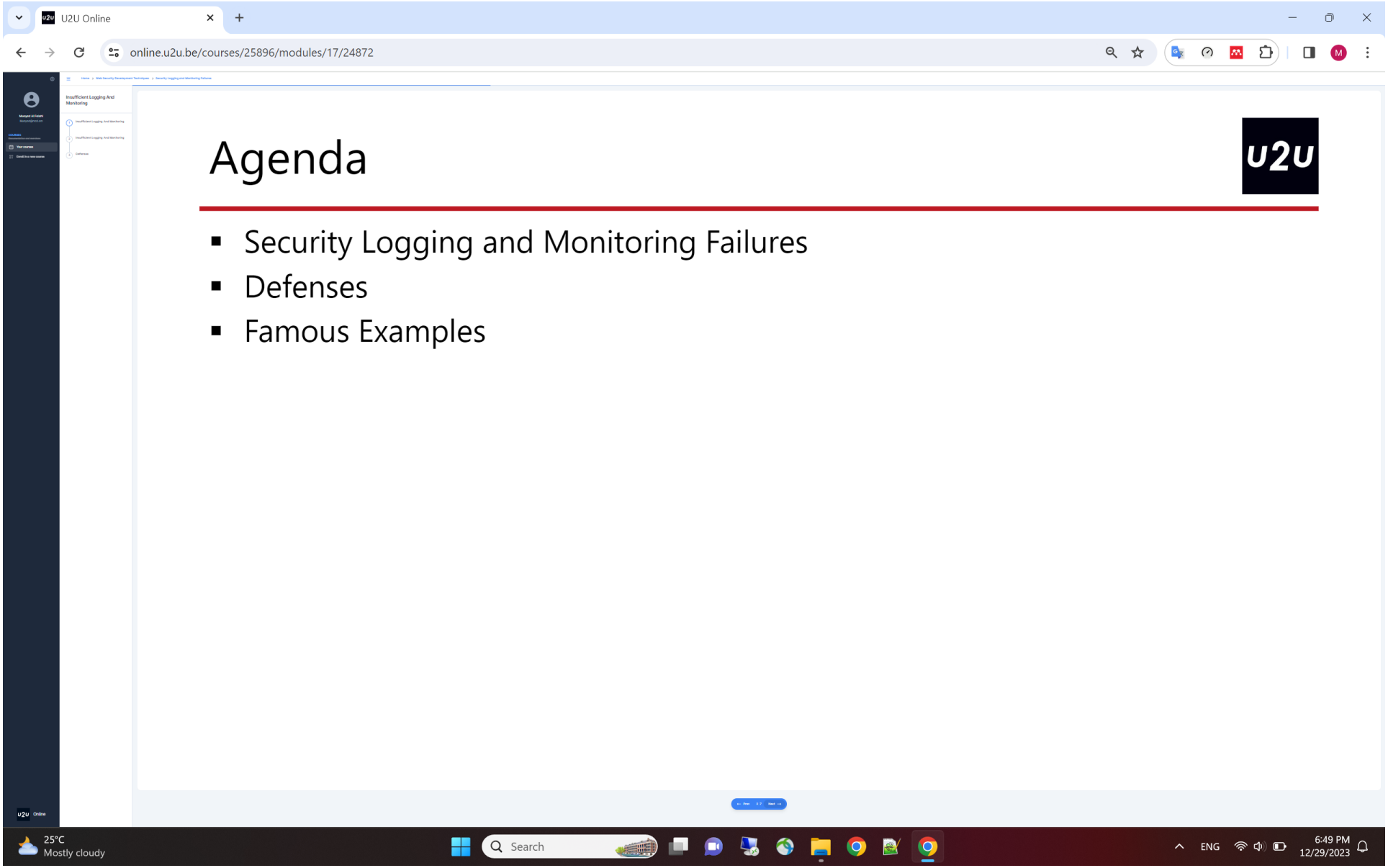
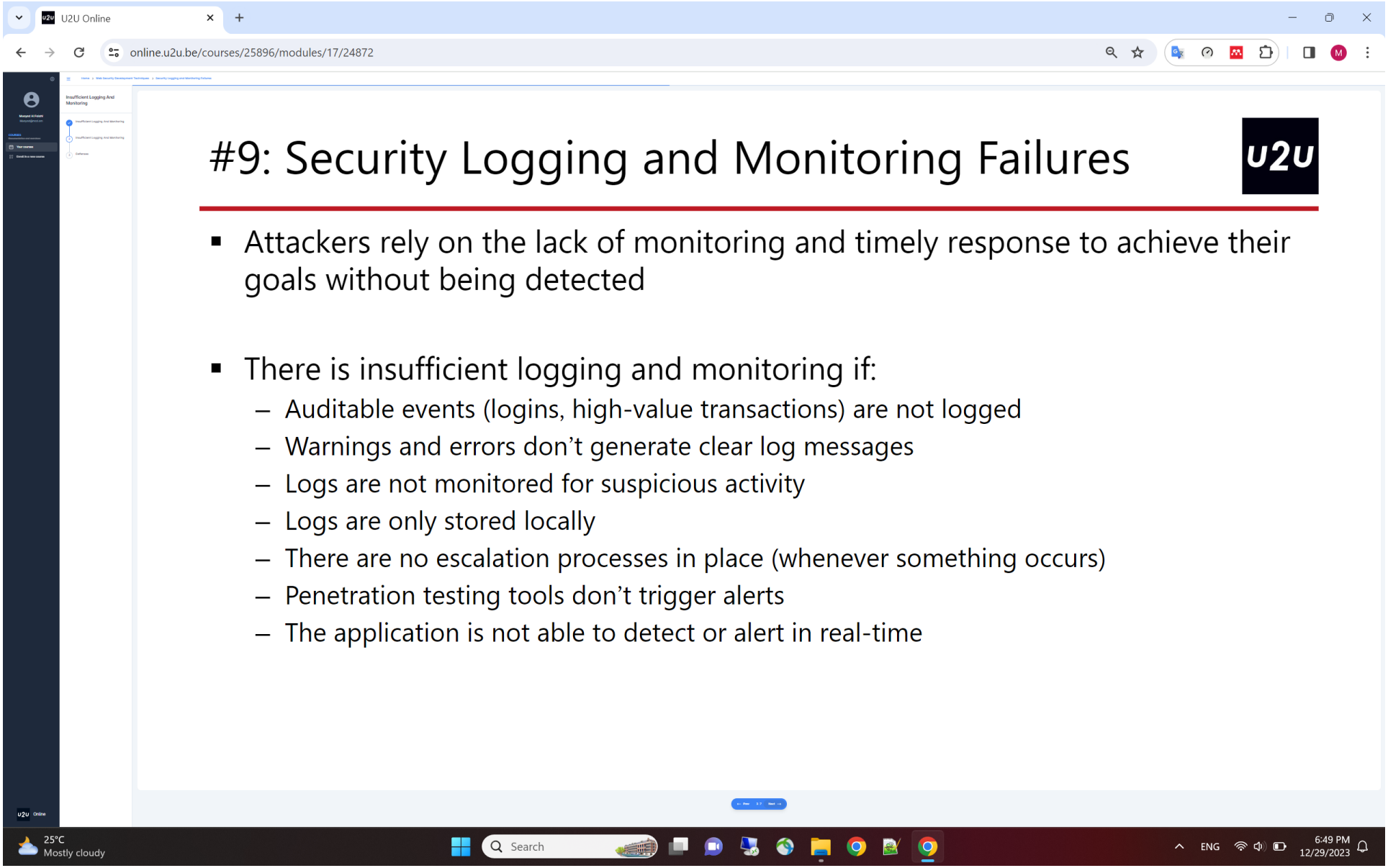
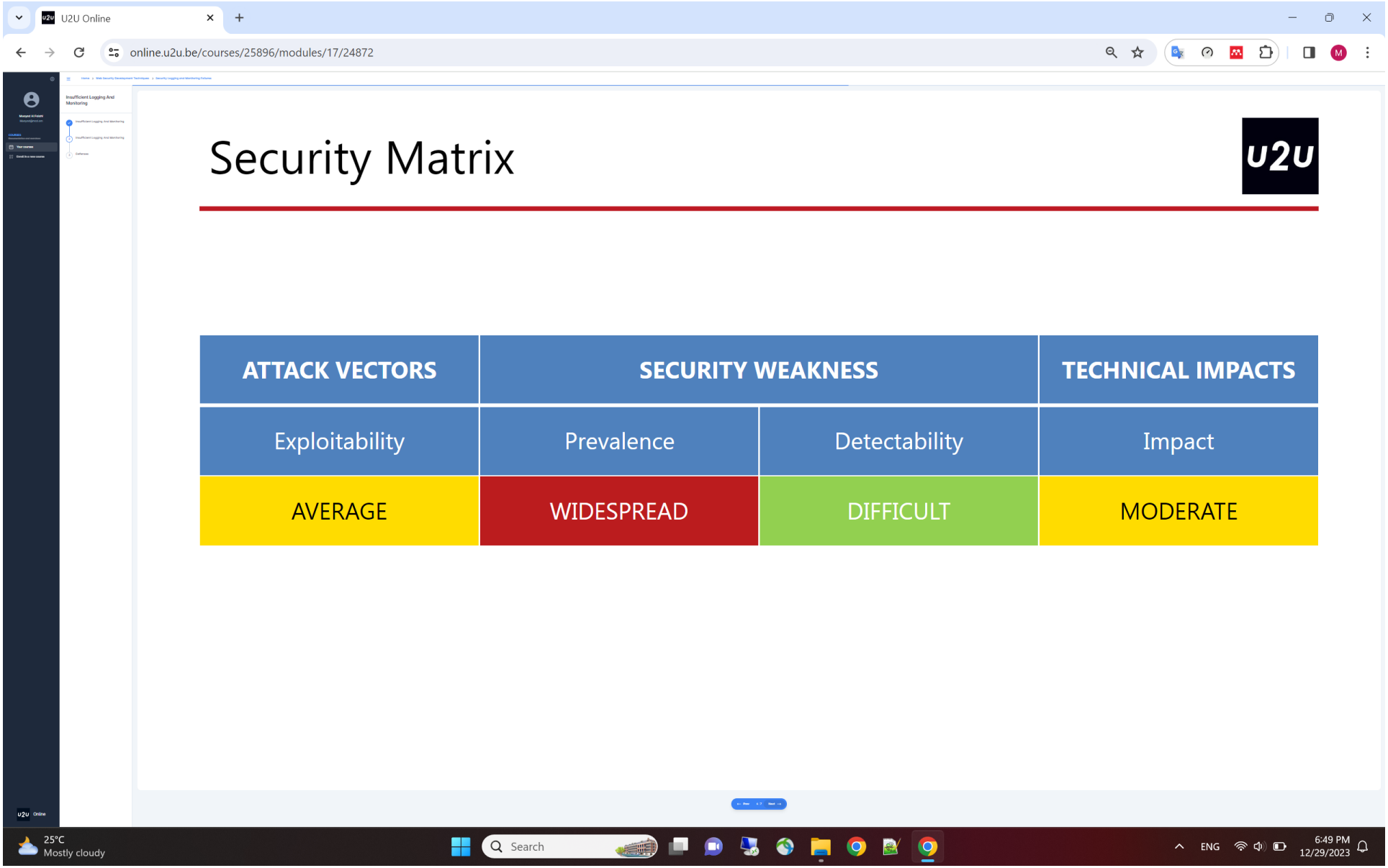
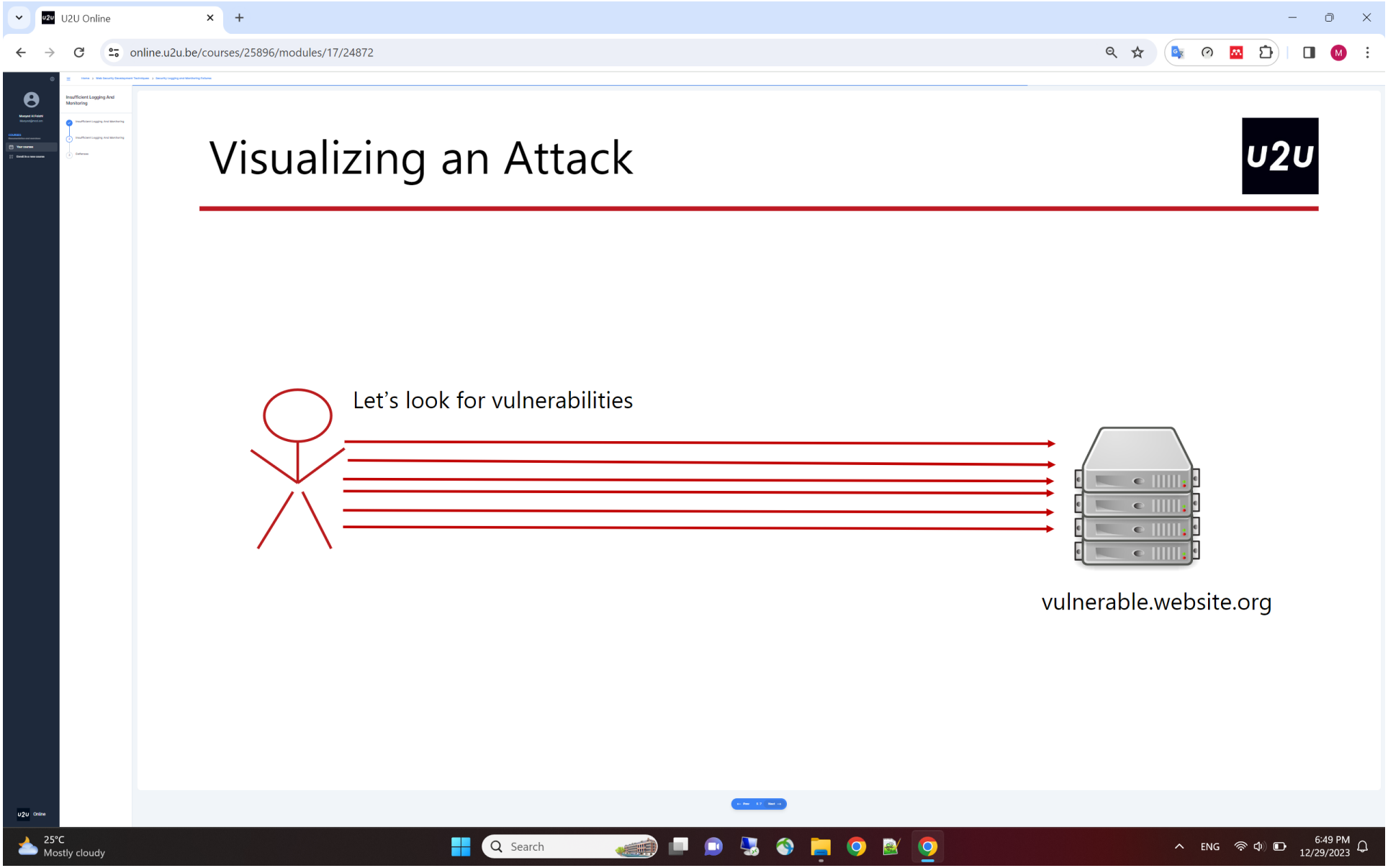
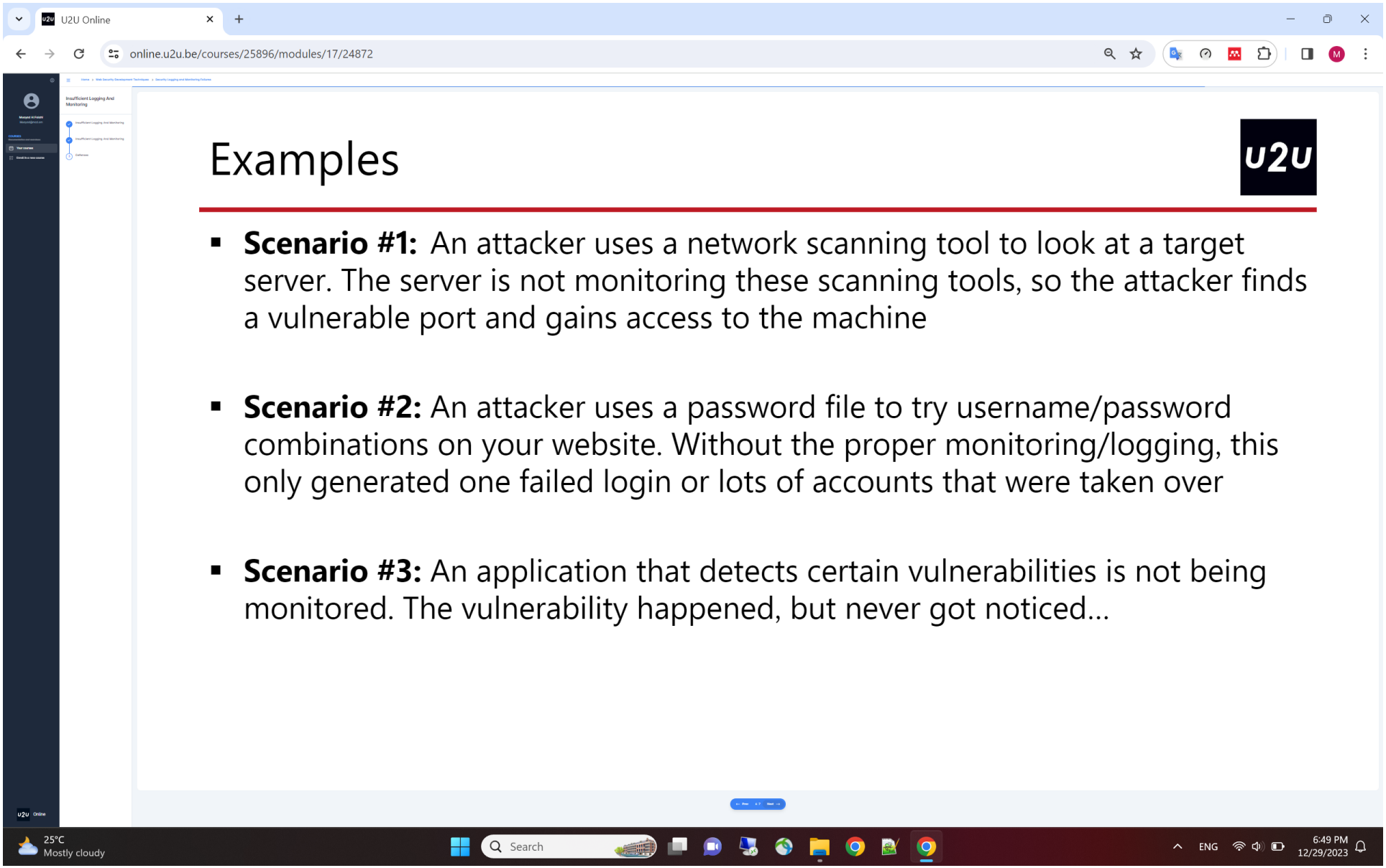

U2U Online
online.u2u.be/courses/25896/modules/17/24872
Developer and IT Training
u2u
Security Logging and Monitoring Failures
OWASP Web Security Threat #9
25°C
Mostly cloudy
Search
ENG
6:49 PM
12/29/2023

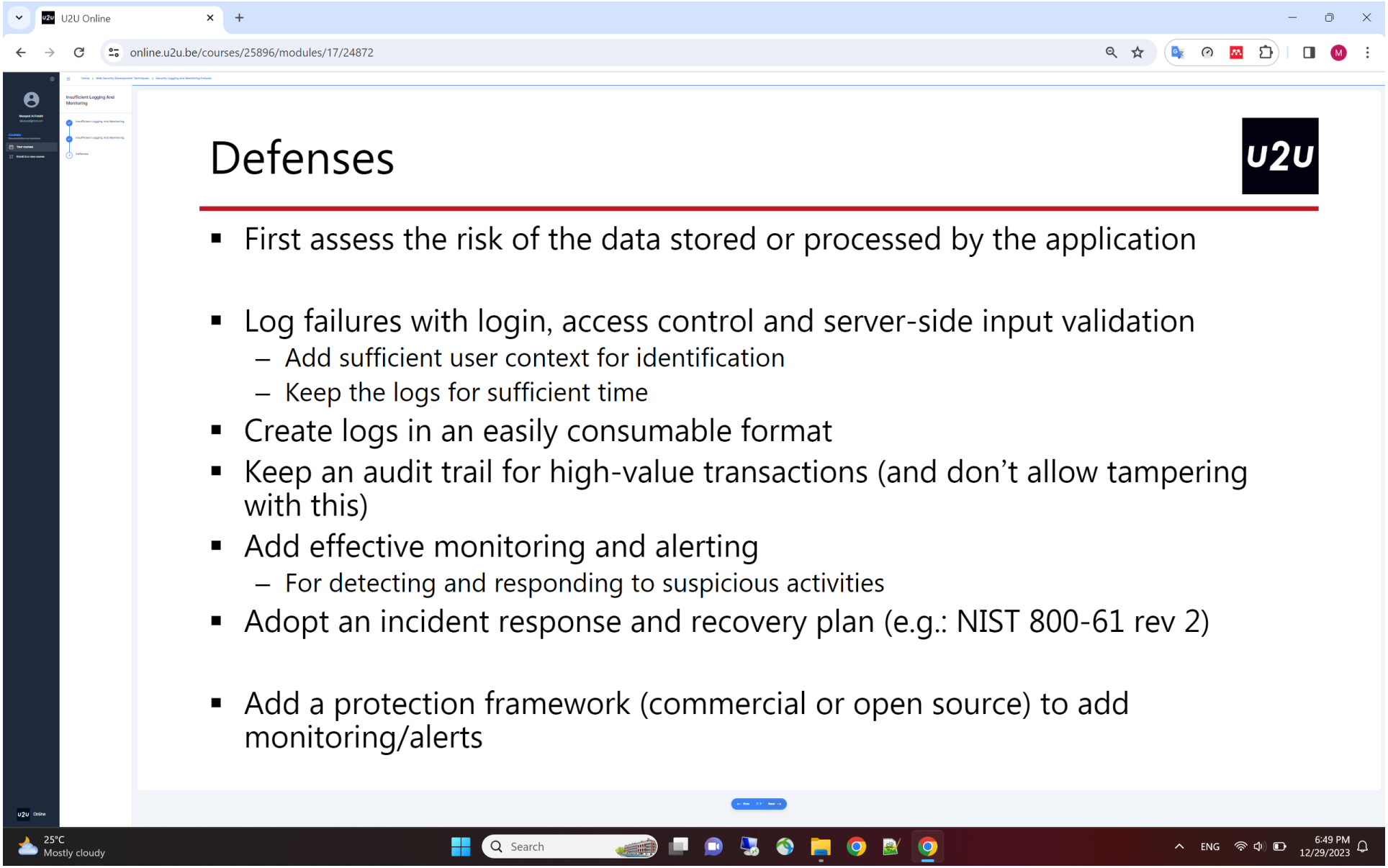

U2U Online
online.u2u.be/courses/25896/modules/17/24872
Insufficient Logging And Monitoring
