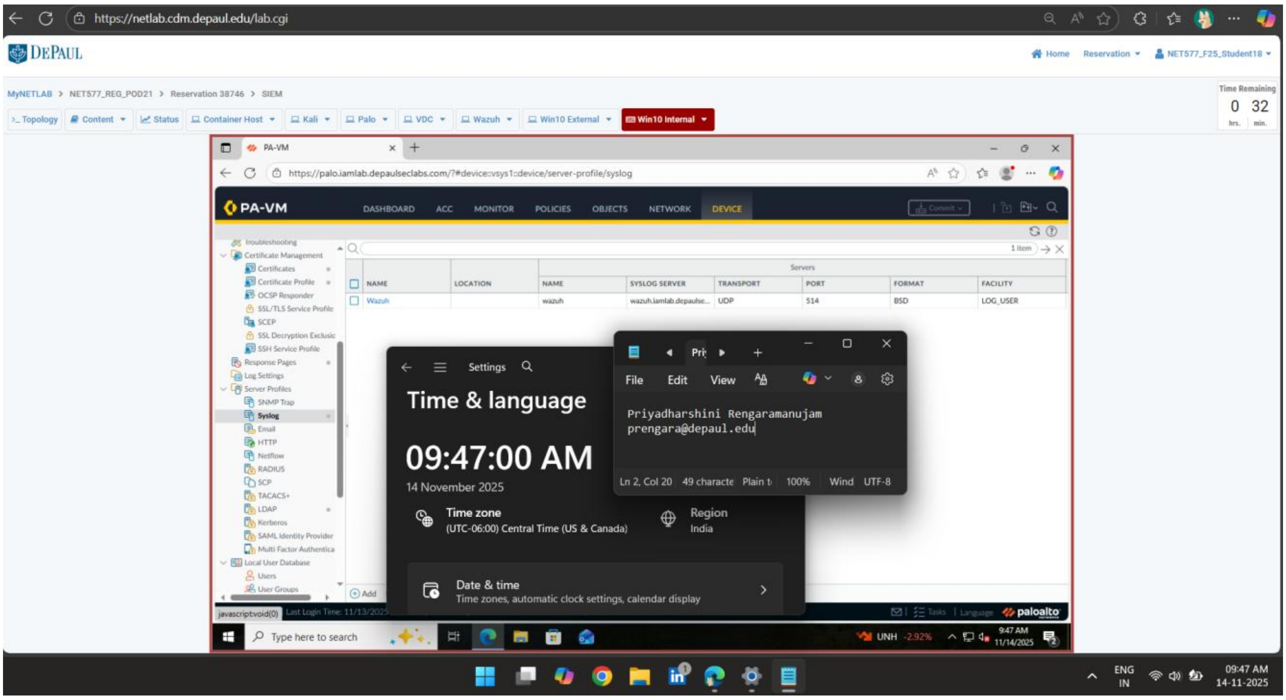
NET_577_LAB 7_SIEM

Priyadharshini Rengaramanujam

1. Syslog server profile on the Palo



https://palo.iamlab.depaulseclabs.com/?#device::vsys1::device/server-profile/syslog

☐	NAME	LOCATION	Servers NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
☐	Wazuh		wazuh	wazuh.iamlab.depaulse...	UDP	514	BSD	LOG_USER

```
Priyadharshini Rengaramanujam
prengara@depaul.edu
```

