Terafence
IoT and Cyber Security

CCTV Network

ICS
WHITE PAPER

Terafence CCTV Cyber Security Solution

info@terafence.us | www.terafence.us

INTRODUCTION

The precursors of modern video surveillance were Closed-Circuit Television (CCTV) systems, used analog signals over coax cables to communicate in a closed infrastructure. No networking features existed, and the entire system was closed to any external electronic access, hence – Closed Circuit TV. As technology advanced, digital cameras supporting TCP/IP communication came into existence and got integrated into the organization LAN infrastructure. Nowadays, video surveillance with IP cameras is used not only in large corporations and highly secure locations, but also in most public buildings and increasingly in private home automation systems, and for many organizations are consider "Eyes and Ears" for everything outside the Security Operation Center (SOC) by providing visual information.

Modern video surveillance systems are composed of the following components:

~ IP Cameras, which provide video monitoring of physical locations. They can be grouped into CCTV (analog) and IP (digital) cameras, which, as opposed to their analog versions, can be directly connected to an Ethernet network. In this work, our focus is on IP cameras only.

~ Network Video Recorders, which store camera footage. Dedicated device that records and stores video in a digital format, called a Network Video Recorder (NVR). Some advanced IP camera models also integrate Video Management software (VMS) for local storage of recorder footage.

~ Monitors, which are used to watch real-time or recorded footage. Monitors can also be analog or digital, such as a computer, smartphone or almost anything with a screen that can display video.

~ Advanced Intelligence / Analytics, Devices dedicated for processing video either for forensics or for real-time processing for pre-configured events and alarms.

~ Video Storage, Devices which store video information, either locally or in the cloud.

More complex systems can also contain media servers, gateways, routers, and switches. Based on the components present on an enterprise network, we can differentiate three types of surveillance systems:

~ Analog systems contain devices that cannot communicate on the Ethernet network. They are less prone to cyberattacks and are out of the scope of this report.

~ Digital systems comprise IP cameras, NVRs, switches, routers, and digital monitors, which all can send and receive Ethernet network traffic. Most of these devices also support remote access, maintenance, and alerting via HTTP, FTP, SSH, SMTP, and similar protocols, and in some cases, also the old and insecure Telnet protocol. Video streaming uses RTP, RTCP, and RTSP, as explained below.

~ Hybrid systems comprise of both digital and analog devices. Besides the devices mentioned above, these systems can also contain video encoders or hybrid DVRs to connect analog cameras to the IP network and video decoders.

INTRODUCTION

The architecture of a hybrid video surveillance system can be quite complex, containing a variety of legacy and new technologies. Figure 2 shows an example of such a system, where the direction of the arrows indicates the direction of data flow.

