THIRU LABS

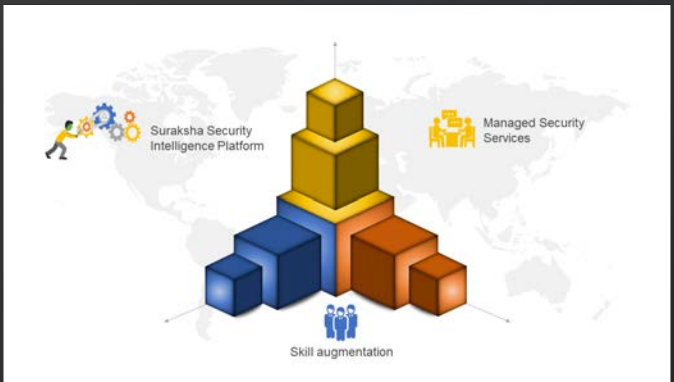
PROFESSIONAL SERVICES

ThIRU Labs

AUSTRALIA
USA
INDIA
CANADA
MIDDLE E

ThIRU lABS adds value to customers by providing a safe environment for businesses to operate without the worry of being robbed, hacked, harassed, blackmailed, attacked and destroyed by malicious elements. ThIRU lABS will provide an environment of low risk and safety for businesses and users to operate without fear in today's insecure globally internet environment.

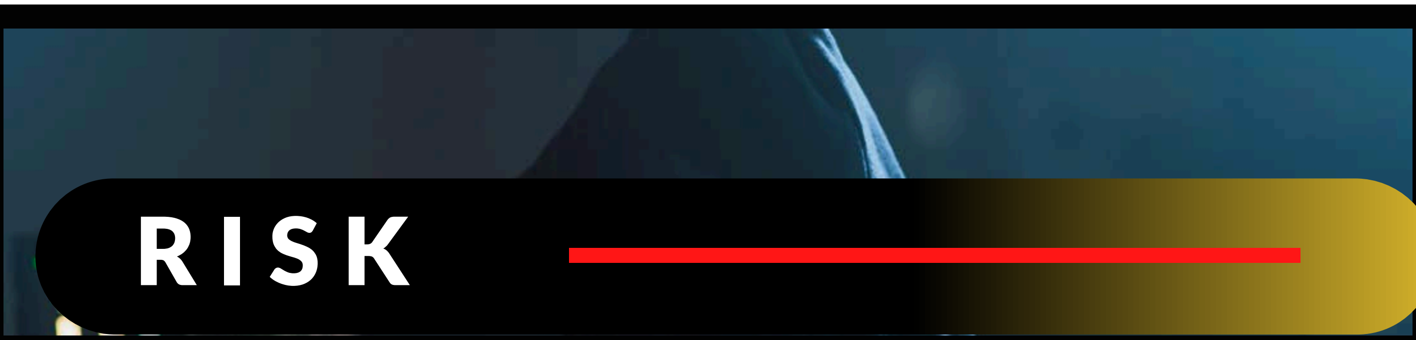
A SAFE PAIR OF HANDS


Suraksha Security Intelligence Platform
Managed Security Services
Skill augmentation

Deep technical expertise with broad governance and standards based services, ThIRU lABS offers necessary and immediate services to assist organisations manage the complexity of the global cyber threat landscape and risk exposures.

ThIRU lABS

www.thirulabs.com



RISK

SailPoint

CYBERARK

proofpoint.

ThIRU
Essentials

1ce

ThIRU EDR

ThIRU
SIRP

ThIRU
SOC | NOC | BOC | COC
Edge Device to End Point

f5

COLORTOKENS

aws

SALTSTACK

McAfee

TREND MICRO

KnowBe4
Human error. Conquered.

