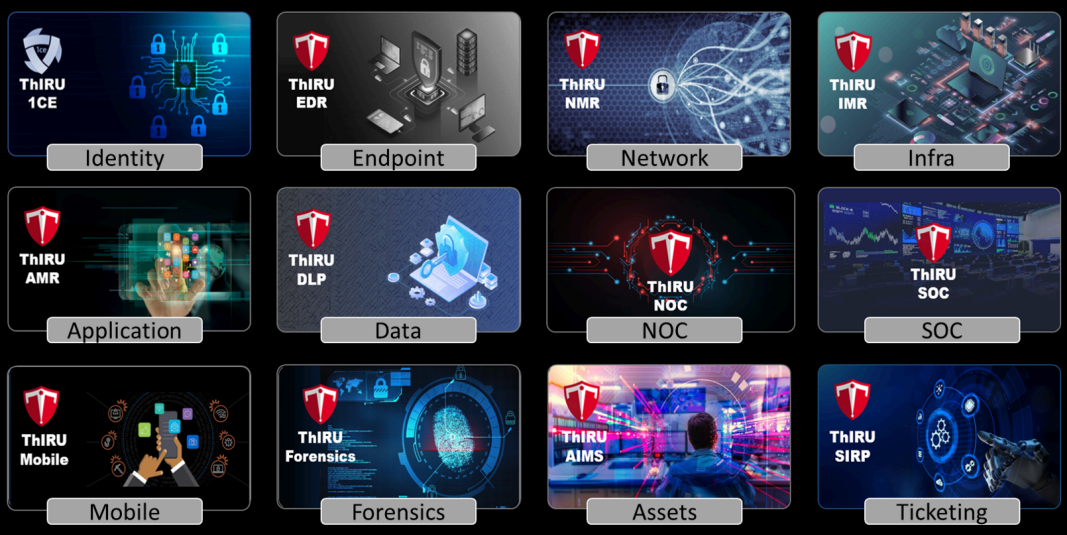
CASE STUDY I

Hamad Port - Qatar

FIFA World Cup 2022

Hamad Port is ranked the eighth most efficient gateway in the world on the World Bank and S&P's Container Port Performance Index 2022. Threat Intelligence and Response Unit (ThIRU) Security Operation Centre (SOC) solution provisions front-line cybersecurity for the port's mission-critical systems.

Inaugurated officially on September 5, 2017, and managed by Mwani Qatar under the Ministry of Transport, Hamad Port is a pivotal component of Qatar's National Vision 2030. Beyond its three container terminals, the port specialises in handling various cargo types, including livestock, automobiles, and bulk grain. With a dedicated offshore and marine support vessel base, the port facilitates the entry of approximately 500,000 vehicles annually.



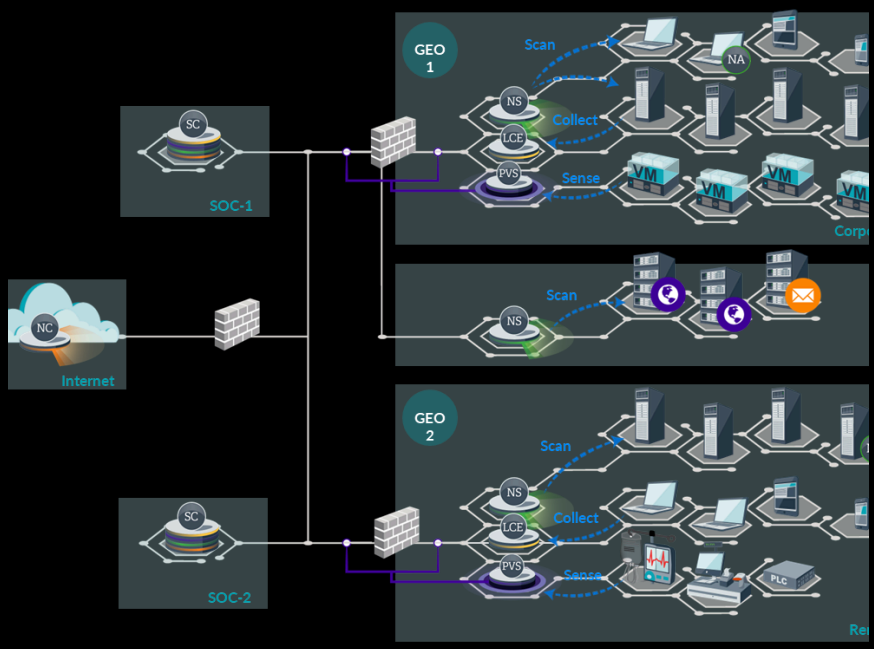
Threat Intelligence and Response Unit (ThIRU) SOC software solution collects, and aggregates log data generated throughout the data centre technology infrastructure, from host systems and applications to network and security devices including firewalls and antivirus filters. The software then identifies and categorises incidents and events, as well as analyses them. EDT, NMR, AMR and SIRP were provided as part of the solution.