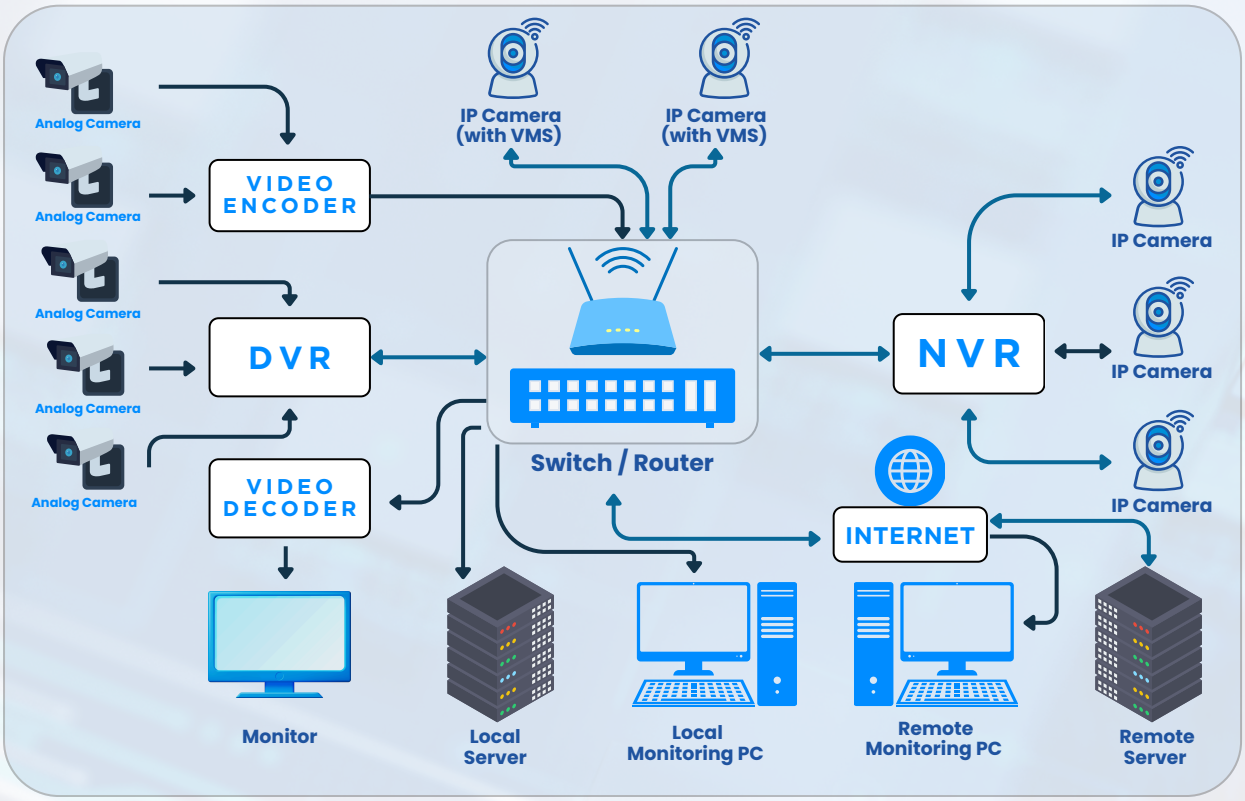


Figure 01. Surveillance system architecture as found in a modern building

Mechanism and Working of the Surveillance System Architecture

1. **Analog Cameras & Encoding**
   - Analog cameras capture video footage.
   - A Video Encoder converts analog signals into digital format for processing.
2. **DVR Processing**
   - Encoded video is sent to a DVR for storage and management.
   - Video Decoder retrieves recorded footage & sends it to a monitor for viewing.
3. **IP Cameras & Network Communication**
   - IP Cameras (with VMS - Video Management Software) connect directly to a Switch/Router for data transmission.
   - NVR collects, processes, and stores video from IP cameras.
4. **Networking & Remote Access**
   - Switch/Router enables communication between DVR, NVR, & monitoring systems.
   - The system connects to the Internet, allowing remote access via a Remote Monitoring PC or a Remote Server.
5. **Monitoring & Storage**
   - Local storage is maintained in a Local Server.
   - Footage can be accessed from a Local Monitoring PC or remotely through Remote Monitoring PCs.

