Citilog
A TAGMASTER COMPANY

INCIDENT MANAGEMENT

Cybersecurity for your CT-IM solution

Created: Feb. 2021

Last updated: Feb. 2021

Rev: A

DISCLAIMER/COPYRIGHT

TRACK CHANGE

List of Modifications

Revision	Date	Notes
Revision A	24/02/2021	Document creation

CONTENTS

Track change 2

1. Introduction 4
   - 1.1 Definition of terms 4

2. Overview 5
   - 2.1. Why protect your AID system? 5
   - 2.2. The main risks 5

3. Risk scenarios 6

4. How Citilog handles the risks? 8
   - 4.1. Human factor 8
   - 4.2. Cyberattack (hacker) 9
   - 4.3. Virus 9
   - 4.4. Security Measures 11

5. List of figures 12

6. Contacting Citilog 13

1. INTRODUCTION

Over the last twenty years, AID systems have come a long way in a matter of technology. What started as an analog video system working in a closed circuit (CCTV) is now often a complex surveillance system relying on multiple servers and a vast network of various equipment connected to each other, communicating through different protocols and using numerous software and applications, most of them offering the possibility of access from anywhere in the world through an internet connection for the sake of operation simplicity.

At the same time, the methods used to hack, or to sabotage computer systems have become more sophisticated and are constantly evolving. It is often impossible to identify them before an attack is launched. What’s more - the more complex a system is – the more potential points of entry it offers for an organized attack. The cybercrime has become a serious threat to any data shared over the system.

The cybersecurity issue has therefore become a number one priority for Citilog. This document describes the actions undertaken by Citilog to improve the protection of customers data in CT-IM 2021R1.

1.1 DEFINITION OF TERMS

Term	Definition
AID	Automatic Incident Detection
ITS	Intelligent Transportation System
CCTV	Closed Circuit TeleVision
GUI	Graphical User Interface
IEEE	Institut of Electrical and Electronics Engineer (world's largest association of technical professionals)
HTTPS	HyperText Transfer Protocol Secure
TLS	Transport Layer Security
RTSP	Real Time Streaming Protocol

2. OVERVIEW

2.1. WHY PROTECT YOUR AID SYSTEM?

The AID system is nowadays an essential tool for efficient management of roads, highways, tunnels, and other infrastructures vital to our society. If it becomes vulnerable, the consequences may have a high impact on the overall operation of the transportation infrastructures and safety of its users.

In addition to that, like any computer system, it contains sensitive data such as user accounts (login and password) or images (live or recorded) that are not intended for external use. If not properly protected, it may also be used as an entry point to the rest of the network providing potential access to different computers, applications and other sensitive data.

2.2. THE MAIN RISKS

In terms of cybersecurity three main categories of risks are commonly identified and were taken into account by Citilog for risk evaluation:

- Human factor - often more important than technology, the human factor is defined as an internal threat, the source of which can range from a lack of attention or a lack of rigor to a malicious intent of an employee.
- Cyber-attack (hacking) - targeting a specific entity, a cyber-attack is an action executed from the outside, using the internet to access the entity network, in an attempt to hijack or damage their system.
- Virus or malware - a broad range attack with several possible outcomes like data deletion or data exploitation, possibly ending in the system failure. This risk occurs as a result of at least one of the two previous risks.

3. RISK SCENARIOS

Context:

A tunnel is an essential infrastructure for a city. It helps to ease traffic flow and allow drivers to save time on their daily commute. What is even more important – it can become vital when it comes to emergency services such as police, ambulances, or firefighters, for whom every lost minute might be a question of life or death.

Because of its importance, the tunnel is monitored by an AID system for early detection and efficient management of any incident.

In our example, this AID system is connected to 30 cameras which analyze the traffic in real-time. It is also connected to 2 Variable-Message Signs and to the traffic control center.

Threats:

#1: Phishing

Joe works at the control center. He loves funny pictures with cats and dogs. When he receives an email with a subject: “ ****Funny dog pictures**** ”, he doesn’t think twice before opening the attachment even if the sender is unknown.

Sadly, Joe’s email was infected by a virus which will spread from his workstation to every other computer in the network.

#2: Hacking

Kenny is a hacker. He is quite gifted and likes to show others what he is capable of, even if this leads to no personal gain. The cameras at the tunnel entrance have attracted his attention already a while ago and he wants to see if he can access it and control it. Since the network is not protected, the only challenge is to find a physical entry point. As soon as he succeeds, Kenny can easily monitor the data exchanged between the cameras and the AID system. He might even take control of the cameras and change PTZ positions.

Kenny will gain more and more access to the system, allowing him to modify the fields of view, the system settings or stealing video clips to share them on the internet.

Potential outcome:

#1: Phishing

If the malicious application is not detected by the antivirus, it will spread quickly to the network. Computers will gradually start to slow down until a complete crash. The AID system will be down and the tunnel operation will be compromised potentially to the extent of a tunnel closure.

#2: Hacking

Kenny will get bored at the end, but playing with the AID system, he totally messed up its settings. The system will no longer be working as planned which can have various consequences from missing some incidents to complete tunnel closure.

