Case Study

Detecting Cyber-Threats in a Simulated Water Treatment Facility at Critical Infrastructure Security Showdown (CISS) 2019

Liron Benbenishti
Cyber Researcher, CTO Team, Radiflow

radiflow

DETECTING CYBER-THREATS IN A SIMULATED INDUSTRIAL WATER TREATMENT FACILITY AT THE CRITICAL INFRASTRUCTURE SECURITY SHOWDOWN (CISS) 2019

INTRODUCTION

The Critical Infrastructure Security Showdown (CISS) 2019 is the third run of iTrust's technology assessment exercise, dubbed the SWaT (Secure Water Treatment) Security Showdown (S3) in 2016 and S317 and 2017.

Organized by iTrust, the CISS 2019 exercise took place at SUTD (The Singapore University of Technology and Design) from the 26th to the 30th of August, 2019, and involved seven Red Teams and five Blue Teams from both academia and industry.

Radiflow's Blue Team was able to showcase the company's detection capabilities facing different types of cyber-attacks in different network layers. By creating an accurate traffic baseline during the learning phase, and by applying iSID advanced engines, Radiflow's Blue Team was able to detect the attacks performed in the challenge.

The Radiflow Team at CISS 2019

THE SWAT CHALLENGE DESIGN

The SWaT testbed consisted of a modern six-stage water treatment physical process that closely mimics a real-world water treatment plant, as follows:

- Stage 1: taking in raw water
- Stage 2: chemical dosing
- Stage 3: water filtering through an Ultrafiltration (UF) system
- Stage 4: dichlorination using UV lamps
- Stage 5: feeding the water into a Reverse Osmosis (RO) system
- Stage 6: applying a backwash process to clean the membranes in the Ultrafiltration (UF) system using the RO permeate

The cyber portion of the SWaT challenge consisted of a layered communications network, Rockwell PLCs, HMIs, a SCADA workstation, and a Historian. Data from sensors was made available to the SCADA system and was recorded by the Historian for subsequent analysis. The SWaT also included an array of monitoring sensors to ensure its safe operation.

The attackers' goals were:

1. To take control over a physical actuator or the process
2. Demonstrate control over sensor readings at different components: historian values, HMI/SCADA values, PLC values, remote I/O values.

The SWaT Lab, simulating a real-life water treatment plant

ISID'S LEARNING PHASE

iSID's process of detecting threats on industrial networks starts with a Learning Phase, during which iSID self-learns the network, including topology, ports and connections, protocols and networked devices, and analyzes each and every component to detect suspect activity. This is done toward constructing a "clean" baseline network model, complete with tagging of critical assets in the network (Historian, HMI, PLCs, etc.) with their names for easy navigation and drill-down.

The Learning Phase at the SWaT exercise found no malicious activity; however, in production networks iSID typically will identify suspect activity or components, which require manual approval or remediation prior to their inclusion in the baseline model.