THREAT ANALYSIS

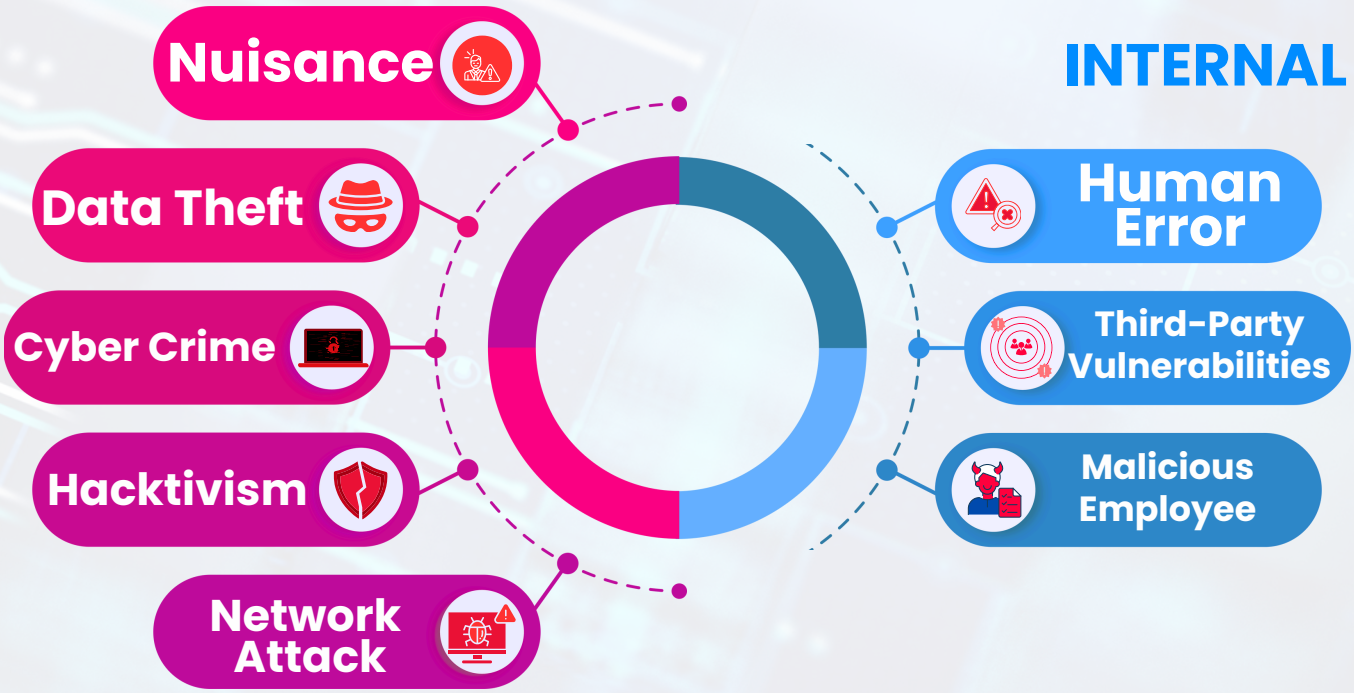
Understanding where threats may come from is crucial for establishing protection measures. It is commonly accepted that only 20% of attacks come from the outside (Internet) and 80% come from internal sources. One can have the state-of-the-art network IDS / IPS and FireWall(s) in place but an infected USB-Disk-on-Key inserted on a desktop / server will bypass everything and possibly infecting the entire network or worse, allowing access to hackers, viruses or worse.

A laptop that was used outside the organization may have picked up malicious code on someone else's network, on an open Wi-Fi link in a café, on the train or at the Airport. As no single solution can provide total security, layered security solutions are often the best way to ensure maximum protection against attacks.

Servers and Desktops computers may run tools as protection like FireWall, Anti-Virus and as such, Network access could use NAC to deny connectivity to unknown devices and advanced network behavior tools could monitor traffic for abnormality and attacks.

A major concern arises when attackers take control over low-maintenance devices, such as IP-Based CCTV cameras, and use them as an entry point into the organization network.

Additionally, taking control over CCTV elements (such as NRV / AI / Forensics) may allow attackers to hide criminal activity or completely blind a SOC during emergencies or terror attacks.



