



# **Quantum SOC Attack Simulation Report**

COMPUTER ARCHITECTURE

Prepared by: Saikumar Krishna Joshi  
USN -: [24MSRDF029]

Course: [DFIS SEM 3]

## Table of Contents

|   |                            |
|---|----------------------------|
| 1 | Summary                    |
| 2 | Objective                  |
| 3 | System Architecture        |
| 4 | Attack Scenarios           |
| 5 | Detection Rules and Alerts |
| 6 | Results and Analysis       |
| 7 | Ethical Statement          |
| 8 | Recommendations            |
| 9 | Conclusion                 |

## **1. Executive Summary**

This report documents the design and implementation of a Quantum SOC (Security Operations Center)

simulation environment. The system integrates quantum computing concepts such as BB84 key

distribution and Grover's search algorithm within a Flask-based SOC dashboard. The objective is to

analyze how future SOC's can detect and respond to potential quantum-enabled threats. All attack

events described herein are synthetic and intentionally generated for testing and demonstration.

## **2. Objective**

The main objective of this project is to simulate quantum-related security threats and evaluate SOC

readiness. It aims to create realistic quantum-based attack scenarios and assess detection logic for

alerting mechanisms within a SIEM-like dashboard

### 3. System Architecture

The Quantum SOC Dashboard is built using Python, Flask, and Qiskit. It features a background

process that continuously generates simulated logs derived from quantum algorithms. Key modules

include Quantum Random Bit Generation, BB84 Key Distribution, and Grover's Search Simulation.

Logs are visualized through a live Flask web dashboard that mimics a SOC environment.

#### **Attack Type / Goal / Detection Outcome**

**BB84 Eavesdropping** Detect quantum channel interference (Eve).

Alert triggered (EAVESDROP\_ALERT)

**Grover-Based Search** Simulate quantum-assisted brute-force key search.

Alert triggered (QUANTUM\_DECRYPT)

**Random Noise Injection** Generate unpredictable noise using quantum random bits.

Alert logged as low-level anomaly.

## **5. Detection Rules and Alerts**

Custom detection rules were designed to raise alerts when certain quantum behavior patterns are

observed. For example, the BB84 error rate threshold is set to 10%. Any session exceeding this triggers

an EAVESDROP\_ALERT. Grover's simulations producing secret collisions generate CRITICAL-level

alerts. All events are logged with a 'simulated=true' tag for audit purposes

## **6. Results and Analysis**

All test scenarios were successfully detected by the dashboard. Eavesdropping attempts raised

accurate warnings, while simulated Grover attacks triggered high-risk alerts. Normal quantum

operations were logged without false positives. The dashboard performed as expected, validating the

alert logic and system stability.

## 7. Ethical Statement

All attack simulations were created intentionally and ethically for educational and research use. No

production networks or real users were affected. Every event was tagged with 'simulated=true' and

unique test identifiers for traceability.

## 8. Conclusion

This project successfully demonstrates the concept of quantum-aware SOC operations. Through

controlled and intentional attack simulation, it provides a foundation for integrating quantum computing

awareness into cybersecurity monitoring. The Quantum SOC Dashboard serves as both a learning tool

