Milestone integration
Scylla

—

Artur Matosyan

15th July 2019

Introduction

1. What is needed
2. Overview
3. Key features
4. How it works
5. Where is it used?

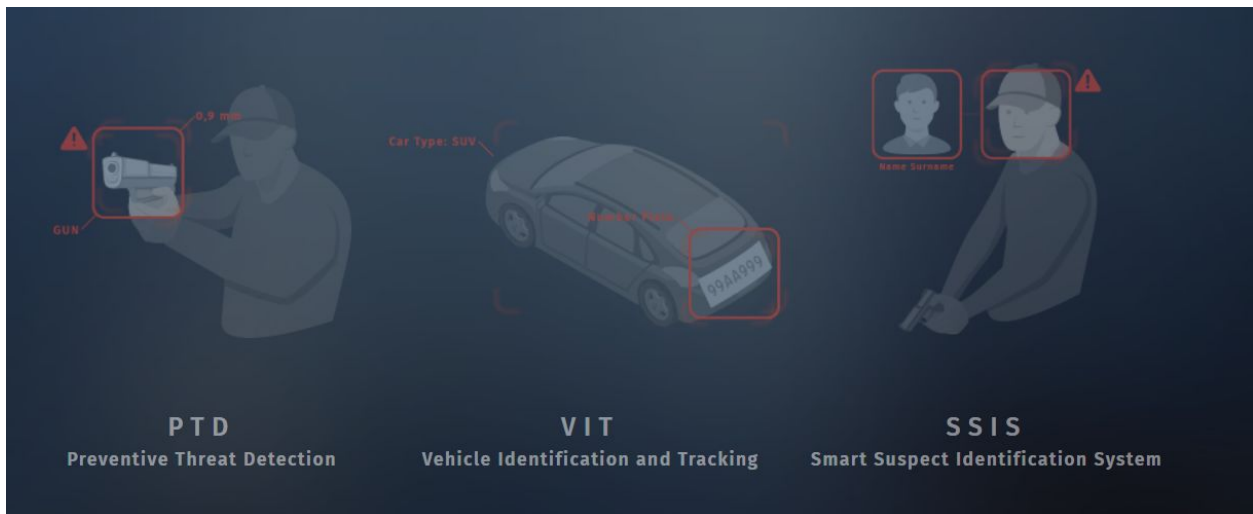## What is needed?

From Scylla

NVIDIA GPU enforced server

From Milestone XProtect

Any version which is compatible with ONVIF Bridge

Overview

Scylla is a modern ai-based protective intelligence suite that enhances operational activities of law enforcement in the three main areas.

Scylla runs on your local security servers A.K.A on-premise 24/7, silently watching the image coming from Stationary or Drone cameras. As soon as Scylla detects a suspicious behavior or object that could possess a threat towards a protected group of people or a guarded facility Scylla will sense that.

The detection process will immediately open up the dashboard with different statistical metrics that will enhance the intelligence about the current situation.

Security operators in the field will receive an alert via Scylla mobile application. By opening the mobile app, they will see vital information about the attack using Scylla SSIS module, including suspect ID, location, and method of the attack.

Industry

City surveillance, airports, schools, hospitals, seaports, traffic monitoring, casinos

Technology

Artificial Intelligence, Computer Vision

Use

Threat / Threat Detection, Localization, Identification

Key Features

1. PTD - Scylla detects threats in real time. Based on state-of-the-art AI and Computer Vision algorithms Scylla analyses video feed that comes from surveillance cameras and detects usage of threatening objects (firearms, cold weapons, sticks), fight, etc. Upon detection, the act of violence captured on a frame is delivered to Security personnel along with additional valuable information on the nature, location, and time of the threat. Moreover, we preprocess false positives to avoid annoying security personnel using Charon - Smart Decision Maker
2. SSIS (Smart Suspect Identification System) feature is used to detects faces, humans, and assets moving between cameras 99.95% accuracy.
3. VIT - If the attacker was detected in the vicinity of a vehicle the latter would be attributed to him, and the relevant information will be attached to the report. Moreover, Scylla can read, identify and match the vehicle number plates. Scylla needs to connect to your local security number plates database to efficiently track the identity of the drivers or passengers.
4. Once the detection of threat takes place, the person (or Vehicle detected near him/her) will be tracked through all the cameras in the network. The consecutive detections of either are reported, and a detailed map with tracking info is available to security forces for indoor/outdoor navigation and localization of the source of threat.
5. Note that Scylla does not store any data unless requested by the client.

How it works

Scylla runs on local or cloud security servers 24/7, silently watching the image coming from Stationary or Drone cameras. As soon as Scylla detects a suspicious behavior or object that could possess a threat towards a group of people or a guarded facility, Scylla detects and sends an alert. The detection process immediately opens up the dashboard with different statistical metrics that enhance the intelligence about the current situation.

Scylla integrated smart decision maker notifies the operator about the potential threat and requests to approve the distribution of alerts via mobile and web channels.

Security operators in the field receive an alert via Scylla mobile application. By opening the mobile app, they see vital information about the attack using Scylla SSIS module, including suspect ID, location, and method of the attack.

Where is it used?

Scylla can be used in any organization to help increase protective intelligence, by providing object and behavior detection.

URLs

Scylla detections examples: https://www.youtube.com/watch?v=cdn8hCGlzGg

Scylla on Drones: https://www.youtube.com/watch?v=HpLfc5uVvVg

Tracking Module at action: https://www.youtube.com/watch?v=-pbgJpFLZjE

Webinar and live example: https://www.youtube.com/watch?v=J9fyqhfpM3k