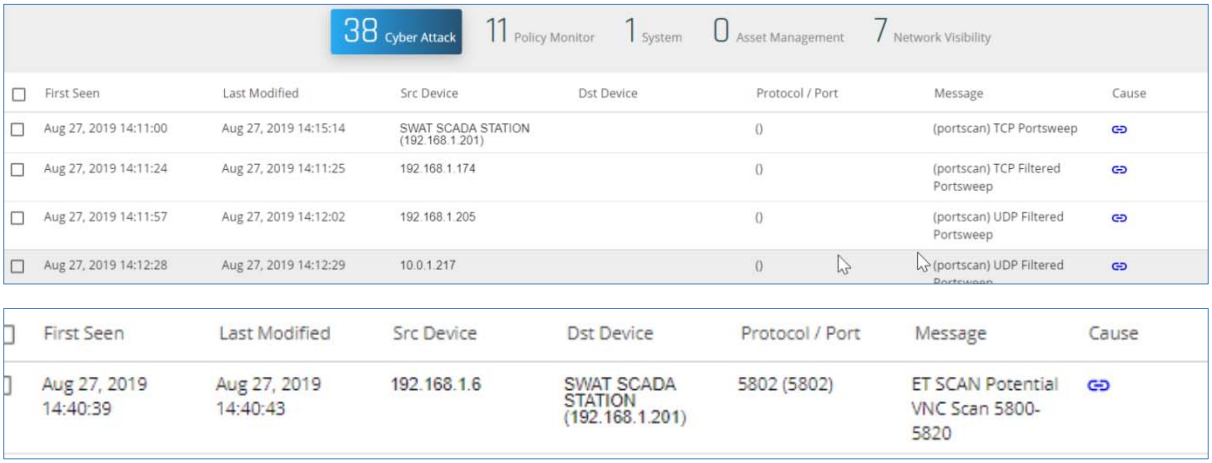
Following the Learning Stage iSID was switched to "Detection Mode". In this mode we were able to detect all "suspicious" traffic addresses, links and assets that were not part of the baseline, but might have been part of the attacker's lateral movement in the network. Unauthorized assets that were not part of the baseline were immediately flagged as potential attackers' machines/ scanners, which caused the iSID Network Visibility Engine to generate alerts.

ATTACK PHASE

SCANNING THE NETWORK

Throughout the SWaT sessions, the first step the attackers took was scanning the network in an attempt to find attack vectors into the OT network. Network scanning involves detecting all active hosts on a network and mapping them to their IP addresses. This is followed by performing port scanning on specific ports on a host and analyzing the responses received, to learn about its running services and/or locate potential vulnerabilities.

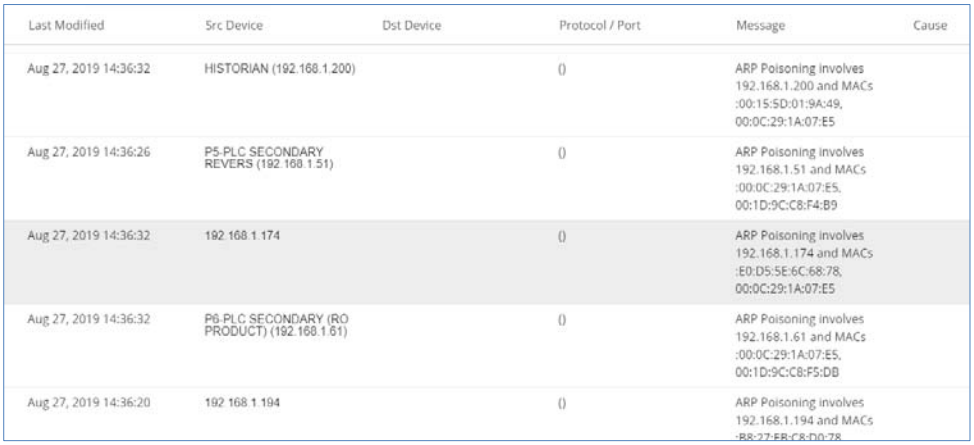
iSID was able to detect all of these scans by scanning engine and signature-based rules, and successfully detected ARP scans, UDP scans, TCP scans and ICMP.



MITM ATTACKS

ARP (Address Resolution Protocol) poisoning is a type of attack where a malicious actor sends falsified ARP messages over a LAN. This type of attack results in the linking of an attacker's MAC address with the IP address of a legitimate computer/server on the network. Once the attacker's MAC address is connected to an authentic IP address, the attacker can begin receiving any type of data that is intended for that IP address.

Most of the red teams performed MiTM and ARP Poisoning attacks in an attempt to take over their target in the OT network. In this example, as shown below, the attack triggered an ARP poisoning alert on the historian and PLCs.



