CHeKT
Intelligent Visual Monitoring

CHeKT Visual Monitoring

Best Practices - 2022

Visual Monitoring
Understanding Threat Levels

Introduction - The Problem

For years, traditional alarm systems have communicated events into central stations. Even in adverse conditions, these alarm systems have reliably delivered alarm signals into a central station. Station operators have specific processes in place for responding to events and processing alarm signals. The automation software in a central station guides the operator's response to each signal so that every signal response is planned and consistent. In addition to guiding signal response, software platforms provide time stamp records of the various steps an operator performs while processing each signal. Automation software is designed this way to ensure a consistent threat response and minimize any liability caused by human error. Maintaining a consistent and planned signal response process in the central station minimizes liability for insufficient or incorrect alarm signal response.

Even with the reliability of a traditional alarm system, consumers, security dealers, and operators have lost confidence in the alarm system. This is because when an alarm occurs, operators are unable to see or understand what is taking place at the protected location, creating uncertainty about what caused the alarm. The uncertainty caused by the inability to see leads to inefficiencies in central station operations and a preserved poor quality of service by the customers. Unfortunately, these inefficiencies have become part of the daily frustration central station operators must deal with when determining the threat level of an alarm.

When processing a traditional alarm signal, an operator may attempt to contact people by phone. When the operator calls, if the customer does not know the cause of an alarm or does not answer the call, procedures often require the operator to contact emergency dispatch despite the possibility of a false alarm. When law enforcement does respond and requires observational assistance, the central station is unable to provide more specific information or guidance. Such situations occur routinely in monitoring stations and add unnecessary time and expense to central station operations and the operator's response.

Most false alarm dispatches result from the inability of the operator to see. These unnecessary dispatches can result in municipal fines for customers and in some cases, false alarm dispatch fines for alarm companies. The issue of false alarms has led some cities to change their alarm response ordinances, prohibiting law enforcement from responding at all unless there is confirmation of a crime in progress. These situations lead to customer frustration and low customer confidence and leave operators with negative feelings about their professional responsibilities.

CHeKT - The Solution

The CHeKT Visual Alarm Monitoring solution is designed to provide operators and customers with a clear understanding of what is happening at the protected location while ensuring the efficiency of operations, and the operator's existing workflow is maintained. CHeKT allows an operator to view video of what caused the alarm without changing the consistent process of the alarm response. All the actions and supervision of the operator's activity and video equipment is stored in the automation software's account history for auditing and transparency. CHeKT is the first video monitoring solution to follow the signaling equipment communication standards of traditional alarm systems while providing operators with the additional advantage of access to the video information needed to respond effectively and accurately to alarm signals.

The integration into alarm automation software allows CHeKT to be effective and scalable for all central stations. In an era where most homes and businesses have an on-site video system, providing the operator with access to Visual Alarm Monitoring gives them the information necessary to communicate with end-users and law enforcement. CHeKT allows an operator to "have eyes" on precisely what caused the alarm.

This document provides central station operation recommendations that allow for consistent alarm signaling, direct emergency contact, immediate threat response, and clear inter-office communication and services provided by CHeKT Visual Alarm Monitoring.

Scope

With the proper preparation, providing visual alarm monitoring services is not as difficult as you may think. This document provides recommendations and guidance to help your organization build Standard Operating Procedures (SOPs) for visual alarm monitoring services.

When providing current alarm monitoring services, operators are trying to visualize what may be happening. An experienced operator draws a mental picture of an alarm in progress every time they process an alarm. This mental picture is created from the specific zones numbers, zone descriptions, additional signals, and previous experience. Example: an entry alarm, followed by an interior alarm, followed by a cancel code provides an operator with a mental picture of what occurred.

As you read through this document, you will see how opening the eyes of an operator will give them the situational awareness and vision needed to provide customers with the alarm monitoring services they genuinely want and expect. This document provides a high-level understanding of how visual alarm monitoring will impact and benefit your monitoring center. We will discuss the type of information and signals your operators will receive from the CHeKT cloud and recommendations for how the operator should respond to each signal received. It is not intended to be the standard to replace existing SOPs but used as guidance through existing company policies, special instructions, and the specific customer needs already in place. Existing policies and instructions for security systems should take precedence.

The Central Station

How Does CHeKT Visual Monitoring Impact the Central Station?

Staffing: The central station should be able to maintain the current staffing requirements needed to handle the volume of alarm signals it is accustomed to handling. Adding the CHeKT solution to an account for visual alarm monitoring does not inherently increase the number or amount of signals a central station will receive. The solution puts eyes on alarm zones, allowing operators to see the protected premises and more efficiently perform their responsibilities. The number of alarm signals received into a station is based on the type of detection systems installed. This is important to note because when CHeKT is installed on an existing or traditional alarm system, operators will process the same alarm events they always have but with real-time video information. It is common for a central station to have added hundreds of CHeKT sites without hiring additional staff in the central station. With Visual Alarm Monitoring, proactive security systems with exterior detection become more common. These types of locations can produce an increased amount of alarm signals based on the site design, services provided, and detection devices used. A system with exterior detection needs to undergo a “soak-test” period where the site activity and events are supervised before being commissioned as a live account in the central station.

Monitoring Station Internet/Bandwidth: Most modern central stations already have a sufficient amount of Internet bandwidth at the monitoring station to stream video to an operator. The minimum recommended amount of download bandwidth needed is a 10MB service. Station bandwidth should be reevaluated as additional visually monitored sites are added to the system.

Premises Internet Bandwidth: The Internet speed at the protected location can impact the performance of the CHeKT visual monitoring portal and the speed at which an operator accesses both the alarm event video and live video from the site. It is recommended that the protected site have a minimum download speed of 2MB and a minimum upload speed of 2MB.

Premises Power or Internet Outage: If a site loses power or there is an Internet service outage when an alarm signal is received, video from the site will likely be unavailable. In these cases, it is recommended that the operator proceeds using traditional verification methods. The CHeKT solution actively supervises video devices and will communicate a trouble condition code to the central station if the video is unavailable. Note: See the list of CHeKT specific at the end of this document.

Automation Software Configuration: Each customer account utilizing CHeKT must be configured correctly and flagged in the automation software to launch the CHeKT monitoring portal when a signal is processed. The response procedures should be documented to ensure that the CHeKT account and surveillance system are configured correctly. Note: The installer or installing company should provide specific response details to ensure the guided response is configured correctly in the automation platform.

The Central Station Services

How Does CHeKT Visual Monitoring Impact the Central Station?

CHeKT Alarm Signal Integration: The CHeKT portal and devices communicate alarm signals, health status, supervisory information, and an audit trail of user activity in the monitoring portal. This information is transmitted to the automation software and the specific customer account alarm history using the Contact ID Alarm Code format. These alarm and audit codes are all enabled by default and can be customized or turned off based on the customer or dealer's need.

Alarm Signal Delivery: When the CHeKT Bridge is installed with a traditional intrusion system, it is important to note that the alarm system will continue to communicate the alarm signals in the same method without CHeKT. CHeKT will not interfere with the alarm system communications. When the automation software receives the signals and the site is flagged as a CHeKT account, the automation platform automatically opens the CHeKT monitoring portal for an operator.

Note: In some applications, the central station and or installation company may choose to use the CHeKT platform as a redundant communicator and send alarm signals. When the CHeKT Bridge is used as a stand-alone video security system or communicates triggers from video analytics, the Bridge should be programmed to communicate the alarm codes for its attached devices. (If the Bridge is used as the alarm communicator, the installation company must be sure to take into consideration back-up power and Internet services.)

Alarm Signal Processing: When an alarm signal is received, the process for an operator does not need to change, and operators can process the signal the same way they would for any traditional alarm system. The automation software should be configured to automatically open the CHeKT Video Monitoring portal for the operator, giving them instant access to the site's alarm video and live video. This signal processing method allows central stations to maintain their standard alarm handling procedures and staffing levels. This approach also reduces training time for operators and allows central stations to use the same staff to monitor traditional systems and accounts with visual monitoring by CHeKT.