ivanti

CROWDSTRIKE

ENDPOINT
PROTECTOR

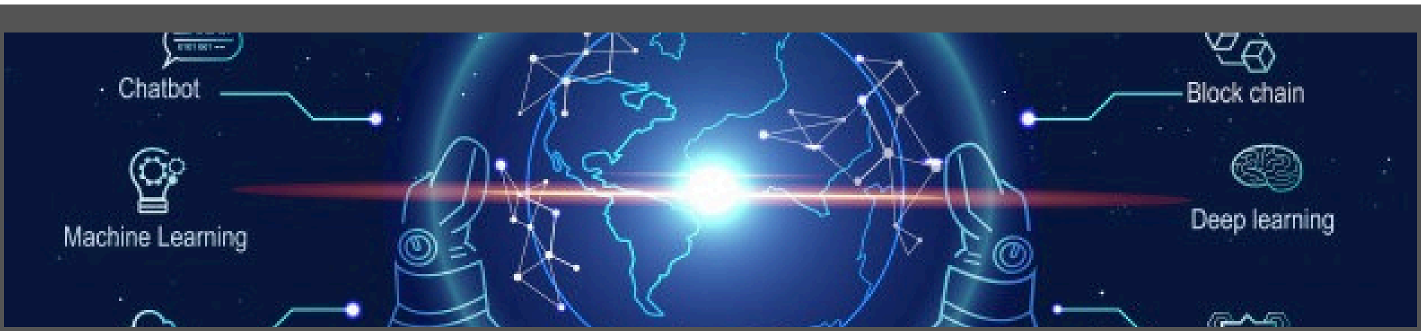
Forcepoint

SOLARWINDS

CRISCOD
AUDIT | ASSURE | TRAIN | MITIGATE RISK

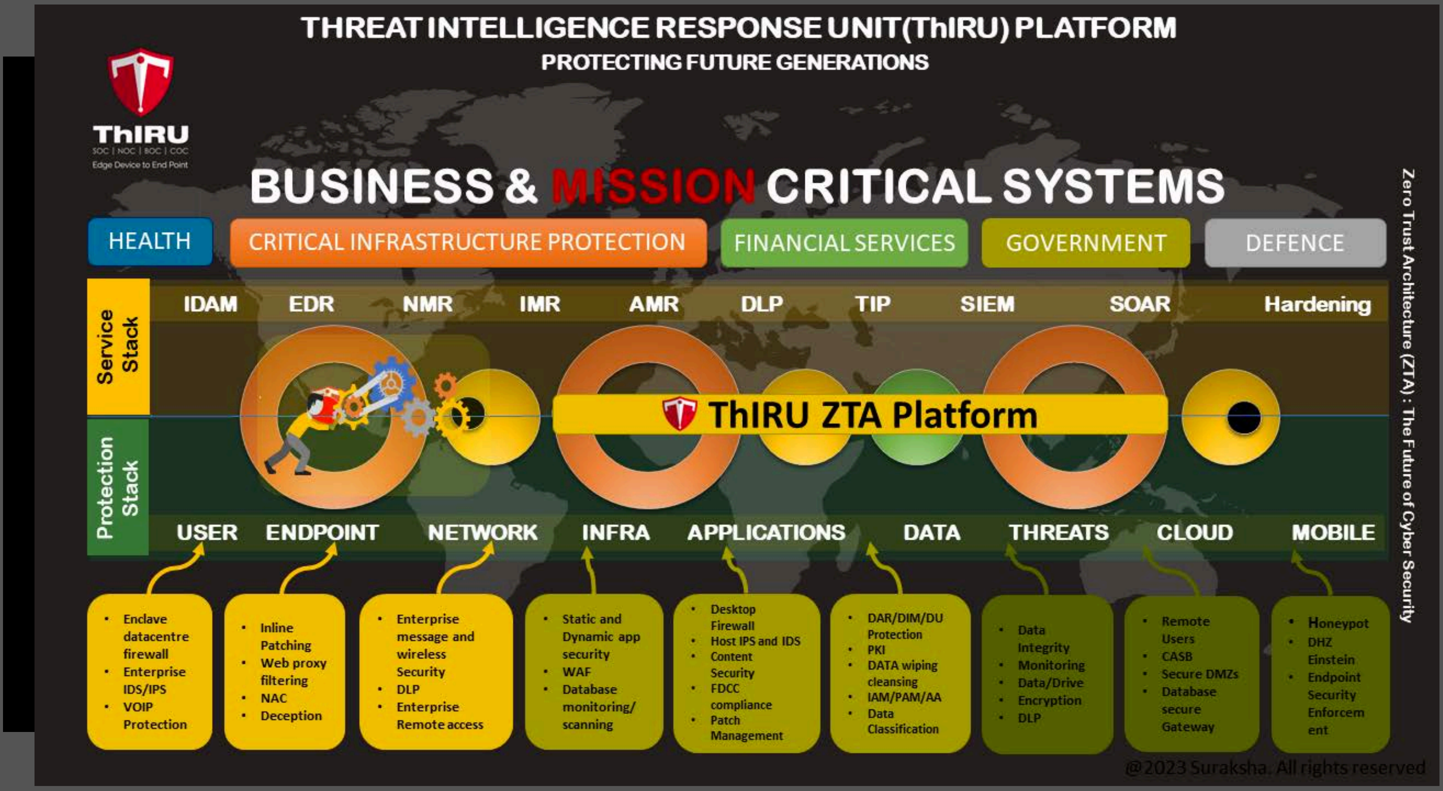
Microsoft

www.thirulabs.com



MITIGATE

Threat Intelligence Response Unit ThIRU



THREAT INTELLIGENCE RESPONSE UNIT(ThIRU) PLATFORM

PROTECTING FUTURE GENERATIONS

BUSINESS & MISSION CRITICAL SYSTEMS

HEALTH | CRITICAL INFRASTRUCTURE PROTECTION | FINANCIAL SERVICES | GOVERNMENT | DEFENCE

- Enclave datacentre firewall
- Enterprise IDS/IPS
- VOIP Protection

- Inline Patching
- Web proxy filtering
- NAC
- Deception

- Enterprise message and wireless Security
- DLP
- Enterprise Remote access

- Static and Dynamic app security
- WAF
- Database monitoring/ scanning

- Desktop Firewall
- Host IPS and IDS
- Content Security
- FDCC compliance
- Patch Management

- DAR/DIM/DU Protection
- PKI
- DATA wiping cleansing
- IAM/PAM/AA
- Data Classification