Last Modified	Src Device	Dst Device	Protocol / Port	Message	Cause
Aug 27, 2019 14:36:32	HISTORIAN (192.168.1.200)		()	ARP Poisoning involves 192.168.1.200 and MACs :00:15:5D:01:9A:49, 00:0C:29:1A:07:E5	
Aug 27, 2019 14:36:26	P5-PLC SECONDARY REVERS (192.168.1.51)		()	ARP Poisoning involves 192.168.1.51 and MACs :00:0C:29:1A:07:E5, 00:1D:9C:C8:F4:B9	
Aug 27, 2019 14:36:32	192.168.1.174		()	ARP Poisoning involves 192.168.1.174 and MACs :E0:D5:5E:6C:68:78, 00:0C:29:1A:07:E5	
Aug 27, 2019 14:36:32	P6-PLC SECONDARY (RO PRODUCT) (192.168.1.61)		()	ARP Poisoning involves 192.168.1.61 and MACs :00:0C:29:1A:07:E5, 00:1D:9C:C8:F5:DB	
Aug 27, 2019 14:36:20	192.168.1.194		()	ARP Poisoning involves 192.168.1.194 and MACs :B8:27:EB:C8:D0:78	

EXPLOITING KNOWN IT VULNERABILITIES

Several red teams exploited known vulnerabilities in order to take over critical assets such as the SCADA station. After taking over the station, the attackers were able to send operational commands to the controllers, control the business process and change physical values.

In the following screenshot, SMBv1 eternalblue vulnerability was being exploited in order to gain control over the SCADA station and the HMI. iSID detected this attack by its cyber -attack signature based engine. iSID also alerted on attempt to execute code on the target using Metasploit.

]	Aug 27, 2019 14:44:54	Aug 27, 2019 14:45:04	192.168.1.6	HMI TOUCH PANEL (192.168.1.100)	SMB (445)	POLICY-OTHER SMBv1 protocol detection attempt	3
]	Aug 27, 2019 14:56:36	Aug 27, 2019 14:56:41	192.168.1.6	SWAT SCADA STATION (192.168.1.201)	SMB (445)	NETBIOS SMB srvsvc named pipe creation attempt	1

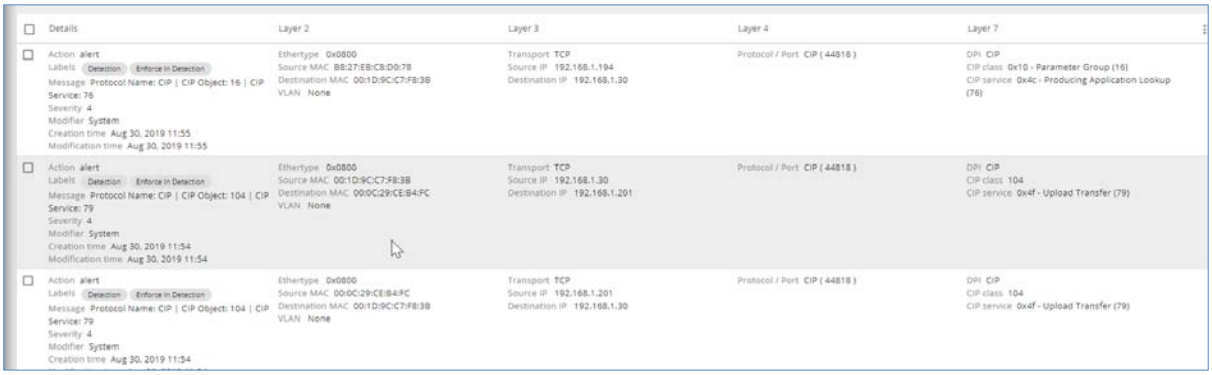
ATTACKS USING SCADA COMMANDS

This type of attack targets controllers using SCADA commands.

The main OT network protocol used at the SWaT was CIP. CIP, like all other OT protocols, introduces a host of vulnerabilities. It is an open-specification object-oriented protocol that can be easily exploited by a high-skills attacker. At the SWaT, highly skilled attackers adept with the CIP protocol sent CIP commands to the Rockwell ControlLogix controllers in an attempt to disrupt the physical process.

iSID's DPI capabilities allowed us, the analysts in of Radiflow blue team to Investigate each packet message and monitor SCADA operational commands performed on the controllers. iSID's DPI engine detected these messages and displayed the CIP service code and the CIP object.