ThIRU Zero Trust principles "Trust No One - Verify Everything"

THIRU SOC
FULLY INTEGRATED

Visualisation & Analytics

Extreme analytics of data for compliance

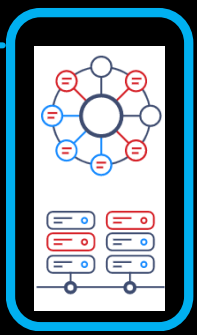


ThIRU

FIFA WORLD CUP Qatar2022

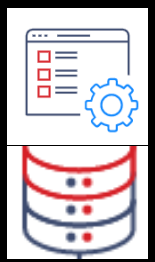
Primary Data Centre (PDC) The Hamad Port PDC comprises a 500 rack major infrastructure with over 65,000 IPs and over 3500 servers set up primarily for the **FIFA 2022 Mens World Cup** to service the new port project, package 64.

Modular DR Centre (SDC) Assessing the security compliance of device endpoints - the hardware accessing your data – desktop, laptop and mobile will be protected to prevent data leakage



Network Monitoring Data from NMS and 3rd party SIEM seamlessly integrated for monitoring provided

Data Transfer Infrastructure monitoring and risk profiling. Data from both the OT & IT infrastructure directly and also through other 3rd party systems integrated for risk mitigation. Securely provided in the solution.



Applications Application level monitoring for the port management system, asset management system and independent local applications including GIS were monitored and protected.

Data & Database Data base monitoring and TDE were established as part of the solution to prevent data leak prevention.

ThIRU Zero Trust principles "Trust No One - Verify Everything"

+61 (0) 417 567 658
info@thirulabs.com
www.thirulabs.com

ThIRU LABS

www. thirulabs.com | www. 1ceid.com
305, 65 Victor Cr. Narre Warren VIC 3805

CASE STUDY II

Ministry of Education - Qatar (25,000 students, 3,000+ staff, 1000+ admin)

Community College of Qatar (CCQ)

Lusail Smart City Qatar - FIFA World Cup 2022

1CE Platform - Identity and Access Management

Objectives

The Ministry of Education and Community College of Qatar is embarking on a transformative project to enhance its cybersecurity infrastructure and ensure the secure and efficient management of user identities, access privileges, and authentication authorization processes.

Challenges

Striking the right balance between security measures and user-friendly access is a challenge. Implementing stringent security measures without compromising user experience requires careful planning and customization.

Solutions

This project aims to provide ThIRU 1CE Identity product platform to facilitate features of:
User Authentication and Authorization, Identity Lifecycle Management, Business workflow, Organization management, Application management and external integration including Azure AD

KEY COMPONENTS

ThIRU 1CE

The 1CE identity platform, developed by ThIRU Labs, is a comprehensive identity and access management (IDAM) solution designed to enhance cybersecurity through a Zero Trust Architecture (ZTA). This platform focuses on securing digital identities and managing them across their entire lifecycle, offering robust protection against unauthorized access and data breaches.

ThIRU 1CE platform, developed in-house, will act as the user interface for the IAM system. It will provide a user-friendly portal for students, faculty, and staff to manage their accounts, access resources, and request additional privileges. ThIRU 1CE will offer a single sign-on (SSO) experience, streamlining access for end-users. ThIRU 1CE is capable of providing functionally of secure access, organization management, lifecycle management, business workflow automation and external integrations including Azure.