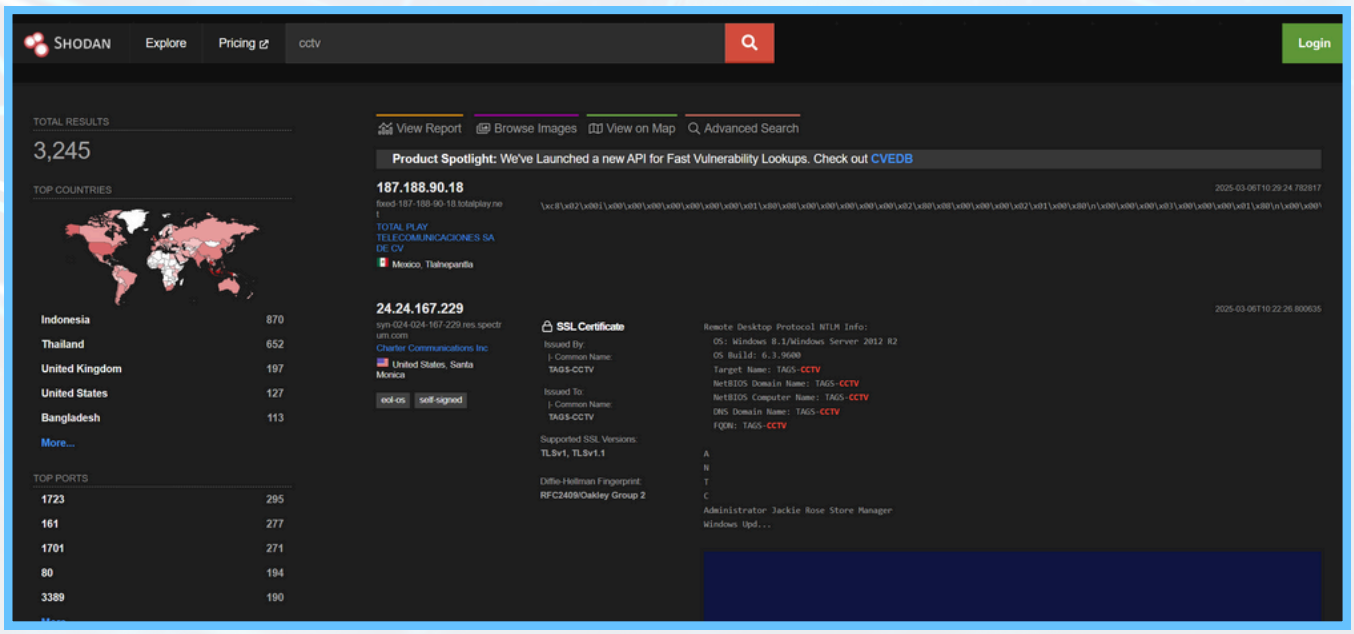
Typically, CCTV systems are handled outside IT “jurisdiction” and quite often serviced by external subcontractor while the actual infrastructure is shared with IT systems. The Security department is responsible for the CCTV and, in many cases, totally depend on sub-contractor’s staff for maintenance, repair and system evolution and even allow remote network access for diagnostics and maintenance, and in worst cases, all without IT department intervention for security (TeamViewer session for example).

A visiting support engineer carrying his LAPTOP coming to update the CCTV elements software / firmware may, unintentionally, carry an undetected virus, trojan hours or ransomware into the network.

CCTV IP-Based cameras should be considered as exceptionally vulnerable for the following suggested reasons:

- In many cases the CCTV default admin password is not changed (and can be found in web-sites like – https://learncctv.com/ip-camera-default- password/).
- CCTV have good computing resources and are connected to power and network 24/7.
- Very few CCTV contain any security tools such as FireWall / Anti-virus etc.
- Most CCTV IP cameras run some version of Linux OS, favorite of hackers.
- CCTVs are not monitored in real-time as the main view screen cannot display all, so are out of SOC’s attention, making them susceptible for manipulation, alteration, and abuse.
- No CCTV camera will block access to anyone running brute-force password cracking attacks.
- Some IP based CCTV camera are physically placed in publicly accessible locations, allowing attacker to use their network cable to hack into the network.
- Some CCTV cameras use Wi-Fi to transmit video, allowing Man-in-the- middle attacks and as such.
- Few CCTV vendors already include back-door vulnerabilities into their product allowing unauthorized access.
- There were incidents were CCTV camera software was modified by attackers to run Bitcoin mining while seemingly operating normally.