Time & language

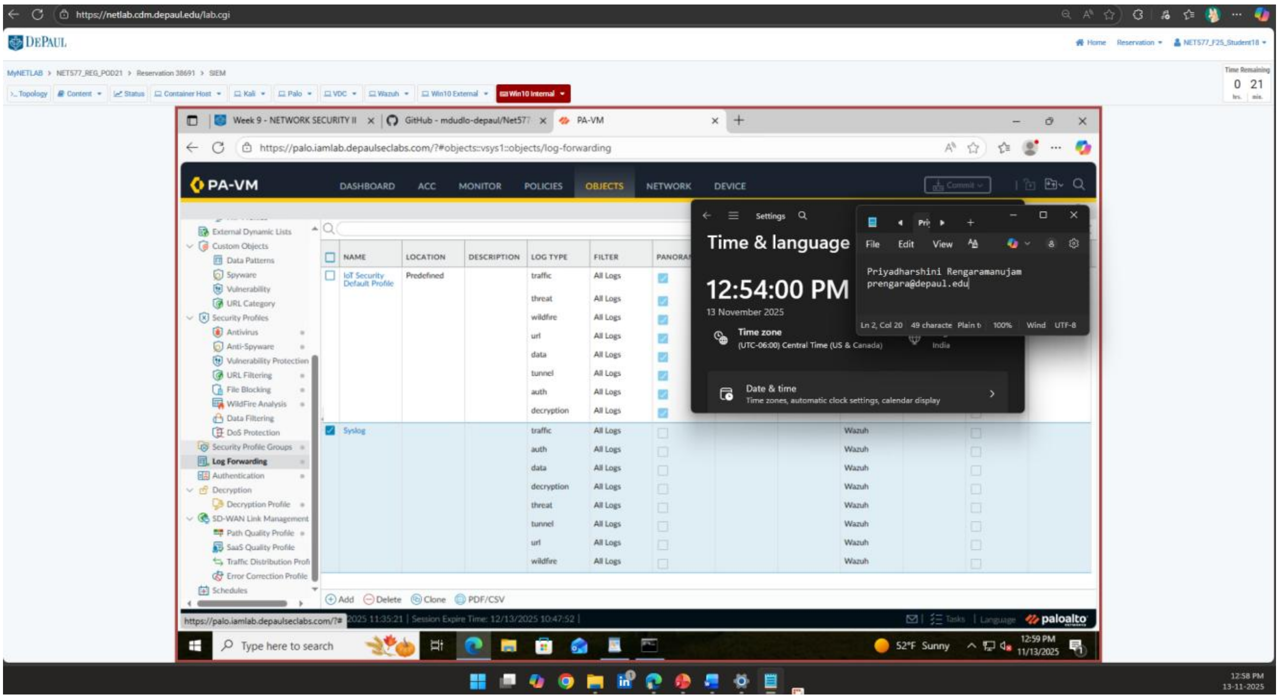
09:47:00 AM

14 November 2025

Time zone (UTC-06:00) Central Time (US & Canada)

Region India

2. Log forwarding object on the Palo



https://palo.iamlab.depaulseclabs.com/?#objects::vsys1::objects/log-forwarding

☐	NAME	LOCATION	DESCRIPTION	LOG TYPE	FILTER	PANORA	
☐	IoT Security Default Profile	Predefined		traffic	All Logs	☑	
				threat	All Logs	☑	
				wildfire	All Logs	☑	
				url	All Logs	☑	
				data	All Logs	☑	
				tunnel	All Logs	☑	
				auth	All Logs	☑	
				decryption	All Logs	☑	
☑	Syslog			traffic	All Logs	☐	Wazuh
				auth	All Logs	☐	Wazuh
				data	All Logs	☐	Wazuh
				decryption	All Logs	☐	Wazuh
				threat	All Logs	☐	Wazuh
				tunnel	All Logs	☐	Wazuh
				url	All Logs	☐	Wazuh
				wildfire	All Logs	☐	Wazuh

```
Priyadharshini Rengaramanujam
prengara@depaul.edu
```