SMS Verification Events: While processing the alarm, operators can forward video of the alarm event to the client using CHeKT's Verify SMS Video feature to engage the customer in the decision-making process. The customer can decide whether an emergency response is necessary. After the operator sends SMS verification, it is forwarded to all the defined site contacts instantaneously. These users may request an immediate dispatch or cancel the alarm processing directly from their phones. This feature directly impacts the central station's efficiency and significantly reduces operator signal response times. In many central stations, operators are instructed to forward the SMS event to the end-user and then process the alarm. Once the SMS message is sent, one of three Contact ID alarm codes will be sent to the central station automation software: a Cancel Alarm, a Dispatch Request, or a No-Response. Important: Specific automation software action plans should be created to specify operator response to Dispatch Request and No-Response signals.

Audio Talk-Down: During an alarm event, an audio message sent by a central station operator to a site is highly effective in providing guidance to someone one site. The messages can inform them of location hours and in many cases deter a criminal from committing a crime.

Account Special Instructions: When a signal is received, any special instructions for the account should take priority. Following a visual verification, the operator should contact the protected premises to communicate with an authorized user. Contacting an authorized user may be avoided if the operator, with a high level of certainty, can determine whether or not a security threat exists on the property.

Intelligent Visual Alarm Monitoring: Video information from a site should be considered alongside other known information about the site. Additional information, such as the site's customary opening and closing times or a "cancel" signal sent by the user's alarm panel, may clarify the operator's overall understanding of the site. This holistic approach enables operators to provide intelligent, real-time information to the customer and emergency responding agencies.

General Principles

When Providing CHeKT Video Monitoring

When an alarm occurs, and a person is visible, this does not mean that criminal activity is underway. False alarms often occur as a result of user error. Family members, employees, delivery people, etc., may trip the alarm by accident. An operator's responsibility is to verify the cause of the alarm signal. Visual information improves the operator's ability to understand what is happening at the protected premises, and the CHeKT Verify SMS Video feature allows the operator to engage the customer for a quick response. This doesn't change the operator's responsibility to verify every alarm signal, but it will speed up the response process. Notating every customer's account with this information will ensure the correct alarm response.

Adding CHeKT Visual Alarm Monitoring to an account does not change the signal processing procedure; it merely improves the overall alarm verification process for the operator and central station. When an alarm occurs, an operator is able to see and understand what caused the alarm to occur with a visual feed of the premises. Any additional, non-video information available to the operator will dramatically improve the level of service the operator provides in responding to alarms.

The CHeKT Visual Alarm Monitoring solution complements existing alarm processing procedures and gives the operators actual intelligence from a site. This improved alarm verification allows even an entry-level operator to process the alarm signal with the accompanying video, as with a traditional alarm signal.

Threat Levels

When Providing CHeKT Video Monitoring

Understanding What Operators Will See: Now that operators can see an alarm activation with visual alarm monitoring, your organization will see a wide variety of events that generate alarm signals. Understanding how to create company procedures in responding to these events and communicating why a specific course of action was taken by an operator is essential in providing video monitoring services. In order to standardize communication and provide guidance for operators, we recommend that all events viewed are classified into one of four categories called Threat Levels. These Threat Levels should be understood as a general awareness of what caused an alarm. From an alarm response standard, all video alarm events that an operator sees can be narrowed down into these Threat Levels and they can be seen as viewing a low, medium and high risk alarm. In this document we will detail each of the Threat Levels. Each Threat Level is color coded and abbreviated as shown below.

⬛	**Threat Level 0 (TL0)**	Alarm event received / VIDEO UNAVAILABLE
🟨	**Threat Level 1 (TL1)**	Objects moving in the cameras field of view, animals etc (nuisance alarm) /LOW
🟧	**Threat Level 2 (TL2)**	Human or Vehicle activity but criminal intent is uncertain. /MEDIUM
🟥	**Threat level 3 (TL3)**	Alarm activity with clear crime in-progess /HIGH

Internal Communication: Using the Threat Level classifications will help standardize your operator training, simplify the decision-making process and reduce mistakes when responding to a video alarm event. Your organization's understanding of these categories will give clarity to an operator's actions, alarm notes, and post-alarm internal office communication when reviewing an account's alarm history. With Threat Levels, your monitoring center can create policies on how a broad range of alarm events are narrowed down into four categories according to the risk associated with the site and the alarm conditions. In the following sections of this document are details of each Threat Level category and how an installing company's monitoring directions will guide the Threat Level Management process.

It is important to understand that operators performing visual alarm monitoring have increased situational awareness and require increased discretion due to the video information available. This visual information allows the operator to provide the client and emergency responders with actual and real-time knowledge of what is occurring on the property.

This real-time knowledge means operators need a standard understanding of Threat Levels for consistent communication and consistent response.

Threat Levels *- continued*

When Providing CHeKT Video Monitoring

External Communication: A clear understanding between the installation company, central station, and end-user of the desired response is always required. Response protocols should be clearly and thoroughly documented in each customer's central station account record. (Refer to the “Customer Threat Level Information Sheet” at the end of this document for sample paperwork.)

Site Example: In providing exterior monitoring, a dealer may install detection zones in an area where it’s common to see people and activity. The client may provide instructions requiring the central station to dispatch the police in cases of clear criminal activity, such as vandalism or theft. (TL3)

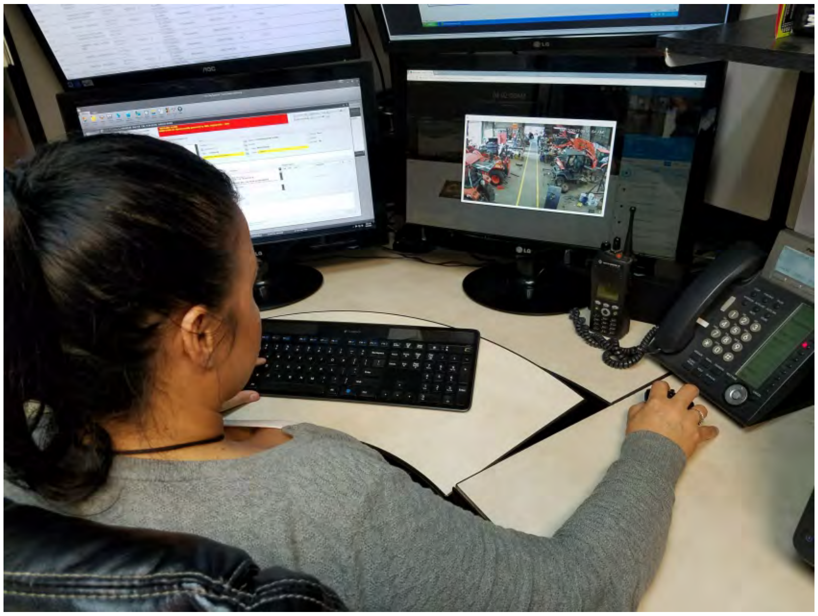
Important: All operators should understand and apply clear-cut procedures for documenting operator observations during an alarm. Consistently notating the account with the Threat Level observed by an operator gives insight into the alarm response and communication among management, office personnel, and installation companies. When providing visual alarm monitoring, notating what was viewed on an account is more important than with traditional alarm monitoring procedures.

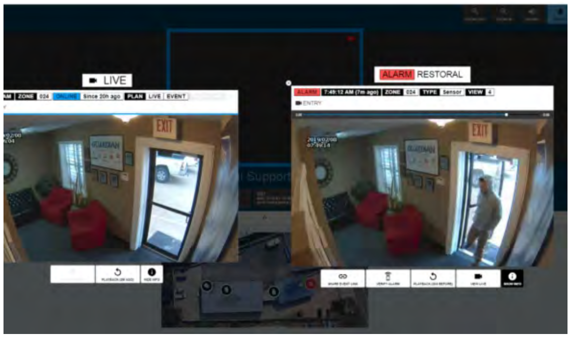
Site Installation Type

Understanding the Type of Monitored Accounts

With the Threat Level categories and an understanding of the Visual Alarm Monitoring site services providing a comprehensive and standardized alarm monitoring response to video becomes manageable and scalable.

When providing the Threat Level response documentation for a site, installation companies should also provide a clear understanding the type of security monitoring services required for a site. The type of visual alarm monitoring services has a direct impact on the nature of each Threat Level and the best response.





Site Installation Type

Continued..

Understanding site design and the installed services for a monitored location will assist central stations in providing operators with the guidance the need to accurately asses the Threat Level of an alarm. Nearly all installation of visual alarm monitoring will fall into one of these four categories for visual alarm monitoring services.