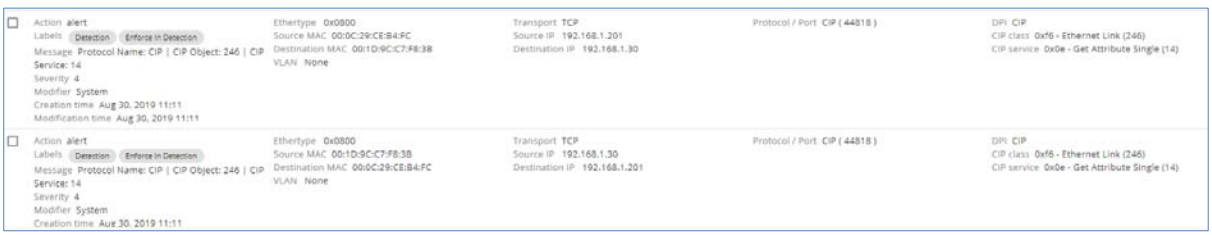
This capability allowed the analyst understand the operations taking place on the network and detect possible attacks.



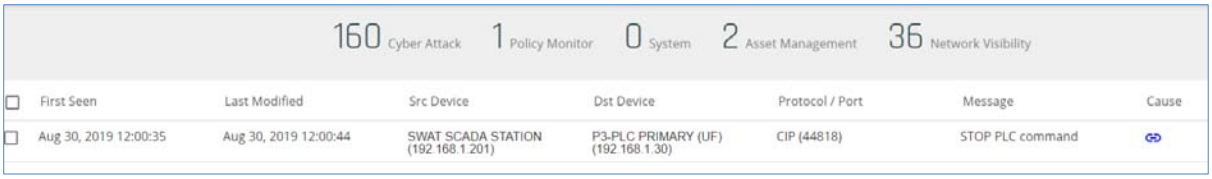
Other common CIP messages we observed at the attack sessions were "Get Attributes" and "Set Attributes".

The "Get Attributes" CIP message allows the attacker to expose data on the controller. This message for the Identity Object returns the Vendor ID, Device Type, device serial number and other identity data.

The "Set attributes" CIP message allows the attacker to conduct configuration changes in the controllers: time, Ethernet link and port.



In the following example, the iSID Policy Monitor DPI engine raised an alert for a “Stop PLC” CIP command (CIP Service= 0x07) sent from the SWaT SCADA station to PLC P3 (which controls UF stage).



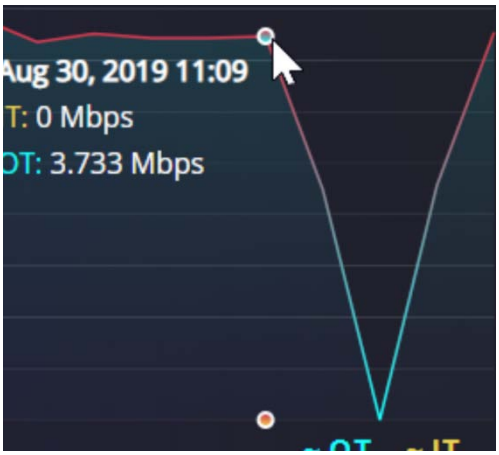
In other attacks, iSID detected “Create Object”, ”Reset”, “Start” and “Upload” CIP commands sent to the controllers in order to disrupt its operation or change its logic. These commands could be easily track by defining rules in Policy Monitor.

