DTS SOLUTION
CYBER SECURITY REDEFINED

White Team
Data Protection and Privacy

Enterprises keep vast amount of data — whether that is corporate data or data related to personal / customer identities. Data classified based on its sensitivity levels needs to be protected with the right level of security, to ensure it does not fall into the hands of the unwanted.

In the modern-day information plays a critical role across the value chain from individuals, organizations, institutes and nations. Data and information has intangible value and the value the data possess drives the cyber risk landscape. The next war is undoubtedly a cyber war, where espionage, data theft, intellectual property compromise, privacy information leak, leaked credentials have gained in significance and have been exposed over the last few years. From nation-state cyber-attacks to hacktivist individuals targeting organizations the requirement to protect sensitive and corporate confidential data is more important than ever before.

Data security protection and privacy services are concerned with the appropriate and legal use of corporate confidential, personal and sensitive personal data throughout the data's lifecycle. This includes how data is collected, processed, stored, maintained, protected and disposed of irrespective of the format and systems used.

DTS Solution — White Team offer comprehensive services for all sizes of organizations to assess and advise on how they manage, protect and process the corporate and personal data of both their customers and staff in line with the organization's legal and regulatory obligations such as **GDPR, NESA, SIA, ISR** and **PCI-DSS**.

Data Protection Program Development

- Design a reporting strategy to meet the objectives of the business stakeholders
- Design and develop a data classification policy and process
- Define processes for data protection policy creation and modification
- Design policy lifecycle including policy tracking, refinement, and review cycles
- Design incident response training
- Design employee communication strategy and security awareness training

Data Classification

Determining how to properly classify your data and implementing the appropriate controls for your organization's critical information assets can be a formidable task. The various methods of how business units create and use their data often make it difficult to properly identify what information is critical and when and how it needs to be protected.

DTS Solution — White Team on Data Protection and Privacy services. uses an effective and concise methodology to help educate your employees, enable your business units to properly document critical information assets with the correct classification and protection. This process is well documented and presented to the security leadership team with a management summary including a description of the information and its use, the relative risk level for each threat, existing controls and the security controls requested by the business owner.

Sample Key Deliverables

- Critical information assets report including process flows and use by business unit
- "How To" guide to data classification for business units and employees daily use
- Manual or Automated Process
- Integration plan with existing Data Loss Prevention program
- Training that enables your staff to conduct re-assessments using the same methodology

Benefits

- Improve current information security controls and strategies
- Identify proper data handling based on approved classification therefore closing gaps in information protection
- Obtain buy-in for information security strategy from key stakeholders
- Provide staff with a repeatable method for current and future data classification needs

Data Loss Prevention

With the ever-increasing data breaches and insider threats that face companies on a daily basis, effectively leveraging Data Loss Prevention technologies can drastically reduce data loss risk.

Implementing DLP technology is the initial step towards protecting a company's most critical data. However, the initial phase is where most companies get stuck and being unable to progress, the true value of a mature Data Loss Prevention program is lost.

Based on leading-edge best practices, DTS provides a repeatable mature method of properly protecting a company's sensitive data and integrating fully in the security ecosystem ensuring that DLP does not operate in a silo fashion.

We start with a health check assessment, identify critical areas of improvement, and provide a methodical action plan to ensure the growth and maturity of DLP into a best-in-class program.

Health Check Assessment

- Comprehensive assessment of current state people, process, and technology of Data Loss Prevention
- DLP Program Maturity Scoring
- Identifying and protecting critical organization data
- DLP Policy Maturity and Lifecycle
  - Design incident response training
  - Business integration with key stakeholders
  - Organizational Communication
- Technical Presence: Review the effectiveness of technology implemented and coverage across the environment

DATA Protection Operation Lifecycle

Leveraging your DLP technology effectively to protect a company's most sensitive data involves the combination of people with the right business processes operating in a consistent manner regardless of the continual changing environment. However, organizations sometimes struggle can dedicate the staff necessary to maintain and build an efficient DLP program.

Our professional services from **DTS – White Team (Advisory and Consulting)** offering provides organizations with the support they need for operational management, strategic development, expansion, and consistent improvement to their DLP program.

DTS delivers customized services to meet your organization's needs. Our consultants provide:

- Engage and manage stakeholder involvement in policy development and remediation workflow
- Define and operationalize DLP Policy lifecycle management procedures
- Develop and implement the Incident Remediation strategy for each phase in the policy lifecycle
- Initial event remediation triage of events and utilizing results to improve policy accuracy
- Implement strategic DLP integration with Finance, Supply Chain, Customer Relationship Management, Human Resources, Corporate Communications, Legal, Compliance , IT processes
- Provide reports, dashboards and recommendations for improved corporate security practices
- Mature the DLP program to a maintainable, repeatable and operational state

Key Benefits

- Augment your current team with highly specialized staff who have extensive experience building effective DLP programs
- Ensure your staff gain the knowledge and expertise needed to manage all aspects of your DLP program
- Mature your DLP program rapidly into a repeatable, sustainable, more automated data protection service