Data Sheet

DTS SOLUTION
CYBER SECURITY REDEFINED

Secure-by-Design
Threat Modeling Critical Services

Protecting critical business services from potential cyber risks should be one of the most important task your IT security team should perform. More often that not the right approach to implementing cyber defense mechanisms to protect critical services are adhoc, inconsistent and most likely follow insecure-by-design principles due to various internal factors. Identifying the multidimensional exact attack surface of the service may not be adequately performed leaving the service vulnerable to potential external and internal cyber threats.

DTS Solution can help your organization identify critical services, perform a complete threat modeling exercise across your critical services that may compose of complex interconnected web applications, API interfaces, middleware systems, databases, authentication servers and many more that all interact with each other to deliver the service.

Performing a **comprehensive threat modeling** exercise not only ensures the data flow diagrams (DFD) across the different systems that compose the service are documented but deliver unpredented level of detail on the security controls required to protect the service such as network zoning and isolation, firewall policies, intrusion prevention signatures, web application firewall policies and profiles, secure coding, access control, auditing, logging and monitoring, encryption requirements etc.

Service interactions are assessed individually and collectivity based on threat level with appropriate controls requirements identified for your DevOps or SecOps team. Whilst looking at the system interaction in totality to ensure if a system does get compromises the likelihood on how that compromise can spread through lateral movement due to trust-relationships across systems.

The output of a single threat model begins with the identification, enumeration, and prioritization of all potential threats against an application.

However, when an organization has hundreds or thousands of applications, the output needs increase. At this level, organizations also need a consolidated view of all their threat models. This is where attack surface analysis becomes necessary within a Threat Modeling Methodology.

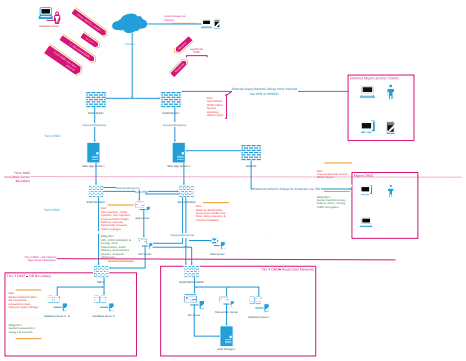
DTS Solution can help your organization in the following areas;

- Develop a Threat Modeling Methodology
- Perform Attack Surface Analysis
- Threat Model Templates
- Threat Trees and Attack Chaining
- Security Threat Case Monitoring

Threat Modeling Methodology

Various Threat Modeling Methodologies exist but mainly related to Software Development (DevOps) which does not provide the complete picture of how services interact as important layers such as networking, zoning, isolation, micro-segmentation, operations, administration and cyber security are not considered. OWASP Application Threat Modeling Methodology although very comprehensive only addresses application security.

DTS Solution will help your organization build a customized Threat Modeling Methodolgy that complements your infrastructure and mapped into your current level of available security controls and capabilities that covers all domains.



Threat Modeling Methodology

Attack Surface Analysis

An attack surface analysis is a measure of all the ways which an attacker can use to infiltrate, steal, damage, delete, or alter the available assets. DTS calculates it as a complex aggregation of all paths into and out of the various applications within an operational system, the valuable assets which are accessible along those paths, and the controls that protect these assets.

While the calculation may be complicated, understanding the resultant measurement is simple. The larger the calculated value, the more vulnerable the organization's applications and infrastructure are to attack.

SQL Injections, XSS, CSRF, API validation, Remote Access, Administrator Access, Authetnication using 2FA/OTP, Unauthorized Database Admin Access, Unknown 3rd party system interactions, storage of backup FTP folder to unknown location, monitoring agent using a Service Account that is not unique etc. are just some attack surface analysis performed, subsequently, identifying the appropriate countermeasures to protect against those threat vectors, leading to a "**Secure-by-Design**" or "**Secured-by-Monitoring**" environment.

Security Threat Case Monitoring

With the completed exercise of threat modeling, **DTS Solution** will help utilize the threat models and attack surface analysis information to develop advance monitoring and correlation rules within your SIEM solution to ensure any attack vectors are identified proacticely through your **Security Operations Center**.

Logging and auditing are key countermeasures identified across the service stack during the process of identifying defense and monitoring mechanism during the attack surface analysis phase.

DTS SOLUTION
CYBER SECURITY REDEFINED

DUBAI: Office 4, Oasis Center, Sheikh Zayed Road, Dubai, United Arab Emirates
T: +971 4 338 3365 | **E:** info@dts-solution.com

800 HACKED

ABU DHABI: Office 253, Al Bateen C6 Tower - Bainunah, King Abdullah Bin Abdulaziz Al Saud Street | **T:** 971 2 2076777
LONDON: 160 Kemp House, City Road, London, EC1V 2NX, United Kingdom | **T:** +44 2081230 387 (DTS)
www.dts-solution.com