Professional Cyber Security Solutions

Real time crisis management and incident response

In today's world organizations suffer from a broad specter of attacks. We offer a service which will provide you a way to manage the crisis by top of the line security experts. Our team will help you to get through the helplessness and clear through the mist of chaos. Our team of experts comes with a lot of experience in a vast number of environments and technologies. The team has years of experience which they share.

How does it work?

- ✓ The company contacts us and provides first details about the incident.
- ✓ We conduct an online meeting to identify the severity of the incident in the meanwhile a crisis management expert is sent to the company to manage the incident on-site.
- ✓ Our team will look for the incident's point of breach and will contain it as fast as possible in order to allow business continuity; the team's years of experience will give it an advantage in the process and reduce dramatically the time needed.
- ✓ Our team will assess the damage and will plan an immediate solution for the company business continuity and will find a long term solution plan which will prevent similar incidents in the future.
- ✓ While the business is getting back to its daily routine, our team will make a forensics analysis to identify the source of the incident and find all possible evidence so the company could take legal actions against the source.

Security analysis and assessment services

According to recent researches almost every company online is being attacked on a daily basis, our team specializes in identifying the attack vectors, finding the solutions and contributing to reduce the attack vectors to a minimum. Our team has years of experience in conducting attacks and implementing security solutions in application, network and host level. Security reviews or penetration testing can be conducted against a specific product, application and even the entire corporate network.

How does it work?

- ✓ Scope definition including identifying the assets and the possible enemies. The analysis is based on the scope and concentrated on trying to harm the assets while impersonating the level of the defined enemy.
- ✓ Conducting the security review or penetration test according to our unique methodology based on a mix of standard methodologies in practice today.
- ✓ Conducting deep analysis of the found vulnerabilities in order to understand their impact on the business and its assets.
- ✓ Production of a detailed report which includes both executive summary and detailed technological descriptions allowing both risk analysis and technological remediation.
- ✓ Tailoring an uncompromising security solution taking into consideration the organization's budget and schedule.
- ✓ Accompanying the company in implementing the recommended solutions.

Secure Development Lifecycle (SDL)

In today's time when cyber security is in the news almost on a daily basis it is important to protect your application from day 1, SDL offers exactly that. The leading concept of SDL is to integrate security solutions at early stages in order to dramatically reduce costs rather than implementing security patches in the future. SDL is a process which is embedded into the application life cycle offering a security point of view on architecture, design, code and deployment. By embedding SDL into your product you reduce significantly the amount of security work that will be required later on in the product's life cycle. Our experts have a lot of experience working with a vast number of technologies and complex environments providing them a unique security-focused point of view on every product.

How does it work?

- Our team of experts meets with the client to understand the product or system and how it works.
- An architecture review is conducted, mapping vulnerabilities based on data entry points, component connectivity, communication protocols, hardware and software in use. Creating a secure foundation for the application to be developed upon.
- A design review is conducted and a threat modeling report is created, helping the client to understand the threats better and to prepare for them reducing the attack vector.
- A code review is being conducted on the whole code helping the developers to adjust to the secure code standards required in the technology world today.
- A security assessment is made to review the general security level of the application and check for missed attack vectors.
- A deployment review is made to make sure the application is deployed in a secure environment complying with the architecture threat analysis conducted in earlier stages.
- The process starts again with the next product update.

Cyber Security Training

Cyber attacks and security incidents are currently very popular and being widely conducted by governments, commercial firms and hacking groups. One of the most important aspects in the organizational security program is cyber training and courses. Our team of experts can provide various courses and trainings tackling security issues from both the offensive and defensive perspectives. We aim for our trainees to acquire practical and useful knowledge therefore all of our trainings are based on live demos, hands-on exercises and real-life examples.

What do we offer?

- Security awareness training Introduction to the world of security and cyber crime and basic vulnerability identification.
- Host Level Security Course. Attack and protect servers and endpoints.
- Network Level Security Course Discover, exploit and remediate network level vulnerabilities.
- Application Level Security Course. Get acquainted with various application hacking methods while discovering, exploiting and remediating vulnerabilities.

- ✓ Secure Development Lifecycle Course. Discover and asses security risks throughout the entire product development lifecycle.
- ✓ Social Engineering Course. Discover the security aspect based on the system's weakest link – the man.
- ✓ Threat Analysis and Risk Management Course

Manage the entire security suit addressing issues varying from asset and risk identification to business impact estimation. We also offer custom, tailor made trainings combining several or all subjects stated above.

Strategic security solutions and risk management

In the world where cyber crime is becoming a major threat, organizations are subject to a new realm of threats and risks leaving managers and executives in unfamiliar territory. Using the experience, expertise and knowledge collected by our experts we are able to deliver a short and long term strategic security roadmap aimed to ensure your assets are protected while effectively using the organization's resources taking into consideration limitations such as budget, schedule and user experience.

What do we offer?

Short term roadmap

- ✓ Asset identification
- ✓ Enemy mapping
- ✓ Threat identification

Long term roadmap

- ✓ Creating a custom risk management policy
- ✓ Risk Assessment Framework Development
- ✓ Incident Response Program Development
- ✓ Vulnerability Management Program Development
- ✓ Strategic Security Roadmap Planning