In other incidents CCTV cameras were converted to BOTs to be used by companies selling them as resource for cyber-attacks. These companies thrive on devices poorly protected and use them to generate revenue. It is surprising how easy it is to find CCTV open for direct internet access.



Here are a few real incidents as publicly published:

SOURCE	DESTINATION	LINK
csoonline.com	Thousands of hacked CCTV devices used in DDoS attacks, Researchers found a botnet of over 25,000 CCTV cameras and digital video recorders	
esecurityplanet.com	Hackers Use 900 CCTV Cameras to Launch DDoS Attacks	
nakedsecurity.sophos.com	Woman hijacked CCTV cameras days before Trump inauguration	
vice.com	How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet.	
washingtonpost.com	She installed a Ring camera in her children's room for 'peace of mind.' A hacker accessed it and harassed her 8- year-old daughter	
PrivSec Report 2020	5 million cyber-attacks on IP cameras blocked, research reveals	
ibtimes.co.uk	Hackers turning millions of smart CCTV cameras into botnets for DDoS attacks	
newsweek.com	Thousands of CCTV cameras hijacked by hackers to attack bank websites	
newindianexpress.com	Robbers use CCTV footage to plan break-ins	
cybersecurity-insiders.com	CCTV systems installed in Toilets of British Schools hacked!	

Articles were written to raise CCTV vulnerability awareness:

SOURCE	DESTINATION	LINK
portnox.com	Why is It So Easy to Hack an IP Security Camera and Any IoT Device?	
networkmiddleeast.com	Cyber security and IP cameras: the threat is real	
darkreading.com	Internet-Connected CCTV Cameras Vulnerable to 'Peekaboo' Hack	
telegraph.co.uk	CCTV vulnerability could allow cyber criminals to hack video surveillance recordings	
tssbulletproof.com	Are Surveillance Cameras Vulnerable To Cyber Attacks?	
Security electronics and networks.com	Cyber Attacks On CCTV Systems: What Are The Risks?	

Terafence Proposed Solution

Nearly all articles suggest, among other measures, to strictly prohibit network access to the CCTV endpoints and devices, some go the distance and suggest network segmentation.

Terafence products are designed to provide CCTV IP-Based camera total Isolation and Segmentation, completely denying ICP/IP access to the CCTV camera. By implementing **Secure-CAM** unit between the IP camera and the network switch total access denial is achieved.

Secure-CAM can be installed to protect a group of CCTV cameras, isolating them from any threat, internal or external. **Secure-CAM** acquires CCTV video streams from the configured IP cameras and makes these streams available on its B side, facing the Network and the CCTV NVR, AI, video storage and alike. All RTSP requests are now handled by **Secure-CAM** B side.

Thus, total Isolation and Segmentation is achieved without compromising CCTV video performance or functionality. **Secure-CAM** can be configured to either allow or deny PTZ commands to selected CCTV cameras via a secure channel (out-of-band to the LAN network) maintaining PTZ functionality.