Video Verification

Interior Visual Alarm Monitoring - Video Verification

Visual Alarm Monitoring installed on a traditional interior alarm system to create a video security system. These types of systems do not increase signal traffic to a monitoring center, they simply add video verification service to traditional alarm monitoring, allowing operators to see exactly what caused the alarm to occur.

⬛ **Threat Level 0 (TL0) - Should be treated like a traditional alarm without video.**

🟨 **Threat Level 1 (TL1) - Should be verified with the customer unless otherwise noted. In a TL1 it's likley the keypad and siren are "In Alarm"**

🟧 **Threat Level 2 (TL2) - Should be verified with the customer using CHeKT Verify SMS Video. If no response, followed by a phone call.**

🟥 **Threat level 3 (TL3) - Should be an immediate dispatch followed by a call to the property owner.**

Exterior Security Secured

Secured Exterior Visual Alarm Monitoring

Visual Alarm Monitoring services install on traditional interior alarm system with additional exterior alarm zone in a secure area. The exterior alarm zones create outdoor proactive security systems by providing clients with exterior and perimeter alarm zone protection within a secure or protected boundary like a wall or fence. Allows operators to see a threat before a crime occurs and is a much higher level of service that many customers desire. Sites like this will have more TL1 and TL3 alarms depending on the detection devices. TL2 alarms on these types of sites are are possible trespassing alarms.

⬛ **Threat Level 0 (TL0) - Should be treated like a traditional alarm without video. (Special Instructions may override this standard.)**

🟨 **Threat Level 1 (TL1) - Special directions are required. An installing company may request that all TL1 alarms outside are ignored.**

🟧 **Threat Level 2 (TL2) - Should be verified with the customer using CHeKT Verify SMS Video. If no response, followed by a phone call.**

🟥 **Threat level 3 (TL3) - Should be an immediate dispatch followed by a call to the property owner.**

Exterior Security Unsecured

Unsecured Exterior Visual Alarm Monitoring

Visual Alarm Monitoring services install on traditional interior alarm system with additional exterior alarm zone in an un-secure area. The exterior alarm zones create outdoor proactive security systems by providing clients with exterior and perimeter alarm zone protection. Allows operators to see a threat before a crime occurs and is a much higher level of service that many customers desire. Sites like this will have more TL1 & TL2 Alarms. Special instructions are need to guide operators on how to handle TL2 Alarms if human or vehicle traffic is common.

⬛ **Threat Level 0 (TL0) - Should be treated like a traditional alarm without video. (Special Instructions may overrider this standard.)**

🟨 **Threat Level 1 (TL1) - Special directions are required. An installing company may request that all TL1 alarms outside are ignored.**

🟧 **Threat Level 2 (TL2) - Special directions required. Alarms can be verified with the customer using CHeKT Verify SMS Video.**

🟥 **Threat level 3 (TL3) - Should be an immediate dispatch followed by a call to the property owner.**

Video Guard Services

Remote Visual Guard Monitoring - Video Guard Services

This service is for locations where a security dealer is requesting a video monitoring solution and requires operator time to watch video from multiple cameras on a site. This service is required on accounts with exterior alarm zones in an "unsecured" area and the location is commonly visited by the public. (Examples: Car Lots, Campus Grounds, Pubic Parking Areas, etc.) It is common to require audio talk-down or controlling onsite lights for the monitoring center.) Sites like this will have more TL1 & TL2 Alarms. Special instructions are need to guide operators on how to handle TL2 Alarms if human or vehicle traffic is common.

⬛ **Threat Level 0 (TL0) - Should be treated like a traditional alarm without video. (Special Instructions may overrider this standard.)**

🟨 **Threat Level 1 (TL1) - Special directions are required. An installing company may request that all TL1 alarms outside are ignored.**

🟧 **Threat Level 2 (TL2) - Special directions required. In most cases operators watch the TL2 to to see if it becomes TL3.**

🟥 **Threat level 3 (TL3) - Should be an immediate dispatch followed by a call to the property owner.**

Threat Level Management

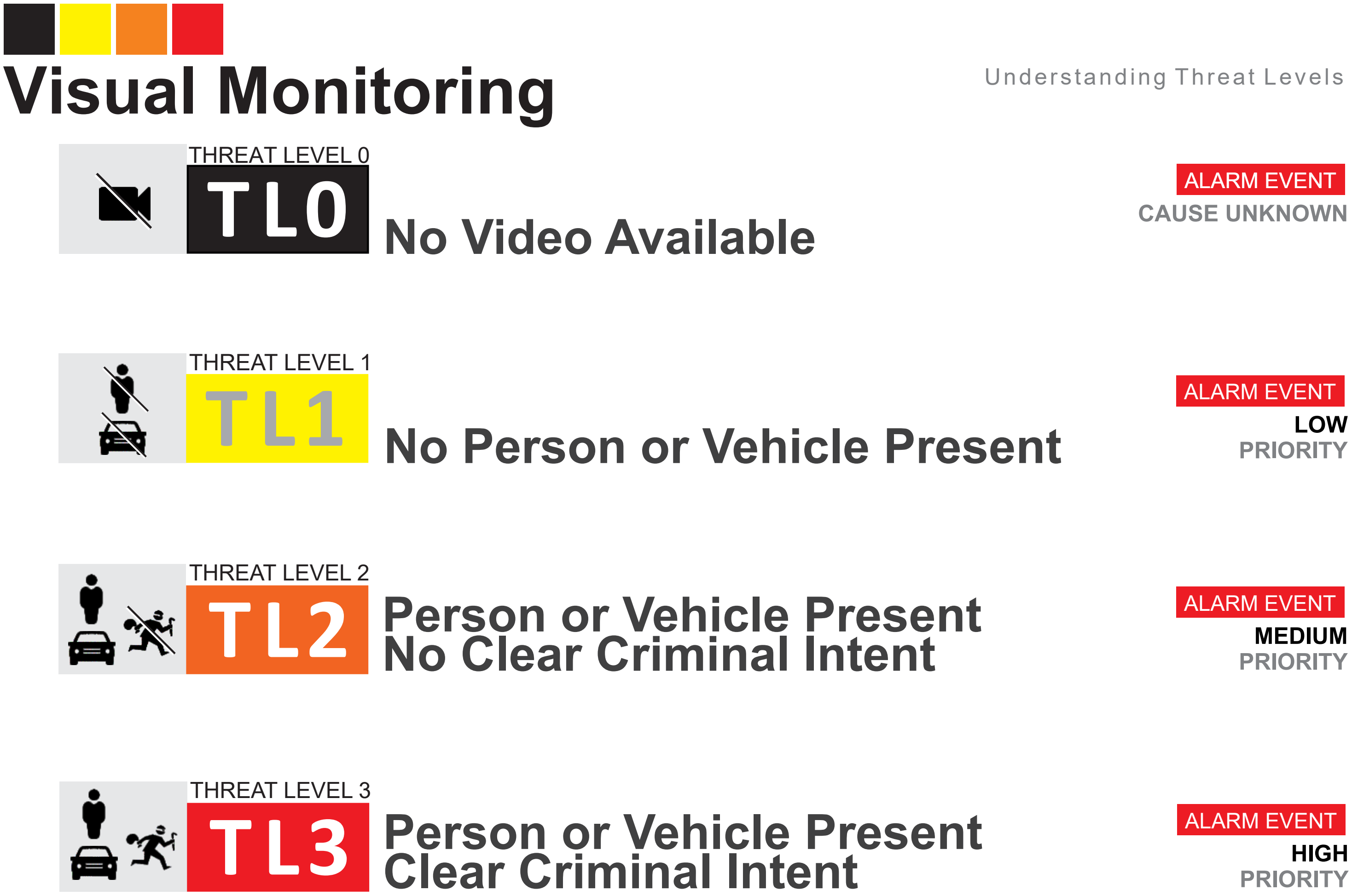
Threat Level Management assigns the correct Site Service category and the desired Threat Level response to a site. When properly done, the Threat Management system will help both the central station and dealer quantify the desired actions and responses for operators and reduce the liability and risk to the protected site. It is essential that the Threat Level Management system is defined and documented clearly and well-understood by central station operators.

There is a concern in many central stations that Visual Monitoring services create uncertainty in the monitoring center. These concerns include, “How much operator time does this service require?” “Do the operators have access to enough information?” and “Is our monitoring center taking on unnecessary risk and increased liability?” Defining Threat Levels and Site Services allows an organization to manage video alarms into a scalable and manageable solution. It equips the monitoring station leadership with an understanding of the total cost of ownership and the liability of visually monitoring accounts. Using a clear Threat Level and Site Services plan allows an organization to control what is viewed and how it is communicated by office personnel.

