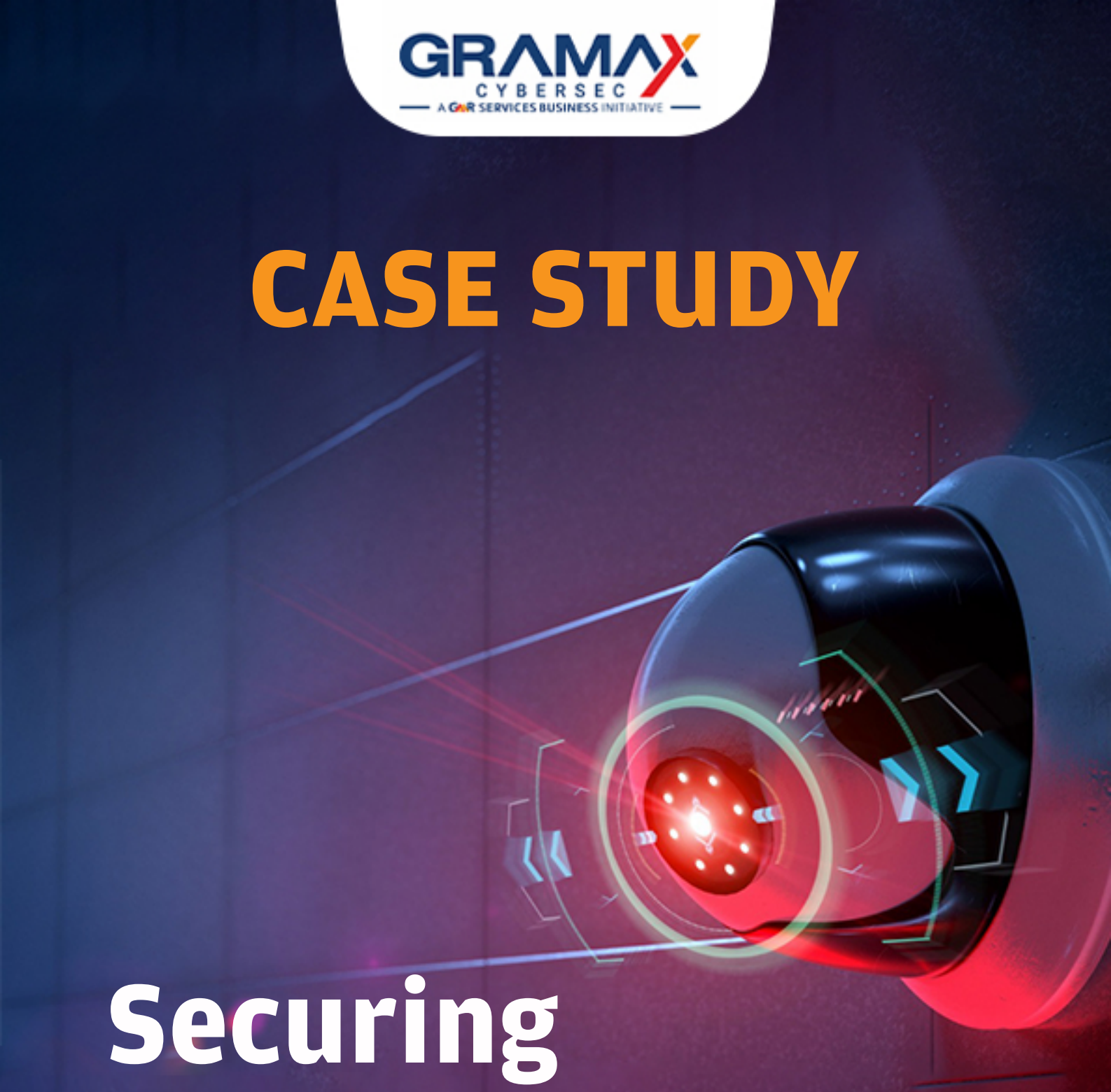
GRAMAX CYBERSEC
A GMR SERVICES BUSINESS INITIATIVE

CASE STUDY



Securing CCTV Cameras from Cyber Attacks

EXECUTIVE SUMMARY

There are nearly 1 Billion CCTV cameras installed all over the world for monitoring, operations, security and compliances. CCTVs also act as the last line of evidence collection and CCTV footage is admissible in a court of law, in case of any legal proceeding. With such a large installation base and huge dependency, CCTV cameras have become one of the largest attack vectors for cyber-attacks like video snooping, MITM, DDOS, Ransomware, etc.

One of our client from the critical infrastructure reached out to GRAMAX Cybersec to figure out the recent threats emerging through CCTV cameras installed at their workplace. The organization was concerned as CCTV cameras have become a potent threat vector that can disrupt operations, such as leaking the information on VIP movements, missing out the evidence of critical events, snooping, breach of privacy, etc.

CHALLENGES FACED BY THE CLIENT

01 Unable to detect vulnerable cameras that expose their streaming URLs unprotected

02 Exposure to Distributed Denial of Service attacks

03 Failed to detect security misconfigurations and vulnerabilities specific to camera manufacturer

04 Unable to detect cameras with visual obstruction to their feeds along with poor quality of stream

HOW GRAMAX CYBERSEC HELPED

In order to conduct the comprehensive assessment of the client's critical surveillance infrastructure, GRAMAX utilized Redinent's enterprise-grade threat scanner for CCTV networks, combined with the expertise of the professional security experts. This solution detects both known (such as security misconfigurations and protocol prone threats) and unknown vulnerabilities that are not available in the public domain. It classifies weaknesses as critical, medium and lesser as per international standards set by MITRE ATT&CK for better appreciation of the faults.

ABOUT OUR SOLUTION

Redinent CCTV Threat Scanning platform empowers the CEOS/CISOS/CSOs of organizations to be fully aware of the security status of their CCTV cameras deployed in their organization as this solution provides them with following capabilities:

01 Discover any misconfiguration/insider threat, weak user authentication

02 Exposed Ports and Network Services

03 Hidden Streams that can be used for video snooping and Espionage

04 Known CVE identification/mitigation for CCTV cameras

05 Detection of Remote code execution

06 Time Stamp Mangling of CCTV cameras

BELOW ARE THE UNIQUE FEATURES OF THE SOLUTION IMPLEMENTED AT OUR CLIENT SITE:

01 Detailed Vulnerability Assessment of Critical Surveillance Infrastructure

02 Mapped to Mitre ATT&CK Framework

03 SaaS and Cloud based options reducing your hosting costs

04 Powerful web based self-assessment tool

05 On-Demand and Scheduled Scans

06 Threat Intelligence Analytical Dashboard with detailed insights

07 Patented Signature Detection Algorithms

08 Continuous Cyber Risk Monitoring of CCTV cameras

09 Automated ISO 27001 Gap Analysis for CCTV Network

10 Reports assisting in compliances like ISO 27001, COBIT, NIST
Pre-Integrated with CWE and CVE classification