- Data Integrity
- Monitoring
- Data/Drive
- Encryption
- DLP

- Remote Users
- CASB
- Secure DMZs
- Database secure Gateway

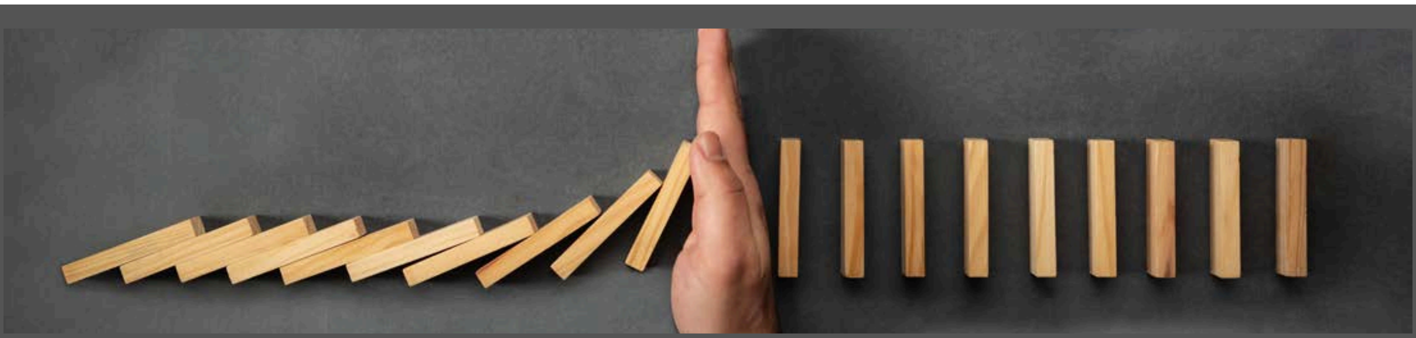
- Honeypot
- DHZ Einstein
- Endpoint Security Enforcem ent

@2023 Suraksha. All rights reserved

Monitoring across the architectures

Orchestration across the architectures

www.thirulabs.com



CYBER GOVERNANCE

CYBER THREAT AND RISK MANAGEMENT

- Plan Cybersecurity Risk Assessment
- Identify your critical business services and processes and associated information assets
- Conduct Business Impact Analysis (BIA) and Risk Assessment
- Map your critical information assets with defined cybersecurity
- Establish missing or not applicable cybersecurity capabilities
- Report to CIO/CISO/EXEC
- Annual Cybersecurity Risk Assessment

CYBER SECURITY INTERNAL AUDIT

- Plan
- Identify scope
- Execute the audit
- Formalize findings
- Report

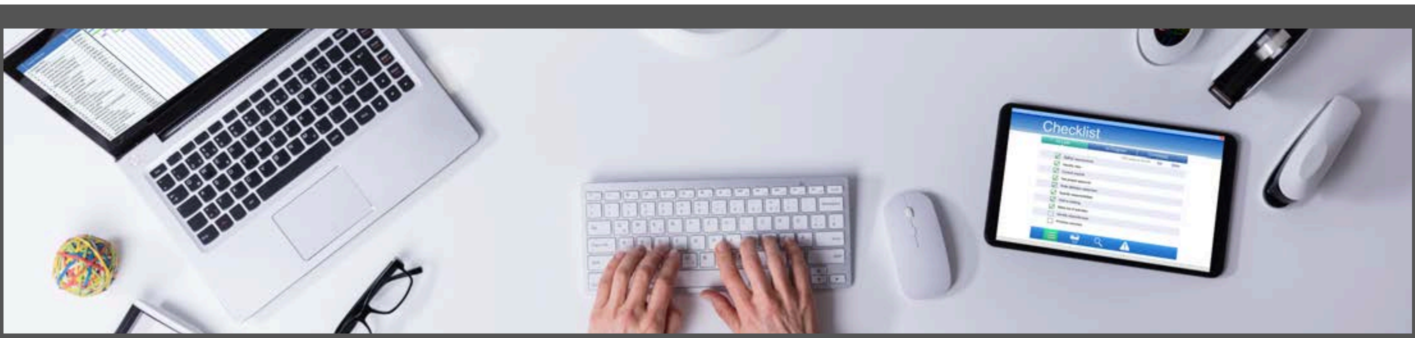
CYBER SECURITY AWARENESS & TRAINING

- Improve your learning and understanding of cybersecurity capabilities, latest cyber risks, current trends, and threat landscape
- Adequate planning and implementation of identified cybersecurity capabilities
- Develop techniques to identify, assess, manage & monitor your cybersecurity capabilities

CRISCOD
AUDIT | ASSURE | TRAIN | MITIGATE RISK

www.thirulabs.com

CRISCOD
A DIT | ASSURE | TRAIN | MITIGA E RISK



ENDPOINT SECURITY PROTECTION

A capability for protecting all endpoints such as servers, desktops, laptops, wireless devices, mobile devices and other OT/IoT devices connected to the network from cyber threats. This capability will implement the processes, controls and technologies required to build a sustainable endpoint protection program aligned to your business and focused on protecting all endpoints that matters most with respect to services provided fully protected

Harden ·

- Implement and enforce endpoint security configurations by applying it on operating system, application and network layers
- Define an endpoint security policy that dictates the type of configuration required on endpoint devices by supporting industry leading practices · Ensure that best practice security configurations are applied on endpoints ·
- Ensure that application whitelisting is applied on endpoints

Manage ·

- Track asset inventory of endpoint devices on asset repository by gathering all the details of hardware, operating systems, and applications changing and configurations·
- Ensure that endpoint changes, patches and configuration go through a controlled change management process to continuously log and track security requirements
- · Install security applications on endpoint devices to ensure that right protection is applied
- · Integrity checking mechanisms are used to verify software, firmware, and information integrity
- · Manage mobile devices, related applications, and apply security controls on mobiles devices including BYOD (bring your own device) and COPE (corporate-owned, personally enabled) devices

