GEOFFREY O. OCHIENG-SOC *Analyst-Incident Responder-Grey Teamer, CA Kenya.*
LinkedIn Profile Link : www.linkedin.com/in/geoffrey-o-ochieng™-85127a285

As a seasoned SOC Analyst, Grey Teamer, and Incident Responder with 5 years of hands-on experience, Geoffrey specialises in protecting organisations from cyber threats through proactive monitoring, threat hunting, and swift incident response. His expertise spans across conducting advanced threat analysis, deploying security measures, and collaborating with both offensive and defensive teams to identify and mitigate vulnerabilities. With a deep understanding of attack vectors and a commitment to continuous learning, he excels in maintaining robust security postures and minimising risk exposure. His goal is to safeguard critical assets and ensure business continuity in the face of evolving cyber threats.

TIP 1. EMBRACE ZERO TRUST ARCHITECTURE

Traditional perimeter-based security models are increasingly obsolete. Implement a Zero Trust model, where no user or device is trusted by default, even if they are within the network. This approach includes verifying identities, and devices, and ensuring least-privilege access.

TIP 2. BEHAVIOURAL ANALYTICS FOR THREAT DETECTION

Beyond traditional monitoring, use behavioural analytics to identify anomalies in user activities. Machine learning models can detect patterns that deviate from the norm, signalling potential insider threats or compromised accounts.

TIP 3. SUPPLY CHAIN SECURITY

Ensure that all third-party vendors and partners adhere to your security standards. Regularly audit their practices, as vulnerabilities in their systems can be exploited to target your organisation.

TIP 4. ADVANCED ENCRYPTION STANDARDS

Adopt quantum-resistant encryption methods as a forward-looking security measure. With the advent of quantum computing, traditional encryption may be at risk, so being ahead of the curve is crucial.

TIP 5. CYBER RESILIENCE STRATEGY

Develop not just a cybersecurity strategy but a cyber resilience one. This involves not only protecting systems, but also ensuring that the organisation can quickly recover and continue operations after an attack.

TIP 6. DECENTRALIZED IDENTITY MANAGEMENT

Consider using decentralised identity (DID) systems, which give users control over their own identity data. This reduces the risk of centralised breaches and helps protect personal information across multiple platforms.

TIP 7. THREAT HUNTING PROGRAMS

Proactively seek out threats within your network by establishing a dedicated threat-hunting team. This goes beyond reactive defence, identifying and mitigating potential threats before they can cause damage.

TIP 8. SECURE DEVELOPMENT LIFECYCLE (SDLC)

Integrate security practices into every phase of the software development lifecycle. From design to deployment; ensure

that security is a priority, including regular code reviews, static analysis, and vulnerability assessments.

TIP 9. ISOLATION OF CRITICAL SYSTEMS

Segment your network to isolate critical systems from less secure areas. Use virtual LANs (VLANs) or micro-segmentation to ensure that sensitive data and systems are protected - even if other parts of the network are compromised.

TIP10. DARK WEB MONITORING

Regularly monitor the dark web for mentions of your company, employees, or products. This can provide early warning signs of impending attacks, data breaches, or brand impersonation efforts that can be addressed proactively.