SIGAGUARD

CISS
Critical Infrastructure Security Showdown
2019

CASE STUDY

SigaGuard's Success at CISS 2019's Water Infrastructure Cybersecurity Showdown

BACKGROUND

The Critical Infrastructure Security Showdown (CISS) 2019 is the third annual technology assessment exercise established by iTrust (The Centre for Research in Cyber Security) and Singapore University of Technology and Design (SUTD). The August 2019 simulation had seven red Teams and ten blue Teams from both academia and leading industry Cyber OT players competing. SIGA partnered with ST Engineering alongside leading global Cyber OT solution providers.

CHALLENGE

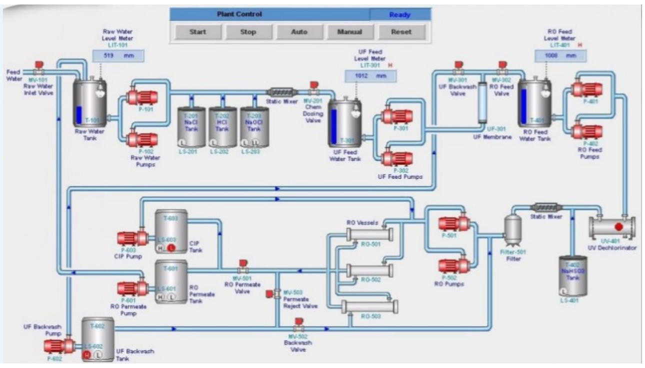
The testbed consisted of a modern water treatment process that closely mimics an existing one. Among the objectives of the exercise was to enable blue teams to showcase their detection capabilities against cyber-attacks performed by the red teams. There were 9 different attacks on the OT and SCADA systems of the water treatment process and the blue teams, (with SIGA amongst them), were required to detect the attacks in real time.

THE PROCESS

The physical process begins by taking in raw water (Stage 1), followed by chemical dosing (Stage 2), filtering it through an Ultrafiltration (UF) system (Stage 3), dechlorination using UV lamps (Stage 4), and then feeding it to a reverse osmosis (RO) system (Stage 5). A backwash process (Stage 6) then cleans the membranes in UF. The network and cyber portion of SWaT consist of a layered communications network, PLCs, HMI workstation and a data historian.

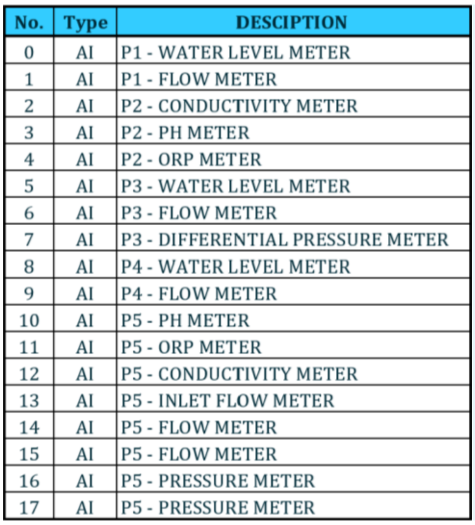
AUTONOMOUS · RELIABLE · SMART

The SCADA's HMI of the water treatment plant testbeds. (SIGA dashboard)



SIGA'S SOLUTION - LEVEL 0 MONITORING AND ANOMALY DETECTION

SIGA activated the SigaGuard solution for Level 0 monitoring by listening to the electrical signals of the water treatment process, detecting anomalies in the process behavior, and gaining direct visibility into the OT process. The integration was made into 18 critical analog I/O's (as depicted below) and provided an isolated, out-of-band monitoring environment which cannot be manipulated or circumvented at the network level, therefore, reflecting the exact behavior of the critical asset being protected from a cyber-attack.