Monitor ·

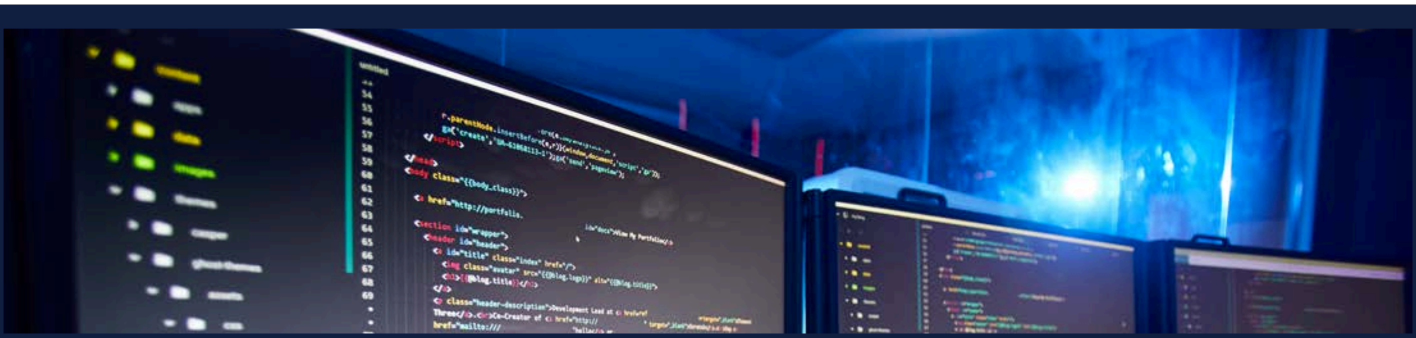
- Detect unprotected endpoints via security operation centre
- · Identify, track and detect abnormal behaviours or malicious activities
- · Ensure endpoint protection is applied

Dispose ·

- Manage reuse or final disposition of expired, obsolete devices, and unwanted endpoints in a secure manner
- · Ensure the information stored on obsolete, expired, and unwanted endpoints storage/media are appropriately sanitized

ThIRU EDR

www.thirulabs.com



APPLICATION SECURITY

Application Security capability is the processes use to prevent/detect/correct security weaknesses during the development, acquisition of applications and while using existing applications. Thereby reducing the application vulnerabilities before they are deployed and reduce the likelihood of successful exploitation.

Identity

- Software platforms and applications within the organization are inventoried
- · Identify in which of the following application lifecycle phases the application is:
  - Development
  - Implementation

Quality

- Select appropriate application security method based on the phase the application is

Application lifecycle phase

1. Application Security Method
   - Development
   - · Secure Coding
   - · Threat Modelling
   - · Design Review
2. Implementation
   - · SAST
   - · DAST
   - · Application – level vulnerability shielding

ThIRU
Essentials

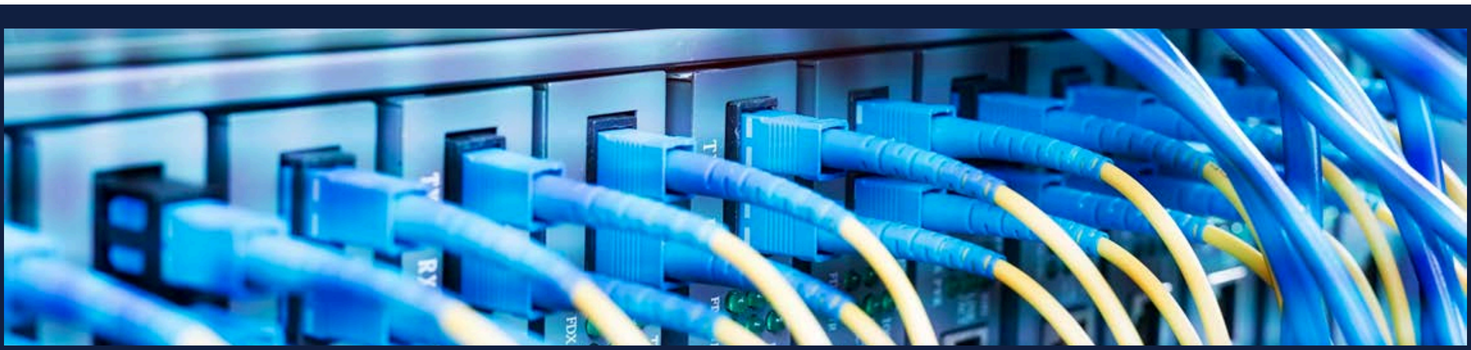
Test

- Test the application with the selected application security method

Treat

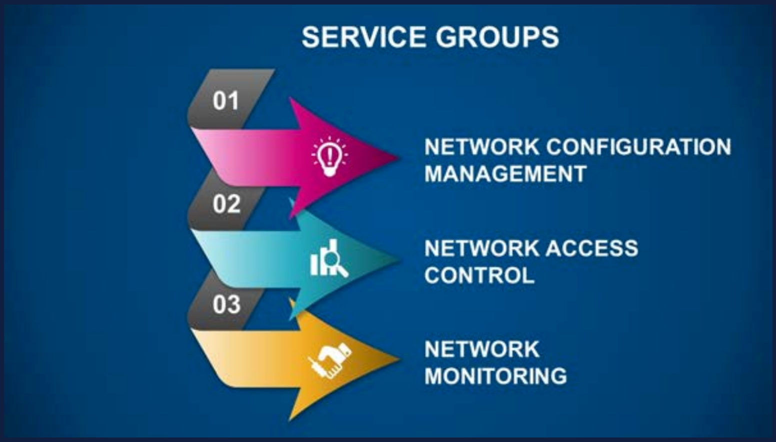
- Treat · The development and testing environments are separate from the production environment
- · Determine and document remediation of issues
- · Schedule treatment activity based on defined service levels
- · Apply remediation steps, adhering to established procedure
- · Track all changes made to the application

www.thirulabs.com



NETWORK SECURITY

A critical capability for protecting the Infrastructure and hardware used to interconnect devices and systems for communication internally and externally. This capability will implement the processes, controls and technologies required to build an effective Network Security program that is aligned to the business and focused on protecting all systems that matters most with respect to services provided for you.