Standardizing what is viewed on a site and categorizing the Threat Level will allow an organization to understand the different causes of alarms and the expected response on the visually monitored site.

Once a central station has implemented a Threat Level Management system, It is recommended that the Threat Level response is built into the alarm handling action plan so that the management team can generate the appropriate report for each Threat Level.

The next section will guide and discuss each Threat Level in detail.



Visual Monitoring

Understanding Threat Levels

THREAT LEVEL 0

TL0

No Video Available

ALARM EVENT
CAUSE UNKNOWN

THREAT LEVEL 1

TL1

No Person or Vehicle Present

ALARM EVENT
LOW
PRIORITY

THREAT LEVEL 2

TL2

Person or Vehicle Present
No Clear Criminal Intent

ALARM EVENT
MEDIUM
PRIORITY

THREAT LEVEL 3

TL3

Person or Vehicle Present
Clear Criminal Intent

ALARM EVENT
HIGH
PRIORITY

THREAT LEVEL 0

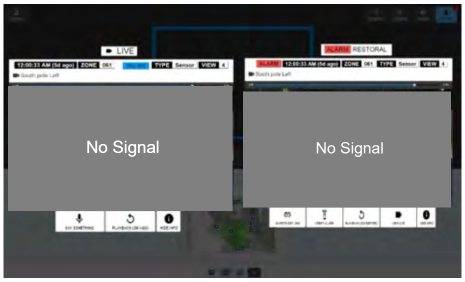
TL0 No Video Available

ALARM EVENT
CAUSE UNKNOWN

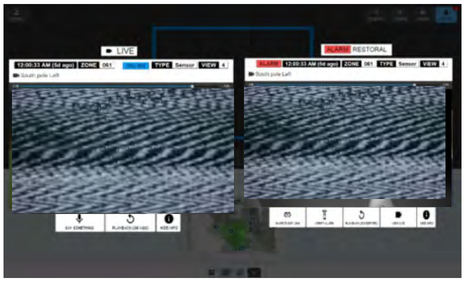
A Threat Level 0 occurs when an alarm signal is received by the operator, but the video is unavailable. A TL0 will require a specific response from the operator based on the account's specified instructions.
Required operator response to a TL0 is important and will be different for each customer. This should be clearly understood by the central station, installing company, and end-user.
Operator Response: This is ABC Security. We have received a signal from your system, but the video feed is unavailable. I am unable to determine if someone is on the property. How would you like me to proceed?

- **Note:** If it is exterior detection, it is recommended that an end-user verify the alarm and the police not be dispatched. If it is interior detection, standard verification processes should be followed.
- **Note:** Keep in mind that the intruder can disable the video before committing a crime.

In response to TL0 alarm signals, central stations will often instruct operators to follow a set of standardized alarm handling procedures.



Possible Power / Network Outage



Poor Connection / Service Needed on Site

Threat Level 0 (TL0)
EXAMPLES

THREAT LEVEL 1

TL1 No Person or Vehicle Present

ALARM EVENT
LOW
PRIORITY

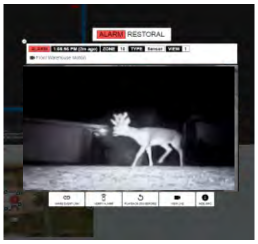
A Threat Level 1 occurs when an alarm signal is received, and human or vehicle is not present. A TL1 may include animals, environmental conditions or an object moving in the camera's field of view. This type of alarm is often called a nuisance alarm. A TL1 is the lowest priority, but it is still important to document what was viewed on the camera and why the alarm was triggered.

Examples: Door Opened by Wind, Interior Motion Alarm from a fan or animal.

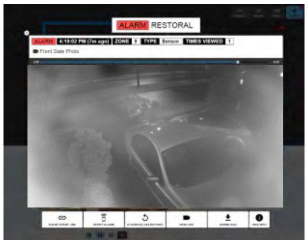
Important: It should be understood by the operator whether or not an audible alarm is active. (An audible alarm generally requires someone to silence the alarm)

On Exterior Secure/Unsecured & Remote Video Guard Sites some central stations may give their operators or supervisors an increased level of discretion of whether or not to call an end-user on TL1 events.

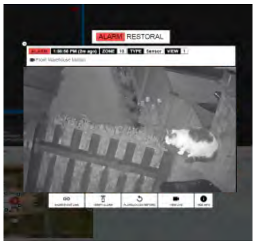
TL1 Example (Exterior Secure Site): *Received an alarm signal from the front motion detector. I viewed a small animal in the parking lot. I also viewed additional cameras on the property. No further action was taken—completed TL1.*
Important: If there is any level of uncertainty as to the cause of the alarm, a notification and call should be made to the end-user.
Operator Response: This is ABC Security. We received an alarm signal from your location. I am currently viewing the cameras, but I am unable to determine with certainty if someone is there. How would you like me to respond?
Alternate Response: This is ABC Security. We received an alarm signal from your location. I am currently viewing the cameras, and it appears that an animal triggered the motion. I am unable to determine with certainty if someone is there.
I do not see anyone, how would you like me to respond?
Response to audible alarm: This is ABC Security. We have received an alarm that was caused by an animal. Contacting a responding agency is not necessary, but be advised that an audible alarm is sounding.



Motion Detector / Animal



Inclement Weather / Poor Lighting



Motion Detector / Household Pet

Threat Level 1 (TL1)
EXAMPLE

THREAT LEVEL 2

TL2 Person or Vehicle Present No Clear Criminal Intent

ALARM EVENT
MEDIUM
PRIORITY

A Threat Level 2 occurs when an alarm signal is received, and human presence is confirmed, but the operator is uncertain whether or not there is a crime in progress. TL2 signals generally require more detailed observation from an operator. With a TL2, the operator needs clear instructions from the installing company on the correct course of action. In some cases a TL2 alarm can turn into a TL3 alarm.

Things to consider when a TL2 is in progress:

- What are the Site Services?
- Is the area in which the person is present a secure area? (fenced or inside)
- Do the site direction mention if TL2 events are expected for this location?

Note: An exterior location that is not surrounded by a fence may allow people and vehicles to pass through the area freely. In these areas, a person may be present without committing a crime. (This may be a common occurrence and if so the monitoring service rates may need to be reassess due to increased operator time in responding to TL2 alarms.

TL2 Example 1 (Exterior Unsecured): A homeless person sleeping behind a building may be in the camera's field of view for an extended period but is not committing a crime. It should be understood by the central station, installing company, and end-user precisely what should be done when a non-threatening person is present in the video feed.

Audio Talk-Down Message: Attention: This is private property. Leave immediately!

Example 2 (Remote Video Guard): An automobile dealership may want people looking at vehicles after they are closed. These environments require an operator to take more time to assess the threat. A plumbing company, on the other hand, may expect a more strict response when any evidence of human activity is seen on the property.

Audio Talk-Down Message: Attention: This location is closed. For your safety and protection, this property is under live remote video monitoring.

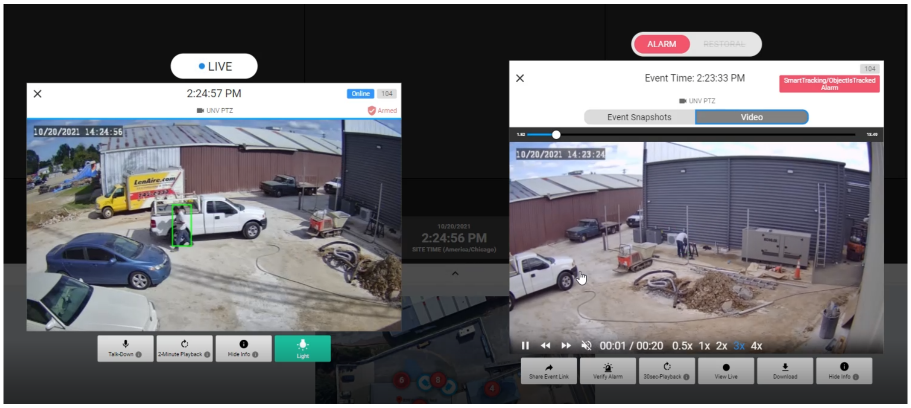
Operator Response: This is ABC Security. We have received an alarm signal. There is someone currently on the property, and I am unable to determine with certainty if this person is committing a crime or not. How would you like me to respond?