and a conceptual framework for future quantum threat detection research

code-:

```

aes.py  p3.py  p4.py  p7.py  p9.py  q1.py  therat.py 1  p6.py
q1.py > ...
1  from flask import Flask, jsonify, render_template_string
2  import threading, random, time, json
3  from datetime import datetime
4  from qiskit import QuantumCircuit, transpile
5  from qiskit_aer import AerSimulator
6
7
8
9  def quantum_random_bit():
10     """Generate a random bit using a quantum Hadamard gate."""
11     qc = QuantumCircuit(1, 1)
12     qc.h(0)
13     qc.measure(0, 0)
14
15     simulator = AerSimulator()
16     qc = transpile(qc, simulator)
17     result = simulator.run(qc, shots=1).result()
18     counts = result.get_counts()
19     return int(max(counts, key=counts.get))
20
21 def grover_search(secret="101"):
22     """Simulate a basic quantum search (mocked for threat pattern discovery)."""
23     qc = QuantumCircuit(3)
24     qc.h([0, 1, 2])
25     qc.barrier()
26     qc.measure_all()
27
28     simulator = AerSimulator()
29     qc = transpile(qc, simulator)
30     result = simulator.run(qc, shots=100).result()
31     counts = result.get_counts()
32     return counts
33
34
35 LOGS = []
36 THREAT_PATTERNS = ["QKD-Anomaly", "Qubit-Leak", "Quantum-Decryption", "QTI-Suspect"]
37 LOCK = threading.Lock()
```

```

aes.py  p3.py  p4.py  p7.py  p9.py  q1.py  therat.py 1  p6.py
q1.py > ...
38
39 def generate_log_entry():
40     """Simulate a SOC log with random or quantum-based patterns."""
41     bit = quantum_random_bit()
42     log_level = random.choice(["INFO", "WARN", "ERROR", "CRITICAL"])
43     threat_type = random.choice(THREAT_PATTERNS)
44     src_ip = f"10.0.{random.randint(0,255)}.{random.randint(0,255)}"
45     dst_ip = f"192.168.{random.randint(0,255)}.{random.randint(0,255)}"
46     timestamp = datetime.now().strftime("%Y-%m-%d %H:%M:%S")
47
48     log = {
49         "timestamp": timestamp,
50         "source_ip": src_ip,
51         "destination_ip": dst_ip,
52         "level": log_level,
53         "event": threat_type if bit else "Normal Traffic",
54         "quantum_bit": bit
55     }
56
57
58     if log["level"] == "CRITICAL" and log["quantum_bit"] == 1:
59         log["alert"] = "Quantum Threat Detected"
60
61     return log
62
63 def log_generator():
64     """Continuously generate mock logs."""
65     while True:
66         entry = generate_log_entry()
67         with LOCK:
68             LOGS.append(entry)
69             if len(LOGS) > 100:
70                 LOGS.pop(0)
71         time.sleep(2)
72
73
74 app = Flask(__name__)
```

```

aes.py  p3.py  p4.py  p7.py  p9.py  q1.py  therat.py 1  p6.py  p8
q1.py > ...
77 TEMPLATE = """
78 <!DOCTYPE html>
79 <html>
80 <head>
81     <title>Quantum SOC Dashboard</title>
82     <style>
83         body { font-family: Arial; background: #0b0c10; color: #66fcf1; margin: 20px; }
84         h1 { color: #45a29e; text-align: center; }
85         table { width: 100%; border-collapse: collapse; margin-top: 20px; }
86         th, td { border: 1px solid #45a29e; padding: 8px; text-align: center; }
87         th { background: #1f2833; }
88         tr:nth-child(even) { background: #1f2833; }
89         .alert { color: #ff4444; font-weight: bold; }
90     </style>
91 </head>
92 <body>
93     <h1>Quantum SOC Dashboard</h1>
94     <table id="logTable">
95         <thead>
96             <tr><th>Time</th><th>Source IP</th><th>Destination IP</th><th>Level</th><th>Event</th><th>Q-Bit</th><th>Alert</th></tr>
97         </thead>
98         <tbody></tbody>
99     </table>
100
101     <script>
102         async function loadLogs() {
103             const res = await fetch('/api/logs');
104             const data = await res.json();
105             const tbody = document.querySelector('#logTable tbody');
106             tbody.innerHTML = '';
107             data.reverse().forEach(log => {
108                 const tr = document.createElement('tr');
109                 tr.innerHTML = `
110                     <td>${log.timestamp}</td>
111                     <td>${log.source_ip}</td>
112                     <td>${log.destination_ip}</td>
```

```

aes.py p3.py p4.py p7.py p9.py q1.py therat.py 1 p6.py p8
q1.py > ...
109         tr.innerHTML =
110             <td>${log.timestamp}</td>
111             <td>${log.source_ip}</td>
112             <td>${log.destination_ip}</td>
113             <td>${log.level}</td>
114             <td>${log.event}</td>
115             <td>${log.quantum_bit}</td>
116             <td class="alert">${log.alert || ''}</td>
117         };
118         tbody.appendChild(tr);
119     });
120 }
121 setInterval(loadLogs, 2000);
122 loadLogs();
123 </script>
124 </body>
125 </html>
126 """
127
128 @app.route('/')
129 def home():
130     return render_template_string(TEMPLATE)
131
132 @app.route('/api/logs')
133 def get_logs():
134     with LOCK:
135         return jsonify(LOGS)
136
137 if __name__ == "__main__":
138     print(" Starting Quantum SOC Dashboard on http://127.0.0.1:5000")
139     t = threading.Thread(target=log_generator, daemon=True)
140     t.start()
141     app.run(debug=False)
142

