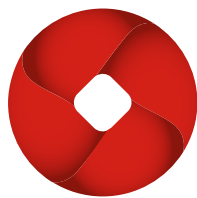


# Greenfield Security

Building a security program  
from ground up for a  
security-critical  
government agency in Asia

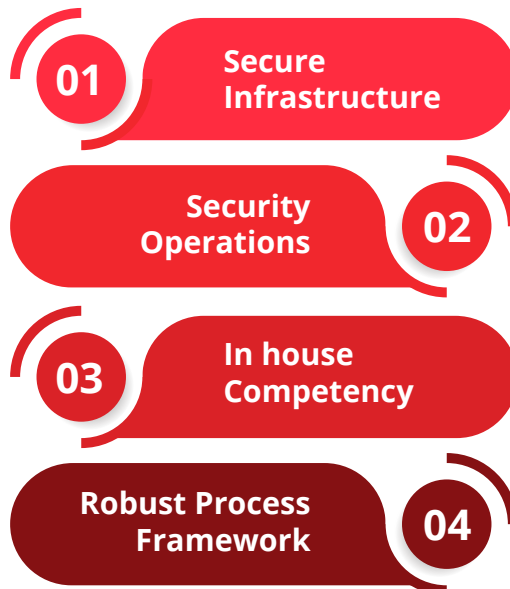


**Payatu**

## CHALLENGES



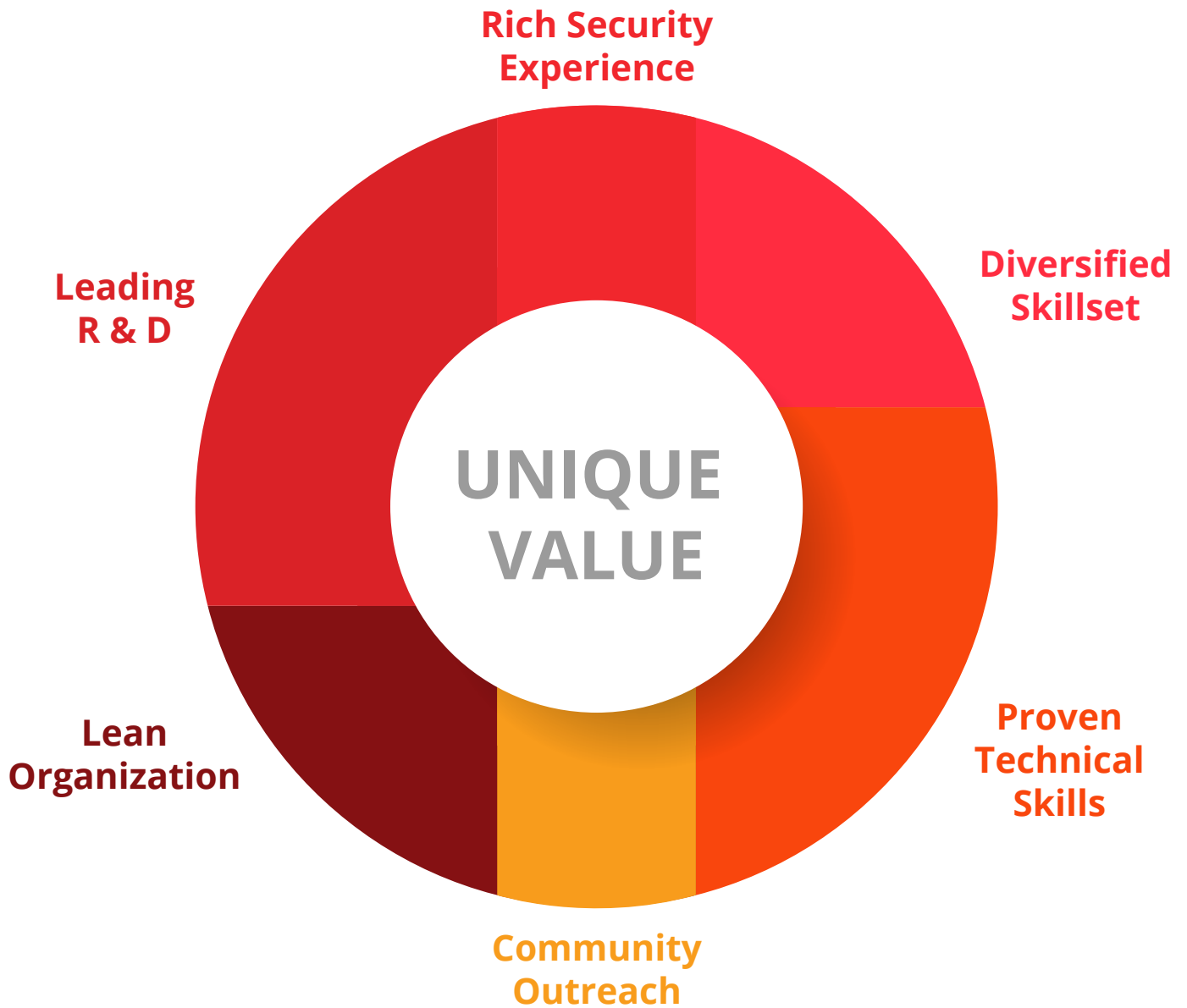
## SOLUTIONS



## ACHEIVEMENTS



## VALUE TO CUSTOMERS



## OUR STORY

This is a success story of how we built a sustainable security program for a heavily targeted Government Agency in Asia, from scratch.

Our Client – The Government Agency in Asia, was under attack by neighboring nation states. They experienced targeted malware and APTs day in and day out. Lack of security program, infrastructure & skills to mitigate the threats was not the only challenge they had.

The challenge was to contain the current attacks on one hand and on the other it was important to develop an effective program to build a security infrastructure from grounds up, secure their daily operations, develop skills and competency within the organization and sustain the program without external dependency and gear up the organization from zero security state to a robust 360o security state within the limited resources, funds and time available.

Entrusted with this responsibility for our proven technical skills, cutting edge research & development ability, experience of creating & driving a thriving community outreach in the information security ecosystem and lean structure, we accepted the Challenge.

We architected & implemented a complete security program encompassing infrastructure, operations, security response ability and competency development to make the Organization skilled enough to sustain and address the future security needs.