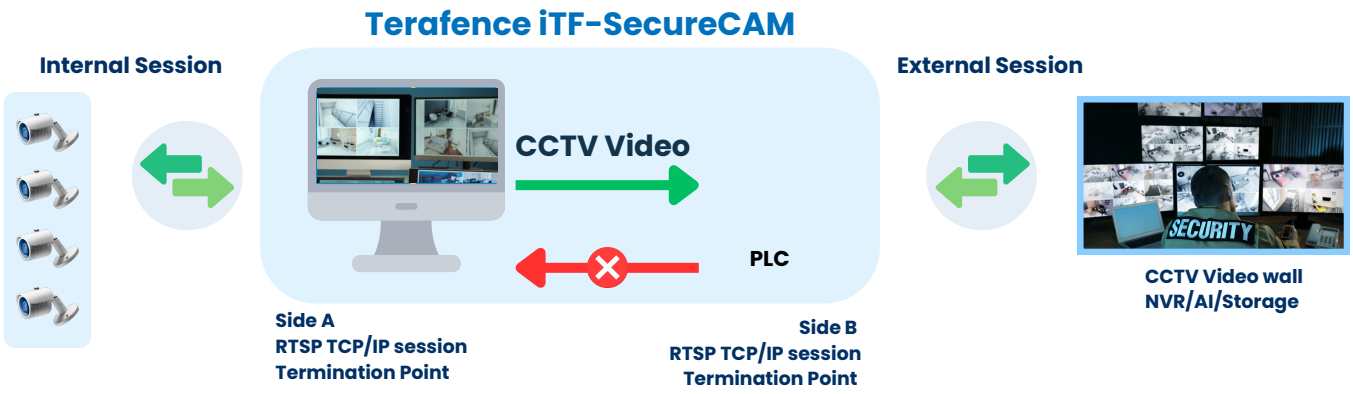


Figure 04. Secure-CAM CCTV segmentation

Terafence Advanced Cyber Security Features

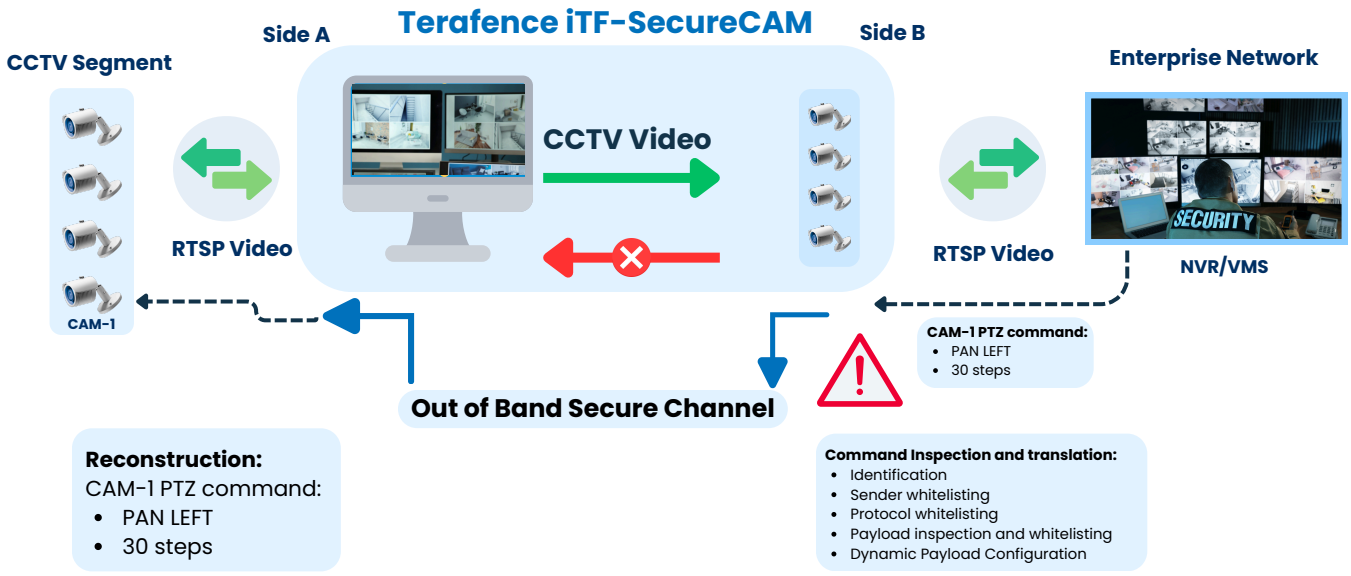


Figure 06. Secure-CAM Advanced Cyber Protection of CCTV Systems

Terafence
IoT and Cyber Security

CONTACT US

www.terafence.us

info@terafence.us

12788, Royal Oaks Lane,
Farmers Branch,
TX 75234