



DeTaSECURE

Attack Path Modelling

Every business, knowingly or without knowing has a certain amount of data exposed in public.

We fix that! and improve your data protection without any resistance to your business continuity.



WHO ARE WE?

We are accomplished cyber security experts, with industry experience in leadership roles in enterprises PwC, PayPal, Walmart, Thoughtworks and EY, taking care of cyber security practices and global delivery in sectors like web3, finance, e-commerce, healthcare, insurance and telecom domains. We help companies in discovering their exposed data over the Internet. Post analysis, we score them on the basis of their existing security frameworks and recommend ways to improve their overall security posture. We also provide a threat protection program to make companies ready for any unforeseen future attacks.

Our Clients



Certifications



Conferences



Threat Modelling & Security Architecture Review

Threat modelling examines your security risk by adopting a hacker's perspective and Discover your main threats. It serves as the foundation for our security monitoring. We evaluate the risks posed to your vital assets and work with you to create use cases based on plausible scenarios that also consider the efficacy of current safeguards. Then, in order to give Security Analysts and Incident Responders useful alerts, we develop enhancements to SIEM rules tailored to the use cases.

Threat Model

- Prioritized assets based on risk
- threats listed in order of likelihood
- Most likely to occur are attacks
- current defence's chances of success or failure
- Remedial actions to lessen the dangers

Benefits of Threat Model

- Before writing a single line of code, identify issues in the SDLC as early as possible.
- Spot design flaws that traditional testing methods and code reviews might overlook
- Target your testing and code review to get the most out of your testing budget.
- Find the gaps in your requirements procedure.
- Avoid spending money on pricey code rewrites and fixing issues with software before it is released.

Security Architecture Review

1. Review current security architecture of organization and provide recommendations
- Conduct meetings and discussions with organization along with the key stakeholders to understand the existing security & network architecture
 - Gain an understanding of the network topology of all managed and unmanaged devices and the placement of various network and security components
 - Identify global information security framework and standards comprising of security best practices
 - Obtain the configuration for respective managed devices through tools and placement of unmanaged devices
 - Examine the current security architecture layout, its design and functioning
 - Identify the security risks associated with the existing network & security architecture
 - Prepare security architecture review report along with the recommendations



OUR PROCESS

SECURITY ARCHITECTURE REVIEW

Governance, risk and compliance

Policy Management

Governance framework

Standard/ Guidelines/
Regulatory requirements

Security metrics

Risk management

Management review

Management commitment

Audit and assessment

Governance, risk and compliance

Business security architecture

Information security management system

Data security architecture

Data leakage prevention

Data migration

Data protection and privacy

Data Sharing

Data retention and disposal

Data in rest and transit

Data encryption

Data classification

Data backup and recovery

Application security architecture

Authentication

Access control

Input validation

Key management

Session management

Secured SDLC

Secure transmission

Sensitive data handling

Infrastructure security architecture

Data center security

Computing environment security

Network security

Data Sharing

Physical security

Perimeter security

Storage security

Disaster recovery

Cloud security



CONTACT US! GET SECURED!



DeTaSECURE



SEND US AN EMAIL

contact@detasecure.com



VISIT OUR WEBSITE

www.detasecure.com



contact@detasecure.com