Example 3 (Interior Video Verification): A small convenience store or fast food restaurant with an interior alarm that uses only interior cameras. A back-door alarm occurs at 4:00 A.M. and the operator sees a man in a delivery uniform carry into the building what looks like stock for the store.

Operator Response: This is ABC Security. We have received a back-door alarm. There is someone currently on the property, and the security system has not been disarmed. They appear to be delivering food to the property. How would you like me to respond?

Example 4 (Interior/Exterior): If any operator receives an alarm and can see a person at the keypad preparing to disarm the alarm system, the central station may create an SOP instructing central station staff to wait for the system to disarm before responding to the alarm.

On Exterior Unsecured & Remote Video Guard Sites some central stations may give their operators or supervisors an increased level of discretion of whether or not to call an end-user on TL2 events.



Undetermined Threat at Location

Threat Level 2 (TL2)
EXAMPLE

THREAT LEVEL 3

TL3 Person or Vehicle Present Clear Criminal Intent

ALARM EVENT

HIGH
PRIORITY

A Threat Level 3 occurs when an alarm signal is received, a person or vehicle present, and the operator believes that there is a crime in progress. Depending on the specific notes on the account, this will generally escalate to emergency dispatch and, if required, direct contact between central station, emergency response, and end-user.

Operator discretion is also important for TL3 signal response. When an operator sees a crime in progress, they can communicate accurate and critical information to police dispatch. Giving operators a level of discretion in response to TL3 alarms will ensure that valuable time is not lost.

Audio Talk-Down Message: Attention: An alarm has occurred at this location. Leave immediately!

Operator Response to Law Enforcement: This is ABC Security. We have visual evidence of a crime in progress at (protected property). I am currently viewing the video cameras. I see two males; one is wearing blue jeans and a dark shirt, the other is wearing blue jeans and a white hoodie. They appear to be breaking into a vehicle in the northwest parking lot.

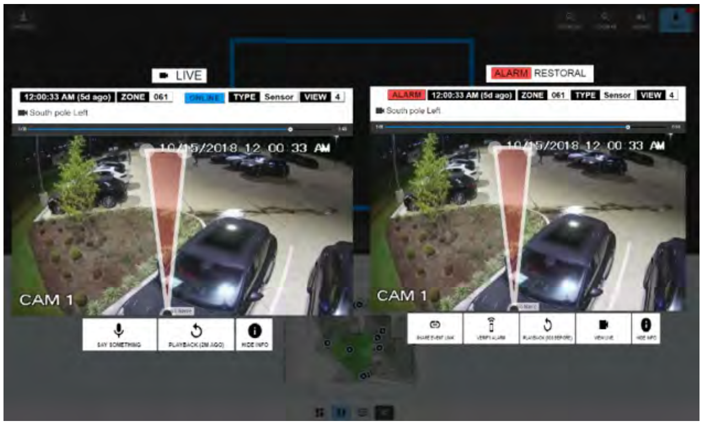
Note: Like central station operators, police operators accept emergency calls every day. The central station operator's verbiage with police dispatch should clearly indicate that video is presently being viewed and there is currently criminal activity taking place.

Operator Response to End-User: This is ABC Security. We received an alarm signal at your location. We observed two males attempting to break into one of the vehicles. We have contacted law enforcement, and emergency response is currently in progress.

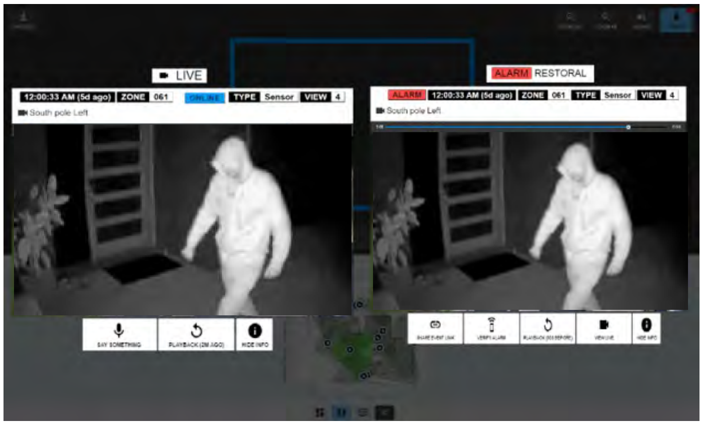
Operator discretion is also important for TL3 signal response. When an operator sees a crime in progress, they can communicate accurate and critical information to police dispatch. In some TL3 cases, an operator may not use the Talk-Down services in increase the likelihood of apprehending the criminal. Giving operators/supervisors a level of discretion in response to TL3 alarms will ensure that valuable time is not lost.

Threat Level 3 (TL3)

EXAMPLES



Unauthorized Vehicle On Property - System Armed

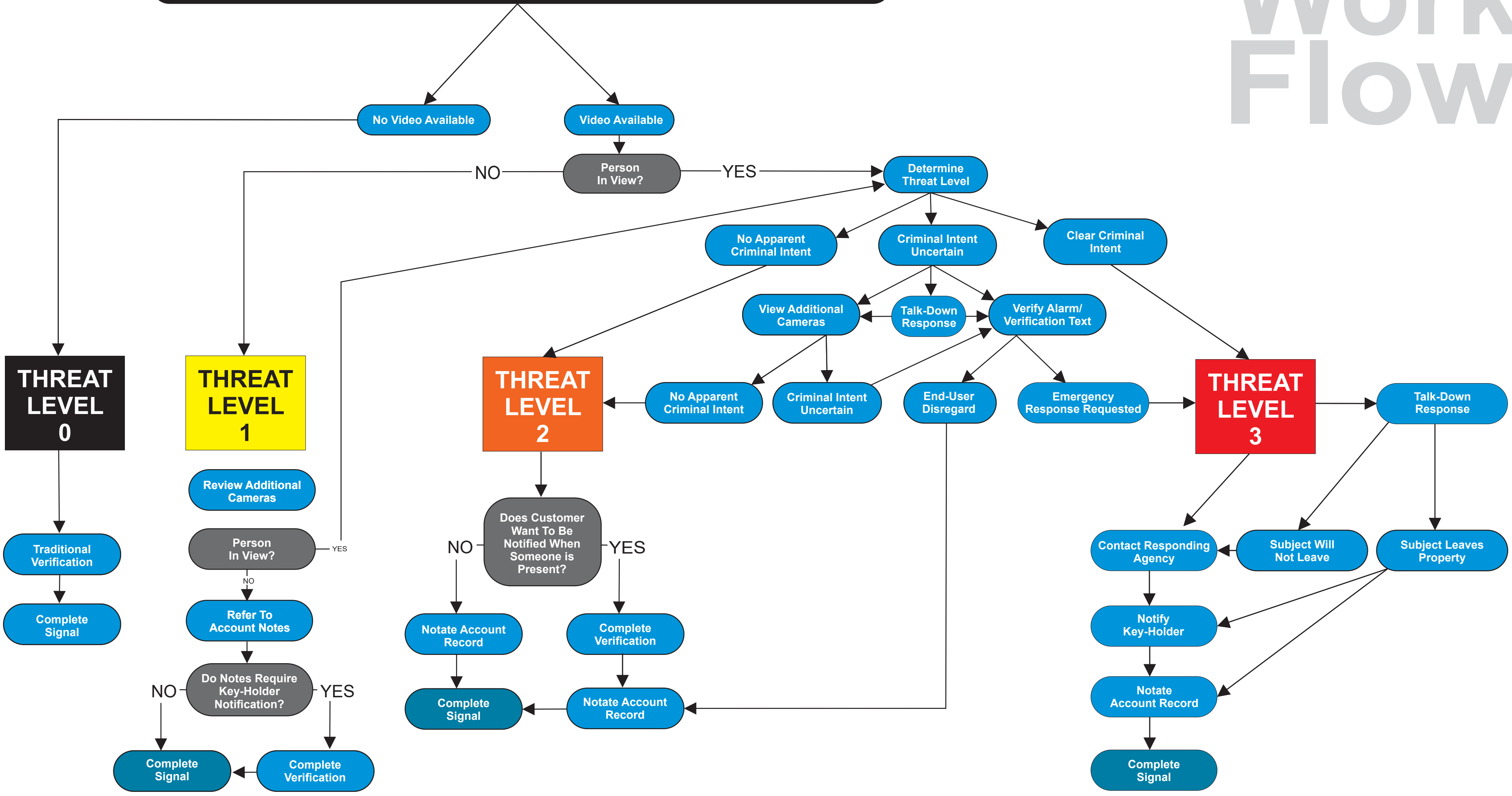


Suspicious Activity/Clothing On Property - System Armed

Video Monitoring Signal

Visual Monitoring
Understanding Threat Levels

Work Flow



No Video Available

Video Available

Person In View?