This document summarizes our efforts and strategy to transform the organization from having no overall security to proactive and responsive security within two years.

## THE CHALLENGE

The scope of the engagement was as wide as the organization itself. They requested us to scope the work based on our understanding and experience in securing large organizations against advanced and targeted attacks.

**VULNERABLE CURRENT STATE**

- Continious advanced malware attacks
- Espionage and Cyber Threatsby Nation States

- Wide Organization, diversified needs
- Build Security Infrastructure from scratch

**WIDE SCOPE**

**LIMITED RESOURCES**

- Urgent need of Security
- Limited Time, Skills & Resources

- Needed Dependable in house competency
- Self Susutainability was paramount

**ACHIEVE SELF RELIANCE**

**OUR APPROACH**

After our onsite analysis and research that lasted for 4 weeks, comprising of visiting the different departments, the backend infrastructure, interviews with employees, understanding the current architecture, we came up with recommendations and roadmap for the organization which primarily included

Building the network & computing infrastructure

Making the daily operations secure and accountable

An Advanced Security Monitoring Incident Response Center

Developing skills and competency to manage and sustain security needs

**INFRASTRUCTURE**

- Network Topology & Layout, Firewalls, IPS/IDS, Honeypots
- Network Serivces DNS, SFTP, SAMBA, APT Solution, SIEM
- Network Operation Center

**OPERATIONS**

- Identity & Access Management
- SSO, Domain Control
- Data Management, Backup/Recovery
- Roles, Responsibility Mgmt