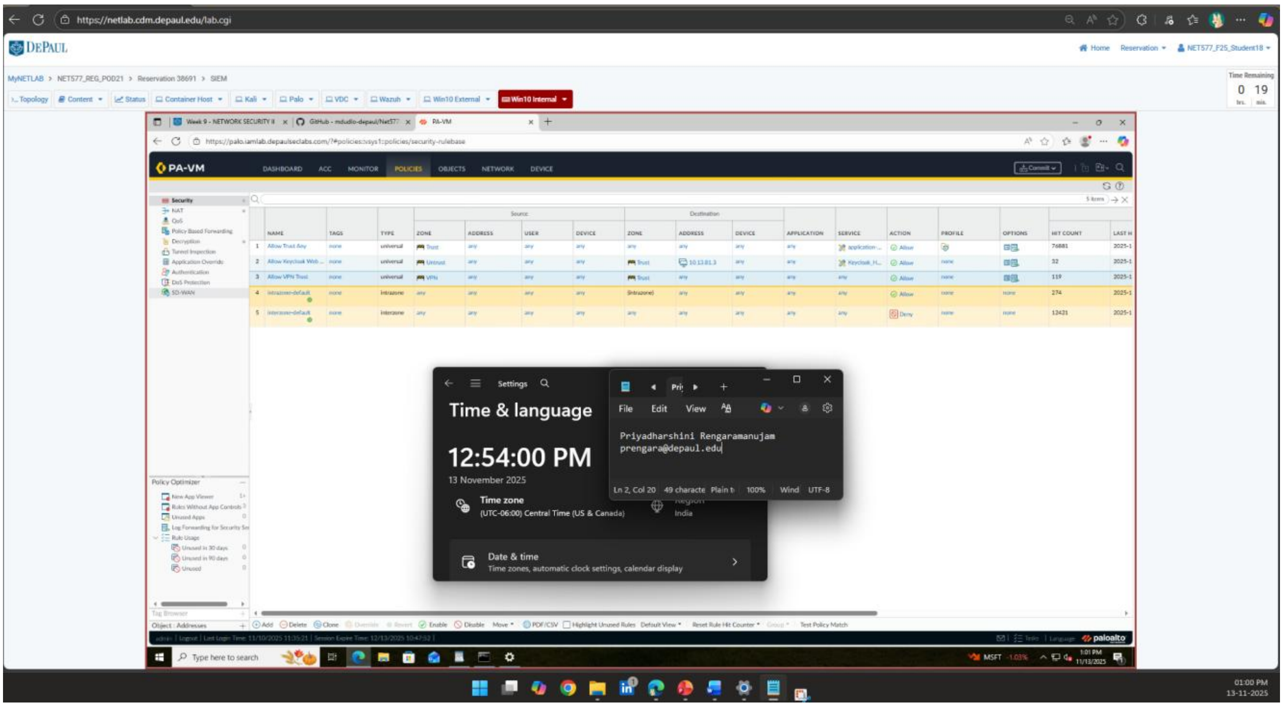
Time & language

12:54:00 PM

13 November 2025

Time zone (UTC-06:00) Central Time (US & Canada)

3. Firewalls rules configured to send syslog



https://palo.iamlab.depaulseclabs.com/?#policies::vsys1::policies/security-rulebase

	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT
1	Allow Trust Any	none	universal	Trust	any	any	any	any	any	any	any	application-...	Allow			76881
2	Allow Keycloak Web ...	none	universal	Untrust	any	any	any	Trust	10.13.81.3	any	any	Keycloak_H...	Allow	none		32
3	Allow VPN Trust	none	universal	VPN	any	any	any	Trust	any	any	any	any	Allow	none		119
4	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none	none	274
5	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	none	none	12421