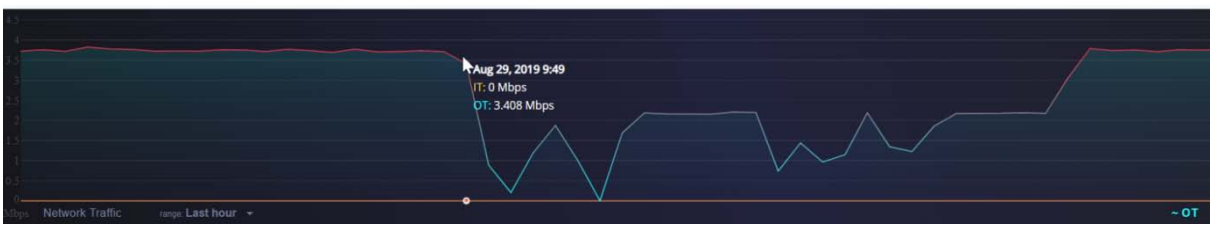
INSIDER ATTACKER

During the attack sessions, in addition to remote access, the Red Teams were also granted physical access to the SWaT, and challenged us to discover attacks performed by an insider attacker. The Insider attacker had good knowledge of the system, including administrator passwords and the ability to operate the HMI.

The insider also had physical access to the system where control valves and network topology could be manipulated. In addition, the insider attacker had access to ICS-specific tools such as Studio 5000 (Engineering station).

In this case, iSID’s Online Traffic Graph, which monitors IT and OT traffic, showed significant changes in the graph trend which could indicate disruption in traffic, for example, the shutdown of a controller.





EXPLOITING KNOWN SCADA VULNERABILITIES

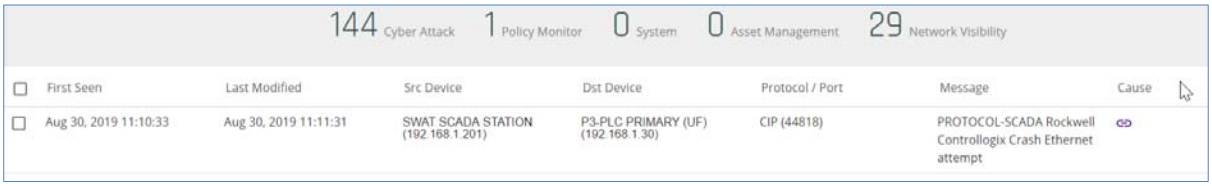
Rockwell ControlLogix controllers have several known exploitable vulnerabilities. They can be exploited remotely to enable MiTM attacks, DDoS attacks, Improper Input Validation, and information disclosure attacks, which could cause loss of availability as well as disruption of communications with other connected devices.

At the SWaT, this type of exploit took the form of a ControlLogix crash ethernet module attack, which iSID cyber-attack engine alerted on. The attack exploited a known vulnerability (CVE-2012-64own 38) in the ControlLogix ethernet module:

Improper Input Validation—NIC

The device does not properly validate the data being sent to the buffer. An attacker can send a malformed CIP packet to Port 2222/TCP, Port 2222/UDP, Port 44818/TCP, or Port 44818/UDP, which creates a buffer overflow and causes the NIC to crash. Successful exploitation of this vulnerability could cause loss of availability and a disruption in communications with other connected devices.

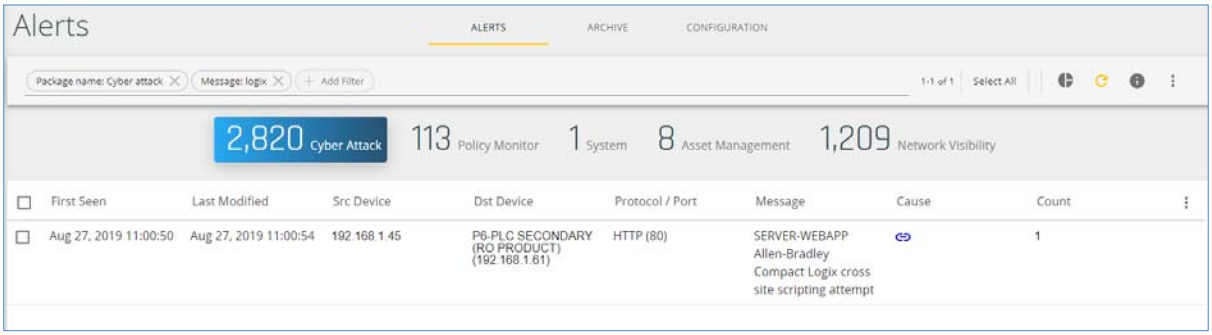
This attack was performed from the SWaT SCADA station to the PLC P3 (UF stage).



