CODE{▲}ITS
Thinking Beyond

**Codewits Solutions Pvt Ltd.**

Role: Head Security Researcher
Location: Pune
Exp: 4+ years

- Security and compliance enthusiasts to catalyze product R&D for a breakthrough product in the hyperactive world of SaaS, who are/have:
- driven by a strong desire to seek challenges, observe patterns, analyze impacts, present insights, share experiences, and continually build upon the discovered information, for maintaining the latest knowledge about the state of Internet security
- keenly follow the ever-evolving space of Web enabled supply chains and contribute towards securing interactions in the application layer
- hands-on with leading open source tools and methodologies relevant to threat hunting, PoC development, and remediation management
- strong background in application security, and a high degree of familiarity with resources such as OWASP Top 10 for API / Web / Cloud / Mobile, MITRE, CIS, and similar leading projects from OffSec, SANS, NIST, CSA, et al
- conversant with industry standards, guidelines and best practices regarding pentesting focused on data and interactions concerning modern applications that are powered by DevOps and microservices
- able to quickly skill up or adapt their techniques to keep step with the rate of innovation for business enablement as well as improvisation in adversary tactics
- familiarity with relevant data-protection requirements prescribed by regulatory bodies / best practices / standards for compliance, information security or privacy, e.g. HIPAA, GDPR, PCI-DSS, ISO27001, etc.

**Advantage points**

- The above, along with one or more listed below, would form a great combination:
- able to share relevant credentials: CVE records, patents, papers, or other work-samples
- conversant with projects such as OpenVAS, OpenCSPM, OpenSCAP, or any other implementations, tools, or use-cases with SCAP constituents, JOVAL or OSCAL
- comfortable working with application and device logs
- ability to translate threat reports or synopses into articles/ blogs, or educational content such as for subject oriented whitepapers, business oriented webinars, developer oriented guidelines, etc.
- familiarity with IaC / SecOps / DevOps concepts & tools

**To carry out:**

Research and development in the field of SaaS security, specifically the trending sprawl of software services consumed over the Web, covering various domains that are essential for achieving – and maintaining – a robust security posture, including but not limited to:

- hardening, or locking down, a Web-based / SaaS app to protect the data, users, and other assets for an enterprise
- weighing the pros and cons of all the settings that a parameter can be configured to; using the app's admin panel, service API, or ordinary user interface, especially in the context of introduction, withdrawal or otherwise modification of application\service features by the vendors, advisories published by the security community, and other mandates or disruptions affecting the Cloud \ Web-based or SaaS ecosystem
- recommending and documenting –accompanied by proof of concept where relevant to demonstrate or prescribe – the best security setting for a configuration parameter
- researching diligently, through the app's official documentation, developer resources such as APIs, community boards/repositories, and so on, to generate hypotheses, knowledge-bases and evidences supporting the recommended security configuration
- analyzing controls, tools and resources to preempt and manage threats to the security posture in terms of identities, use cases and user entity behaviors
- researching, analyzing and advising best practices to protect the enterprise from data exposure, corruption, or leakage, resulting from its SaaS security posture
- suggesting, reviewing, and updating the recommended configurations, across specific apps, or groups of similar apps, or other logical constructs
- creating, reviewing, analyzing, correlating, mapping, and updating the list of controls from diverse compliance standards, frameworks or best-practices, as they correspond to relaxing, toughening, or altogether omitting one or more configuration settings.
- contributing to the larger effort, and exchanging or developing ideas with cross-functional colleagues, in the spirit of Agile product development.