Taj Badshah

Home : Pakistan

Email: tajbadshah95@gmail.com **Phone:** (+92) 3122950539

LinkedIn: www.linkedin.com/in/tajbadshah-215197168

Nationality: Pakistani

ABOUT ME

Passionate and dedicated SOC Engineer with extensive experience in cybersecurity and threat hunting. Skilled in alert triage, incident investigation, and root cause analysis, I excel in orchestrating crossteam incident response and implementing containment strategies. With a strong focus on post-incident reviews to continuously enhance security posture, I'm ready to apply my analytical skills and expertise to protect your organization from evolving cyber threats and keep your defenses ahead of the curve.

WORK EXPERIENCE

[Nov 2022 – Current]

Specialist SOC

Askari Bank Ltd.

City: Islamabad | **Country:** Pakistan

- Streamlined security alert monitoring processes to enhance detection accuracy
- Conducted comprehensive log analysis and triaged alerts, enhancing threat identification by 20%
- Resolved high-severity security incidents through rootcause analysis and strategic mitigation
- Designed and implemented threat-hunting strategies, identifying 10+ zero-day vulnerabilities
- Create incident reports and maintain documentation of security events
- Automated security workflows using XDR tools, reducing manual intervention by 30%
- Spearheaded incident response efforts, effectively containing breaches with a 98% resolution rate within SLA

[Oct 2020 – Nov 2022]

SOC Analyst

ELEV8IS – Cybersecurity Solutions

- Monitored SIEM systems to detect and analyze potential security incidents, ensuring timely responses to threats
- Performed initial alert triage and escalation to senior analysts, maintaining a high accuracy rate for incident prioritization
- Conducted basic log analysis to identify patterns and anomalies, contributing to incident investigations

EDUCATION AND TRAINING

[2014 – 2018]

Bechelors of Engineering

UIT University

SKILLS

Alert Triage

Skilled in analyzing and prioritizing security alerts to identify potential threats and reduce false positives

Incident Response

Skilled in leading incident response efforts, with strong threat analysis and mitigation abilities

Cyber Threat Intelligence (CTI)

Uses threat intelligence to enrich alerts and proactively address emerging threats

SOC Operations

Experienced in daily SOC activities, alert monitoring, threat hunting, and SLA compliance

External Attack Surface Management

Effectivily manages external vulnerabilities, reducing the organization's attack surface

System Health and Log Management

Ensures log collection and system health, with expertise in File Integrity Monitoring

Digital Risk Protection (DRP)

Hands-on experience with Digital Risk Protection (DRP) solutions, effectively safeguarding organizational digital assets from external threats

Security Automation & Orchestration

Playbook & Workflow Automation (Microsoft Sentinel Azure Logic App and IBM SOAR)

XDR (Extended Detection & Response)

Proficient in XDR, especially Vision One and Microsoft Defender 365, for enhanced threat detection and automated responses

DLP Policy Configuration and Management

Proficient in configuring and managing DLP policies to protect sensitive data across endpoints, email, and cloud environments

PROFESSIONAL TRAININGS & CERTIFICATIONS

Certified Ethical Hacker (CEH) EC-Council

Microsoft Certified: Security Operations Analyst Associate (SC-200)

eLearnSecurity Certified Incident Responder (eCIR)

Certified in Cybersecurity (CC) ISC2

Practical Threat Hunting (Mandiant)

Microsoft Certified: Azure AI Fundamentals (AI-900)

LANGUAGE SKILLS

Other language(s): English