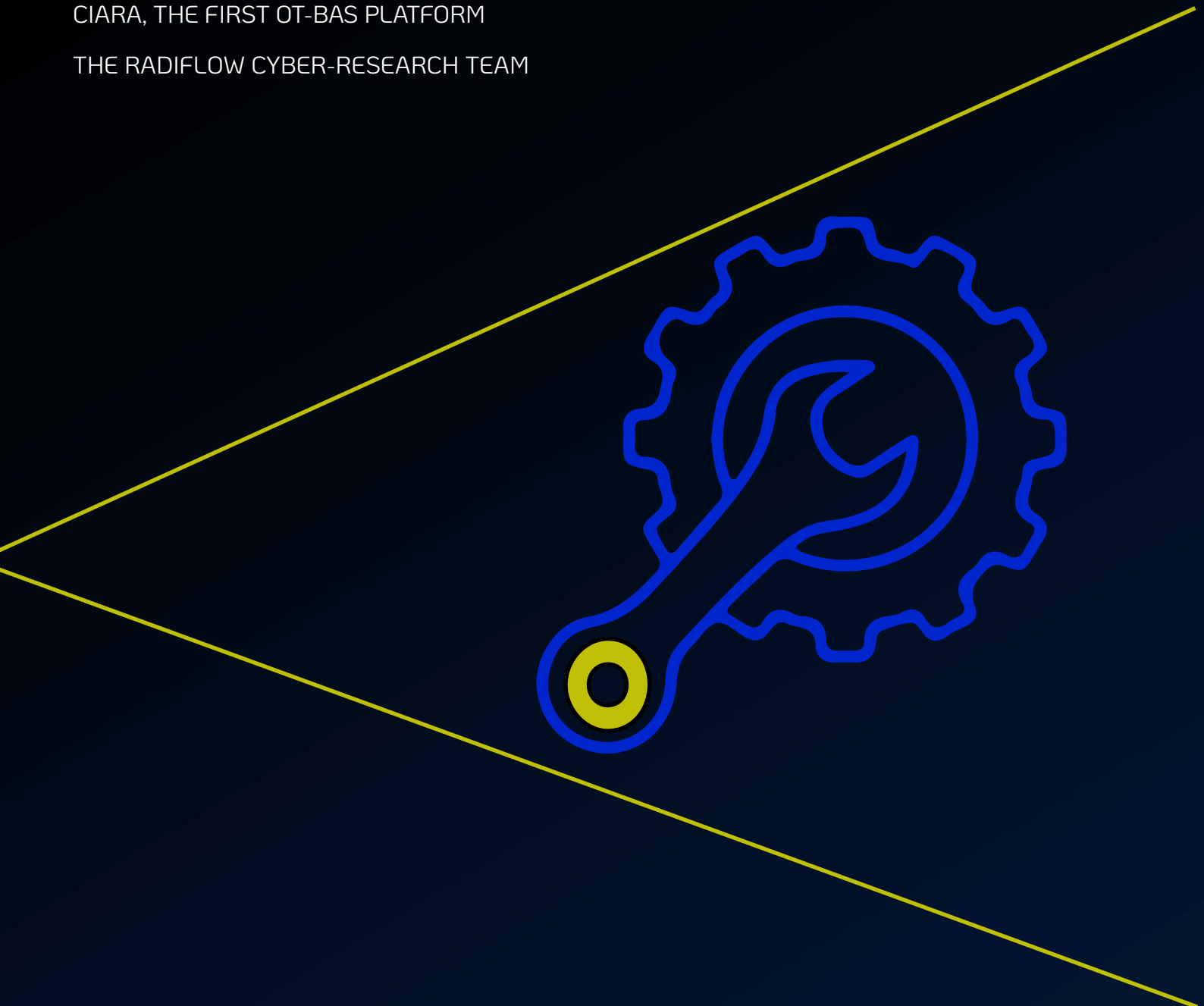
Radiflow

# Fine-Tuning ICS Threat Models to Prioritize Mitigations on the Most Vulnerable Devices

CIARA, THE FIRST OT-BAS PLATFORM

THE RADIFLOW CYBER-RESEARCH TEAM



CISOs responsibe for overseeing cybersecurity for industrial control system (ICS) networks face challenges that are unique to this environment.

For example, server maintenance is typically performed only once or twice a year, so security patches must wait—if they get applied at all.

Given such constraints, the CISO's primary challenge is to determine which devices are most at risk from meaningful threats, and then prioritize the process of applying the appropriate controls and mitigations to reduce or eliminate the threats.

As industrial control systems grow in complexity, the ability to evaluate their vulnerability to attack becomes increasingly important to automate.

Security assessment tools usually begin by determining vulnerabilities of individual hosts. Using this and other information, such as connectivity between hosts, it's possible to show the potential exploits attackers could use and the paths they can take to gain unauthorized access to a device on the ICS network.

Automating this process ensures that every possible attack path is considered, and that the paths contain only those network entities that the intruder is capable of exploiting.