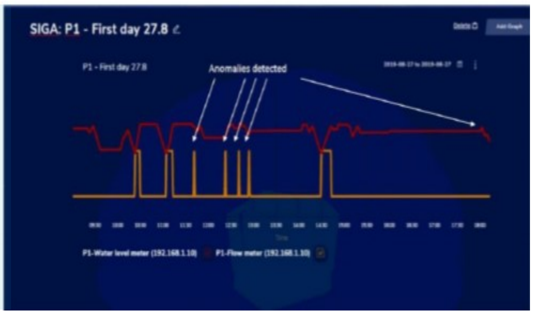
No.	Type	DESCIPTION
0	AI	P1 - WATER LEVEL METER
1	AI	P1 - FLOW METER
2	AI	P2 - CONDUCTIVITY METER
3	AI	P2 - PH METER
4	AI	P2 - ORP METER
5	AI	P3 - WATER LEVEL METER
6	AI	P3 - FLOW METER
7	AI	P3 - DIFFERENTIAL PRESSURE METER
8	AI	P4 - WATER LEVEL METER
9	AI	P4 - FLOW METER
10	AI	P5 - PH METER
11	AI	P5 - ORP METER
12	AI	P5 - CONDUCTIVITY METER
13	AI	P5 - INLET FLOW METER
14	AI	P5 - FLOW METER
15	AI	P5 - FLOW METER
16	AI	P5 - PRESSURE METER
17	AI	P5 - PRESSURE METER

SigaGuard's I/O Table

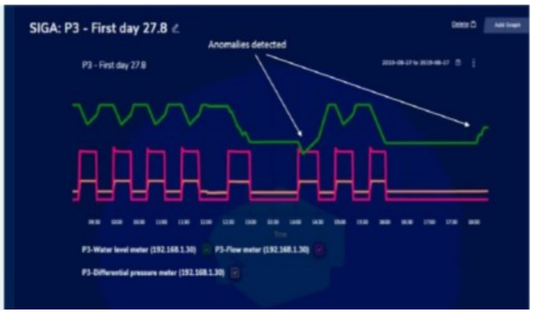
RESULTS

More than 90% of documented successful attacks were Level 0 attacks (i.e., the attacker's objective was the manipulation of the actual OT Level 0 process). This reiterates that in OT environments, the attacker's ultimate objective will always be to reach down to the physical process (Level 0) and impact it.

SIGA's dashboard screenshot of anomaly detection at the water treatment Phase 1 during the CISS Showdown

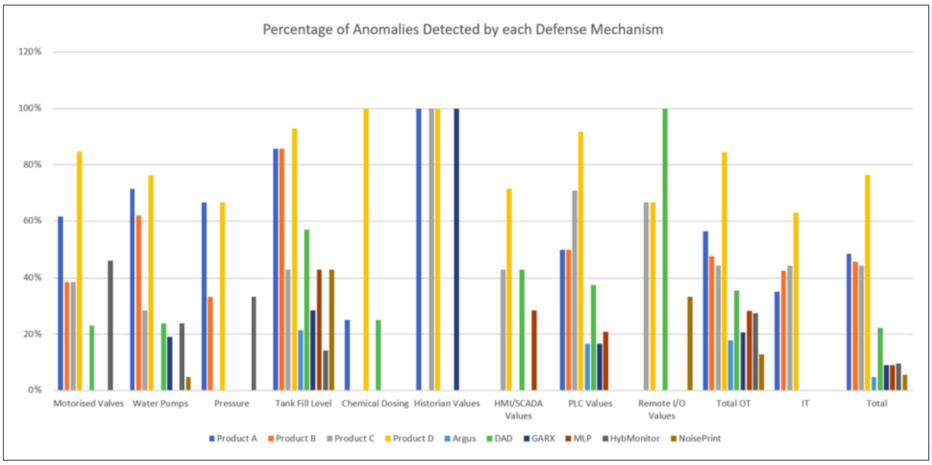

SIGA: P1 - First day 27.8
P1 - First day 27.8
Anomalies detected
P1-Water level meter (192.168.1.10)
P1-Flow meter (192.168.1.10)

SIGA's dashboard screenshot of anomaly detection at the water treatment Phase 3 during the CISS Showdown


SIGA: P3 - First day 27.8
Anomalies detected
P3 - First day 27.8
P3-Water level meter (192.168.1.30)
P3-Flow meter (192.168.1.30)
P3-Differential pressure meter (192.168.1.30)

The results show that 85% of total OT anomalies were detected by Product D (including SigaGuard)—with the next runner-up detecting only 57%. In total, 54 physical process anomalies were recorded. With respect to sensor data anomalies, the technical report stated: "Product D performed significantly better than all other technologies… Product D detected 30 out of 35 attacks i.e., about 85% of the attacks." As depicted in the graph below: "Across the commercial products, Product D outperformed the other products. It had a 100% detection rate for (e) and superior detection rates for attacks (a) to (d)."

SigaGuard's Level 0 monitoring outperforms every other tool detecting real-time cyber-attacks on critical OT processes.



Percentage of anomalies detected by each defense mechanism by attack type (yellow= Product D)