```

## Output :

| Quantum SOC Dashboard |              |                 |          |                |       |                         |
|-----------------------|--------------|-----------------|----------|----------------|-------|-------------------------|
| Time                  | Source IP    | Destination IP  | Level    | Event          | Q-Bit | Alert                   |
| 2025-10-25 10:19:02   | 10.0.92.182  | 192.168.250.53  | CRITICAL | Normal Traffic | 0     |                         |
| 2025-10-25 10:19:00   | 10.0.41.197  | 192.168.134.197 | CRITICAL | Normal Traffic | 0     |                         |
| 2025-10-25 10:18:58   | 10.0.159.100 | 192.168.124.204 | ERROR    | Normal Traffic | 0     |                         |
| 2025-10-25 10:18:56   | 10.0.235.186 | 192.168.174.243 | CRITICAL | Normal Traffic | 0     |                         |
| 2025-10-25 10:18:53   | 10.0.155.176 | 192.168.182.57  | WARN     | Normal Traffic | 0     |                         |
| 2025-10-25 10:18:51   | 10.0.229.85  | 192.168.221.87  | CRITICAL | Normal Traffic | 0     |                         |
| 2025-10-25 10:18:49   | 10.0.55.221  | 192.168.255.227 | CRITICAL | Qubit-Leak     | 1     | Quantum Threat Detected |
| 2025-10-25 10:18:47   | 10.0.197.213 | 192.168.201.36  | CRITICAL | QTI-Suspect    | 1     | Quantum Threat Detected |
| 2025-10-25 10:18:45   | 10.0.61.154  | 192.168.173.211 | ERROR    | Qubit-Leak     | 1     |                         |
| 2025-10-25 10:18:42   | 10.0.30.179  | 192.168.9.173   | INFO     | QKD-Anomaly    | 1     |                         |
| 2025-10-25 10:18:40   | 10.0.140.139 | 192.168.133.189 | CRITICAL | Normal Traffic | 0     |                         |
| 2025-10-25 10:18:38   | 10.0.152.227 | 192.168.92.204  | CRITICAL | Normal Traffic | 0     |                         |
| 2025-10-25 10:18:36   | 10.0.182.202 | 192.168.70.132  | CRITICAL | QTI-Suspect    | 1     | Quantum Threat Detected |
| 2025-10-25 10:18:34   | 10.0.140.20  | 192.168.173.232 | CRITICAL | Normal Traffic | 0     |                         |
| 2025-10-25 10:18:32   | 10.0.229.24  | 192.168.207.158 | CRITICAL | Normal Traffic | 0     |                         |



1

```
127.0.0.1 - - [25/Oct/2025 10:18:59] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:00] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:02] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:04] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:07] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:09] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:11] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:13] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:15] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:17] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:19] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:21] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:23] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:25] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:27] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:29] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:31] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:33] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:35] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:37] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:39] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:41] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:43] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:45] "GET /api/logs HTTP/1.1" 200 -
127.0.0.1 - - [25/Oct/2025 10:19:48] "GET /api/logs HTTP/1.1" 200 -
```



