GEORGE MASON UNIVERSITY

CYSE 587 Project: EverWatch

Cybersecurity Systems Engineering Tool for OpenEMR

Anthony Palma, Matt Manganello, Geetha Meka, Justin Rockwell, Neil Sharma, Christine Ziu

Group 4

May 6th 2026

Agenda

THE PROBLEM: LOGS EXIST, OVERSIGHT LAGS

SYSTEM CLARITY: WHAT EVERWATCH IS AND IS NOT

THREAT AND RISK REASONING

ARCHITECTURE AND OPENEMR INTEGRATION

FEASIBILITY, VALUE, AND INNOVATION

DEMO V2: EVERWATCH IN ACTION

The Problem: The Logs Are There. The Oversight Is Not.

“OpenEMR can record activity, but evidence does not automatically become oversight.”

The Problem: Why Raw Logs Are Not Enough

Problem	Why it matters
Too much activity	Reviewers cannot manually inspect every event
Weak context	Logs show actions, but not always risk
Delayed review	Misuse may go unnoticed until after harm
Valid-account misuse	Bad activity can look like normal access
Healthcare pressure	Emergency workflows make review harder

System Clarity: Boundary, Stakeholders, and Context

Boundary

- **EverWatch does:**
  - Run outside OpenEMR
  - Analyze approved logs and telemetry
  - Produce alerts and review summaries
  - Support human oversight
- **EverWatch does not:**
  - Modify OpenEMR
  - Block care
  - Change workflows
  - Replace the EMR

Stakeholders

- IT and security teams
- Privacy and compliance officers
- Hospital leadership
- Clinicians and nurses
- Patients
- Regulators and auditors

Operating Context

- 24/7 clinical operations
- High-pressure care workflows
- Strict privacy and compliance rules
- Limited ability to change core systems
- Mixed user trust levels

Threat Analysis

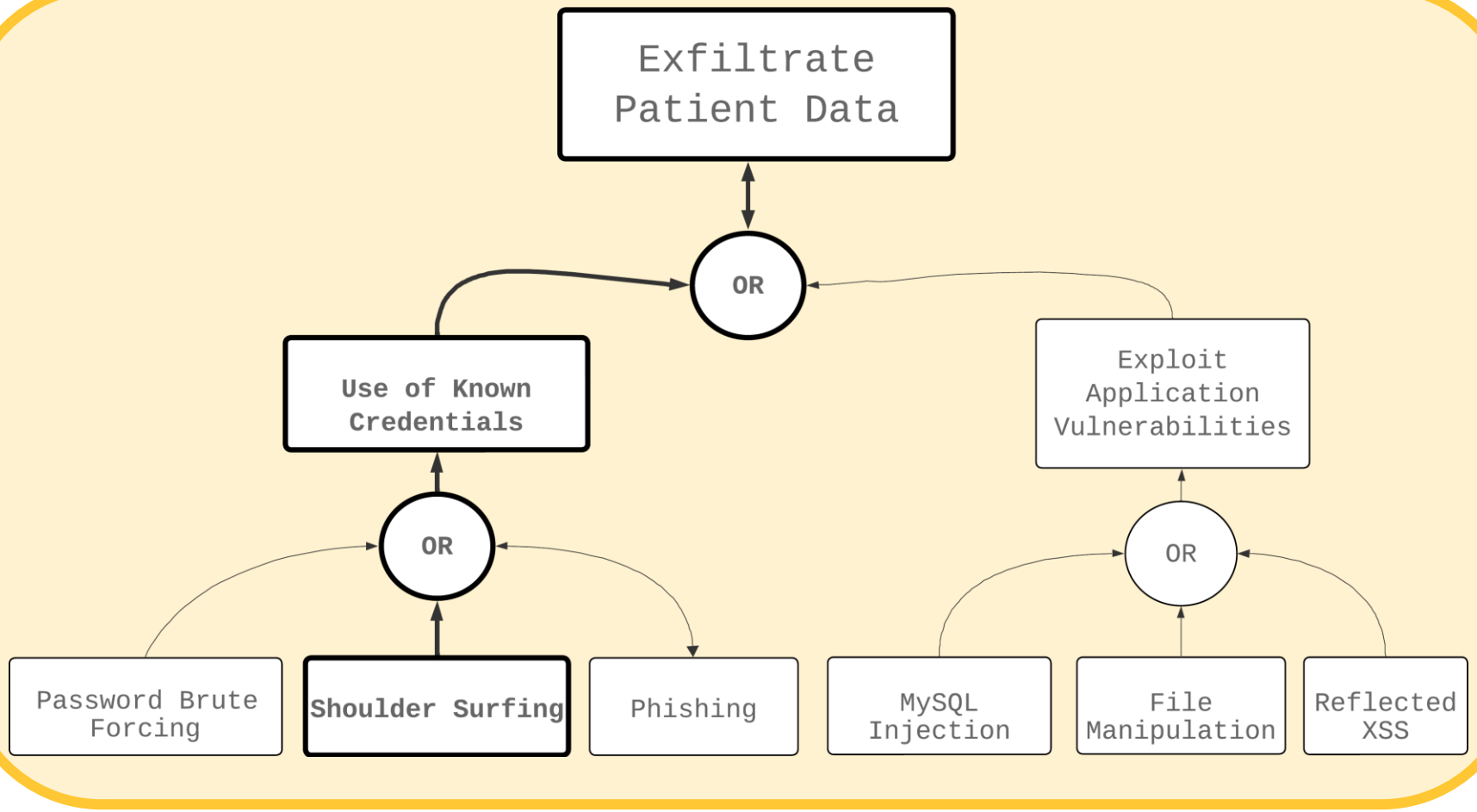
Core Trust Assumptions:

- Generated logs are correct
- Path between the OpenEMR and Everwatch is secure
- Relying on people to review alerts

Risk Propagation:

- Detection failure leads directly to mass HIPAA violations
- If a breach remains undetected, an attacker could tamper with clinical data.
- Breaches can affect trust between the hospital and the community.

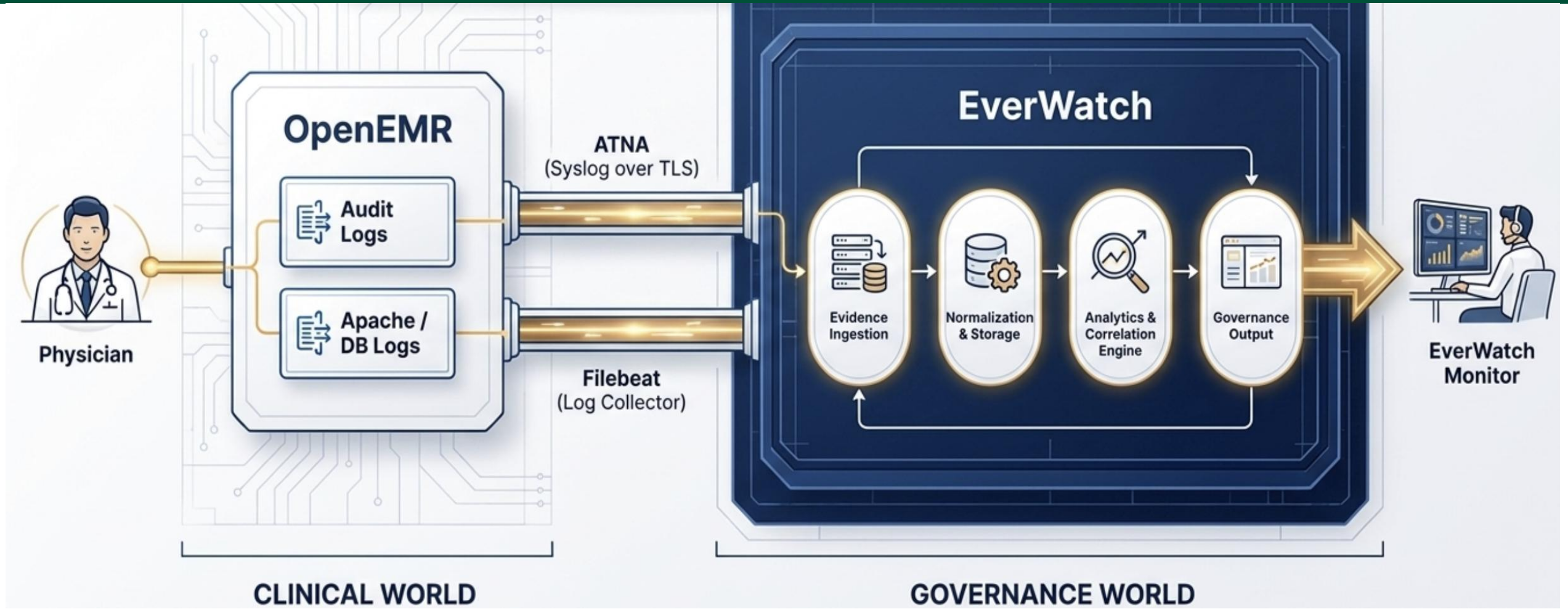
Threat Analysis



Threat and Attack surfaces:

- Actors will prioritize in exporting patient data
- One path is using known credentials

EverWatch Architecture Overview



Architecture Design Feasibility

Requirement	Solution
(Realistic) How easy is it to begin integrating EverWatch in a hospital setting?	Installing EverWatch is extremely simple for your IT team; it requires only basic configuration changes to OpenEMR.
(Operational plausibility) How easy is it to use EverWatch to monitor for incidents?	EverWatch is specifically designed to make anomaly detection trivial for administrators; administrators can easily determine if the OpenEMR system is being abused.
(Healthcare constraints) Does EverWatch affect the healthcare environment around it?	No. EverWatch only observes and processes data that OpenEMR sends to it solely through approved interfaces.

Innovation and Value of EverWatch

Product Output	Value
Prioritized alert queue	Cut alert fatigue Reduce response time
Evidence summary / case record	Streamline audit preparation
Trends and dashboard views	Improve staffing decisions Improve operational efficiency
Plain-language explanation	Accelerate decision-making across technical and non-technical teams

Innovation and Value of EverWatch

Product Output	Value
Prioritized alert queue	Cut alert fatigue Reduce response time
Evidence summary / case record	Streamline audit preparation
Trends and dashboard views	Improve staffing decisions Improve operational efficiency
Plain-language explanation	Accelerate decision-making across technical and non-technical teams

Innovation and Value of EverWatch

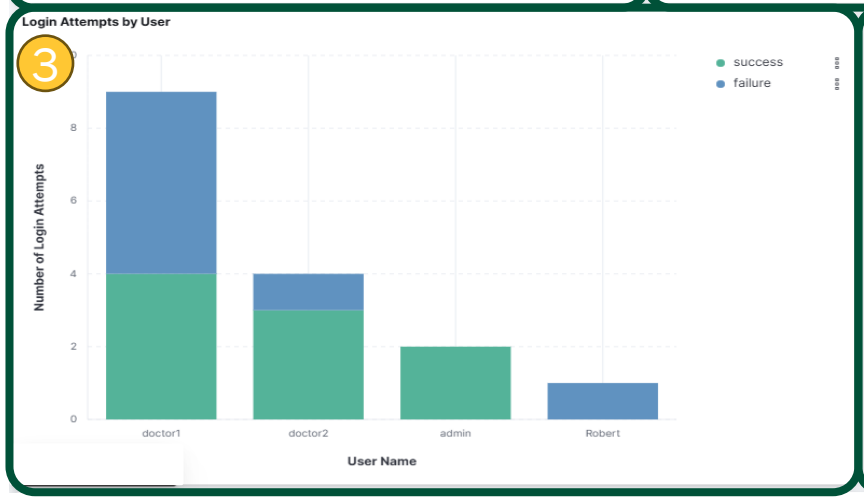
Product Output	Value
Prioritized alert queue	Cut alert fatigue Reduce response time
Evidence summary / case record	Streamline audit preparation
Trends and dashboard views	Improve staffing decisions Improve operational efficiency
Plain-language explanation	Accelerate decision-making across technical and non-technical teams