Agenda
u2u
Security Logging and Monitoring Failures
Defenses
Famous Examples
25°C
Mostly cloudy
Search
ENG
6:49 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/17/24872
#9: Security Logging and Monitoring Failures
U2U
Attackers rely on the lack of monitoring and timely response to achieve their goals without being detected
There is insufficient logging and monitoring if:
– Auditable events (logins, high-value transactions) are not logged
– Warnings and errors don't generate clear log messages
– Logs are not monitored for suspicious activity
– Logs are only stored locally
– There are no escalation processes in place (whenever something occurs)
– Penetration testing tools don't trigger alerts
– The application is not able to detect or alert in real-time
25°C
Mostly cloudy
Search
ENG
6:49 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/17/24872
Insufficient Logging And Monitoring
Security Matrix
u2u
ATTACK VECTORS
SECURITY WEAKNESS
TECHNICAL IMPACTS
Exploitability
Prevalence
Detectability
Impact
AVERAGE
WIDESPREAD
DIFFICULT
MODERATE
25°C
Mostly cloudy
Search
ENG
6:49 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/17/24872
Insufficient Logging And Monitoring
Visualizing an Attack
u2u
Let's look for vulnerabilities
vulnerable.website.org
25°C
Mostly cloudy
Search
ENG
6:49 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/17/24872
Examples
U2U
Scenario #1: An attacker uses a network scanning tool to look at a target server. The server is not monitoring these scanning tools, so the attacker finds a vulnerable port and gains access to the machine
Scenario #2: An attacker uses a password file to try username/password combinations on your website. Without the proper monitoring/logging, this only generated one failed login or lots of accounts that were taken over
Scenario #3: An application that detects certain vulnerabilities is not being monitored. The vulnerability happened, but never got noticed…
25°C
Mostly cloudy
Search
ENG
6:49 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/17/24872
Defenses
U2U
First assess the risk of the data stored or processed by the application
Log failures with login, access control and server-side input validation
Add sufficient user context for identification
Keep the logs for sufficient time
Create logs in an easily consumable format
Keep an audit trail for high-value transactions (and don't allow tampering with this)
Add effective monitoring and alerting
For detecting and responding to suspicious activities
Adopt an incident response and recovery plan (e.g.: NIST 800-61 rev 2)
Add a protection framework (commercial or open source) to add monitoring/alerts
25°C
Mostly cloudy
Search
ENG
6:49 PM
12/29/2023