Quantum SOC Dashboard

| Time                | Source IP      | Destination IP  | Event    | Class               | Alert                   |
|---------------------|----------------|-----------------|----------|---------------------|-------------------------|
| 2025-10-26 10:00:00 | 10.0.1.150     | 102.166.174.217 | WARM     | Out-Look            | 1                       |
| 2025-10-26 10:00:00 | 102.176.157.77 | 102.166.158.77  | CRITICAL | QTI-Support         |                         |
| 2025-10-26 10:00:06 | 11.0.104.82    | 102.166.160.48  | ENHANC   | Normal Traffic      | 0                       |
| 2025-10-26 10:00:24 | 10.0.166.160   | 102.166.166.167 | ENHANC   | Normal Traffic      | 0                       |
| 2025-10-26 10:00:31 | 11.0.166.160   | 102.166.166.167 | WARM     | Normal Traffic      | 0                       |
| 2025-10-26 10:00:37 | 10.11.30       | 102.166.220.220 | CRITICAL | Normal Traffic      | 0                       |
| 2025-10-26 10:00:27 | 10.0.176.160   | 102.166.161.17  | RFO      | Normal Traffic      | 0                       |
| 2025-10-26 10:00:25 | 10.0.166.160   | 102.166.161.17  | RFO      | Quantum-Description | 0                       |
| 2025-10-26 10:00:27 | 10.0.166.160   | 102.166.161.166 | CRITICAL | Normal Traffic      |                         |
| 2025-10-26 10:00:27 | 10.0.166.160   | 102.166.161.166 | CRITICAL | Normal Traffic      | Quantum Threat Detected |
| 2025-10-26 10:00:30 | 11.0.166.80    | 102.166.80.40   | ENHANC   | Normal Traffic      | 0                       |
| 2025-10-26 10:00:30 | 10.0.166.160   | 102.166.80.26   | CRITICAL | QMI-Assessory       | 1                       |
| 2025-10-26 10:00:30 | 10.0.166.160   | 102.166.80.26   | WARM     | Normal Traffic      |                         |
| 2025-10-26 10:00:30 | 11.0.166.160   | 102.166.159.69  | CRITICAL | QTI-Support         | 0                       |
| 2025-10-26 10:00:30 | 10.0.166.160   | 102.166.159.177 | RFO      | QMI-Assessory       | 1                       |
| 2025-10-26 10:00:30 | 10.0.166.160   | 102.166.159.24  | ENHANC   | Quantum-Description | 1                       |
| 2025-10-26 10:00:30 | 10.11.30       | 102.166.16.243  | RFO      | QMI-Assessory       | 1                       |
| 2025-10-26 10:00:35 | 10.0.166.160   | 102.166.48.71   | RFO      | Out-Look            | 1                       |
| 2025-10-26 10:00:31 | 10.0.204.157   | 102.166.77.220  | WARM     | QMI-Assessory       | 1                       |
| 2025-10-26 10:00:30 | 10.0.204.157   | 102.166.16.166  | CRITICAL | Quantum-Description | 1                       |
| 2025-10-26 10:00:30 | 10.0.159.176   | 102.166.25.58   | CRITICAL | QMI-Assessory       | 1                       |
| 2025-10-26 10:00:34 | 10.0.166.160   | 102.166.150.167 | ENHANC   | Normal Traffic      | 0                       |
| 2025-10-26 10:00:32 | 10.0.166.160   | 102.166.80.26   | RFO      | Out-Look            | 1                       |
| 2025-10-26 10:00:32 | 10.0.177.220   | 102.166.25.74   | RFO      | QTI-Support         | 1                       |
| 2025-10-26 10:00:48 | 10.0.159.172   | 102.166.152.76  | ENHANC   | Normal Traffic      | 0                       |
| 2025-10-26 10:00:46 | 10.0.246.115   | 102.166.114.115 | RFO      | Normal Traffic      | 0                       |
| 2025-10-26 10:00:45 | 10.0.24.20     | 102.166.166.160 | ENHANC   | QMI-Assessory       | 1                       |
| 2025-10-26 10:00:47 | 10.0.24.100    | 102.166.16.166  | CRITICAL | Out-Look            | 0                       |
| 2025-10-26 10:00:50 | 11.0.166.160   | 102.166.150.211 | CRITICAL | Normal Traffic      | 0                       |
| 2025-10-26 10:00:50 | 10.0.166.160   | 102.166.200.202 | ENHANC   | QTI-Support         | 1                       |
| 2025-10-26 10:00:50 | 10.0.166.160   | 102.166.139.138 | CRITICAL | Normal Traffic      | 0                       |
| 2025-10-26 10:00:51 | 10.0.166.160   | 102.166.162.17  | WARM     | Normal Traffic      | 0                       |
| 2025-10-26 10:00:51 | 11.0.17.186    | 102.166.102.4   | RFO      | Normal Traffic      | 0                       |
| 2025-10-26 10:00:58 | 10.0.27.78     | 102.166.166.160 | CRITICAL | Normal Traffic      | 0                       |
| 2025-10-26 10:00:58 | 10.0.166.161   | 102.166.166.160 | CRITICAL | Out-Look            | 1                       |
| 2025-10-26 10:00:58 | 10.0.166.160   | 102.166.151.10  | WARM     | QMI-Assessory       | 1                       |
| 2025-10-26 10:00:58 | 11.0.166.160   | 102.166.16.140  | RFO      | Quantum-Description | 1                       |
| 2025-10-26 10:00:58 | 10.0.274.122   | 102.166.176.71  | WARM     | Out-Look            | 1                       |
| 2025-10-26 10:00:58 | 10.0.166.160   | 102.166.166.160 | WARM     | Normal Traffic      | 0                       |
| 2025-10-26 10:00:58 | 11.0.166.160   | 102.166.220.220 | RFO      | Normal Traffic      | 0                       |
| 2025-10-26 10:00:58 | 10.0.226.142   | 102.166.80.56   | ENHANC   | Normal Traffic      | 0                       |
| 2025-10-26 10:00:51 | 11.0.23.201    | 102.166.20.200  | ENHANC   | QMI-Assessory       | 1                       |
| 2025-10-26 10:00:58 | 10.0.20.47     | 102.166.80.110  | WARM     | Quantum-Description | 1                       |
| 2025-10-26 10:00:57 | 10.0.166.160   | 102.166.58.79   | WARM     | QMI-Assessory       | 1                       |
| 2025-10-26 10:00:58 | 11.0.166.160   | 102.166.160.1   | ENHANC   | Normal Traffic      | 0                       |
| 2025-10-26 10:00:58 | 10.0.24.100    | 102.            |          |                     |                         |