NO

YES

Determine Threat Level

No Apparent Criminal Intent

Criminal Intent Uncertain

Clear Criminal Intent

View Additional Cameras

Talk-Down Response

Verify Alarm/ Verification Text

No Apparent Criminal Intent

Criminal Intent Uncertain

End-User Disregard

Emergency Response Requested

THREAT LEVEL 0

Traditional Verification

Complete Signal

THREAT LEVEL 1

Review Additional Cameras

Person In View?

YES

NO

Refer To Account Notes

Do Notes Require Key-Holder Notification?

NO

YES

Complete Signal

Complete Verification

THREAT LEVEL 2

Does Customer Want To Be Notified When Someone is Present?

NO

YES

Notate Account Record

Complete Verification

Complete Signal

Notate Account Record

THREAT LEVEL 3

Talk-Down Response

Contact Responding Agency

Subject Will Not Leave

Subject Leaves Property

Notify Key-Holder

Notate Account Record

Complete Signal

THREAT LEVEL 0	THREAT LEVEL 1	THREAT LEVEL 2	THREAT LEVEL 3
TL0	TL1	TL2	TL3

Visual Monitoring / *Best Practices*

CHeKT Contact ID Alarm Codes

The CHeKT Alarm codes are communicated into an automation platform and account number using the alarm signal Integration feature. This integration is key to ensuring events associated with the CHeKT monitoring portal, operator actions and the network health status of CHeKT devices are sent to your automation platform for logging or proper signal response by an operator. The CHeKT Monitoring Portal and associated devices transmit Contact ID alarm codes into the automation platform. All signals are transmitted to the customer account in the central station automation software. This allows the monitoring center to audit actions from the CHeKT Monitoring Portal in their automation software.

*NOTE: As with all Contact ID alarm codes, this the Signal ID component and the Zone or Device ID component.

CHeKT Zone Numbers and Device ID Standards

Zone 900: CHeKT Cloud or Monitoring Portal location.

Zone 901-9XX: Each Bridge installed on a secure site has a unique identifier that begins at 901 and increases by one with each additional Bridge added to the system

Zone 9XXA-L: Each camera installed on a Bridge has a default zone number of the Bridge identifier and a letter to identify the video channel of the Bridge. For example, 901A is the first Bridge on a site, and the camera is on channel 1 of the Bridge.

Examples:

901A: Channel 1 camera on the first Bridge
901D: Channel 4 camera on the first Bridge
902A: Channel 1 camera on the second Bridge
903B: Channel 2 camera on the third Bridge

Note: The installing companies are instructed to change the default camera zone number to match the associated alarm panel zone supervised by the camera. This step is essential to ensure that an operator is directed to the correct camera when an alarm occurs.

The following are Contact ID Signals generated by the CHeKT cloud:

E306 Programming Change

Following the initial configuration of a Bridge or camera, any changes to the configuration of the Bridge or connected cameras will be communicated to the central station as an E306. If changes to the configuration of the Bridge are made, an E306 and Bridge Device ID will be sent to the central station. If changes to the camera or zone configuration are made, an E306, followed by the zone number, will be sent to the central station.
Zone Information: The device that has been changed, as well as either the Bridge ID or the Camera Channel ID.

Response: This is ABC Security. We have received a signal indicating that the programming on a Bridge or zone connected to the Bridge has been changed. A programming change can affect the system's integrity and testing the system to ensure proper operation is recommended. (Contacting the installing company is not required.)

Note: After completing the initial installation, each zone must be tested and confirmed to ensure that the system is functioning properly. This alarm code notifies the central station that something on the site has changed that may affect the system's integrity. The CHeKT Dealer portal retains a detailed audit of any changes made to the configuration of the system. This information should be communicated to the installing company.

E401/R401 Arm/Disarm

Each Bridge will communicate an opening or closing signal. A central station will receive an open or close signal from the alarm system and additional open and close signals from each Bridge. This is done to allow operator supervision of each device. The delivery of open or close signals can be disabled in the alarm library codes.

Zone Information: Will be the Bridge Device ID.

Response: (Optional Auto-Log)

E414 Bridge Remote Reboot

If it is necessary to reboot a Bridge, this can be done from the CHeKT portal by going to the Bridge settings in the device list. After a reboot command is sent to the Bridge, an E414 will be sent to the central station automation software. When a remote reboot is performed, the central station should also receive an E751 "Power on Restart" once the restart is completed and the Bridge is online.
Zone Information: Will be the Bridge Device ID.

Response: (Optional Auto-Log) This signal is generally auto-logged in the automation platform for informational purposes

E575 Zone Swinger Bypass

This signal is sent from the CHeKT one of the reporting alarm zones of the Bridge is automatically bypassed by the Swinger Bypass feature. The feature allows a dealer to auto-bypass a detector after (X) alarms while armed.

Zone Information: Will be the camera zone number.

E609 Monitoring Portal Opened

This signal is sent from the CHeKT cloud when the monitoring portal is first opened. After an alarm signal is received, the automation platform launches the CHeKT portal. Once the monitoring portal is viewable, the signal is sent to automation. This does not mean that the operator performed any action, but simply that the portal has been launched.
Zone Information: Will be the CHeKT Portal ID: 900.

Response: (Optional Auto-Log) This signal is generally auto-logged in the automation platform for informational purposes.

E750/R750 Bridge Network Connection

This signal is sent to the operator when a Bridge disconnects from the CHeKT cloud. The causes of a Bridge disconnect could be due to internet connectivity or onsite power failure. The response for each site will require a different response depending on the level of service provided by the central station.
Zone Information: Will be the Bridge Device ID.

Response: This is ABC Security. We have received a signal indicating that a Bridge has disconnected from the Internet and is not available. If an alarm occurs in this area, we will not have access to the video feed.

Note: (Important) Internet Service Providers (ISPs) can reset their services periodically without giving notice to their customers. This often takes place late at night. Internet resets will cause the Bridge to lose internet connectivity temporarily. To prevent unwanted signals from being delivered to the central station during these times, a disconnect signal is suppressed for 10 minutes by default. This timeframe can be changed in the alarm library codes of the account.

E751 Bridge Power On/System Reset

Once the Bridge is successfully registered, an E751 signal is communicated to automation. This signal is sent after a power failure or remote reboot and indicates that the Bridge has successfully powered up.
Zone Information: Will be the Bridge Device ID.

Note: This signal will not be sent the first time that the Bridge connects to the CHeKT cloud.

E753 No Response on Verification Text

If an SMS message is sent to the end-user and the configured wait time or "the window of time in which the end-user is required to respond" expires, an E753 will be sent to the central station automation software indicating that none of the contacts responded with a decision to either "Dispatch or Cancel" the alarm.
Zone Information: Will be the CHeKT Portal ID: 900.

Response: Understand how to communicate with the end-user to be prepared to respond to this situation.

Note: (Important) An E753 (no response on verification text) must be presented to an operator to continue the verification process.

E754 Operator Sent Verification Text

When an operator sends the video verification to the end-user, an E754 will be sent to the central station automation software.
Zone Information: Will be the camera zone number or Channel ID.

Response: (Optional Auto-Log): This signal is generally auto-logged in the automation platform for informational purposes.

E755 End-User Checked Verification

After the operator sends the video verification event to the end-user and they click on the event to view the video E755 will be sent. Depending on the automation platform, this alarm signal is sent with the name of the user or just the user#.
Zone Information: Will be the CHeKT Portal ID: 900

Response: (Optional Auto-Log): This signal is generally auto-logged in the automation platform for informational purposes.

Note: This signal is generally auto-logged in the automation platform for informational purposes. If the automation platform only supports the user# in the signal package, then the users should be added to the automation platform for a clear description of the username who checked the video verification event.