## "CIA" DEFINES THE DEVICE PROPERTIES THAT DEFENDERS WANT TO PROTECT

Devices and zones in the ICS network may have different defense strategies. These strategies are often dependent on the three properties described in the Common Vulnerability Scoring System (CVSS) specification, which is the widely accepted metric for measuring the severity of individual vulnerabilities.

With this metric, it's possible to determine the impact of the vulnerability using ***Confidentiality, Integrity & Availability*** (CIA):

- Confidentiality refers to limiting information access and disclosure to only authorized users.
- Integrity refers to the trustworthiness and veracity of information.
- Availability refers to the state of readiness for use of a specific component.

For example, the availability of a safety PLC is much more critical than the availability of a monitoring HMI.

## ATTACKERS HAVE DIFFERENT LEVELS OF CAPABILITIES

Modeling attacker capabilities is an essential, though often overlooked, step in estimating the person's route through an ICS network.

For instance, a highly skilled or knowledgeable person is likely to be more capable of exploiting industrial protocols to compromise network devices and pivot throughout the network.

There are three levels of attacker capabilities for exploiting various protocols:

- Low – attackers who are capable of only exploiting common IT protocols.
- Medium – attackers who are capable of exploiting IT and OT protocols. However, they are capable of exploiting only OT protocols that have open specifications.
- High – attackers who are capable of exploiting IT and OT protocols, including reverse-engineering of proprietary OT protocols.

Likewise, an attacker's capabilities can be modeled on his ability to exploit device vulnerabilities to affect a device's functionality.

The three levels of attacker capabilities for exploiting device vulnerabilities are:

- Low – attacker is capable of exploiting only publicly known vulnerabilities with publicly available exploits.
- Medium – attacker is capable of developing his own exploits for known vulnerabilities.
- High – attacker is capable of performing extensive research to find zero-day vulnerabilities and is capable of exploiting them.

Therefore, the attacker model accounts for the attacker's level of expertise in both exploiting legitimate network protocols and in exploiting device vulnerabilities.

## THE IMPORTANCE OF CONSIDERING BOTH CIA AND ATTACKER CAPABILITIES IN THE THREAT MODEL

Radiflow is the only threat assessment provider that utilizes a threat model that considers both the CIA defense strategy and the levels of attacker capabilities.

These elements are essential for truly evaluating the threats

against specific devices inside an industrial network, which in turn helps a CISO select and prioritize the actions needed to protect the network.

For example, say there are two servers inside an industrial network. One server is an HMI, which uses an open OT protocol that anyone can learn. An attacker really doesn't need high level skills for that.

The second server is an engineering station that also communicates with the controller, but it uses a proprietary protocol to change the PLC configuration. For an attacker to use those protocols, he needs some expertise dedicated to OT systems.

The CISO needs to decide how to prioritize which server to patch first—the HMI or the engineering station. While the engineering station might be a standard Windows PC that is easier to patch, if the threat model points toward someone who is an IT hacker who has no specific industrial knowledge, the engineering station is probably out of his league.

It would be better to prioritize patching the HMI server because the low-skilled attacker is more likely to go after the HMI server than the engineering station. What's more, availability of the HMI server is more important than its confidentiality or integrity, so it's crucial that the server not be knocked offline by an attacker.

However, if the threat model indicates an attacker that has an expertise in a proprietary protocol, which makes him a more expert attacker, then the CISO's effort should be focused on patching the engineering station and protecting it over the HMI. This is because the attacker can cause much more damage to the engineering station since he has knowledge of the proprietary protocol.

## CONCLUSION

Many companies have very limited time and resources for deploying and maintaining security measures on their industrial networks.

Thus, anticipating and accurately estimating potential cyber intruder activities and what attack path they may take to access critical assets is important in understanding how to prioritize security measures.

Radiflow's sophisticated threat models encompass the pertinent situational data that allows a CISO to prioritize resources to the right mitigations on the most vulnerable devices.

For more in-depth information on Radiflow's threat modeling, read our white paper, "What's Your Next Move? Optimizing OT Security through Automatic Attacker Evaluation".

### ABOUT RADIFLOW

Radiflow develops trusted Industrial Cyber-Security Solutions for Critical Business Operations. Our portfolio of game-changing solutions for ISC/SCADA networks empowers users to maintain visibility and control of their OT networks. Our intelligent Threat Detection and Analysis Platform for industrial cyber-security minimizes potential business interruption and loss within your OT environment.

Radiflow's team consists of professionals from diverse backgrounds, from cyber-experts from elite military units and automation experts from global cyber-security vendors. Founded in 2009, Radiflow' solutions, are successfully deployed by major industrial enterprises and utilities protecting more than 5,400 critical facilities worldwide. More at www.radiflow.com.

**US and Canada:**
Tel: +1 (302) 547-6839
sales_NA@radiflow.com

**EMEA:**
Tel: +972 (77) 501-2702
sales@radiflow.com

**UK:**
Tel: +44 (0) 800 246-1963
sales_UK@radiflow.com

**France:**
Tel : +33 1 77 47 87 25
sales_FR@radiflow.com

**DACH:**
Tel: +49 (160) 109 75 65
sales_DACH@radiflow.com

(C) 2021 Radiflow Ltd. All rights reserved. Radiflow reserves the rights to change product specifications without prior notification.