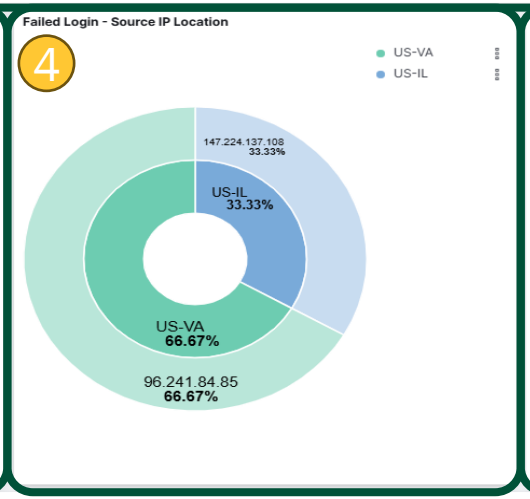
Innovation and Value of EverWatch

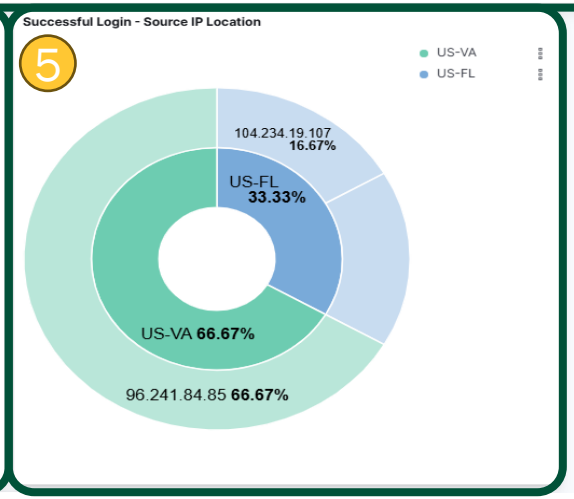
Product Output	Value
Prioritized alert queue	Cut alert fatigue Reduce response time
Evidence summary / case record	Streamline audit preparation
Trends and dashboard views	Improve staffing decisions Improve operational efficiency
Plain-language explanation	Accelerate decision-making across technical and non-technical teams

