DTS SOLUTION
CYBER SECURITY REDEFINED

White Team
Enterprise Security Architecture

The purpose of the security architecture blueprint is to bring focus to the key areas of concern for the enterprise, highlighting decision criteria and context for each security domain. Since security is a system property it can be difficult for enterprise security groups to separate the disparate concerns that exist at different system layers and to understand their role in the system as a whole.

DTS Security Architecture Design blueprint provides a framework for understanding disparate design and process considerations; to organize architecture and actions toward improving enterprise security.

Security services provide confidentiality, integrity, and availability services for the platform. Security services are implemented as protection services – such as authentication and authorization, detection services – such as monitoring and auditing, and response services – such as incident response and forensics. These services have served as the goals and objectives for information security programs for many years, but they do not provide an actionable blueprint as such. DTS Security Architecture Design enables your organization to map these security services into an overall enterprise security architecture blueprint.

The Enterprise Security Architecture Design Blueprint service is modeled on the following;

- Risk Management
- Security Policy and Standards
- Security Processes
  - Threat Management
  - Vulnerability Management
- Defense in Depth
  - Network Security
  - Host and Systems Security
  - Endpoint Security
  - Application Security
  - Data Security
- Metrics
  - Risk Metrics
  - Enterprise Reporting
  - Balanced Scorecard
- Assurance

DTS Solution Professional Services team specialize in developing standardized Information and Security Service Flow Analysis that are based on your Enterprise I.T architecture. Security Service Flow Analysis enables your organization to have complete visibility of services and applications within your infrastructure. Enabling your business to rapidly provision new services, understand application and server dependencies, how applications and services traverse your infrastructure and assist in identifying potential security risks. The end outcome of the Information and Service Flow results is a representation of the logical security architecture based on security domains and zones; and how services and applications interact within the infrastructure.

By developing Service Flows across the architecture and analyzing them, provide great in-depth knowledge, visibility and awareness in how security is maintained as services and traffic traverses different security environments.

Creating such a standardized framework for Security Service Flow; organizations are able to apply common service flow standards on existing infrastructure. More importantly such a standard is extensively used for organizations that need to provision and commission new services. Provisioning new services within your infrastructure can pose numerous challenges and as part of the service design phase many different teams within your organizations will require inputs that all need to be mutually agreed upon. With such challenges and having no common architecture framework, provisioning new services can indeed be a lengthy process. By developing a common architecture that illustrates the existing infrastructure and then by layering using security service flows can significantly enhance your understanding into how new services can be provisioned. The Information and Service Flow can also be utilized for operational and maintenance functions; where a complete end-to-end traffic flow can help in identifying, isolating and troubleshooting issues.

Network Security Audit

Network Security Audit is a fundamental part of any IT Security standard; with security dynamics within your organization ever changing, new threats materializing, risks exposure increasing, new applications provisioned with inherent security concerns, auditing becomes an integral process to ensure risks are contained and controlled.

Frequent Network Security Audit allows your organization to periodically assess and review the security posture of a certain environments; identifying key risk factors, categorizing them based on priority and severity level, quantifying the risk and placing an action on the risk. Risk management process is tightly integrated with our Network Security Audit service.

With qualified Information Systems Auditors, our Network Security Audit service is based on;

- Audit Scope and Statement of Work – Identifies which environment the audit will take place
- Identification of Risks within the particular environment – information gathering and assessment
- Categorization of Risk based on severity
- Quantify the Risks based on probability and likelihood
- Business Impact Analysis
- Risk Management recommendation – mitigate, acceptance, transference and action for residual risk
- Audit reporting and communication

Network Security Audits can be requested in the following areas;

- Network Firewalls
- Intrusion Prevention System
- Web Application Security
- Database Security
- Network and System Management Security
- Infrastructure Hardening