Identity Lifecycle Management

1CE will serve as the core IAM solution, providing a centralized platform for managing user identities and access. The integration will automate the provisioning and de-provisioning of user accounts, ensuring timely and accurate access management.

Business Workflow Management

The workflow management feature of the 1CE platform by ThIRU Labs streamlines and automates the processes of user creation, deletion, and provisioning, ensuring secure and efficient identity management.

Secure Access through 1CE Authentication and Authorization

1CE will be employed for seamless and secure authentication and authorization processes. Multi-factor authentication (MFA) and adaptive authentication will be implemented to enhance security while providing a user-friendly experience.

1CE Integration with Active Directory

The 1CE platform by ThIRU Labs includes robust integration capabilities with Active Directory (AD) and Azure Active Directory (Azure AD), facilitating seamless identity and access management across on-premises and cloud environments.

ThIRU Labs

CASE STUDY III

Strengthening Cybersecurity at Dr. Dixit Medical Center

Results

A “One stop shop” for medical record and data protection in public and private hospitals, community centers, pathologies, radiology practices and medical laboratories. ThIRU offers necessary and immediate services to assist organizations manage the complexity of medical record protection.

By implementing ThIRU Essentials and the cybersecurity practices, Dr. Dixit Medical Center achieved significant improvements in its cybersecurity posture:

- Enhanced Protection
- Regulatory Compliance
- Increased Resilience

Client Overview

Dr. Dixit Medical Center, a renowned healthcare facility, is committed to providing exceptional medical services to its patients. With a wide range of specialties and state-of-the-art medical equipment, the center caters to diverse healthcare needs. However, in the digital age, safeguarding patient data and ensuring the integrity of critical systems against cyber threats has become a paramount concern.

Challenge

As technology increasingly integrates into healthcare operations, Dr. Dixit Medical Center faces the challenge of protecting sensitive patient information and maintaining the confidentiality, integrity, and availability of its digital assets. With the rise of sophisticated cyber threats targeting the healthcare sector, including ransomware attacks and data breaches, the center recognized the urgent need to enhance its cybersecurity posture.

Solution: ThIRU Essentials

To address the cybersecurity needs of Dr. Dixit Medical Center, ThIRU Essentials, a leading provider of comprehensive cybersecurity solutions, was engaged to implement a robust defense strategy tailored to the unique requirements of the medical sector. Leveraging its advanced capabilities, ThIRU Essentials designed a multifaceted cybersecurity framework to fortify the center's digital infrastructure and mitigate cyber risks effectively.

1. Endpoint Protection: ThIRU Essentials deployed advanced endpoint security solutions across all devices and endpoints within the medical center's network. This included endpoint detection and response (EDR) systems, and device encryption to safeguard against malware, ransomware, and unauthorized access.
2. Network Security: A comprehensive network security architecture was established, incorporating firewalls, intrusion detection systems (IDS), and secure access controls to monitor and manage network traffic proactively.
3. Data Encryption: To protect sensitive patient information stored within databases and electronic health records (EHR) systems, ThIRU Essentials implemented robust encryption mechanisms. This safeguarded patient data both at rest and in transit, mitigating the risk of unauthorized disclosure or tampering.
4. Identity and Access Management: ThIRU Essentials' implementation of identity and access management (IAM) solutions provided granular control over user access to sensitive systems and data. This ensured that only authorized personnel could access patient records and critical resources, reducing the risk of insider threats and unauthorized access attempts.
5. Security Awareness Training: Recognizing the critical role of employees in maintaining cybersecurity hygiene, ThIRU Essentials conducted tailored security awareness training sessions for staff members at Dr. Dixit Medical Center. This initiative aimed to educate employees about common cyber threats, phishing attacks, and best practices for safeguarding sensitive information.