SERVICE GROUPS

01 NETWORK CONFIGURATION MANAGEMENT

02 NETWORK ACCESS CONTROL

03 NETWORK MONITORING

SERVICES

Establish formal policies, procedures and guidelines

- Define program scope and identify target assets
- Establish governance and define roles & responsibilities (refer organization structure in Cybersecurity Governance chapter and compendium section of this chapter)
- Define availability criteria and acceptance standards
- Deploy/configure appropriate solutions to align with establish standards
- Deploy and train team members to support
- Identify opportunities of automation where applicable
- Define services levels for remediation activity
- Define rules of engagement which will be followed
- Continually improve policy, procedure & guidelines with changing risks and lessons learned

ThIRU
SOC | NOC | BOC | COC
Edge Device to End Point

www.thirulabs.com

NETWORK CONFIGURATION MANAGEMENT

Network Security Configuration Management is the process, in which the secure configuration baseline of network components is formalized and subsequently verified against the actual state.

PREPARE

- Network infrastructure devices within the organization are inventoried
- · Organizational communication and data flows within the system and between interconnected systems are mapped

IMPLEMENT

- A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
- · Network integrity is protected (e.g. network segregation, network segmentation)
- · Configuration change control and patch processes are in place and followed through change and patch management (refer
- change and patch management capability chapter)
- · Communications and control networks are protected
- · Mechanisms (e.g. failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations

www.thirulabs.com

MAINTAIN

- A baseline of network operations and expected data flows for users and systems is established and managed
- · Vulnerability scans are performed in collaboration with Security Monitoring and Operations

REVIEW

- Management and dashboard reporting of identified Security Configuration
- · Deviations.
- · Event detection information is communicated to appropriate parties
- - In case of Alert, Network Security Team will execute response actions
- - In case of Incident/Breach, Incident Response Team will execute response actions

Network Automation

Bandwidth Analysis

IP Address Management

Manage Configs

NETWORK ACCESS CONTROL MANAGEMENT

Network Access Control Management is the process to control – who (user) or what (devices) has authorized permission to access the network

PREPARE

- Physical devices and systems within the organization are inventoried
- Organizational communication and data flows within the system and between interconnected systems are mapped
- Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners)are established

PROVISION

- Physical and network access to assets is managed and protected
- Remote access of users and devices are managed
- Network integrity is protected (e.g., network segregation, network segmentation)
- Data-at-rest is protected (refer Data Protection capability chapter)
- Data-in-transit is protected (refer Data Protection capability chapter)
- Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
- Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction
- Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
- Mechanisms (e.g. failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations

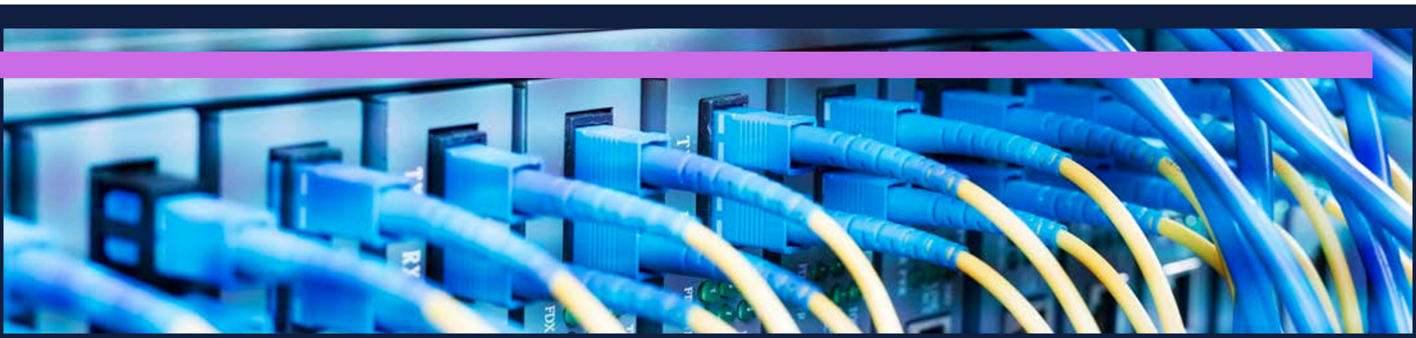
MAINTAIN

- A baseline of network operations and expected data flows for users and systems is established and managed
- Vulnerability scans are performed in collaboration with team responsible for Security Monitoring and Operations

REVIEW

- Management and dashboard reporting of identified Network Access Control deviations.
- Event detection information is communicated to appropriate parties
  - In case of Alert, Network Security Team will execute response actions
  - In case of Incident/Breach, Incident Response Team will execute response actions

www.thirulabs.com



NETWORK MONITORING MANAGEMENT

Network Monitoring Management, part of the Network Operations Centre (NOC), is a process to handle incidents and alerts that affect the performance and availability of the network.

