CryptoGen Nepal

Proposal for Incident Response Retainer Service

MSSP Alert
A CyberRisk Alliance Production

TOP 250

ICT AWARDS

STARTUP CATEGORY

EST. 2019

ISO/IEC 27001:2022

Certificate of Registration

This is to certify that

Cryptogen Nepal Pvt. Ltd.

Manakamana Marg, Naxal Nagpokhari, Kathmandu, 44600, Nepal.

has been assessed by RICL and found to comply with the requirements of

ISO 27001 : 2022
Information Security Management Systems

For the following activities:

Providing Information System and Cyber Security Professional Solution and Services, Sales, Support, Audit, Assessment, Training and Consultancy to its Customers.

(SOA Version: SOA/CNPL/01, Dated 03/07/2024)

This Certificate is Valid from 12/09/2024 Until 11/09/2025

Date of Initial Certification: 12/09/2024
Ist Surveillance on or before: 11/08/2025
IInd Surveillance on or before: 11/08/2026
Certification Valid Until: 11/09/2027

Certificate No.:
24RN09CQ

CB-MS-26213

Director
Royal Impact Certification Ltd.

This certificate can be verified online at www.iafcertsearch.org

United Accreditation Foundation INC, 400 North Center Dr Ste 202, Norfolk, VA 23502, United States of America.

Cyber Security Incidents and Consequences

In today's digital landscape, cyber security incidents have become increasingly prevalent and sophisticated. These incidents, ranging from data breaches and ransomware attacks to phishing schemes and insider threats, pose significant risks to organizations of all sizes. The consequences of such incidents can be severe, including financial losses, reputational damage, legal liabilities, and operational disruptions. As a managed security service provider, we understand the critical importance of safeguarding your digital assets and ensuring business continuity.

Third party risk

Remote workforce

Phishing attacks

Latest Cybersecurity Threats In Banking

Ransomware

Malware

AI-related cyber threats

Trojans and keyloggers
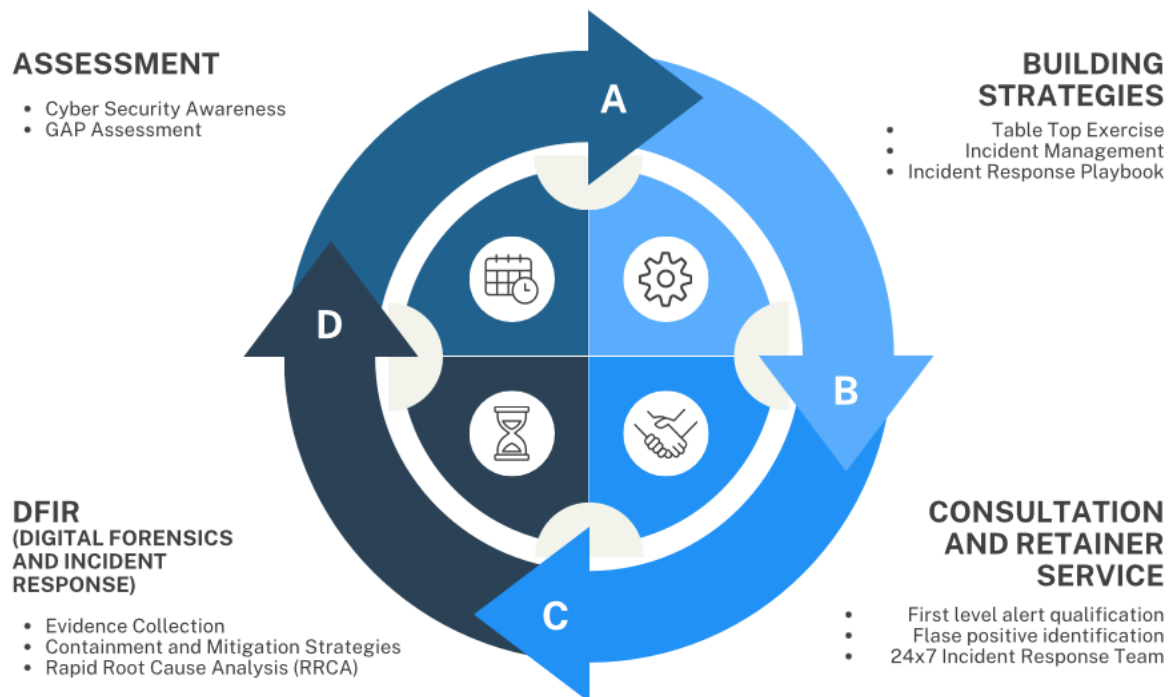
DDoS attacks

Data breaches

Incident Response Service

CryptoGen Nepal has years of experience in threat assessment, monitoring and response on various sectors i.e. banking, insurance, government, NGO, etc. Our Incident Response as a Service (IRaaS) is a retainer service which enables organizations to instantly consult regarding security incidents, false positive validation along with access to Incident Response Team (IRT) in a vendor agnostic approach to build, train and perform organized Incidence Handling to any escalated cyber security alerts. Our team assists through consulting and Digital Forensics to identify, contain and remediate cyber security incident. The primary goal of our service is to perform a Rapid Root Cause Analysis (RRCA) through expert analysis, reverse engineering, accelarated forensic analysis and provide post-incident planning to assure the discovered threat are not residing at the organization and planned steps to reinforce early detection and migitation strategies.

Incident Response Service Offering:

Service	Description
Tabletop Exercise*	Practice sessions where teams strategize responses to simulated security incidents.
IR Gap Assessment*	Examine organization's incident response program for weaknesses and review documents.
Incident Management*	Documented effective incident handling planning to critical asset identification, minimize damage, business continuity review and recovery planning for security incidents.
Cyber Security Awareness (Bi-Yearly)	Empowerment of organization's executive and workforce to mobilize regarding identification, response and safeguarding of sensitive information system.
Digital Forensic and Incident Response*j	Triage, Analyze, Contain, Remediation strategies, recovery planning and post incident review
Cyber Security Consultation	Oversee, communicate, support, qualify and first response to an incident

Progressive Response

ASSESSMENT
- Cyber Security Awareness
- GAP Assessment

BUILDING STRATEGIES
- Table Top Exercise
- Incident Management
- Incident Response Playbook

DFIR (DIGITAL FORENSICS AND INCIDENT RESPONSE)
- Evidence Collection
- Containment and Mitigation Strategies
- Rapid Root Cause Analysis (RRCA)

CONSULTATION AND RETAINER SERVICE
- First level alert qualification
- Flase positive identification
- 24x7 Incident Response Team

Benefits of IR Retainer

- Ensure availability of Incident Responders and assistance with cyber security incident qualification
- On-boarding process to build familiarity with client's environment, technologies and policies to expedite investigation process and current gaps
- DFIR expertise during the time of incident for Rapid Root Cause Analysis (RRCA)

Core Competencies

- Network Traffic Analysis
- Windows & Linux Host Forensics evidence collection and investigation
- Malware analysis and Reverse Engineering
- Threat and Anomaly Qualification
- Remediation recommendations from domain experts

High Level Service planning