Security Alert Dashboard

1. Patient Access
2. Security Alerts
3. Login Attempts
4. Failed Login IPs
5. Successful Login IPs

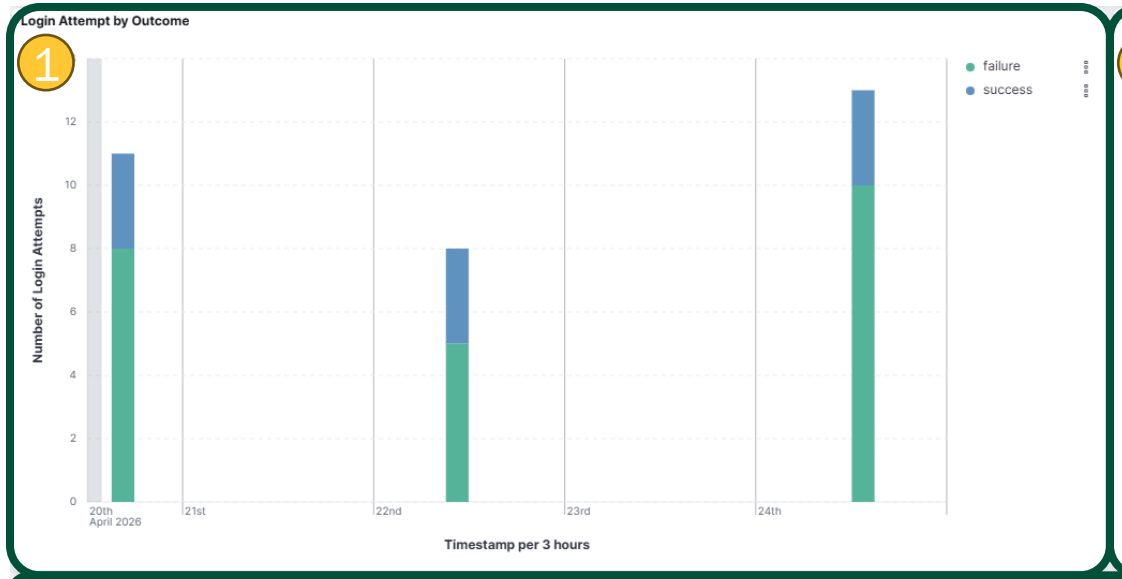


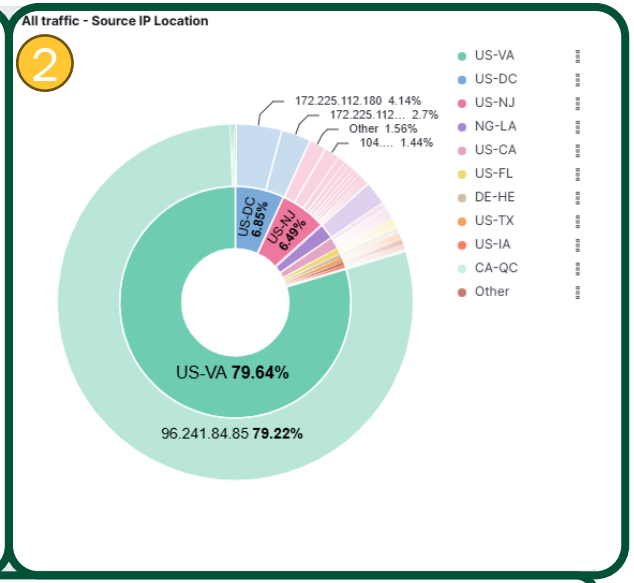


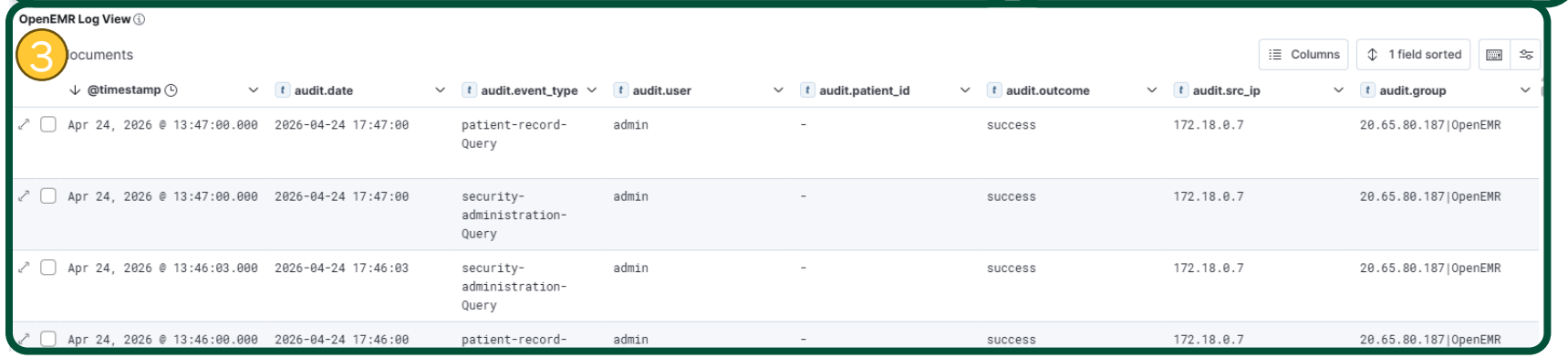


Macro View Dashboard

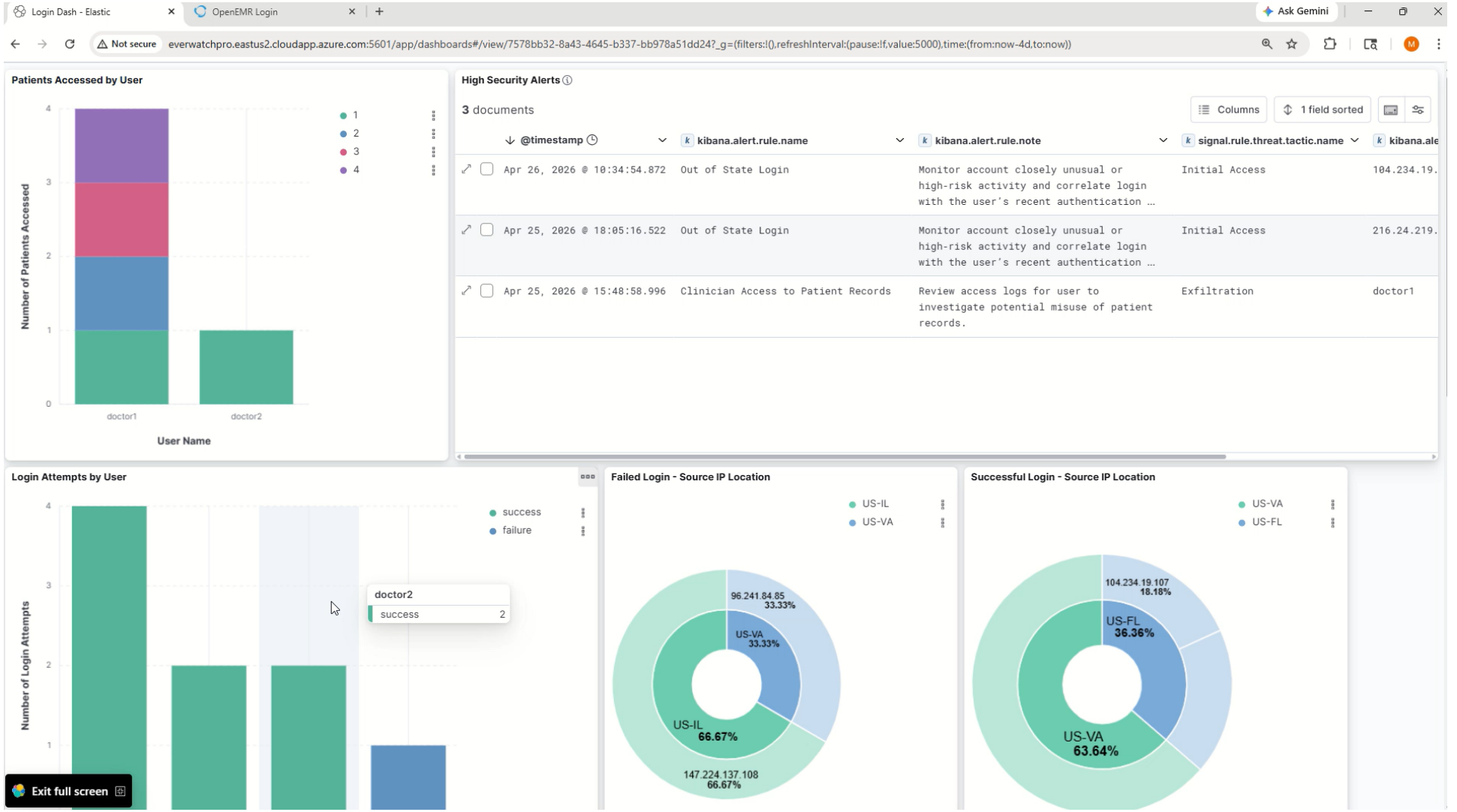
1. Temporal Login Attempts
2. Traffic Source IPs
3. Log View







Demo Video


Login Dash - Elastic
OpenEMR Login
Ask Gemini
Not secure
everwatchpro.eastus2.cloudapp.azure.com:5601/app/dashboards#/view/7578bb32-8a43-4645-b337-bb978a51dd24?_g=(filters:!(),refreshInterval:(pause:!f,value:5000),time:(from:now-4d,to:now))
