Monitoring IoT Security Devices: Icinga Case Study

AUTHORED BY

Chris Prance
Product Manager, Icinga

Jeff Williams
Senior Icinga Consultant

Brandon Engelberth
Icinga Consultant

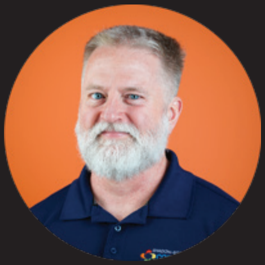
Sharbel Shaaya
Icinga Support Engineer

ABOUT THE AUTHORS

Chris Prance

Product Manager, Icinga

Chris leads the Icinga product team at Shadow-Soft. He works with North American customers to understand their needs and continue to improve the Icinga product offering.



Jeff Williams

Senior Icinga Consultant

Jeff is Icinga's senior consultant in North America. He leads the Icinga support team, helping customers with support tickets, professional services, training, and consulting.

Brandon Engelberth

Icinga Consultant

Brandon provides clients with strategic guidance around Icinga. He's involved in planning, architecting, and implementing Icinga.

Sharbel Shaaya

Icinga Support Engineer

Sharbel assists clients with customizing their Icinga environments and integrating Icinga with 3rd party products and plugins.

ICINGA Premium PARTNER

MONITORING IOT SECURITY DEVICES: ICINGA CASE STUDY

Abstract - In the last decade, the Internet of Things (IoT) has grown from a concept to an entire movement. Many analysts predict that by 2020, IoT will globally consist upwards of 29 billion connected devices. In today's app-centric world, IoT devices provide additional data points and metrics that may not have been easily and immediately accessible previously. However, to ensure system availability and operational functionality, these devices require a specialized and extensible monitoring system. Icinga, an infrastructure monitoring system, is explored as a viable solution to this problem.

Index Terms – Internet of Things (IoT), infrastructure monitoring, Simple Network Management Protocol (SNMP), Icinga

1. INTRODUCTION

In an environment where intellectual property is stored, supporting infrastructure and physical security is crucial to business operations. An IoT monitoring strategy is key to keeping your business secure. Utilizing a monitoring solution like Icinga and IoT strategy that includes physical security sensors and network devices, organizations today can capture data in a secure way. This data can then be presented in a valuable and timely manner when it matters most. IT Administrators and Facilities management can use this valuable data to make their jobs more efficient.

Industry standard states that this data should be collected and stored in real-time, allowing operations to access it on-demand. This allows you to know when physical security issues occur and gives you the ability to solve the problem immediately. That means that you can respond to an incident sooner rather than after the security incident has occurred and passed; this value is immeasurable when every minute matters.

The solution should be able to handle multiple streams of data from disparate sources, as well as have the ability for the data to be structured and displayed in a way that makes quick analyzation possible. The data gathered should also be retained for as long as your operations require it. This will allow historical data to be reviewed after the incidents have occurred.

2. CHALLENGES WITH EXISTING SYSTEMS

The Internet of Things greatly complicates the network and makes it even harder for network engineers and IT administrators to monitor their devices. IoT brings possibilities to the Internet/cloud that before may not have existed on an always-on connection. These can run the gamut from a good thing to a bad thing, especially where security is concerned. In order to proactively understand what is going on, you need a solution that can quickly deliver easy-to-read insights so you can respond and remediate issues as soon as possible.

The lack of integration between physical security and cybersecurity can create several challenges, such as:

A. Lack of Industry Best Practices

Organizations often tend to apply a copy-paste approach in the case of physical security. They choose to do what other organizations are doing to implement security. This approach ends up overlooking their individual and organization needs. This may be effective when companies are of the same size and deal with the same intellectual or physical property, but not when they differ. To overcome this copy-paste tendency, a risk-based monitoring approach of your physical security utilizing a sound IOT strategy is the best way to address this challenge.

B. Lack of Physical Monitoring of Security Devices

Our IT operations team needed the ability to determine if our physical security devices were online and operating as expected, as well as not being tampered with. For example, if a camera was to go offline or be tampered with, how would you discover this unless you were staring at the video feed? If a door sensor or a motion detector were to fail, how would you know?

Seeing as some of these devices don't necessarily have an easy-to-use interface or much less a Web or Smartphone application, how can we gather data from them and make it easy for our small IT operations team to know exactly what is going on in our building and when to actually take action?

3. SOLUTION: IOT STRATEGY

The real value of an IoT strategy is gathering data from devices and leveraging it to increase operational efficiency, reliability, and security. As your company grows, your monitoring solution should be able to grow and scale with you.

We have been able to provide this type of IoT strategy to our IT team, utilizing devices we use to keep our people and office safe and secure. By combining an open source monitoring tool like Icinga and our physical security devices, we can collect this data and be alerted immediately to any anomalies in our system that could affect our physical security.