**SECURITY**

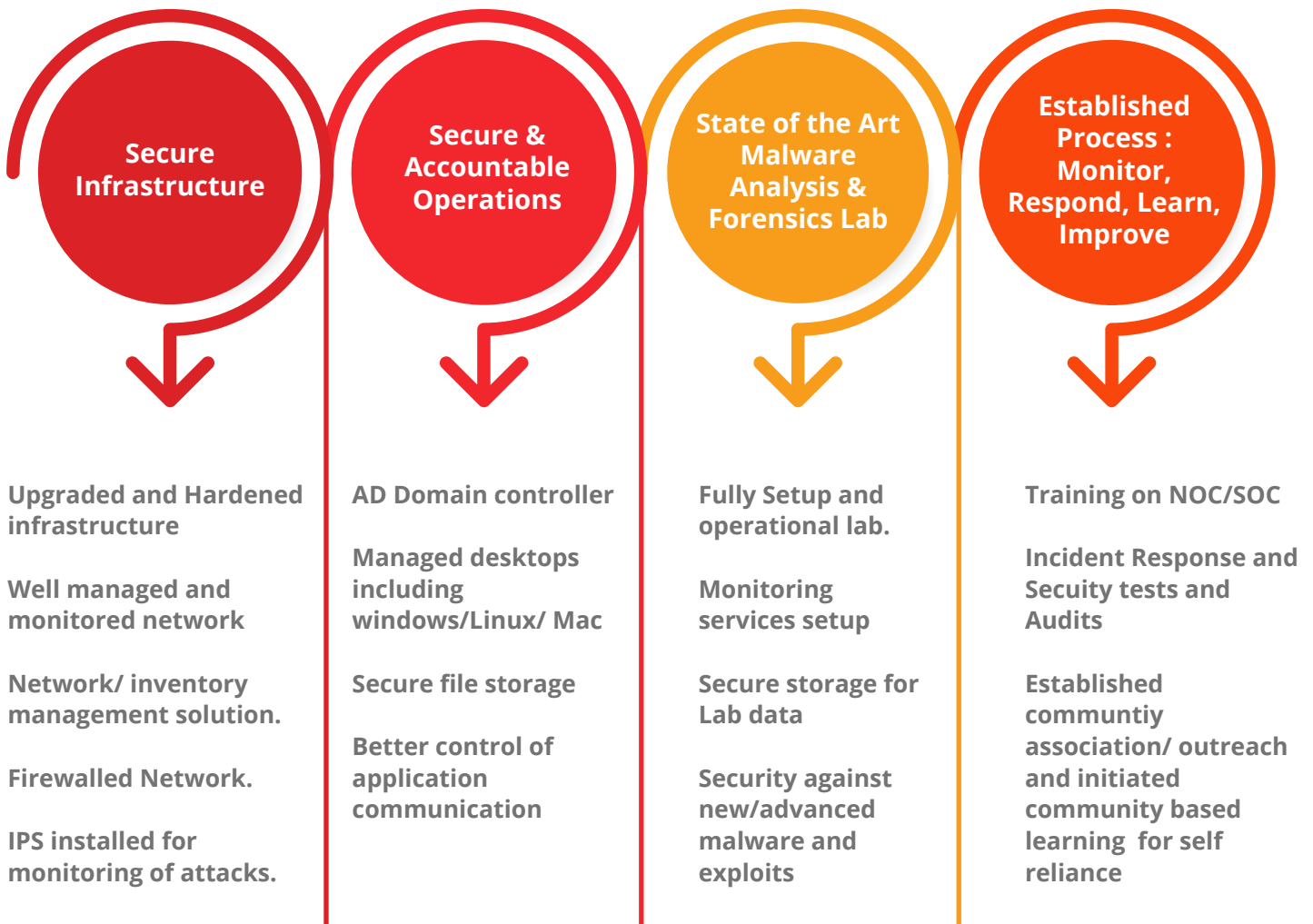
- Protect : Network and End points
- Detect : Attacks, Anamoly, breach
- Respond : Malware Analysis, Forensics, Incident Response

**COMPETENCY**

- Security Basics for all
- Incident Response, Forensics
- Assessments & Audits
- Continious Training for Sustainability