Time & language

12:54:00 PM

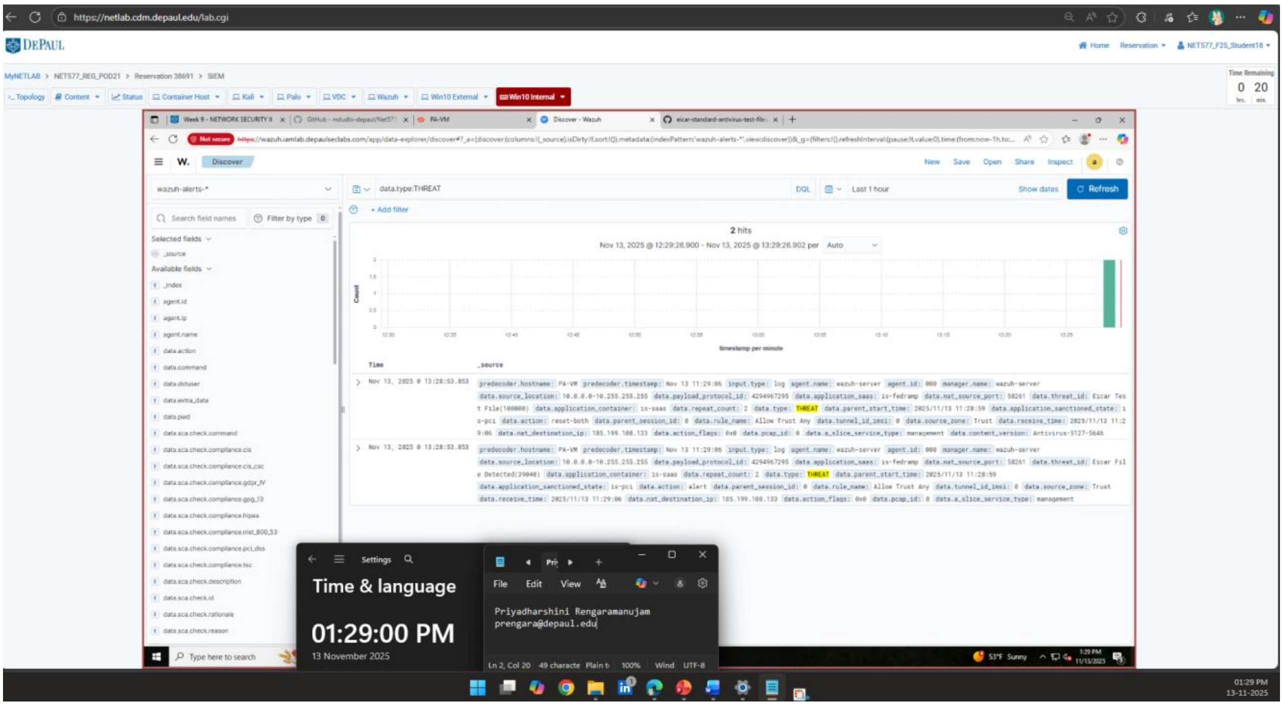
13 November 2025

Time zone (UTC-06:00) Central Time (US & Canada)

Date & time — Time zones, automatic clock settings, calendar display

```
Priyadharshini Rengaramanujam
prengara@depaul.edu
```

4. Blocked malware log in Wazuh (data.type:THREAT)



```
wazuh-alerts-*    data.type:THREAT    Last 1 hour

2 hits
Nov 13, 2025 @ 12:29:26.900 - Nov 13, 2025 @ 13:29:26.902 per Auto

Time                        _source
> Nov 13, 2025 @ 13:28:53.853  predecoder.hostname: PA-VM predecoder.timestamp: Nov 13 11:29:06 input.type: log agent.name: wazuh-server agent.id: 000 manager.name: wazuh-server
data.source_location: 10.0.0.0-10.255.255.255 data.payload_protocol_id: 4294967295 data.application_saas: is-fedramp data.nat_source_port: 58261 data.threat_id: Eicar Tes
t File(100000) data.application_container: is-saas data.repeat_count: 2 data.type: THREAT data.parent_start_time: 2025/11/13 11:28:59 data.application_sanctioned_state: i
s-pci data.action: reset-both data.parent_session_id: 0 data.rule_name: Allow Trust Any data.tunnel_id_imsi: 0 data.source_zone: Trust data.receive_time: 2025/11/13 11:2
9:06 data.nat_destination_ip: 185.199.108.133 data.action_flags: 0x0 data.pcap_id: 0 data.a_slice_service_type: management data.content_version: Antivirus-5127-5646
> Nov 13, 2025 @ 13:28:53.853  predecoder.hostname: PA-VM predecoder.timestamp: Nov 13 11:29:06 input.type: log agent.name: wazuh-server agent.id: 000 manager.name: wazuh-server
data.source_location: 10.0.0.0-10.255.255.255 data.payload_protocol_id: 4294967295 data.application_saas: is-fedramp data.nat_source_port: 58261 data.threat_id: Eicar Fil
e Detected(39040) data.application_container: is-saas data.repeat_count: 2 data.type: THREAT data.parent_start_time: 2025/11/13 11:28:59
data.application_sanctioned_state: is-pci data.action: alert data.parent_session_id: 0 data.rule_name: Allow Trust Any data.tunnel_id_imsi: 0 data.source_zone: Trust
data.receive_time: 2025/11/13 11:29:06 data.nat_destination_ip: 185.199.108.133 data.action_flags: 0x0 data.pcap_id: 0 data.a_slice_service_type: management
```