4. IOT USE CASES

A. Surveillance Camera Feeds

In the event that a camera should go offline or be tampered with, how would you detect this? In the past, you would only know about this if your system was monitored 24 hours a day by a security guard or monitoring agency. Over a period of several months, our IT team noticed that one of our cameras feeds kept cutting out multiple times a day, and the frequency was increasing. However, we were unable to determine the exact cause due to lack of an actual monitoring system that could alert us at the time of the outage.

4. IOT USE CASES

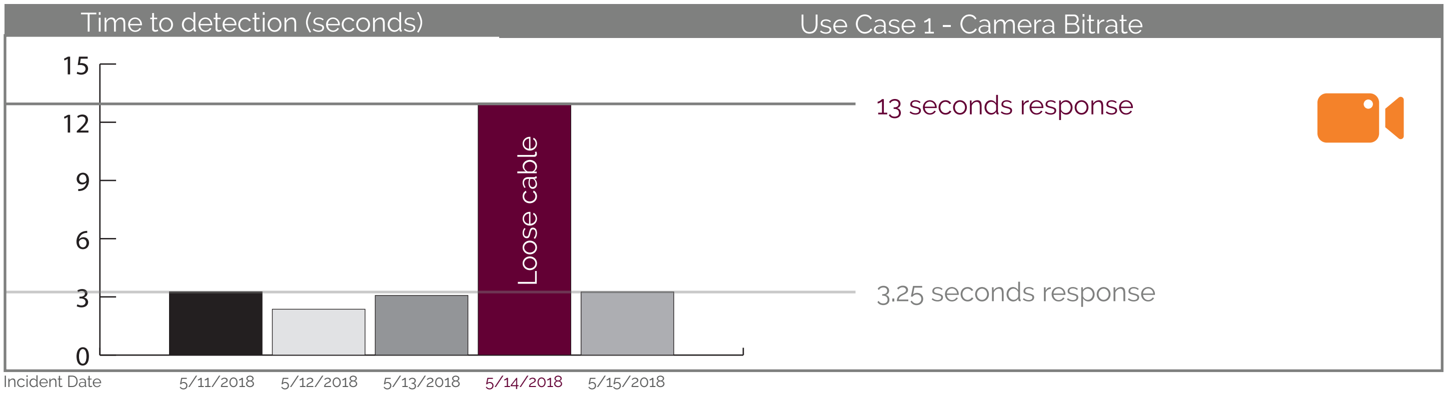


Figure 1: Log data from Surveillance Camera Feed

By using Icinga and monitoring the camera feed, this would show up as a decrease in throughput on the network. Through an SNMP interface check, we can monitor the throughput of the camera's interface and determine if it has gone offline or been tampered with. A notification would be sent to the appropriate IT personnel for immediate remediation. With this ability, we were able to respond to an alert within minutes and determine that there was another patch cable being jostled by another team member and causing the connection on the camera to become loose, resulting in the intermittent feed issues.

In addition to that, we could monitor the HTTP portal to ensure that it is up and functioning properly, thus determining if it has been tampered with or hijacked by an intruder in order to facilitate an easy way to enter our facility unnoticed.

4. IOT USE CASES

B. Badged Entry Reader / Door Controller

Physical security is just as important as the ability to view the area of entry/exit. In the event that an intruder was able to bypass the camera system and gain entry into the facility, we wanted to check the system for any anomalies that could indicate an unauthorized person was able to bypass the badge reader to gain access inside the facility.