Focus will be on: DDoS Attacks, power outages, network failures; Remote hands support, the configuration of hardware (such as firewalls and routers) routing black-holes; Port management; Communications with network users when a major incident occurs, impacting network services; and First level triage of network change requests; once validated, then forward to appropriate stakeholders

IDENTIFFY

- Physical devices and systems within the organization are inventoried
- Organizational communication and data flows within the system and between interconnected systems are mapped
- External network systems are catalogued
- Adequate capacity to ensure availability is maintained

www.thirulabs.com

DETECT

- Detected events are analysed to understand attack targets and methods
- Event data are collected and correlated from multiple sources and sensors
- Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
- Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
- Network Vulnerability scans are performed in collaboration with team responsible for Security Monitoring and Operations
- Network Monitoring processes are tested
- Network Audit/log records are determined, documented, implemented, and reviewed

RESPONSE

- Notifications from detection systems are investigated
- Coordination with internal and external stakeholders occurs consistent with response/escalation plans
- Event detection information is communicated to appropriate parties
- In case of Alert, Network Security Team will execute response actions
- In case of Incident/Breach, Incident Response Team will execute response actions

RECOVER

- In collaboration with Teams responsible for Security Monitoring and Operation and Incident Handling and Response
- Recovery plan is executed during or after a cybersecurity incident
- Incidents are contained
- Incidents are mitigated
    - · Newly identified vulnerabilities are mitigated or documented

Network Automation

Bandwidth Analysis

IP Address Management

Manage Configs

DATA

DATA PROTECTION & MANAGEMENT

A capability that prevent classified information from leaving an entity's boundaries without authorization or unauthorized use of data in general. This service will help in implementing the processes, controls and technologies required to build a sustainable data protection program aligned to the business and focused on protecting the data that matters most with respect to services provided to you.

IDENTIFFY

- Understand the entity's information assets
- Identify all information sources that needs to be protected based on its level of sensitivity, value, and criticality

CLASSIFY

Data labelling as it is created, using labels that are clear and meaningful

- Data classification process according to its value, sensitivity, risk of loss or compromise, legal and retention requirements for you
- Data categorized in terms of its need for protection (i.e. Public, Internal, Sensitive, Restricted, etc.)
- As per regulatory standards, this will be classified and managed

PROTECT

Protect data based on its classification, with the highest protections applied to the most sensitive data

DLP

MONITOR

- Understand how data is used and identify existing behaviour that puts data at risk
  - Monitor all data movement to gain visibility into sensitive data movement and determine the issues that need to be addressed

IMPROVE & REMEDIATE

- Improve and remediate · Continuously improve and remediate identified errors and processes
- Data Declassification or destruction and secure disposal

www.thirulabs.com

CHANGE & PATCH MANAGEMENT

The Change and Patch Management capability is a centre for all technological changes occurring in a technology environment. In other words, all information assets changes on endpoints, IoT, and OT devices configurations, patch deployment, and recovery activities undergo through a controlled environment and will be managed with this SERVICE.

Requirement Gathering

- Activities and processes are defined to ensure that business and security requirements are met
- Secure communication channels are established and maintained for communicating change, configuration, and patch requirements

AUTHORISATION

- Define authorization mechanisms to ensure change, patch, and required configurations activities are consistent and inline security/business requirements

IDENTIFICATION

- Define a process to allocate/identify required changes, patches, configuration and disposal of information assets requirements
- Establish a process to alert/notify relevant stakeholders on the required procedures for secure change, patch and configuration deployment
- Define a process to assess the change and security impact associated with all changes, patches, and configuration of assets
- Define rollback/recovery procedures to help restore undesired outcomes resulting impact on business/security operations
- Define a process to continuously log and document change, configuration, and patch deployments plan
- Establish a process to notify stakeholders in the event of breach and downtime resulting from changes, configuration, and patch deployment
- Define a process to detect, alert, investigate, and notify relevant stakeholders for unauthorized changes
- Establish a process to receive timely notification/alerts of required patches on information assets from third-party vendors

APPROVALS

- Define a process to ensure that deployed proposed changes, patches, and required configurations meet business and security requirements
- Establish and maintain secure communication channels to communicate, agree, and approve service outage and business outage resulting from change, configuration, and patch deployment activities within the change control committee

SALT

www.thirulabs.com

Thiru Essentiial
CYBER SESCURITY

CHANGE & PATCH MANAGEMENT

The Change and Patch Management capability is a centre for all technological changes occurring in a technology environment. In other words, all information assets changes on endpoints, IoT, and OT devices configurations, patch deployment, and recovery activities undergo through a controlled environment and will be managed with this SERVICE.

IMPLEMENTATION

- Establish a process to define and document change, configuration, and patch deployment plans
- Define mechanisms to address security requirements on production systems
- Define a process to ensure that changes, configuration, and patch deployment are tested in testing environment and meet security requirements
- Define mechanisms to alert/notify respective teams for change, configuration, and patch deployment and monitoring activities
- Maintain segregation of duties in deployment activities and environments in terms of approvals, testing/verification, development, and deployment
- Establish a process for notifying internal and external stakeholders for planned and unplanned outages

LOGGING

- Define and maintain an asset repository to log all changes, configurations, and patches in terms of requirement descriptions, impact ratings, category, authorizations, and approvals
- Establish a process to log and track issues and risks associated with the changes, configurations, and patches are communicated and audited/reviewed by respective stakeholders
- Establish a process to capture, log, and report change, configuration, and patch deployment outcomes are correctly distributed among respective stakeholders
- Define escalation mechanisms and actions plans with internal and external stakeholders in the event the security breach/unauthorized changes have occurred

ThIRU
SIRP

www.thirulabs.com

SECURITY MONITORING

Security monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. As a pre-requisite of security monitoring a baseline of network operations and expected data flows for users and systems is established and managed.

