Security Gap Analysis

Security Architecture Review – Review & Identify opportunities for improvement in your security infrastructure by assessing the current state of your security posture and provide insightful recommendations based on security industry best practice guidance.

Penetration Testing - Conduct a full suite of technical testing (focus on OWASP Top 10) to validate the effectiveness of your security controls and determine the integrity of your network, system, or application. We will partner with you to understand your needs and objectives, whether they are driven by compliance and regulations or simply a desire to be as secure as possible, and then build the appropriate test scenarios.

Based on the findings of our assessment and testing, we make recommendations for specific mitigations to reduce risks and prevent incidents in your organization's business and operational environment.

Trinethra Offering

LTE – Long Term Engagement

- Threat Modeling
- Code Review
- Penetration Testing using both inbuilt & commercial tools that the PSO purchase.

This is a sophisticated program offered as a paid program to the customers of SHIFTLEFT INFOSEC CONSULTANTS LLP. This program covers the products that are owned and released by Customers and as well as an On-Demand service for the products that are owned and managed by the customer's customer. As part of this paid program, the PSO work with the customers on a monthly basis or quarterly or half yearly or even on a yearly subscriptions.

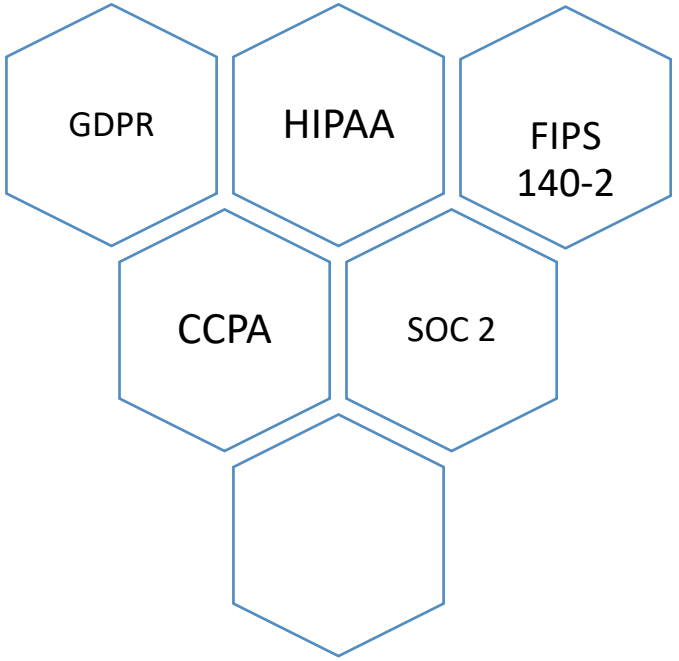
This program covers a threat modeling activity of the product in scope , manual code review of the product in scope and a manual penetration testing of the product in scope. This program uses a few commercial tools that the PSO purchase as well as few internal developed tools.

A detailed report on the findings will be shared to the customers with details of the expected remediation as well. PSO will adopt Secure Development Lifecycle within the program and ensure customers have a security program within their software development lifecycle and ensure early feedback on the security is provided on a timely basis

Audit & Compliance

We will ensure you are meeting the compliance standards that are applicable to you and protect the confidentiality, integrity, and availability of data/information.

Based on your need, we will ensure our best efforts are in place to pursue and help you out with other compliances if required.



- Health Insurance Portability and Accountability Act (HIPAA) compliance
- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA) compliance
- Federal Information Processing Standard (140-2) compliance
- SOC compliance.

SHIFTLEFT PLUS (SL PLUS)

Incident Handling : You can trust our team to be by your side if your company runs into a data security breach or any know vulnerabilities identified publicly or by any of the customers. Our incident response/management service will quickly respond and halt the breach. We then assess the damage done in an effort to minimize the business impact and restore the network/system to a positive state. We make sure any issues created by an attack on your preventative measures are handled by our incident handling team.

A newsletter or a monthly report which also includes basic security trainings as well as happenings within the security community will be shared to the customers as part of this engagement.

Continuous Monitoring: Continuous Monitoring is a service that ensures the network or the product which is deployed, is monitored 24x7 to ensure there are no attacks initiated. This is a service that is at a basic level at this moment & is expected to evolve in future as the team plan to integrate few commercial tools as well.

Security Maintenance:

Security maintenance covers all the software components within the customers products like third party libraries and other open source / components used during the product development. This service ensure all the above said files or components are tracked for known vulnerabilities and this service ensure proper and timely communication to customers in case of publicly disclosed vulnerabilities or in case of any identified impact for the customers.