Figure 1: tunnel closure

The final outcome in both cases is a closed tunnel. During rush hour, the tunnel unavailability, can lead to major traffic congestions, leaving the drivers stranded for what may become even hours in a worst-case scenario. That could also mean that the emergency services will have to use another road to go from one part of the city to another one and waste precious time.

4. HOW CITILOG HANDLES THE RISKS?

Over the past few years, companies' exposure to cyberattacks proved to be more important than expected and often due to factors that could have been fairly easily eliminated. Multiple studies show that a large portion of the attacks could have been be prevented simply by patching known vulnerabilities and ensuring that security configurations are correctly set.

In this context, Citilog has taken all the necessary steps to evaluate possible risks and their impact on the security of its products and to identify the weak points in order to provide a safer and more reliable solution to its clients.

Based on this risk assessment, Citilog has developed and applied the appropriate security measures to minimize the identified external threats.

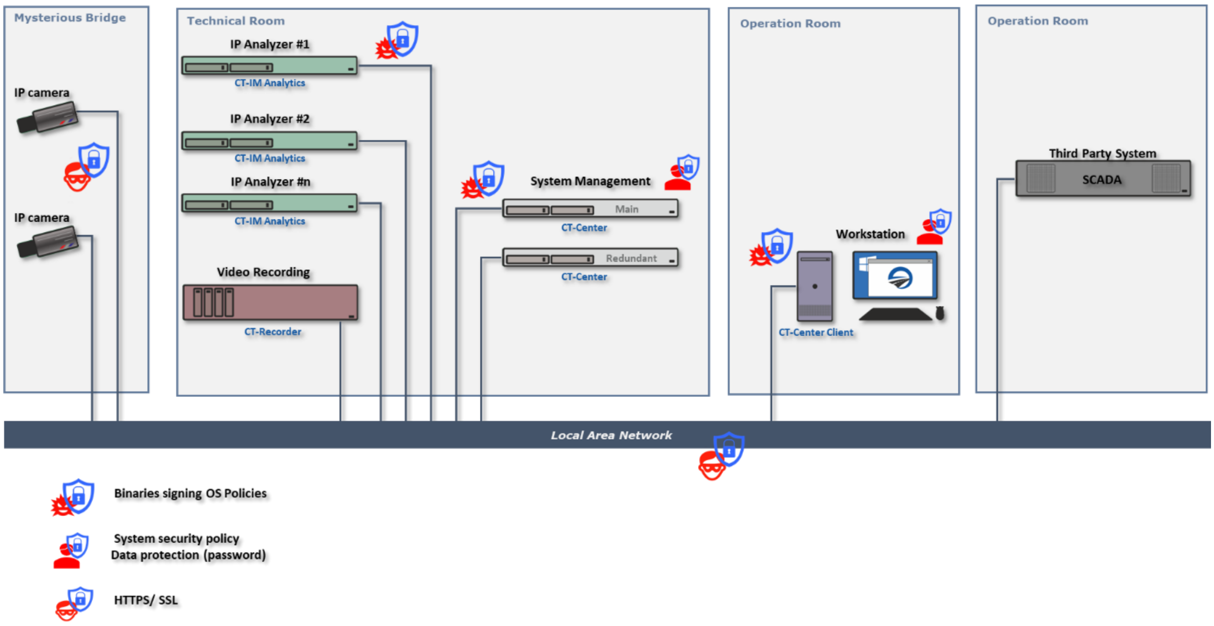


Figure 2: Citilog risks analysis and security measures

4.1. HUMAN FACTOR

While technical upgrades are important, minimizing human error is even more crucial. People have been proven to be the weak link in numerous attacks. Violations of standard procedures, misconfigured settings, weak passwords – they all open the door to potential attacks.

Although the risks associated with the human factor cannot be completely eliminated, Citilog has implemented different safeguard mechanisms to limit these risks as much as possible.

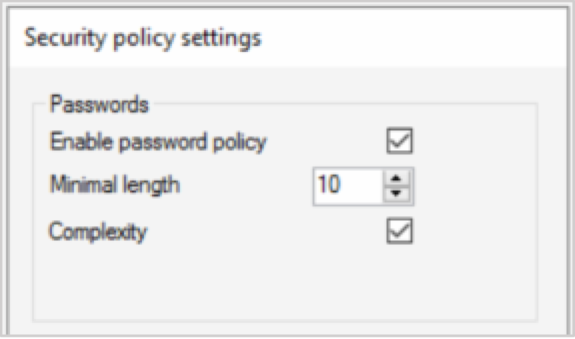
1. *Automatic lock down of admin session*

To make sure that no unauthorized person ever gets the access to the application settings that may have been left open on the workstation, the Citilog IM solution gets locked out in case of a prolonged inactivity.

After a pre-defined delay, the administrator will need to enter the password to return to his session.

2. *Passwords*

Each user - operator, administrator, or other - has its own personal password. CT-IM imposes the use of strong and complex passwords including the combination of alphanumeric characters and special characters for a better security.