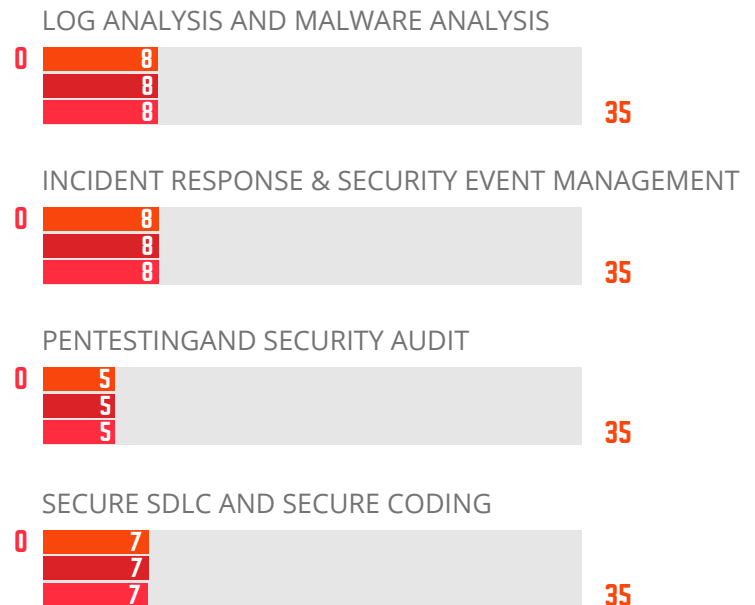
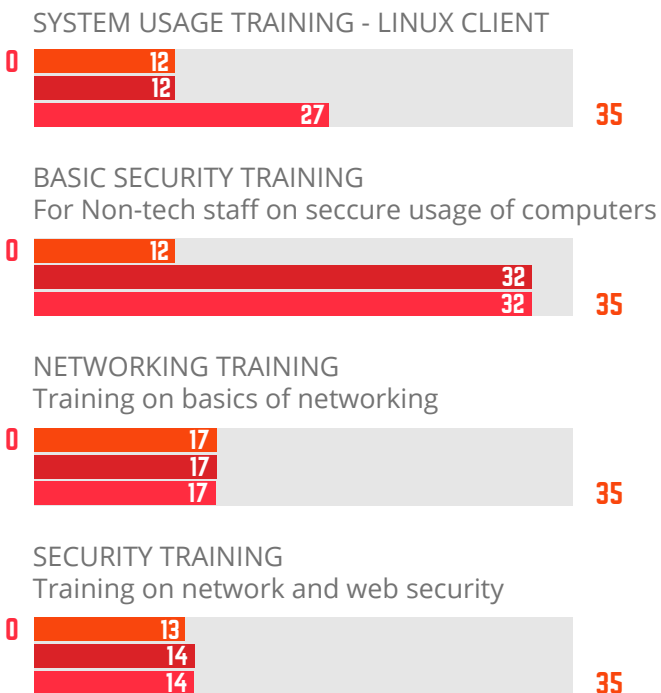
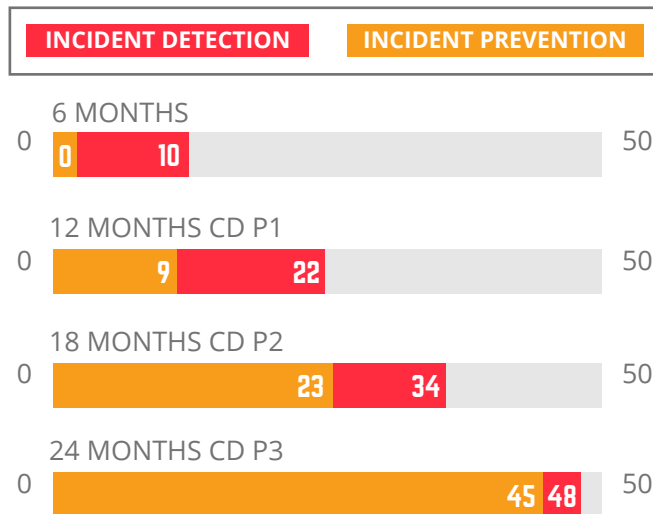
# ACHIEVEMENTS

After seeking approval for our recommended roadmap, it was time to implement and execute the plans. For close to two years we worked on multiple fronts. Progressing through the meticulously planned phases and skillful execution we were able to achieve exemplary results. Few of the prominent turnarounds were: Hardened and Secure Infrastructure, Secure operations, State of the Art Malware Analysis & Forensics Lab and Highly Competent Staff with a robust framework of processes to address current and future security needs.



# SELF-RELIANCE AND SUSTAINABILITY

The primary aim of the project was to help our client achieve self-reliance in security and sustainability in the current security operations and future security needs. Our Competency development program trained the staff in wider range of security aspects based on their roles and responsibilities. We also helped them initiate security community outreach programs for further learning, skill enhancement and keeping up-to-date with current happenings in the security world.



## DELIVERING THE VALUE

Our hands-on technical experience, carved niche in the information security ecosystem, wide reach of our core team gives us a distinguished advantage.

Innovation, Research & Development driven approach in the diverse areas in Information technology makes us better equipped with a better understanding of what will work & how to deliver it.

Our wider community association connects us with thousands of brains globally. This helps us quicker acquisition of skills, talent, or consultation in a very cost effective manner.

Our almost flat organization allows us to operate with minimum resources, and optimum cost. Our commitment to LEAN philosophy helps to reduce wastage and delivery time.

All these virtues help us to offer unique value to our customers and deliver exemplary results and more success stories, one after another.