Note: Understanding SMS verification signals. If the account alarm history for a customer shows an E754 (operator sent verification text), an E755 (end-user checked verification), and an E753 (no response on verification text), this means that the end-user looked at the video event but made no action to respond to the text message verification.

E756 Verification Response (Disregard/Cancel)

After the operator has initiated a "verify event" command and an SMS message is sent to the end-user, the end-user can select "request dispatch" or "disregard" inside the body of the SMS message. If an end-user chooses to Disregard or Cancel the Alarm, an E756 will be sent to the central station automation software.
Zone Information: Will be the CHeKT Portal ID: 900.

Response: (Optional Auto-Log): An E756 can be treated as a confirmed cancel code.

E757 Verification Response (Dispatch/Call Police)

After the operator has initiated a "verify event" command and an SMS message is sent to the end-user, the end-user can "request dispatch" or "disregard" inside the body of the SMS message. If an end-user requests Dispatch on the alarm, an E757 will be sent to the central station automation software.
Zone Information: Will be the CHeKT Portal ID: 900

Response: An E757 should be treated as a confirmed dispatch and should have a priority response in the automation platform.

E758/R758 Privacy Mode Access Removed/Restored

Specific cameras in the CHeKT portal can be placed in privacy mode. These cameras are only viewable by the operator when the end-user grants access with the end-user verification text. When a camera is in privacy mode, and the operator initiates a verification request (verify event SMS text), the end-user will be prompted to respond if he or she would like to provide the operator with access to that camera for one hour. If the end-user grants operator access to a camera in privacy mode, an E758 will be communicated to the automation platform. In one hour, when the privacy is restored to the camera, an R758 will be sent to the central station.
Zone Information: Will be the CHeKT Portal ID: 900.

Response: (Optional Auto-Log): This signal is generally auto-logged in the automation platform for informational purposes.

E759 Event Link Shared

While processing an alarm signal, the operator can share information with the responding agency or end-user. The video event, live view, site location and address, contact information, and central station information is available to the recipient. If the operator clicks on "Share link," an E759 will be sent to the central station.
Zone Information: Will be the CHeKT Portal ID: 900.

Response: (Optional Auto-Log): This signal is generally auto-logged in the automation platform for informational purposes.

E760 Event Clip Video Viewed

When the monitoring portal is open and an operator views the video event clip, an E760 and zone number will be sent to the central station.
Zone Information: Will be the camera zone number or Channel ID.

Response: (Optional Auto-Log): This signal is generally auto-logged in the automation platform for informational purposes.

E761 Live Video Viewed

When the monitoring portal is in use by an operator during a signal response, every camera the operator clicks on for viewing will be recorded and sent to the central station. This information will include the zone number of each camera viewed.
Zone Information: Will be the camera zone number or Channel ID.

Response: (Optional Auto-Log): This signal should be auto-logged and used for auditing purposes.

Note: The individual camera itself must be clicked on. Once clicked, a blue box will highlight the camera. Rolling the mouse though the monitoring portal, it is evident that all of the cameras will not send a signal to the central station. If the operator views multiple cameras, an E761 signal from each camera he or she viewed will be sent.

E762 Playback Video Viewed

While the operator has the monitoring portal open, a two-minute playback of each specific camera can be requested by the operator. When this feature is used, the two-minute video will be stored for 30 days, and an E762, followed by the zone number, will be sent to automation.
Zone Information: Will be the camera zone number or Channel ID.

Response: (Optional Auto-Log): This signal is generally auto-logged in the automation platform for informational purposes.

E770/R770 Privacy Mode Removed/Enabled by the End-User

Specific cameras in the CHeKT portal can be placed in privacy mode. Once a camera is in privacy mode, only the end-user can turn control whether privacy mode is on or off. Using app.chekt.com, the end-user can switch the privacy mode on or off.
Zone Information: Will be the camera zone number or Channel ID.

Response: (Optional Auto-Log): This signal is generally auto-logged in the automation platform for informational purposes.

E776 Audio Broadcast Announcment

An audio message was sent to the site by the operator. When this feature is initiated, an E757 will be sent to the central station automation software.
Zone Information: Will be the CHeKT Portal ID: 900.

Response: (Optional Auto-Log): This signal is generally auto-logged in the automation platform for informational purposes.

E790 Bridge/Camera Added

After the initial site set-up, an E790 will be sent when a Bridge or camera is added.
Zone Information: Will be the device added. Either the Bridge ID or the Camera Channel ID.

Response: This is ABC Security. We have received the signal that a Bridge or Camera is being added to the system. This information must be updated to the central station to ensure proper system response.

Note: This signal is sent to the central station, so the central station has the information that the installing company has altered the system in some way. Contacting the installing company is not required but is recommended.

E791 Bridge/Camera Removed

After the site is set-up and completion of device configuration, an E791 will be sent to the central station if a Bridge or camera is removed or deleted. An E791, followed by the device ID, will be sent if a Bridge is removed. An E791, followed by the zone number, will be sent if a camera is deleted.
Zone Information: Will be the device added. Either the Bridge ID or the Camera Channel ID.

Response: This is ABC Security. We have received a signal indicating that a Bridge (or camera) has been removed from the system. Removing a Bridge (or camera) will affect the system's integrity and testing the system to ensure proper operation is recommended.

Note: Contacting the installing company is not required but recommended.

E796/R796 Camera Connection Status

If the camera stream disconnects from the Bridge, an E796, followed by the zone number, will be sent to the central station. Once the camera stream is restored, an R796, followed by the zone number, will be sent to the central station.
Zone Information: Will be the camera zone number or Channel ID.

Operator Response: This is ABC Security. We are receiving a signal indicating that a camera on (Zone number/Zone Description) has disconnected. This will affect our ability to provide monitoring services.

Note: During this conversation, an operator should look at the other cameras at the site to determine whether they are viewable in the monitoring portal.

Camera Analytics: It's critical to note whether the zone is using camera analytics. If a camera with analytics is offline, then the detection method for that zone will likely be affected.

Contact I.D. Codes

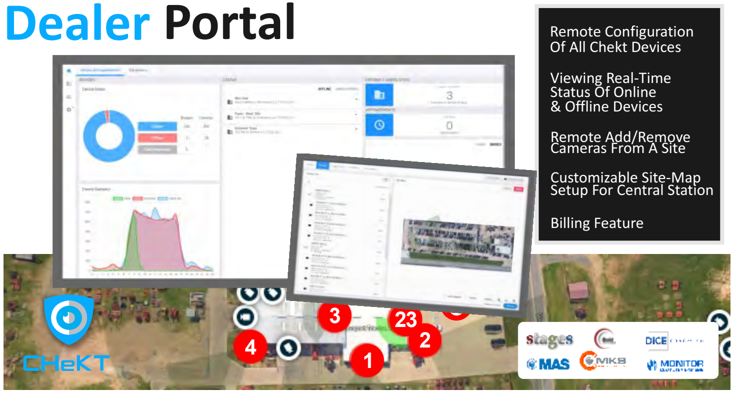
CHeKT

E306	Programming Change
E401/R401	Arm / Disarm
E414	Bridge Remote Reboot
E609	Monitoring Portal Opened
E750/R750	Bridge Network Connection
E751	Bridge Power on/System Reset
E753	No Response on Verification Text
E754	Operator Sent Verification Text
E755	End User Checked Verification
E756	Verification Response (Disregard/Cancel)
E757	Verification Response (Dispatch/Call Police)
E758/R758	Privacy Mode Access Removed/ Restored
E759	Event Link Shared
E760	Event Clip Video Viewed
E761	Live Video Viewed
E762	Playback Video Viewed
E770/R770	Privacy Mode Removed/Enabled by the End-User
E776	Text to Speech Audio
E790	Bridge/Camera Added
E791	Bridge/Camera Removed
E796/R796	Camera Connection Status

Online Resources

Introduction to the CHeKT

Dealer Portal



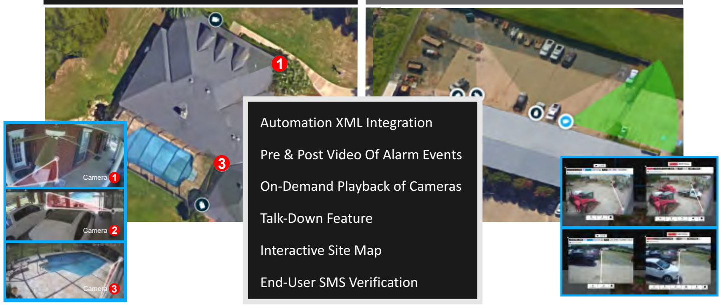
- Remote Configuration Of All Chekt Devices
- Viewing Real-Time Status Of Online & Offline Devices
- Remote Add/Remove Cameras From A Site
- Customizable Site-Map Setup For Central Station
- Billing Feature