Another example of Red team exploiting a known ControlLogix vulnerability is exploiting the cross-site scripting XSS (CVE-2009-0473) via its web interface. The Rockwell ControlLogix uses a web interface to display log files and status information. The web interface contains a cross-site scripting vulnerability that may allow an attacker to spoof data or redirect end users to other sites or executing arbitrary HTML or script code in the user's browser session.

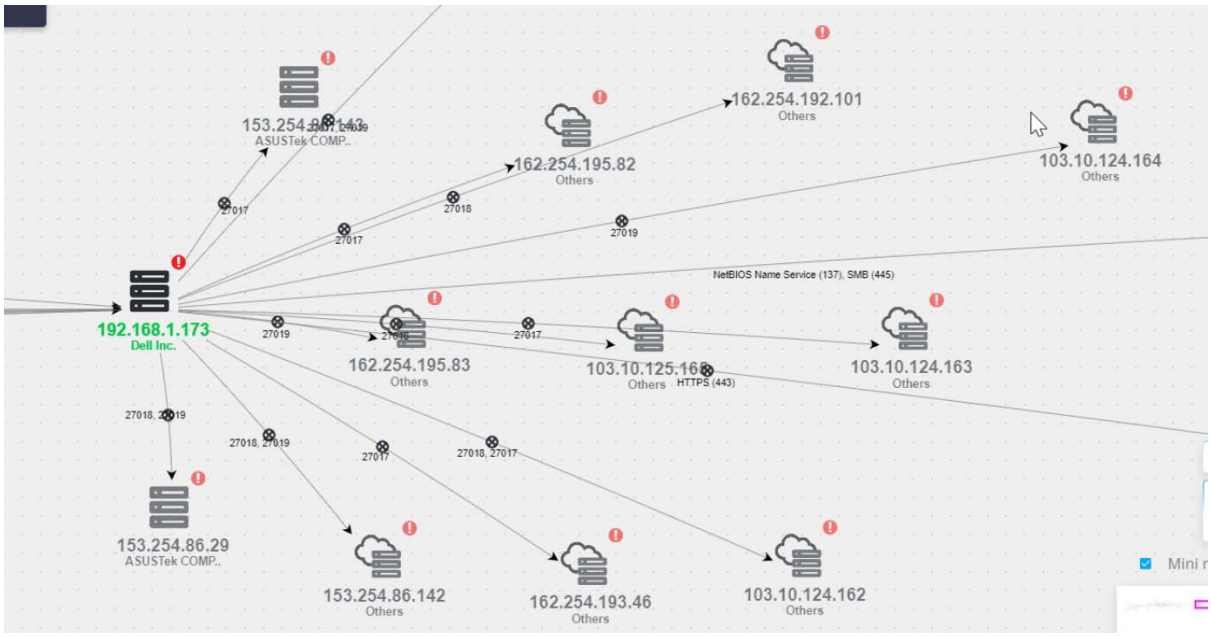
iSID alerted on this attack attempt successfully with its cyber-attack engine.

iSID also has the capability to discover PLCs type, model and firmware version and match the relevant CVEs for these types.



UNAUTHORIZED LINKS TO INTERNET IP ADDRESSES

During one of the attack sessions, iSID detected assets that opened unauthorized connections to internet IPs that might provide access to C2 servers or malicious IPs. Using iSID baseline and external IPs engine we got alerts on these links and internet IPs. iSID also displays these IPs with “cloud” image because they outside the secured monitored network. (”behind a router”)



CONCLUSIONS

At CISS 2019 Radiflow’s Blue Team was able to showcase the company’s detection capabilities facing different types of cyber-attacks in different network layers. By creating an accurate traffic baseline during the learning phase, and by applying iSID advanced engines, Radiflow’s Blue Team was able to detect the attacks performed in the challenge.