SWETA GUPTA *Head Of Operations, Clavax*
LinkedIn: https://www.linkedin.com/in/sweta-gupta-9563a956/

Sweta Gupta is a seasoned Software Engineer with nearly two decades of experience in the tech industry. Currently serving as the Head of Operations (Software) at a prominent multinational corporation, Sweta is renowned not only for her coding prowess but also for her adeptness as a certified programmer, manager, and leader.

Having worked across diverse geographies including the USA, Australia, and India, Sweta brings a global perspective to her role. Her passion for technology is evident in her dedication to contributing to the dynamic advancements in the tech world.

In recognition of her exemplary leadership and project management skills, Sweta was honored by being named among the top 150 female project managers worldwide in both 2019 and 2020. Her remarkable journey was documented in the book "Unlocking the Opportunity," published in 2020, where she shared the stage with other exceptional women.

TIP 1. IMPLEMENT ZERO TRUST ARCHITECTURE

Adopt a "never trust, always verify" approach to network access, ensuring continuous authentication and verification of user identities and device security status.

TIP 2. CONDUCT REGULAR PENETRATION TESTING

Regularly test your systems for vulnerabilities through simulated attacks to identify and mitigate weaknesses before they can be exploited by real attackers.

TIP 3. DEPLOY ENDPOINT DETECTION AND RESPONSE (EDR) SOLUTIONS

Utilise EDR tools to monitor and respond to threats on endpoints in real-time, providing detailed visibility and automated response capabilities.

TIP 4. USE DATA ENCRYPTION

Encrypt sensitive data, both at rest and in transit, to protect it from unauthorised access, ensuring that even if data is intercepted, it remains unreadable.

TIP 5. IMPLEMENT NETWORK SEGMENTATION

Divide your network into smaller segments to limit the spread of malware and restrict access to sensitive information based on user roles and needs.

TIP 6. CONDUCT SECURITY AUDITS AND ASSESSMENTS

Regularly review and assess your security policies, procedures, and controls to ensure that they remain effective and aligned with current threats and compliance requirements.

TIP 7. ADOPT SECURE CODING PRACTICES

Ensure that developers follow best practices for secure coding to prevent vulnerabilities in software, such as Structured Query Language (SQL) injection and cross-site scripting (XSS).

TIP 8. UTILISE THREAT INTELLIGENCE

Leverage threat intelligence services to stay informed about the latest threats and vulnerabilities, allowing you to proactively defend against emerging risks.

TIP 9. ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Add an extra layer of security by requiring a second form of verification, such as a text message or authentication app.

TIP 10. EDUCATE EMPLOYEES AND USERS AND ESTABLISH A SECURITY OPERATIONS CENTER (SOC)

Provide cybersecurity training to raise awareness about common threats and safe practices.
Implement policies for safe internet usage and data handling. Create a dedicated team and facility to monitor, detect, and respond to cybersecurity incidents, providing a centralised approach to managing security operations.