IEEE Al-balqa Applied University
Faculty of Engineering Technology

CIPHER

Notice when a device breaks its routine.

Learn normal activity. Explain unusual behavior.
Let the operator decide how to respond.

Zakaria Alqarra · Belal Hamdan · Raneem Abdullah · Ayham Idais

Contributor: Omar Eid

An allowed connection can still look unusual.

The laptop's routine

A few familiar services.
A familiar amount of traffic.

A sudden change

Many different service ports.
More rejected traffic.

A port is a service's "door". Trying many doors can be a scan.

Unusual does not automatically mean malicious.

Small summaries travel. Packets stay at the router.

Linux router	→	Rust sensor	→	Rust server	→	Dashboard
eBPF / XDP Traffic hook		Summarize metadata		Statistics + AI review		Review + respond

Sensor → server: FlatBuffers reports over a TLS WebSocket

Response returns to the sensor; the dashboard waits for acknowledgment.

Four signals describe a device's routine.

Incoming bytes	How much incoming payload was observed.
Outgoing bytes	How much outgoing payload was observed.
Dropped events	How many reported packet events were blocked.
Port entropy	How spread out the observed port use is.

These are sampled observations, not complete traffic totals.

Learn “normal”, then measure the difference.

50 reports

Build a baseline:
the usual level and variation
for each signal.

Deviation score

distance from the baseline
÷ expected variation

Above 3 on any signal → an alert

Example: a 24 KiB change ÷ 4 KiB scale = 6. Illustrative values.

Statistics raise the flag. AI adds an explanation.

Evidence in	Baseline, unusual measurements and recent reports.
Review out	An explanation, a block recommendation and a score.
Operator sees	Why it was flagged, what happened and what to review.

Model confidence is self-reported, not measured accuracy.

Automatic quarantine needs every gate to pass.

Cloud-reviewed isolation

Permission	Automatic mode is on; the device is not trusted.
Evidence	At least two statistical signals are abnormal.
Review	Valid AI review says block, with a score ≥ 85/100.
Fresh decision	Incident stays open; policy revision has not changed.

Default: monitor. A person can isolate, restore or trust a device.

Follow one laptop from alert to response.

Monitor	Simulate a scan. Read the alert and its evidence.
Allow response	Enable automatic mode; repeat and check the acknowledgment.
Trust + recover	Trust the device; test reviewer failure; reset the demo.

Real backend. Simulated sensor. Scripted offline reviewer.
The booth demonstration does not block real packets.

A working software demo. Hardware proof comes next.

Implemented + rehearsed

Statistical alerts + saved baselines
Trust + incident review
Command acknowledgments
Reconnect + retry handling

Still to measure

Actual gateway packet blocking
Correct traffic attribution
Missed attacks + false alarms
Speed, resource use + AI value

Meet The Four Horsemen.

PROJECT TEAM

Zakaria Alqarra

Belal Hamdan

Raneem Abdullah

Ayham Idais

Contributor: Omar Eid

CHOOSE A LAYER TO EXPLORE

Networks + Linux

Follow a packet through the router and its filters.

Rust + data

Trace one report from the sensor to an incident.

Testing + interface

Reproduce a scenario and make its evidence clearer.

Next: gateway testing, security review and small-office pilot feedback.

https://belalhamdan.com/cipher/