ThIRU Labs

CASE STUDY III

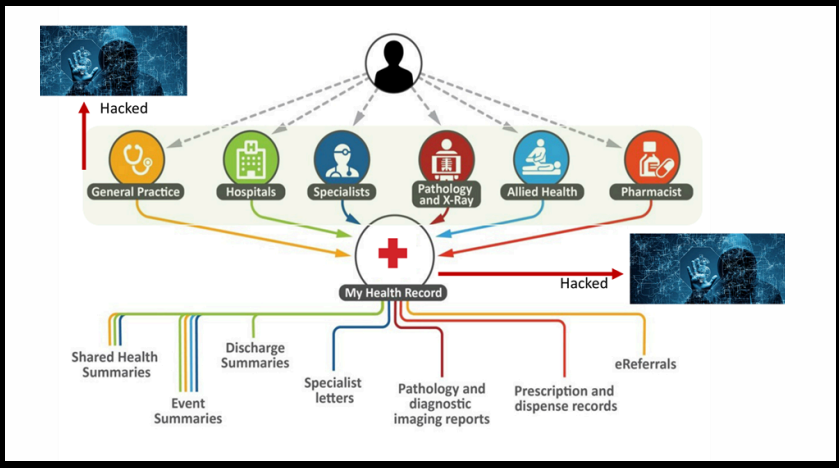
Strengthening Cybersecurity at Dr. Dixit Medical Center

Client Overview

Dr. Dixit Medical Center, a renowned healthcare facility, is committed to providing exceptional medical services to its patients. With a wide range of specialties and state-of-the-art medical equipment, the center caters to diverse healthcare needs. However, in the digital age, safeguarding patient data and ensuring the integrity of critical systems against cyber threats has become a paramount concern.

Challenge

As technology increasingly integrates into healthcare operations, Dr. Dixit Medical Center faces the challenge of protecting sensitive patient information and maintaining the confidentiality, integrity, and availability of its digital assets. With the rise of sophisticated cyber threats targeting the healthcare sector, including ransomware attacks and data breaches, the center recognized the urgent need to enhance its cybersecurity posture.



- Medicare billing process & data
- Patients' identity data
- Patients' privacy data
- Practice management application
- Referals & clinical application
- Online & remote consulting
- E-prescriptions

HIGH RISK EXPOSURE

Solution: ThIRU Essentials

To address the cybersecurity needs of Dr. Dixit Medical Center, ThIRU Essentials, a leading provider of comprehensive cybersecurity solutions, was engaged to implement a robust defense strategy tailored to the unique requirements of the medical sector. Leveraging its advanced capabilities, ThIRU Essentials designed a multifaceted cybersecurity framework to fortify the center's digital infrastructure and mitigate cyber risks effectively.

1. Endpoint Protection
2. Network Security
3. Data Encryption
4. Identity and Access Management
5. Security Awareness Training

Results

A "One stop shop" for medical record and data protection in public and private hospitals, community centers, pathologies, radiology practices and medical laboratories. ThIRU offers necessary and immediate services to assist organizations manage the complexity of medical record protection.

By implementing ThIRU Essentials and the cybersecurity practices, Dr. Dixit Medical Center achieved significant improvements in its cybersecurity posture:

- Enhanced Protection
- Regulatory Compliance
- Increased Resilience

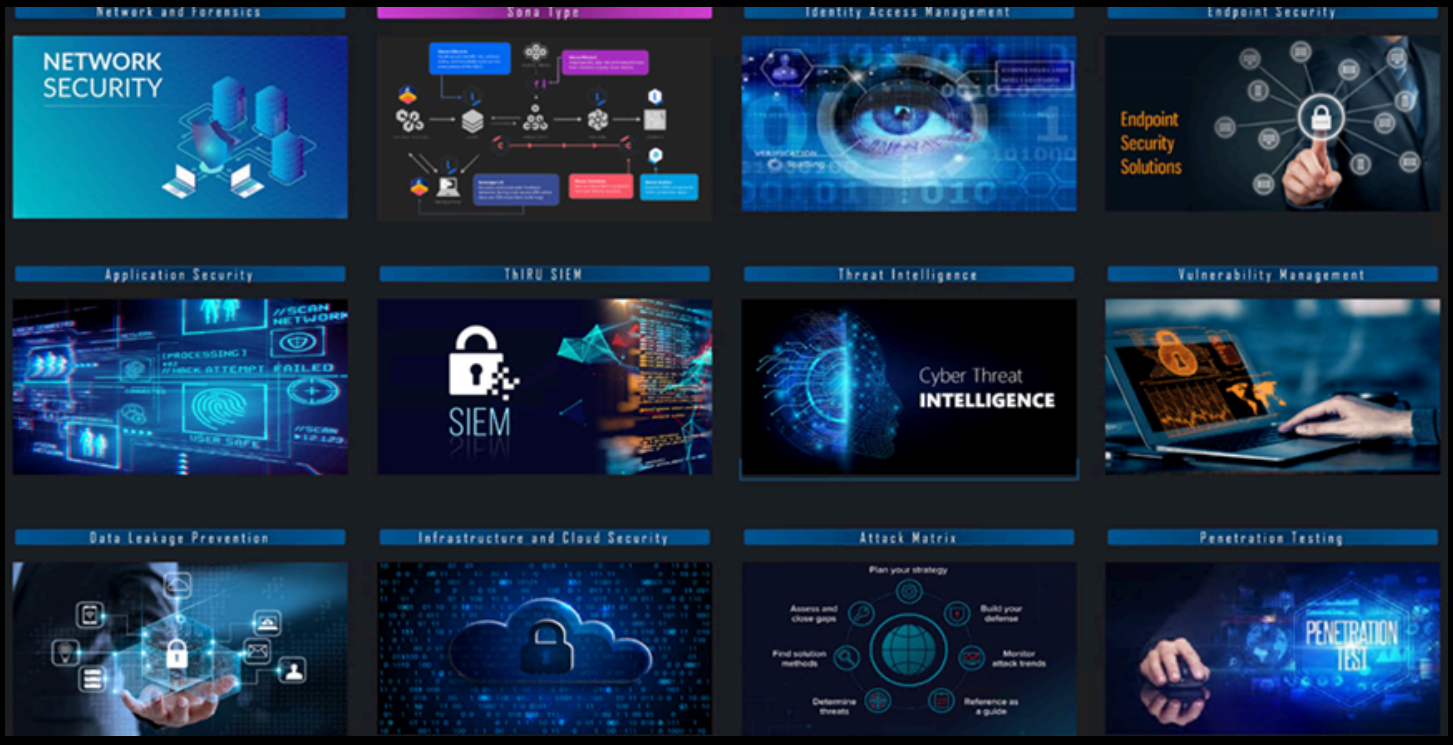
305, 65 Victor Cr. Narre Warren VIC 3805
www.thirulabs.com
1300 816 688

ThIRU OT-IT Platform

Case Study IV

Threat Intelligence and Response Unit (ThIRU) SOC software solution collects, and aggregates log data generated throughout the organization's technology infrastructure, from host systems and applications to network and security devices such as firewalls and antivirus filters. The software then identifies and categorizes incidents and events, as well as analyzes them.