COLLECTION

- Security audit/log records are determined, documented, implemented, and reviewed in accordance with policy
- Roles and responsibilities for order of operation are well defined to ensure accountability
- Detection activities comply with all applicable requirements
- Cyber threat intelligence is received from information sharing forums and sources

FUSION

- Event data are aggregated and correlated from multiple sources and sensors
- Malicious code is detected
- Unauthorized mobile code is detected

ANALYSIS

- Detected events are analysed to understand attack targets and methods; accordingly, triage is conducted
- Impact of events is determined
- Incident alert thresholds are established
- Monitoring for unauthorized personnel, connections, devices, and software is performed
- The network is monitored to detect potential cybersecurity events
- The physical environment is monitored to detect potential cybersecurity events
- Personnel activity is monitored to detect potential cybersecurity events
- Vulnerability scans are performed
- External service provider activity is monitored to detect potential cybersecurity events

ACTION

- Event detection information is communicated to appropriate parties
  - In case of Alert, Security Monitoring Team will execute response actions
  - In case of Incident/Breach, Incident Response Team will execute response actions
- Detection processes are tested
- Detection processes are continuously improved

ThIRU
SOC | NOC | BOC | COC
Edge Device to End Point

www.thirulabs.com

INCIDENT HANDLING & RESPONSE

A reactive capability that addresses and manages effects of an attack or anomalous activity. It is an essential capability required to respond all incidents occur with respect to your environment

PREPARATION

- Incident Response plans are prepared, in place and managed
- Personnel know their roles and order of operations when a response is needed
- Prepare Incident Response Contact List which should include contact information of all internal and external stakeholders
- Define a secure way of communication such as encryption software (Rights Management Servers/PGP Keys/Digital Certificates) for communication among stakeholders, especially external
- Response plans are tested
- Response planning and testing are conducted with critical suppliers/providers

DETECTION & ANALYSIS

- Events are reported consistent with established criteria
- Notifications from detection systems are investigated and triage is conducted
- An Incident Response plan will be executed during or after an event
- Incidents are categorized and the impact of the incident is understood
- Malicious code is detected which have been identified as a part of analysis
- Forensics are performed, where required,
- Newly identified vulnerabilities are mitigated
- Information is shared consistent with response plans
- · Mechanisms shall be put in place to monitor, track and quantify the types and volumes of cyber security incidents
- · Processes are established to receive, analyse and respond to vulnerabilities

CONTAINMENT ERADICATION & RECOVERY

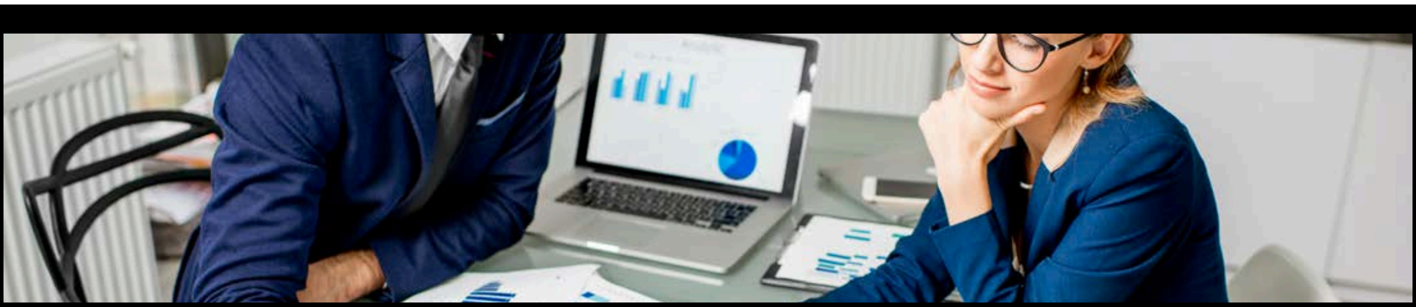
- Incidents are contained
- Incidents are mitigated
- Coordination with stakeholders occurs consistent with response plans
- Voluntary information sharing occurs to achieve broader cybersecurity situational awareness
- Recovery plan is executed during or after an event
- · Recovery activities are communicated to internal stakeholders and executive and management teams
-

POS INCIDENT ACTIVITY

- Response plans incorporate lessons learned
- Response strategies are updated
- Recovery plans incorporate lessons learned
- Recovery strategies are updated
- Public relations are managed
- Reputation after an event is repaired

www.thirulabs.com

ThIRU
SIRP



DATA PRIVACY

A capability that ensures compliance to legally binding regulation for protecting personally identifiable information as per the privacy and international regulations. This capability will implement the processes, controls and technologies required to build a sustainable data Privacy capability

DESIGN

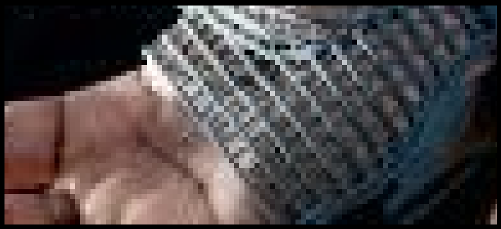
- Establish an overall sense of direction and principles for action with regards to protection of Data/Information in the Entity
- · Establish the Governance for management of Privacy Framework
- · Provide direction and support for implementing controls to protect Data/Information, compliance with applicable laws and regulations and to implement best practice
- · Define purpose for collection, lawful/rightful usage, disclosure, transfer, retention, archival and disposal process of private data

IMPLEMENT

- Establish Privacy Impact Assessment (PIA) to analyse how Personally Identifiable Information (PII) is collected, used, disseminated, and maintained
- · PIA and implementation of controls shall be performed on those Personal Identifiable Information (PII) data elements as identified in the PII inventory
- · The PIA report shall identify and assess the impacts of all business functions on the privacy of personal information of customers, employees, & vendors/contractors together with the suggested remediation for treating or mitigating those impacts including level of risk associated to the processing ofthat information