Security policy settings

Passwords

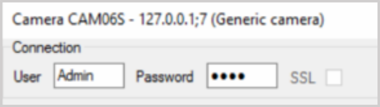
Enable password policy ☑

Minimal length 10

Complexity ☑

Figure 3: CT-Center Client - Security policy settings

In addition to that, passwords are encrypted in the system and cannot be displayed on the GUI. Passwords ‘real length is also invisible.



Camera CAM06S - 127.0.0.1;7 (Generic camera)

Connection

User Admin Password •••• SSL □

Figure 4: CT-Center Client – concealed credentials

4.2. CYBERATTACK (HACKER)

We have witnessed an important increase in cyberattacks recently and often the hackers are no longer working on their own but gather in efficient and well-organized criminal groups who can cause substantial damages attacking the system from the outside of the company, through an existing network.

To attack the AID, computer criminals will have to defeat first the security measures deployed by the network administrator such as ***Firewalls, IEEE 802.1x Authentication, Transport Layer Security (TLS) protocol*** etc.

Nevertheless, when security measures are weak, Citilog software can be exposed to a cyber-attack.

To reduce the risk of any intrusion, all communications between the different elements of the Citilog system are encrypted (using **Transport Layer Security)** making it impossible to access any confidential data transmitted through the network between the system's components.

Please refer to *Security measures* chapter for a complete list of implemented features.

4.3. VIRUS

Equally important is a virus issue. Even though it is not necessarily aimed directly at a particular company it remains no less dangerous. Designed to spread to other computers, it exploits the flaws of the security in the OS and can disrupt the operation of the infected computer to various degrees.

It can use several entry points like insecure USB keys, unverified attachments in the email or even a software installed recklessly from the internet. Once executed, it replicates itself and affects other programs and may lead to a complete shutdown of the entire system.

To prevent any unauthorized interference all the OS security measures should be applied:

- **User Account Control**

- **Antivirus**
- **Latest Windows updates**

The CT-IM solution is compatible with Windows Defender antivirus included in Windows 10 Pro and Windows Server 2019.

Every new release of the CT-IM solution is tested in an environment where Windows Defender is activated.

4.4. SECURITY MEASURES

The following features have been implemented in the latest CT-IM solution version to counter possible security breaches:

Feature	Description
IEEE 802.1x Authentication	Security guard forcing the user or a device to authenticate before allowing them to access the network - the user identity must be validated before getting an IP address and a fully functional wired or wireless adapter.
Transport Layer Security (TLS) protocol	Encrypts online transactions and confidential data relayed between cameras and the video management systems keeping the connections between equipment and server secure and private. TLS requires the use of a digital certificate.
HyperText Transfer Protocol Secure (HTTPS)	Communication protocol guaranteeing a secure communication over computer network. It is encrypted via TLS.
RTSP with authentication	Possibility to use RTSP with authentication in the system. The video streams will require login and password to be visualized.
User Authentication	Enforces a strong password policy.
No backdoor accounts	Citilog does not implement any backdoor in its systems for remote support.
Digest Authentication	Only an encrypted version of a password is saved on the server protecting it from easy decoding.
System auto-lock	Every sensitive element of the GUI (such as Administration tab) is protected by an auto-lock feature which automatically locks the GUI access if the system is not being used.
Cybersecurity oriented GUI	The CT-Center Client GUI is designed to conceal the passwords and their length.
Firewall compatibility	The CT-IM solution is compatible with every firewall and Citilog provides a list of ports that can safely be opened for network configuration.
Antivirus compatibility	The CT-IM solution is fully compatible with Windows Defender (Windows 10 Pro and Windows Server 2019).
Citilog software updates	Citilog regularly releases patches fixing the latest cybersecurity threats.
Firmware updates	Releases of new firmware versions improving the software stability and cybersecurity are regularly provided for Axis cameras.
Operating System updates	Citilog recommends installing all the Microsoft's updates for a better protection, detection, and response to emerging cybersecurity threats.

5. LIST OF FIGURES

FIGURE 1: TUNNEL CLOSURE 7
FIGURE 2: CITILOG RISKS ANALYSIS AND SECURITY MEASURES 8
FIGURE 3: CT-CENTER CLIENT - SECURITY POLICY SETTINGS 9
FIGURE 4: CT-CENTER CLIENT – CONCEALED CREDENTIALS 9

6. CONTACTING CITILOG

For further information, please contact Citilog:

<table>
<tr><th colspan="2">Global</th></tr>
<tr><td colspan="2">Citilog S.A.S.
42/46 avenue Aristide Briand
9220 Bagneaux – France
Tel: +33 1 40 96 69 00
citilog@citilog.com</td></tr>
<tr><th>Iberoamerica</th><th>North America</th></tr>
<tr><td>Citilog Iberoamerica
Av. Jacarandas, 2 Oficina 110
46100 Burjassot, Valencia - Spain
Tel: +34 96 136 3971
espana@citilog.com</td><td>Citilog Inc
2 Bala Plaza, Suite 300
Bala Cynwyd, PA 19004 - USA
Tel: +1 (215) 609 4945
citilogusa@citilog.com</td></tr>
</table>