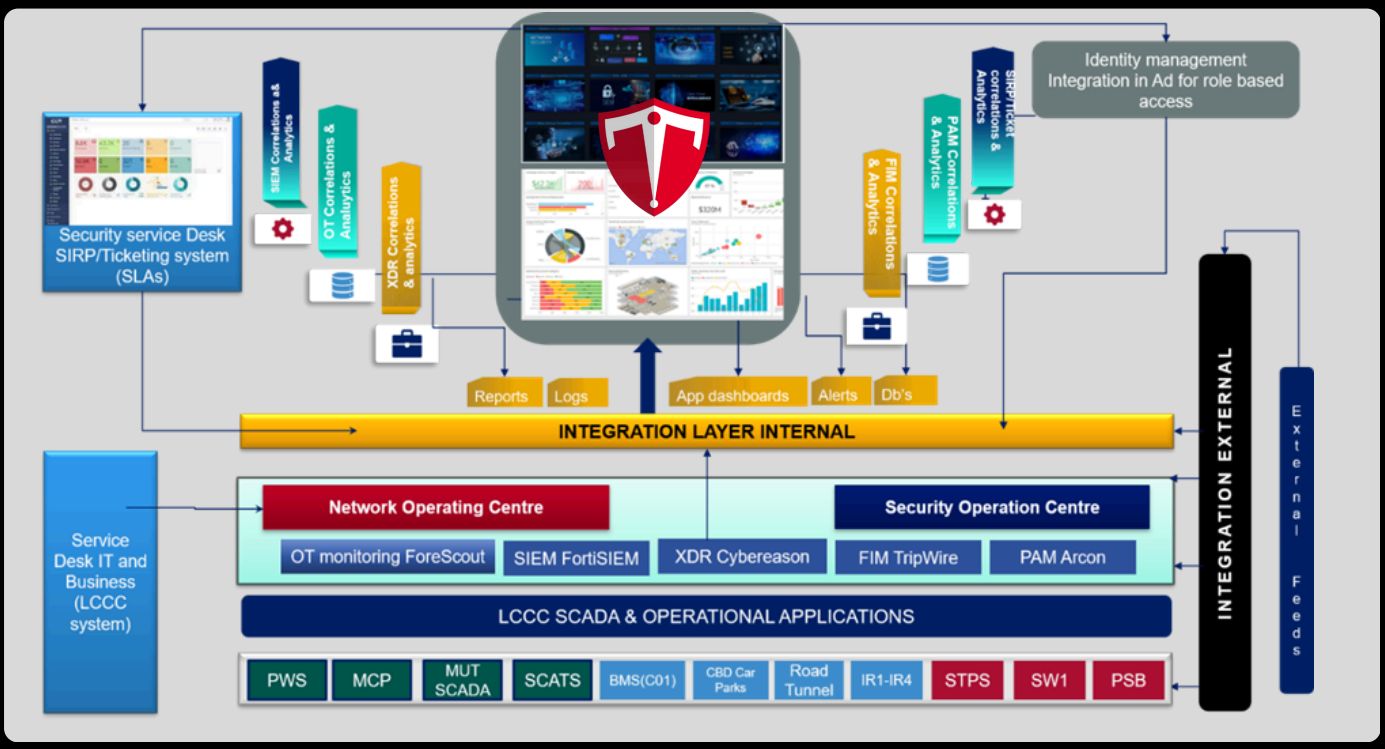
ThIRU Zero Trust principles "Trust No one- Verify Everything"

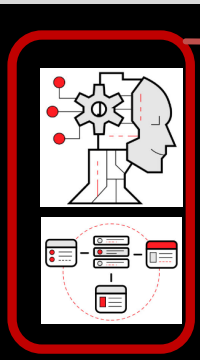


SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)
OPERATIONAL TECHNOLOGY (OT) MONITORING
ENDPOINT DEVICE MONITORING
PRIVILEGE ACCESS MANAGEMENT (PAM)
FILE INTEGRITY MANAGEMENT (FIM)
SIRP (TICKETING SYSTEM)

THIRU SOC
FULLY INTEGRATED

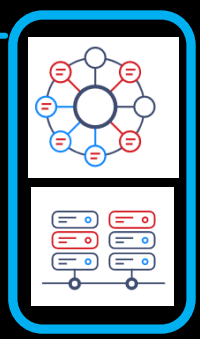
Visualization & Analytics Extreme analytics of data for compliance





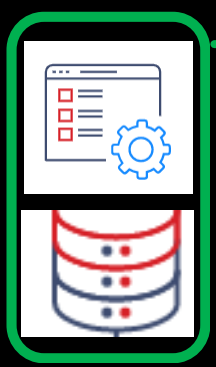
User Identity All users will be identified, verified and only the people, devices and processes that have been granted access to your resources can access them.

Device – Endpoints Assessing the security compliance of device endpoints - the hardware accessing your data – desktop, laptop and mobile will be protected to prevent data leakage



Network Monitoring. Data from NMS and 3rd party SIEM seamlesslessly integrated for monitoring

Data transfer Infrastructure moniutoring and risk profiling. Data from both the OT & Ity infrastrcuture directly and also through other 3rd party systems integrated for risk mitigation.



Applications This oversight applies to your applications too, whether local or in the Cloud, as the software-level entry points to your information.

Data & Database And finally, protection of the data itself across your files and content, as well as structured and unstructured data wherever it resides

ThIRU Zero Trust principles "Trust No one- Verify Everything"

+61 (0) 417 567 658
info@THIRULABS.COM
WWW.SURAKSHA.COM.AU