VALIDATE

- Establish a process for evaluating the effectiveness of privacy structure and continuously improve the composure of the Entity
- · Conduct periodic audits and performance reviews of the Privacy Management Framework
- · Review if implemented privacy and security controls are functioning as required



OPTIMISE

- Embed Privacy within the organization’s culture
- · Include management of Data/Information as part of organizational core values and effective management
- · Establish a process for evaluating the effectiveness of privacy structure and continuously improve the composure of the organization and the consequences of nonconformity
- · Raise, enhance and maintain awareness of Privacy through an ongoing education and awareness programme for all
- employees and stakeholders

www.thirulabs.com

CRISCOD
AUDIT | ASSURE | TRAIN | MITIGATE RISK

IDENTITY & ACCESS MANAGEMENT

AA capability that manages the right individuals to access the right resources at the right times for the right reasons. Identity and access management (IAM) addresses the mission-critical need to ensure appropriate access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices with respect to services provided for the global market.

DESIGN

- Directory services have been implemented.
- Unique, Digital identities have been identified including people (internal employees, contractors, external constituents, or business partners), systems, and services.
- Remote access logins are considered while defining strategy for identity and access management.
- Consider mobility and cloud as future drivers for how IAM could be enforced having a maturity self-measurement mechanism
- Security risks have been identified for identities and its access rights during the risk assessment

IMPLEMENT

- Establish formal IAM policies, procedures and guidelines
- Define IAM program scope
- Establish governance and define roles & and responsibilities
- Define acceptance standards
- Deploy/configure appropriate solutions to align with established policies and standards
- Deploy and train team members to support IAM processes and continually improve IAM policy, procedure guidelines with changing risks and lessons

VALIDATE

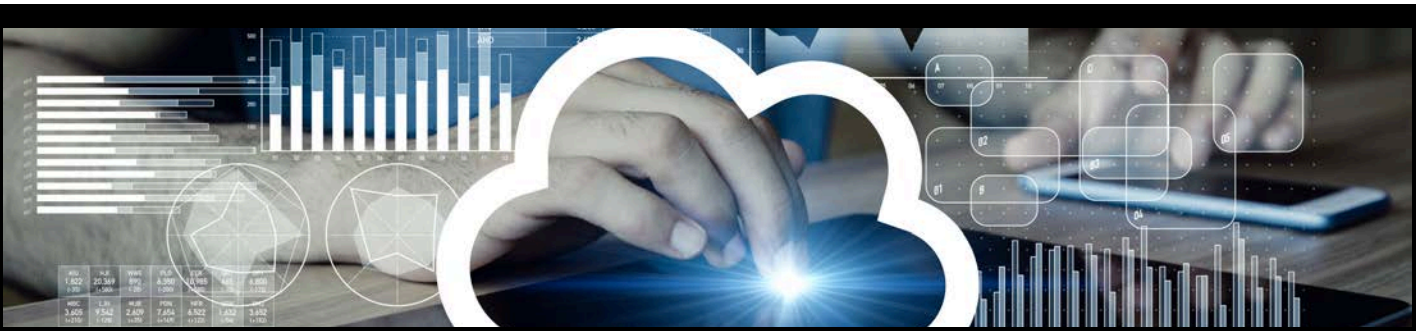
Establish processes and tools to understand the health of the various IAM components

- Identify opportunities for improvement in processes
- Provide evidence for access reviews,audit activities,
- Demonstration of compliance to policies, standards, and regulations.
- Access and review certification
- Policy compliance monitoring
- Role and definition certification

OPTIMISE

- Identity & Access Administration:
- Access Control:
- Provisioning:
- Role Management:
- EntitlementManagement:
- Access Logging and Monitoring:
- Identity Audit:

www.thirulabs.com



CLOUD ASSET SECURITY HARDENING

A proactive capability that ensures the secure operations of the entity cloud services offered by a local Cloud Service Provider (CSP). The capability will focus on how to ensure proper hardening for your cloud-based assets.

STRIPPNG APPS

- · Removing unnecessary software apps
- All systems come with a predefined set of software packages and software modules that are generic and assumed to be useful for
- general use. Based on your intended use of the system, you should disable/remove all unnecessary software

STRIPPING CREDENTIALS

- Disabling or removing unnecessary usernames and credentials (Several software has come with predefined user accounts for various uses - from remote support to service accounts for specific services.)
- Removing all remote support and service accounts which are not to be used Besides changing, all default passwords

STRIPPING SERVICES AND CONNECTIVITY

- Disabling or removing unnecessary services and ports
- · (Remove all services, which are not used in production. You can always just disable them, but if you have the choice remove them altogether. This will prevent the possible errors of someone activating the disabled service further down the line)

PATCHING & BASELINING

- Applying security and functionality patches (Covering operating system and all approved applications)

VERFICTION

- Performing a full scan for verification purposes preferably twice a year

ThIRU
SIRP

www.thirulabs.com

TRANSPORT & INFRASTRUCTURE

Financial
services
Banking
Insurance
Investment
Houses

Government
Departments
Agencies
Statuotory
authorities

Critical
Infrastructure
Electricity
Water
Airports
Infrastructure
Telecommunications

Health
Hospitals
Community centres
Field emergency

Defense
Airforce
Land force
Navy

WWW.THIRULABS.COM
305, 65 VICTOR CR
NARRE WARREN VICTORIA
AUSTRALIA 3805

ThIRU Labs