Patients Accessed by User
Number of Patients Accessed
User Name
doctor1
doctor2
1
2
3
4
High Security Alerts
3 documents
Columns
1 field sorted
@timestamp
kibana.alert.rule.name
kibana.alert.rule.note
signal.rule.threat.tactic.name
Apr 26, 2026 @ 10:34:54.872
Out of State Login
Monitor account closely unusual or high-risk activity and correlate login with the user's recent authentication …
Initial Access
104.234.19.
Apr 25, 2026 @ 18:05:16.522
Out of State Login
Monitor account closely unusual or high-risk activity and correlate login with the user's recent authentication …
Initial Access
216.24.219.
Apr 25, 2026 @ 15:48:58.996
Clinician Access to Patient Records
Review access logs for user to investigate potential misuse of patient records.
Exfiltration
doctor1
Login Attempts by User
Number of Login Attempts
success
failure
doctor2
success 2
Exit full screen
Failed Login - Source IP Location
US-IL
US-VA
96.241.84.85
33.33%
US-VA
33.33%
US-IL
66.67%
147.224.137.108
66.67%
Successful Login - Source IP Location
US-VA
US-FL
104.234.19.107
18.18%
US-FL
36.36%
US-VA
63.64%

Conclusion

Questions

GEORGE MASON UNIVERSITY