COMPANY PROFILE

PT GREEN COMMUNICATION NETWORKS

NETWORK SECURITY DIVISION

PROFILE

PT Green Communication Networks a.k.a Greencomm, provides a unique set of capabilities that encompass a broad knowledge of networking, technologies and security architectures. This combination of expertise helps bridge the gap in many organizations to create solutions that meet the demands of dynamic and ever-changing needs of today's IT organizations. With our experience dealing with many Indonesia enterprises, we are ready to help in the most complex situations and become a valued member of your team, either on a short term multi-month engagement or longer term with an annual contract.

OUR **COMPETENCIES**

- Standard Operation Procedure (SOP) Assessment
- Network Security Assessment
- E-Commerce Security Assessment
- Network Security Training

OUR **CLIENTS**

- Financial Company (Banks) - Indonesia
- Payment Gateway Company - Indonesia
- Secure Printing Company
  (Passport, Bank Cheque, Vehicle License) - Indonesia
- Web Ticketing Company - Indonesia
- Container Company - Singapore

OUR **MISSION**

PROTECT

Build and maintain technology, processes and procedures to secure and control access to critical information

IDENTIFY

Identify assets taht support critical business functions, assess risk, govern and prioritize security efforts

DETECT

Build system and intellegence to recognize potential cybersecurity events as they happen.

RECOVER

Restore affected system to quickly return to normal business operations

RESPOND

Contain and limit the effects of cybersecurity events through planning and eaction

Redefining security through identity

Greencomm Networks is focused on solving the #1 problem in cybersecurity – Eliminating Identity-Related Breaches. We're constantly raising the bar by continuously assessing risk and enabling trust to improve identity security. Are you?

WHAT WE DO

SYSTEM PENETRATION TESTING

What is Penetration Test ?

A penetration test, or "pen test," is an attempt to evaluate the security of IT infrastructures using a controlled environment to safely attack, identify, and exploit vulnerabilities. These vulnerabilities may exist in operating systems, services, networks, and application. They may also exist due to improper configurations or risky end-user behavior.

Penetration testing assessments are also useful in validating the efficacy of defensive mechanisms and determining how well end-users adhere to security policies.

Intelligently manage security weaknesses

Penetration tests provide detailed information on actual, exploitable security threats. By performing a penetration test, you can proactively identify which security weaknesses are most critical, which are less significant, and which are false positives helping you prioritize resources and response.

Avoid the cost of downtime

Recovering from a security breach can cost an organization millions of dollars in IT remediation efforts, customer protection and retention programs, and legal activities. Penetration tests help you discover and remediate potential risks before they lead to a security compromise.

Penetration testing helps IT professionals measure risk and evaluate the consequences that attacks, or similar incidents, may have on resources and operations.

Meet regulatory requirements

Greencomm Netsec help organizations address the general auditing & compliance aspects of regulations. The detailed reports penetration tests generate can help your organization avoid significant fines and help you document ongoing due diligence through maintaining required security controls.

Preserve corporate image and customer loyalty

Each incident of compromised customer data can be costly: negatively affecting sales and tarnishing an organization's public image. Penetration testing helps you prevent data incidents that put your organization's reputation and trustworthiness at stake.

OUR SOLUTIONS

Energy & utilities

Utilities and energy organizations are part of the critical infrastructure of every economy. This makes them prime targets for cyber criminals. The use of technology and digital transformation has modernized this sector, but also increased its threat surface. A cyber-attack targeting even a small utility provider could create devastating economic and security consequences.

Although the backbone of utilities networks, supervisory control and data acquisition (SCADA) systems often contain critical vulnerabilities and lack basic security controls.

Financial services

Despite being governed by stringent compliance mandates; the financial services sector is a high-value target for cybercriminals. Digital transformation initiatives have increased the attack surface, adding urgency for ensuring compliance with industry regulations as well as maintaining trust with customers and other stakeholders. Legacy technologies that were once state of the art are now stifling business operations and customer experience while also exposing the organization to additional risk.

Healthcare

Technology is changing every industry in significant ways. Healthcar e is no exception. This digital disruption is forcing healthcare providers and insurance companies to move to provide a modern model that is centered on customer needs – their choices and their control.

Higher education

Today's modern higher education institution is a complicated maze of physical campuses, online learning, students, faculty, alumni, and research partners from both the public and private sectors. More people from more groups than ever before need access to various applications, intellectual property (IP), and systems. The vast number and varying types of identities in a typical academic environment create a large and evolving threat surface that makes institutions a target for bad actors – and they are seeking any vulnerability to find a way inside.

Public sector

Year-over-year increases in the breadth and depth of cyberattacks coupled with ever-growing concerns surrounding insider threats have governmental agencies and local – looking to strengthen security policies and controls.

Retail

More than most industries, retailers must dynamically deal with identity, access and security risks. With salaried, hourly, and seasonal employees, an ever-changing global network of suppliers, and increasingly fickle and demanding consumers, the threat landscape is vast for retailers.

Attackers love the sheer volume and value of consumer information present in retail environments. A single breach can result in significant damages to brand reputation, customer confidence, and even ruin careers.

OUR PRICE

Please contact us to define your cost for redefining your digital/internet security environment. Don't thinking too long ! Attacker is always looking into your system. Unless you happy to lost your data, money or your operation stuck suddenly.

CONTACT US

PT GREEN COMMUNICATION NETWORKS

NPWP : 02.754.821.3-901.000

ADDRESS	: JL. Moh. Yamin IV No 12, Renon, Denpasar – Bali | Indonesia
EMAIL	: ZULFADLY@GREENCOMM.ID
CONTACT NAME	: ZULFADLY [DIRECTOR]
PHONE	: 0818-793043