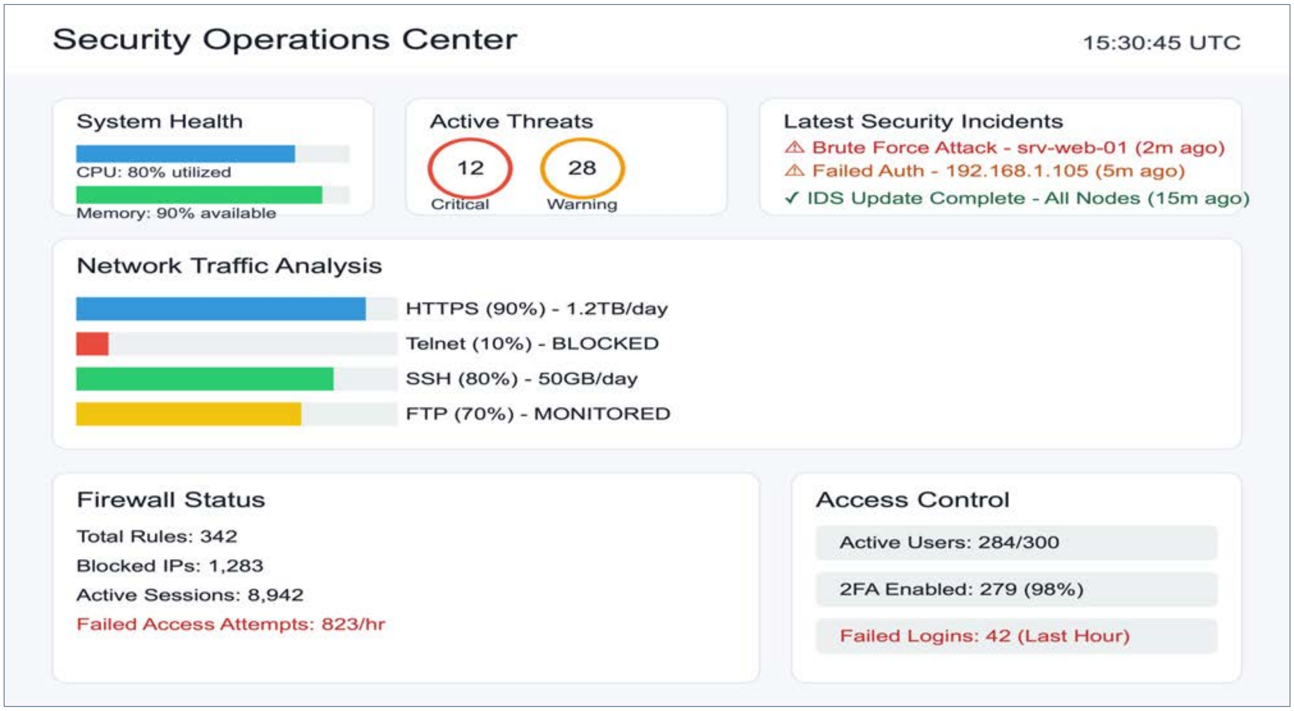
Cybersecurity Dashboard Discussion



Security Operations Center

15:30:45 UTC

System Health

CPU: 80% utilized

Memory: 90% available

Active Threats

12 Critical

28 Warning

Latest Security Incidents

⚠ Brute Force Attack - srv-web-01 (2m ago)

⚠ Failed Auth - 192.168.1.105 (5m ago)

✓ IDS Update Complete - All Nodes (15m ago)

Network Traffic Analysis

HTTPS (90%) - 1.2TB/day

Telnet (10%) - BLOCKED

SSH (80%) - 50GB/day

FTP (70%) - MONITORED

Firewall Status

Total Rules: 342

Blocked IPs: 1,283

Active Sessions: 8,942

Failed Access Attempts: 823/hr

Access Control

Active Users: 284/300

2FA Enabled: 279 (98%)

Failed Logins: 42 (Last Hour)

Key Security Terminology

active threats • system health • firewall status • network traffic • incident response • critical alerts

access control • CPU utilization • blocked IPs • traffic monitoring

authentication • system logs • security protocols • user access • real-time alerts

System Analysis

- What is the overall system health?
- How many critical alerts are present?

Network Analysis

- What protocols are being monitored?
- Which services are blocked?

Security Assessment

- What is the blocked IP count?
- How many active sessions exist?

Access Control

- What is the user capacity status?
- How many users have 2FA enabled?
- Are there suspicious activities?

Discussion Points

- What improvements could enhance system security?
- How can we reduce the number of critical alerts?

Possible answers

System Analysis:
- Overall system health shows CPU at 80% utilized and memory 90% available, indicating the system is running with high CPU load but good memory capacity
- There are 12 critical alerts and 28 warning alerts currently present

Network Analysis:
- Four protocols are being monitored: HTTPS (1.2TB/day), Telnet, SSH (50GB/day), and FTP
- Telnet service is specifically marked as BLOCKED in the traffic analysis

Security Assessment:
- The blocked IP count is 1,283
- There are 8,942 active sessions currently running

Access Control:
- User capacity status shows 284 active users out of 300 total capacity (94.7% utilized)
- 279 users (98%) have 2FA enabled
- There are suspicious activities indicated by:
  - 823 failed access attempts per hour
  - 42 failed logins in the last hour
  - A brute force attack reported 2 minutes ago
  - Failed authentication for IP 192.168.1.108 from 5 minutes ago

Discussion Points - For system security improvements, I suggest:
1. Investigate and resolve the 12 critical alerts as a priority
2. Look into the high rate of failed access attempts
3. Consider expanding user capacity as it's nearing its limit
4. Investigate the recent brute force attack and implement additional protections if needed
5. Review why CPU utilization is at 80% and optimize if possible