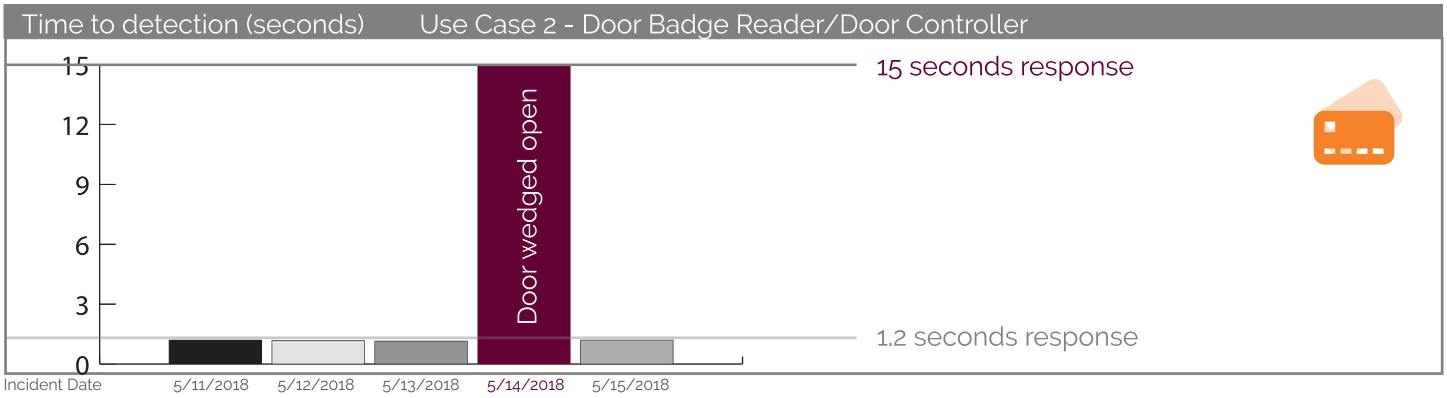


Figure 2: Door Badge Reader

By collecting the data points of entry and exits via an SNMP check, we can store and graph this data and formulate when a person was able to prop a door open to allow unauthorized entry into an office. By utilizing this way of formulating data and displaying it on a dashboard inside our office, we were able to detect someone leaving an office door open over a period of time that was outside of a normal exit/entry.

In addition to that, by utilizing a FTP check, we can ensure that the badge reader/door controller is online and running. An unexpected shutdown or outage would alert us to a user trying to disable the device and create an opportunity to gain unauthorized entry into the facility.

4. IOT USE CASES

C. Motion Detectors / Embedded System

When it comes to security basics, sensors and monitoring are two of the most important components you should know about. In the event that someone manages to bypass your physical security such as badge readers and video cameras, having motion detectors and emergency lighting can help deter would-be intruders from your premises.

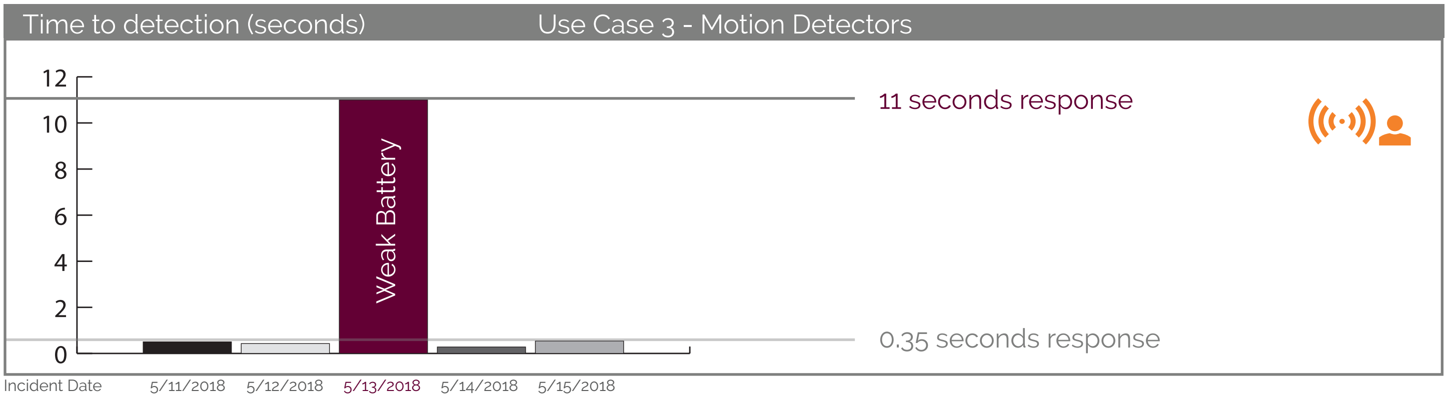


Figure 3: Motion Detector

However, should any of these systems go offline due to an error, you would need to know about it immediately. A standard "hostcheck" will ensure that the device is online, but is that enough? What if the embedded system is online and but not functioning correctly? Using a standard SSH check with Icinga, we have the ability to query the SSH protocol on the device to ensure that the embedded operating system is online and functioning. This allows us to ensure connectivity to the network and the ability to see that our devices are online. We are now able to detect any failures instantly by utilizing our Dashboards in the IT Operations Center.

5. CONCLUSION

Due to the extraordinary growth in IOT devices, increasing security concerns, and the extensibility of Icinga, we saw an excellent opportunity to give more insight. By providing near real-time data to our operations team, they were able to decrease the amount of time it took for them to respond to incidents. This, in turn, increased the value of our security systems in addition to what they were providing already.

Shadow-Soft is an enterprise partner with Icinga and the official provider of support in the North America region. Our partnership status recognizes our experience and past performance in leveraging open source technology like Icinga to provide our customers with the best possible solution to meet their organizational needs

Learn more about how Icinga and Shadow-Soft can help you overcome IoT security challenges.

770-546-0077

shadow-soft.com or **email contact@shadow-soft.com**

Since 2008, Shadow-Soft has been evangelizing and deploying open source software and open standards to help customers “take the power back” from their technology vendors. Shadow-Soft provides consulting and managed services across three specialties: DevOps, Application Infrastructure, and Cloud.