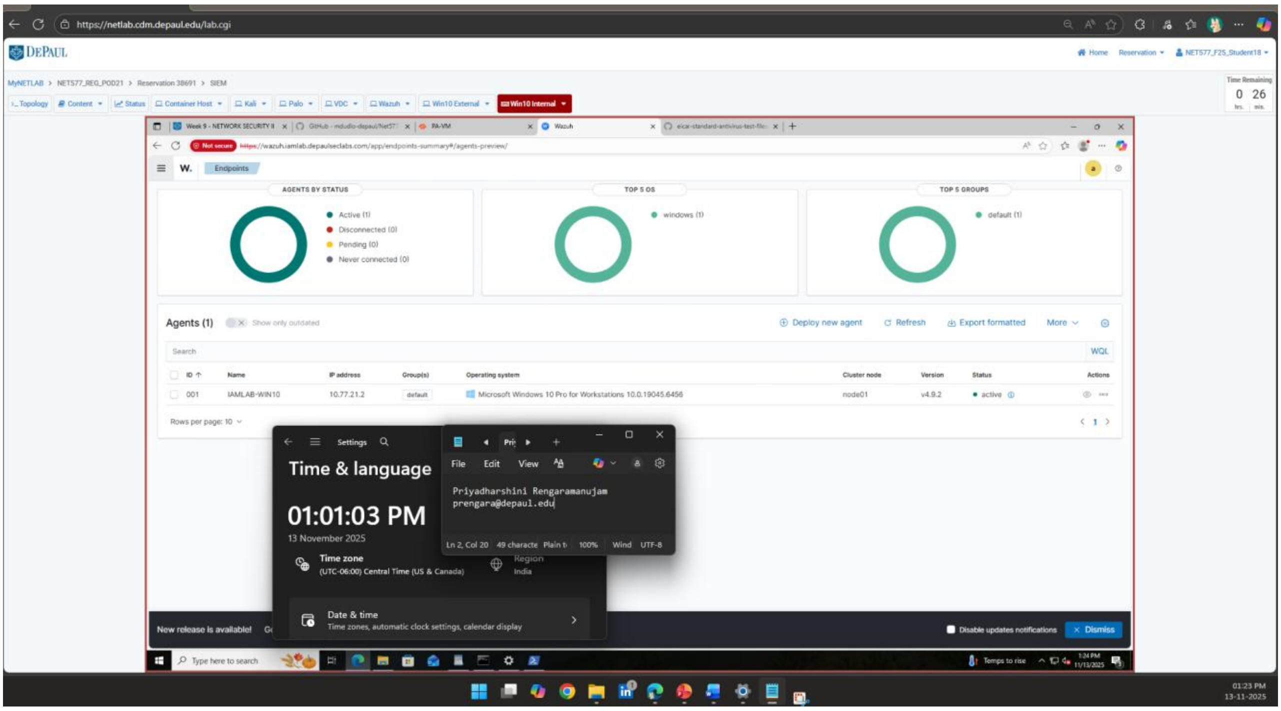
Time & language

01:29:00 PM

13 November 2025

```
Priyadharshini Rengaramanujam
prengara@depaul.edu
```

5. Endpoint in endpoint manager



https://netlab.cdm.depaul.edu/lab.cgi

MyNETLAB > NET577_REG_POD21 > Reservation 38691 > SIEM

https://wazuh.iamlab.depaulseclabs.com/app/endpoints-summary#/agents-preview/

AGENTS BY STATUS: ● Active (1) ● Disconnected (0) ● Pending (0) ● Never connected (0)

TOP 5 OS: ● windows (1)

TOP 5 GROUPS: ● default (1)

Agents (1)

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	IAMLAB-WIN10	10.77.21.2	default	Microsoft Windows 10 Pro for Workstations 10.0.19045.6456	node01	v4.9.2	● active	

Time & language

01:01:03 PM

13 November 2025

Time zone: (UTC-06:00) Central Time (US & Canada)

Region: India

Date & time: Time zones, automatic clock settings, calendar display

```
Priyadharshini Rengaramanujam
prengara@depaul.edu
```

New release is available!

Reflection Questions

1. What did you do in this lab that is beneficial in a production network when done on every network device?
   In this lab, configuring centralized logging through Syslog and integrating with a SIEM (Wazuh) is highly beneficial in a production environment. When applied to all network devices, it enables comprehensive visibility into network activity, security events, and potential threats. This centralized approach simplifies monitoring, supports faster incident detection and response, and aids in compliance reporting by aggregating logs from multiple sources into one platform for analysis.

2. What downsides are some potential downsides?
   The main downsides include increased network traffic and storage requirements due to continuous log forwarding from all devices. Additionally, misconfigured log forwarding or excessive logging can overwhelm the SIEM, leading to performance issues or alert fatigue. There is also a risk of sensitive data exposure if logs are not encrypted during transmission, and the setup requires ongoing maintenance and tuning to ensure accuracy and relevance of alerts.