Introduction to the CHeKT

Operator Portal

Residential Sites

Commercial Sites



- Automation XML Integration
- Pre & Post Video Of Alarm Events
- On-Demand Playback of Cameras
- Talk-Down Feature
- Interactive Site Map
- End-User SMS Verification

Dealer Launch Site

Visual Verification Bridge
Powered by CHeKT

www.chekt.com/launch

click here

Everything You Need To Successfully Deploy Visual Monitoring

CHeKT

www.chekt.com
224-44-chekt
support@chekt.com

Visual Monitoring

Threat-Level Dealer Worksheet

TL0

Threat Level 0

ALARM EVENT

No Video Available

TL1

Threat Level 1

ALARM EVENT

No Person or Vehicle Present

TL2

Threat Level 2

ALARM EVENT

Person or Vehicle Present
No CLEAR Criminal Intent

TL3

Threat Level 3

ALARM EVENT

Person or Vehicle Present
CLEAR Criminal Intent

Customer Information Sheet

Customer Information

Date Created: 06/29/2018 12 18:53 pm
Customer Name:
Address City: Status: Zip: Country:

Chekt Site ID: 2234
TimeZone: America/Chicago

Monitoring Center

Account Number: CHE-000000

Reference ID:

Customer Video Verification List

Name:

Phone Number:
+

Device List

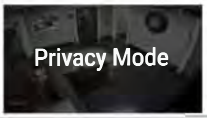
Bridge	Name: 4 Pin Bridge	Device ID: 901	F/W Version: 2.6.0.0.dev	MAC Address: B827EBA5D5C8	IP: 198.0.24.237

Arming Status	Voltage Arming		Loss of Voltage Arming		Always Arming	✓	Always Disarmed	

Bridge Alarm Inout Zone	Alarm Panel Zone #	Description	Camera IP Address/URL Path	Camera MAC	DVR/DVR Channel	Zone Type	Zone Trigger	XML Alarm
DI1	157	OPTEX's CMOD	rtsp://172.16.239.150/live/ch00_2	B827EBA5D5C8	1	24 Hour	nc	E426
DI2	32	Kitchen	172.16.4.212	4C11BF8CD5E8	0	Entry/Exit	nc	
DI3	151	UDP Entry Analytics	172.16.4.203	0013230A4E10	0	Instant	nc	E426
DI4	152	Analytics Dome	172.16.4.112	A0BD1D02A5D8	0	Instant	nc	E130

Thumbnail

DI1:

DI2:


DI3:

DI4:

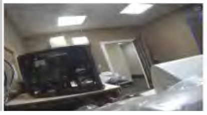
relay	Name		Status Label	Assigned Camera	Description
			energized/normal	No Assigned Camera	

Bridge	Name: Lights	Device ID: 902	F/W Version: 2.6.0.0.dev	MAC Address: B827EB89F231	IP: 198.0.24.237

Arming Status	Voltage Arming		Loss of Voltage Arming		Always Arming	✓	Always Disarmed	

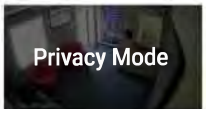
Bridge Alarm Inout Zone	Alarm Panel Zone #	Description	Camera IP Address/URL Path	Camera MAC	DVR/DVR Channel	Zone Type	Zone Trigger	XML Alarm
DI1	902A	Hanwha	172.16.4.105	E4302201C2E6	0	Instant	nc	E130
DI2	161	HD Thermal Analytics	172.16.4.103	A41437810636	0	Exterior(Entry/Exit)	nc	E146
DI3	162	Thermal Analytics	172.16.4.103	A41437810636	1	Exterior(Instant)	nc	E140
DI4	204	Lobby	172.16.4.215	08EDED18B306	0	Instant	nc	E130

Thumbnail

DI1:


DI2:

DI3:

DI4:


Alarm Zone Event Codes

Zone	Zone Description	Event Alarm Code	Restoral Alarm Code	Alarm Description		
157	24 Hour Zone	E426	R426	24 Hour Zone		
151	Instant Zone	E426	R426	Instant Zone		
152	Instant Zone	E130	R130	Instant Zone		
902A	Instant Zone	E130	R130	Instant Zone		
161	Exterior(Entry/Exit) Zone	E146	R146	Exterior(Entry/Exit) Zone		
162	Exterior(Instant) Zone	E140	R140	Exterior(Instant) Zone		
204	Instant Zone	E130	R130	Instant Zone		

CHeKT Portal Alarm Code Events

	Zone Information	Event Alarm Code	Restoral Alarm Code	Alarm Description	Enabled	Condition
	Bridge Device ID	E401	R401	Arm/Disarm	Yes	O/C
	Bridge Device ID	E751		Power On/System Reset	Yes	System Message
	Bridge Device ID or Camera Zone Number	E790		Bridge/Camera Added	Yes	System Message
	Bridge Device ID or Camera Zone Number	E306		Programming Change	Yes	System Message
	Bridge Device ID or Camera Zone Number	E791		Birdge/Camera Removed	Yes	System Message
	Bridge Device ID	E303	R303	Bridge Trouble Output	Yes	Trouble
	Camera Zone Number	E760		Video Event Clip Viewed	Yes	System Message
	CHeKT Portal - Zone 900	E609		Camera Live View	Yes	System Message
	Camera Zone Number	E761		Live Video Viewed	Yes	System Message
	Bridge Device ID	E750	R750	Bridge Connection/Disconnected	Yes	Trouble
	Camera Zone Number	E796	R796	Camera Loss	Yes	Trouble
	Bridge Device ID	E603		Periodic Test	Yes	System Message
	Camera Zone Number	E762		Playback Video Viewed	Yes	System Message
	Camera Zone Number	E758	R758	Privacy mode access granted/restored	Yes	System Message
	Camera Zone Number	E770	R770	Privacy Mode Removed/Enabled by End User	Yes	System Message
	CHeKT Portal - Zone 900	E759		Event Link Shared		System Message
	Bridge Device ID	E414		Remote Shutdown		System Message
	CHeKT Portal - Zone 900	E763		Timelapse Video Viewed	Yes	System Message
	CHeKT Portal - Zone 900	E606		Listen in on Audio	Yes	System Message
	CHeKT Portal - Zone 900	E757	E756	Dispatch/Disregard	Yes	Alarm/Cancel
	CHeKT Portal - Zone 900	E755		End User Checked Verification Text	Yes	System Message
	Camera Zone Number	E754		Operator Sent Verification Text	Yes	System Message
	CHeKT Portal - Zone 900	E753		No Response on Verification Text	Yes	System Message

Customer Threat Level Management Sheet

Visual Monitoring

Site Installation Type

□ Interior Visual Alarm Monitoring - Video Verification

□ Exterior Visual Alarm Monitoring - Unsecured Area

□ Exterior Visual Alarm Monitoring - Secured Area

□ Remote Visual Guard Monitoring - Video Guard Services

THREAT LEVEL 0

TL0

Required Response:

□ Traditional Verification

□ View Other Cameras

□ Contact Key-Holder

□ Contact Integrator/Service

□ Email Integrator/Service

□ Notate Account Record

Notes:

THREAT LEVEL 1

TL1

Required Response:

□ Check for Audio

□ Disregard

□ Contact Key-Holder/Call

□ Contact Integrator/Service

□ Email Integrator/Service

□ Notate Account Record

Notes:

THREAT LEVEL 2

TL2

□ Activate Relay

Required Response:

□ Disregard

□ View Additional Cameras

□ Talk-Down Response

□ Verify Alarm/Text

□ Contact Key-Holder/Call

□ Notate Account Record

Notes:

THREAT LEVEL 3

TL3

□ Activate Relay

Required Response:

□ Request Emergency Services

□ Talk-Down Response

□ Verify Alarm/Text

□ Contact Key-Holder/Call

□ Contact Integrator

□ Notate Account Record

Notes: