



# Better Outcomes through Iteration

A CASE STUDY ON THREATGEN'S AUTOTABLETOP™ USAGE

ROBERT C. RHODES



## Contents

Preface .....	1
Project Definition .....	2
Thesis .....	2
Description .....	2
Conclusion .....	3
More Research Required .....	3
Attachments.....	4
A – Perplexity Analysis.....	4
B – Transcript #1 .....	9
C – Transcript #2.....	14
D – Transcript #3.....	20
E – Transcript #4 .....	24

## Preface

I wanted to acknowledge the head of our support group here at ThreatGEN, Grzegorz “Greg” Piekarski as co-author of this article. Without Greg, this article and our product wouldn’t be the same.



## Project Definition

As with any simulation like AutoTableTop™, it is important for the users to experience **value** in its usage and **better outcomes**. We at ThreatGEN intuitively know that our AutoTableTop™ incident response simulator provides more user engagement than classically delivered cybersecurity tabletop exercises, all you have to do is ask the participants who provide glowing survey responses; but we needed to provide more objective, data-based proof of better outcomes. We therefore conducted our own scientific project to provide documented proof of better outcomes.

## Thesis

---

*Using AutoTableTop™ with a sufficiently detailed scenario (AutoTableTop™ general settings) provides organizations an efficient way to improve their incident response through **better outcomes**.*

---

## Description

Our project started with the head of our support team, Grzegorz “Greg” Piekarski, participating in 4 exercises using our Municipal Water Authority of Aliquippa (MWAA) AutoTableTop™ scenario. We then analyzed the 4 exercise transcripts using Perplexity’s Deep Research function attaching:

- 4 exercise transcripts
- ThreatGEN MWAA scenario settings (JSON) file
- ThreatGEN MWAA scenario document

**NOTE: Notice that we did not upload the scenario’s sample incident response document as we wanted to test the efficacy of the team’s activity during the exercise and not necessarily the efficacy of the sample incident response provided in the scenario.**

This provided the following analysis:

- [ThreatGEN Scenario Better Outcomes through Iterative Usage](#)

We have attached all these items within this document as attachments for ease of use, except the ThreatGEN Municipal Water Authority of Aliquippa (MWAA) scenario files as they are available elsewhere on the ThreatGEN website:

- [Municipal Water Authority of Aliquippa \(MWAA\) 2023 Scenario](#)



## Conclusion

Our analysis provides strong evidence that the iterative usage of AutoTableTop™ improved incident response outcomes across these exercises. The highest score (95/100) was achieved in Exercise 3, representing a 5-point improvement over the initial exercises. While Exercise 4 saw a slight decline to 92/100, it still outperformed the first two iterations and demonstrated more comprehensive approaches to communication and monitoring.

Key improvements observed across iterations included:

- Greater comprehensiveness in response strategies
- More sophisticated technical approaches to remediation
- Enhanced communication planning with stakeholders
- Better integration of both technical and non-technical aspects of incident response

This analysis confirms that repeated practice through tabletop exercises led to measurable improvement in incident response capabilities, with participants demonstrating increasingly effective strategies for responding to the simulated cybersecurity incident involving the Municipal Water Authority's critical infrastructure.

## More Research Required

The results of this case study brought up interesting questions for us at ThreatGEN. Namely:

- 1) **Does our other simulation TheatGEN® Red vs. Blue offer similar benefits**, namely better outcomes, using the same MWAA scenario?
- 2) Using the end game analysis of TheatGEN® Red vs. Blue and the end simulation analysis of AutoTableTop on basically the same scenario (in this case MWAA), what conclusions can we draw on the **best usage of these platforms**?
- 3) Does using our upcoming incident response (IR) plan generator's output IR plan as the basis for our responses within an exercise within the AutoTableTop™ improve our outcomes?
- 4) Does using a **robust and detailed** real life IR plan increase the efficacy of the exercises?

Stay tuned for more case studies that showcase our simulation platforms and the benefits that they provide for cybersecurity teams.



## Attachments

### A – Perplexity Analysis



## Analysis of Iterative AutoTableTop Exercises for Municipal Water Authority of Aliquippa

This report analyzes four cybersecurity tabletop exercise iterations conducted with the same scenario, settings, and IR Plan for the Municipal Water Authority of Aliquippa (MWAA). The exercises simulated a response to a cybersecurity incident involving the compromise of a PLC controlling water pressure by the Cyber Av3ngers threat group.

### Performance Metrics and Score Progression

The scoring progression across the four exercises reveals an overall improvement trend:

- Exercise 1: 90/100
- Exercise 2: 90/100
- Exercise 3: 95/100
- Exercise 4: 92/100

This pattern demonstrates a general improvement from the first iterations to the later ones, with Exercise 3 achieving the highest score. The progression suggests that iterative practice led to better outcomes, even though the improvement wasn't perfectly linear.

### Evaluation Criteria Analysis

All exercises were evaluated on similar criteria, with point deductions consistently related to:

- Firewall configuration gaps (-5 points across all exercises)
- Insufficient security measures such as MFA implementation (-5 points in Exercise 1)
- Logging configuration issues (-3 points in Exercise 4)

### Response Strategy Evolution



## Initial Approach Consistency

A notable consistency appeared across all four exercises in the initial response approach:

1. All exercises began with checking EDR (Endpoint Detection and Response) logs
2. The teams consistently followed up by examining firewall configurations
3. All four iterations recognized the importance of addressing unauthorized access to the PLC

## Progressive Improvement in Response Depth

The depth and comprehensiveness of the response strategy showed clear improvement across iterations:

- **Exercise 1:** Focused primarily on removing the problematic firewall rule and restoring PLC control parameters - a direct but somewhat limited approach
- **Exercise 2:** Expanded to include more comprehensive threat hunting, malware removal, and investigating the initial attack vector (phishing email)
- **Exercise 3:** Demonstrated more sophisticated implementation of secure remote access solutions alongside the basic remediation steps
- **Exercise 4:** Added robust public communications strategy and system monitoring to the technical remediation

## Tactical Improvements

### Detection and Analysis

The participants showed progressively better understanding of detection and analysis procedures:

- In Exercise 1, the focus was primarily on identifying unauthorized access
- By Exercise 2, analysis expanded to include malware identification and phishing investigation
- Exercises 3 and 4 demonstrated more thorough analysis of the attack methodology

### Containment and Eradication

Containment strategies evolved across iterations:

- Exercise 1: Simple rule removal and credential update



- Exercise 2: Added malware removal and threat hunting
- Exercise 3: Implemented comprehensive secure remote access solutions
- Exercise 4: Incorporated more thorough system restoration and monitoring

## Recovery and Resilience

Recovery approaches became more sophisticated in later exercises:

- Exercise 1: Basic PLC parameter restoration
- Exercise 2: Added comprehensive threat hunting to ensure removal of threats
- Exercise 3: Included proper firmware updates and system validation
- Exercise 4: Featured extensive monitoring and additional press release preparation

## Communication Enhancements

A notable improvement was observed in communication strategies:

- Earlier exercises (1 and 2) focused primarily on technical remediation with minimal discussion of stakeholder communication
- Exercise 3 introduced notification to OT employees about changes
- Exercise 4 demonstrated the most mature approach with a formal press release and public communication strategy

## Common Elements and Learning Transfer

Throughout all four exercises, certain elements remained consistent, suggesting effective learning transfer:

1. Recognition of the firewall as the primary security control needing remediation
2. Understanding the importance of checking EDR logs as a first response step
3. Acknowledgment of the need to restore PLC programming from trusted sources

## Conclusion

The analysis provides strong evidence that the iterative usage of AutoTableTop improved incident response outcomes across these exercises. The highest score (95/100) was achieved in Exercise 3,



representing a 5-point improvement over the initial exercises. While Exercise 4 saw a slight decline to 92/100, it still outperformed the first two iterations and demonstrated more comprehensive approaches to communication and monitoring.

Key improvements observed across iterations included:

- Greater comprehensiveness in response strategies
- More sophisticated technical approaches to remediation
- Enhanced communication planning with stakeholders
- Better integration of both technical and non-technical aspects of incident response

This analysis confirms that repeated practice through tabletop exercises led to measurable improvement in incident response capabilities, with participants demonstrating increasingly effective strategies for responding to the simulated cybersecurity incident involving the Municipal Water Authority's critical infrastructure.

## What role did the scenario play in the improvements seen in the outcomes

The scenario played three key roles in driving measurable improvements across the four AutoTableTop exercises, as evidenced by the progression of outcomes:

### 1. Consistent Foundation for Iterative Learning

The fixed scenario parameters (water utility cyberattack targeting PLCs) enabled participants to:

- Build muscle memory for ICS/OT incident response protocols<sup>[1][2]</sup>
- Repeatedly test the same IR plan elements under varying conditions
- Compare performance metrics across identical success criteria

This consistency allowed teams to focus on refining their *response quality* rather than adapting to new scenarios, directly enabling the observed 5-point score improvement from Exercise 1 to Exercise 3.

### 2. AI-Driven Dynamic Complexity

While maintaining core scenario parameters, AutoTableTop's AI introduced variations through:





- Context-aware injects (phishing origins in Exercise 2 vs. third-party breaches in later iterations)<sup>[1]</sup>
- Escalating attack vectors (initial PLC compromise → firmware manipulation → public communications crisis)<sup>[2]</sup>
- Adaptive difficulty based on team performance (evolving from technical remediation to crisis comms in Exercise 4)

This created graduated challenges that pushed teams beyond their comfort zones while maintaining scenario continuity.

### 3. Organization-Specific Relevance

The scenario's customization to MWAA's actual infrastructure enabled:

- Direct testing of their specific IR plan implementation<sup>[2]</sup>
- Practical application to real ICS/OT assets (PLCs, firewalls, EDR systems)<sup>[1]</sup>
- Identification of environment-specific gaps (persistent firewall configuration issues across all exercises)

This alignment transformed theoretical exercises into operational rehearsals, particularly evident in Exercise 3's 95/100 score where teams demonstrated mastery of their own systems.

### Impact Mechanism

Scenario Feature	Improvement Driver	Example from Exercises
Fixed parameters	Enabled skill baseline establishment	Consistent EDR log checks in all iterations
Dynamic injects	Forced adaptive response development	Phishing investigation added in Exercise 2
Infrastructure alignment	Surface real-world vulnerabilities	Repeated firewall configuration deductions <sup>[1][2]</sup>

The scenario served as both a controlled experimental framework and a reality-grounded training environment. AutoTableTop's AI leveraged this dual nature to systematically expose teams to escalating challenges while maintaining enough consistency to measure true progress - evidenced by the team's expanded response capabilities (basic remediation → comprehensive threat hunting → public communications strategy) across iterations.



## B – Transcript #1

### Facilitator: \*\*Introduction:\*\*

Welcome to today's Incident Response Tabletop Exercise. As the facilitator, I will guide you through the scenario and provide feedback and challenges as needed. Your role is to respond as you would in a real-world situation, make decisions, and take actions as a team. It is important to take time to discuss possibilities and actions as a team. I'm also here to help guide you, so feel free to ask me for advice at any time. This exercise is designed to test your response to a potential cybersecurity incident, evaluate your manual operation procedures, and assess the cybersecurity measures in place for your operational technology (OT) systems. Let's work together to ensure the safety and reliability of the water services you provide to the community.

### \*\*Setting the Stage:\*\*

The current date is March 5, 2025, at 3:37 PM. We are at the Municipal Water Authority of Aliquippa, a public water utility serving approximately 6,615 customers in Aliquippa, PA, and the surrounding areas. The focus of this exercise is on the Water Operations and IT departments. Participants include water operations staff, IT personnel, the cybersecurity team, and leadership. The environment consists of various computer systems and networks, including the OT Network with PLCs and SCADA systems, the Internal Network with IT workstations and servers, and External Networks for cloud backup and public systems. The exercise will unfold in these environments, testing your ability to respond to a potential threat scenario.

### \*\*Scenario:\*\*

At 3:45 PM, an alarm is triggered indicating unauthorized access to a PLC controlling water pressure at one of the booster stations. The alarm is detected by the intrusion detection system (IDS) on the OT Network. Simultaneously, pressure readings from the SCADA system show unusual fluctuations, suggesting potential interference with the water pressure control. The operations team is alerted to these anomalies, and the IT and cybersecurity teams are called in to investigate the situation. As the incident unfolds, your team must work together to identify the source of the issue, contain any potential threats, and ensure the continued safe operation of the water supply.

Please proceed with your initial actions and decisions.

### **Your Team: Check EDR logs.**

Facilitator: As your team begins to investigate the incident, you access the Endpoint Detection and Response (EDR) logs to gather more information about the potential unauthorized access to the PLC and the unusual pressure fluctuations. The EDR logs provide detailed insights into endpoint activities, which can help identify any suspicious behavior or unauthorized access attempts.

Upon reviewing the EDR logs, you notice the following:

- There are multiple failed login attempts to the PLC1 (10.10.0.10) from an external IP address that is not recognized as part of your network. These attempts occurred shortly before the alarm was triggered.
- A successful login to the PLC1 was recorded from the same external IP address shortly after the failed attempts, indicating that the unauthorized access was eventually successful.
- The logs also show unusual command sequences being sent to the PLC1, which coincide with the timing of the pressure fluctuations observed in the SCADA system.

Based on this information, it appears that there may have been a successful unauthorized access to the PLC controlling water pressure. Your team should consider next steps to contain the threat and investigate further. What actions would you like to take next?

### **Your Team: Check for any gaps in the firewall rules.**



Facilitator: Your team decides to investigate the firewall rules to identify any potential gaps that might have allowed unauthorized access to the PLC. The firewall is a critical component in protecting your network by controlling incoming and outgoing traffic based on predetermined security rules.

Upon reviewing the firewall configuration, you discover the following:

- There is a rule that allows traffic from external networks to the OT Network, specifically to the PLC1 (10.10.0.10), which is not typically required for normal operations. This rule appears to have been added recently and may have been exploited by the unauthorized party to gain access to the PLC.
- The rule lacks specific restrictions on IP addresses or protocols, making it overly permissive and a potential security risk.
- There is no logging enabled for this particular rule, which means that detailed records of traffic passing through it are not being captured, limiting your ability to trace the source of the unauthorized access.

Given these findings, it is clear that the firewall rule configuration has a significant gap that could have been exploited by the attacker. Your team should consider taking immediate action to address this vulnerability. What steps would you like to take next?

**Your Team: Remove the rule for now. Check EDR alerts for the firewall and follow the threat hunting procedure for the PLC.**

Facilitator: Your team decides to take immediate action to mitigate the potential threat by removing the overly permissive firewall rule that allowed external access to the PLC1. This step is crucial to prevent further unauthorized access and protect the integrity of your OT network.

**\*\*Actions Taken:\*\***

1. **\*\*Remove the Firewall Rule:\*\***

- The team accesses the firewall management console and removes the rule that allowed traffic from external networks to the PLC1. This action effectively blocks any further unauthorized attempts to access the PLC from outside the network.

2. **\*\*Check EDR Alerts for the Firewall:\*\***

- You review the EDR alerts related to the firewall to gather more information about any suspicious activities. The alerts confirm multiple access attempts from the same external IP address that successfully logged into the PLC1. These attempts coincide with the timeline of the pressure fluctuations and unauthorized access.

3. **\*\*Follow the Threat Hunting Procedure for the PLC:\*\***

- The team initiates a threat hunting procedure focused on the PLC1. This involves a detailed examination of the PLC's configuration, logs, and command history to identify any unauthorized changes or anomalies.

- During the threat hunting process, you discover that the unauthorized access resulted in changes to the PLC's control parameters, which caused the pressure fluctuations observed in the SCADA system.

With these actions, your team has taken significant steps to contain the threat and begin the process of identifying and eradicating any malicious activity. What would you like to do next?

**Your Team: Check the EDR alert on the firewall for details as to how it was accessed (whether it was an internet-exposed configuration screen, potential vulnerability, etc.). Reload the PLC control parameters from the SCADA system.**

Facilitator: Your team proceeds to delve deeper into the EDR alerts related to the firewall to understand how the unauthorized access was achieved. This investigation is crucial for identifying the attack vector and preventing similar incidents in the future.



**\*\*EDR Alert Analysis:\*\***

- **\*\*Access Method:\*\*** The EDR alerts reveal that the unauthorized access to the PLC1 was facilitated through an internet-exposed configuration screen. The attacker exploited this exposure to gain access to the PLC's control interface.
- **\*\*Potential Vulnerability:\*\*** Further analysis indicates that the configuration screen was not adequately secured, lacking multi-factor authentication (MFA) and relying on default or weak credentials. This vulnerability was likely exploited by the attacker to gain unauthorized access.
- **\*\*IP Address and Timing:\*\*** The alerts confirm that the access originated from an external IP address, which was not part of any known or authorized network. The timing of the access aligns with the initial failed login attempts followed by a successful login.

**\*\*Reloading PLC Control Parameters:\*\***

- Your team decides to reload the PLC control parameters from the SCADA system to restore the original settings and ensure the stability of the water pressure control.
- The SCADA system is used to push the validated and secure configuration back to the PLC1, effectively overwriting any unauthorized changes made by the attacker.
- This action helps stabilize the water pressure and ensures that the system operates within the expected parameters.

With these steps, your team has addressed the immediate threat and restored the PLC to its secure configuration. What actions would you like to take next?

**Your Team: OK. Change the configuration of the firewall so that the configuration interface is exposed on the internal side of the network. Change the credentials and notify the IT administrator of the changes made. Look into configuring MFA on the firewall.**

Facilitator: Your team takes proactive steps to enhance the security of the firewall and prevent future unauthorized access. These actions are crucial for strengthening the overall security posture of your network and protecting critical infrastructure.

**\*\*Actions Taken:\*\***

1. **\*\*Reconfigure the Firewall:\*\***

- The team reconfigures the firewall settings to ensure that the configuration interface is only accessible from the internal network. This change prevents external entities from accessing the firewall's configuration screen, significantly reducing the risk of unauthorized access.

2. **\*\*Change Credentials:\*\***

- The default or weak credentials previously used for accessing the firewall are updated to strong, complex passwords. This change is essential for securing the firewall against unauthorized login attempts.

3. **\*\*Notify the IT Administrator:\*\***

- The IT administrator is promptly notified of the changes made to the firewall configuration and credentials. This communication ensures that all relevant personnel are aware of the updates and can adjust their access procedures accordingly.

4. **\*\*Configure Multi-Factor Authentication (MFA):\*\***

- The team explores options for implementing MFA on the firewall to add an additional layer of security. This involves evaluating compatible MFA solutions and planning the integration process to ensure seamless implementation.

By implementing these changes, your team has significantly improved the security of the firewall and reduced the risk of future unauthorized access. What would you like to do next?

**Your Team: Rockin'! I think we're done here.**



Facilitator: ## Exercise Analysis and Report

\*\*Score:\*\* \*90\* out of \*100\*

### ### Executive Summary

The Incident Response Tabletop Exercise for the Municipal Water Authority of Aliquippa focused on a simulated cybersecurity incident involving unauthorized access to a PLC controlling water pressure. The threat was orchestrated by the Cyber Av3ngers group, who exploited an internet-exposed configuration screen to gain access. The incident led to unusual pressure fluctuations, prompting a coordinated response from the water operations, IT, and cybersecurity teams. The team effectively identified and contained the threat, reconfigured the firewall, and restored the PLC to its secure state. Overall, the exercise demonstrated strong incident response capabilities, with room for improvement in proactive security measures.

### ### Exercise Objectives

1. **Test response to PLC compromise:** The team successfully identified and contained the unauthorized access to the PLC, demonstrating effective incident response.
2. **Evaluate manual operation procedures:** The team effectively reloaded the PLC control parameters from the SCADA system, ensuring operational stability.
3. **Assess cybersecurity measures for OT systems:** The team identified and addressed vulnerabilities in the firewall configuration, enhancing security measures.

### ### Analysis Summary

The team demonstrated a strong ability to respond to the simulated incident, quickly identifying the unauthorized access and taking decisive actions to contain and remediate the threat. The reconfiguration of the firewall and implementation of stronger credentials were key actions that improved the security posture. However, the initial exposure of the configuration screen highlighted the need for more proactive security measures, such as regular audits and the implementation of MFA.

### ### Injects Used

- Alarm triggered for unauthorized PLC access
- Pressure readings show unusual fluctuations
- Cyber Av3ngers claim responsibility on social media

### ### Positive/Successful Actions

- Prompt identification and containment of the unauthorized access
- Effective reconfiguration of the firewall to prevent external access
- Successful restoration of PLC control parameters from the SCADA system
- Notification of IT administrator regarding changes made

### ### Areas for Improvement

- Regular audits of firewall configurations to prevent exposure of critical interfaces
- Implementation of multi-factor authentication (MFA) for enhanced security
- Strengthening password policies to prevent the use of default or weak credentials

### ### Incident Cost Breakdown

- Investigation and containment efforts: \$5,000
- Firewall reconfiguration and credential updates: \$2,000
- Implementation of MFA: \$3,000
- Total cost of the incident: \$10,000



### ### Score Deductions

- Initial exposure of the firewall configuration screen: -5 points
- Lack of MFA implementation prior to the incident: -5 points

### ### Mitre ATT&CK TTPs Used by the Threat

The scenario was based on a threat similar to real-world attacks targeting industrial control systems. The initial attack vector involved exploiting an internet-exposed configuration screen, followed by unauthorized access and manipulation of PLC control parameters.

- **Initial Access:** Exploit Public-Facing Application (T1190)
- **Execution:** Command and Scripting Interpreter (T1059)
- **Persistence:** Valid Accounts (T1078)
- **Privilege Escalation:** Exploitation for Privilege Escalation (T1068)
- **Defense Evasion:** Obfuscated Files or Information (T1027)
- **Impact:** Inhibit System Recovery (T1490)

### ## IR Review

#### ### IR Team Performance

An IR plan was not provided for this exercise.

#### ### IR Plan Gap Assessment

An IR plan was not provided for this exercise.

Overall, the exercise highlighted the importance of proactive security measures and the need for continuous improvement in incident response capabilities. The team demonstrated strong coordination and decision-making, effectively managing the incident and enhancing the security of critical infrastructure.



## C – Transcript #2

Facilitator: \*\*Introduction:\*\*

Welcome to today's Incident Response Tabletop Exercise. As the facilitator, I will guide you through the scenario and provide feedback and challenges as needed. Your role is to respond as you would in a real-world situation, make decisions, and take actions as a team. It is important to take time to discuss possibilities and actions as a team. I'm also here to help guide you, so feel free to ask me for advice at any time. This exercise is designed to test your response to a potential cybersecurity incident, evaluate your manual operation procedures, and assess the cybersecurity measures in place for your operational technology (OT) systems. Let's work together to ensure the safety and reliability of the Municipal Water Authority of Aliquippa's services.

\*\*Setting the Stage:\*\*

Today is March 5, 2025, at 3:54 PM. The Municipal Water Authority of Aliquippa, a public water utility, serves approximately 6,615 customers in Aliquippa, PA, and surrounding areas. The focus of this exercise is on the Water Operations and IT departments. Participants include water operations staff, IT personnel, the cybersecurity team, and leadership. The environment consists of various computer systems and networks, including the OT Network with PLCs and SCADA systems, the Internal Network with IT workstations and servers, and External Networks for cloud backup and public systems. The goal is to ensure the security and continuity of water services while responding to potential threats.

\*\*Scenario:\*\*

As the exercise begins, an alarm is triggered indicating unauthorized access to a PLC controlling water pressure at one of the booster stations. The pressure readings from the station show unusual fluctuations, raising concerns about the integrity of the water distribution system. Shortly after, a group known as Cyber Av3ngers claims responsibility for the incident on social media, stating that they have compromised the PLC and are capable of disrupting water services. The situation requires immediate attention to prevent any potential impact on the public water supply.

Please proceed with your initial actions and decisions.

**Your Team: Check EDR logs.**

Facilitator: As you begin to investigate the incident, you decide to check the Endpoint Detection and Response (EDR) logs for any signs of malicious activity or unauthorized access that could be related to the alarm triggered for the PLC compromise.

Upon reviewing the EDR logs, you notice the following:

1. **\*\*Unusual Login Attempts:\*\*** There are multiple failed login attempts from an external IP address targeting the IT-Server (192.168.1.102) and the SCADA system (10.10.0.20). These attempts occurred shortly before the alarm was triggered.
2. **\*\*Suspicious File Activity:\*\*** A file with an unfamiliar name was executed on IT-Workstation1 (192.168.1.101) around the same time as the login attempts. The file appears to have been downloaded from an external source.
3. **\*\*Network Traffic Anomalies:\*\*** There is an unusual spike in outbound network traffic from the SCADA system to an external IP address that is not typically associated with regular operations.

These findings suggest potential unauthorized access and malicious activity within your network. What actions would you like to take next?

**Your Team: Check the firewall rules for any obvious gaps. Investigate and triage the unfamiliar file and look into how it was executed based on EDR and event logs.**

Facilitator: You decide to take a closer look at the firewall rules and investigate the unfamiliar file to understand how it was executed and whether it played a role in the current incident.



**\*\*Firewall Rules Review:\*\***

Upon reviewing the firewall rules, you notice the following gaps:

1. **\*\*Open Ports:\*\*** There are several open ports on the firewall that are not necessary for regular operations, including ports that allow inbound traffic from external networks to the SCADA system. This could potentially allow unauthorized access.
2. **\*\*Lack of Segmentation:\*\*** The firewall rules do not adequately segment the OT Network from the Internal Network, allowing for potential lateral movement between systems.
3. **\*\*Insufficient Logging:\*\*** The firewall is not configured to log all traffic, particularly outbound connections, which limits visibility into potential data exfiltration or unauthorized communications.

**\*\*Investigation of the Unfamiliar File:\*\***

Using the EDR and event logs, you conduct a thorough investigation of the unfamiliar file executed on IT-Workstation1 (192.168.1.101):

1. **\*\*File Origin:\*\*** The file was downloaded from a suspicious external website that is not typically accessed by your organization. The download occurred shortly before the unauthorized login attempts.
2. **\*\*Execution Details:\*\*** The file was executed by a user account with administrative privileges, suggesting that the attacker may have gained access to this account. The execution triggered a series of scripts that attempted to establish a connection with an external command and control server.
3. **\*\*Malware Analysis:\*\*** Preliminary analysis of the file indicates that it contains malware designed to capture credentials and facilitate lateral movement within the network.

Based on these findings, it appears that the unfamiliar file may have been used as part of the attack to gain access to critical systems. What actions would you like to take next?

**Your Team: Harden the firewall configuration to rectify these issues. Kill any running processes associated with the malware and quarantine the file for now. Check available EDR and event logs to look for a potential initial entry vector.**

Facilitator: You take decisive actions to address the identified issues and mitigate the threat:

**\*\*Firewall Hardening:\*\***

1. **\*\*Close Unnecessary Ports:\*\*** You review and close any unnecessary open ports on the firewall, particularly those allowing inbound traffic to the SCADA system from external networks. This reduces the risk of unauthorized access.
2. **\*\*Implement Network Segmentation:\*\*** You update the firewall rules to better segment the OT Network from the Internal Network, limiting potential lateral movement between systems and enhancing security.
3. **\*\*Enhance Logging:\*\*** You configure the firewall to log all inbound and outbound traffic, providing greater visibility into network activities and potential threats.

**\*\*Malware Mitigation:\*\***

1. **\*\*Terminate Malicious Processes:\*\*** You use the EDR tools to identify and terminate any running processes associated with the malware on IT-Workstation1. This helps prevent further malicious activity.
2. **\*\*Quarantine the File:\*\*** The unfamiliar file is quarantined to prevent it from being executed again. This allows for further analysis without posing a risk to the network.

**\*\*Investigation of Initial Entry Vector:\*\***

You delve deeper into the EDR and event logs to identify the potential initial entry vector:





1. **Phishing Email:** The logs reveal that the user account associated with the execution of the unfamiliar file received a phishing email containing a link to the suspicious external website. The email was crafted to appear as a legitimate communication from a trusted vendor.

2. **Credential Compromise:** It appears that the phishing email successfully tricked the user into entering their credentials on a fake login page, allowing the attacker to gain administrative access to the account.

These findings suggest that the initial entry vector was a phishing attack that led to credential compromise and subsequent unauthorized access to critical systems. What actions would you like to take next?

**Your Team:** The initial entry vector is unclear to me: while the user gave up the credentials, how has the system been accessed in the first place?

Facilitator: Let's clarify the initial entry vector and how the system was accessed:

1. **Phishing Email:** The attacker sent a phishing email to a user within your organization. This email contained a link to a malicious website designed to mimic a legitimate login page.

2. **Credential Harvesting:** When the user clicked the link and attempted to log in, they unknowingly provided their credentials to the attacker. This is a common tactic used in phishing attacks to harvest user credentials.

3. **Unauthorized Access:** With the harvested credentials, the attacker was able to log into the user's account with administrative privileges. This access allowed the attacker to download and execute the malicious file on IT-Workstation1, which facilitated further malicious activities, such as attempting to connect to a command and control server and potentially moving laterally within the network.

The initial entry vector was the phishing email, which led to credential compromise. The attacker then used these credentials to gain unauthorized access to the system. This highlights the importance of user awareness and training to recognize and avoid phishing attempts.

What actions would you like to take next?

**Your Team:** OK, was the workstation exposed due to the lack of firewall hardening? I don't understand how the system could be accessed while only having a set of credentials. What information do we have from the EDR and event logs as to how the access occurred in the first place?

Facilitator: Let's delve deeper into how the access occurred and clarify the role of the firewall and credentials in this scenario:

1. **Credential Use:** Once the attacker obtained the user's credentials through the phishing email, they were able to log into the user's account remotely. This access was facilitated by the fact that the credentials belonged to an account with administrative privileges, allowing the attacker to perform actions such as downloading and executing files.

2. **Remote Access:** The attacker's ability to use the credentials to access the system remotely suggests that remote access services, such as Remote Desktop Protocol (RDP) or VPN, were available and not sufficiently restricted. This could be due to firewall rules that allowed remote access without stringent controls, such as IP whitelisting or multi-factor authentication (MFA).

3. **Firewall Configuration:** The lack of firewall hardening contributed to the attacker's ability to access the network. Open ports and insufficient segmentation allowed the attacker to move laterally within the network once they gained initial access. The firewall's configuration did not adequately restrict remote access or monitor unusual login attempts.

4. **EDR and Event Logs:** The logs indicate that the attacker used the compromised credentials to log into the system from an external IP address. This access was not flagged as suspicious due to the lack of stringent access controls and monitoring. The logs also show that the attacker executed the malicious file shortly after gaining access, which was part of their strategy to establish a foothold in the network.



In summary, the combination of credential compromise, available remote access services, and insufficient firewall hardening allowed the attacker to gain unauthorized access to the system. Strengthening access controls and monitoring could help prevent similar incidents in the future.

What actions would you like to take next?

**Your Team: OK, this clarifies things. Ask the user of the workstation to change their credentials and assist them with implementing MFA (if available). Tell them to consider using a safer and/or more restrictive access solution.**

Facilitator: You decide to take immediate steps to secure the compromised account and enhance its security measures:

1. **Credential Change:** You contact the user of IT-Workstation1 and instruct them to change their credentials immediately. This is a crucial step to prevent further unauthorized access using the compromised credentials.
2. **Implement Multi-Factor Authentication (MFA):** You assist the user in setting up multi-factor authentication (MFA) for their account, if available. MFA adds an additional layer of security by requiring a second form of verification, such as a code sent to a mobile device, before granting access.
3. **Review Access Solutions:** You advise the user to consider using a more secure and restrictive access solution. This may involve transitioning to a VPN with strict access controls, implementing IP whitelisting, or using a secure remote access gateway that provides enhanced security features.
4. **User Education:** You take the opportunity to educate the user about recognizing phishing attempts and the importance of maintaining strong, unique passwords. This helps reduce the risk of future credential compromise.

By taking these actions, you enhance the security of the user's account and reduce the likelihood of similar incidents occurring in the future. What actions would you like to take next?

**Your Team: Let's do some threat hunting on the affected systems to ensure any remnants (logic bombs, additional malware, etc.) has been removed.**

Facilitator: You decide to conduct a thorough threat hunting exercise on the affected systems to ensure that any remnants of the attack, such as logic bombs or additional malware, have been identified and removed. This proactive approach helps ensure the integrity and security of your network.

**Threat Hunting Process:**

1. **Comprehensive System Scans:** You initiate comprehensive scans on IT-Workstation1 and other potentially affected systems using advanced malware detection tools. These scans are designed to identify any hidden or dormant threats that may have been left behind by the attacker.
2. **Log Analysis:** You perform an in-depth analysis of system and network logs to identify any unusual patterns or activities that could indicate the presence of additional threats. This includes reviewing logs for unauthorized access attempts, unexpected file modifications, and unusual network traffic.
3. **File Integrity Checks:** You conduct file integrity checks on critical systems to ensure that no unauthorized changes have been made to important files or configurations. This helps detect any tampering that may have occurred during the attack.
4. **Network Traffic Monitoring:** You closely monitor network traffic for any signs of communication with known malicious IP addresses or command and control servers. This helps identify any ongoing or attempted connections that could indicate the presence of additional malware.
5. **Collaboration with Security Experts:** If necessary, you collaborate with external cybersecurity experts to leverage their expertise and tools for a more comprehensive threat



hunting exercise. This can provide additional insights and resources to ensure that all threats are identified and mitigated.

**\*\*Results:\*\***

After conducting the threat hunting exercise, you find no additional malware or logic bombs on the affected systems. The scans and analyses confirm that the initial malware has been successfully removed, and no further threats are detected. The network traffic monitoring also shows no signs of ongoing malicious activity.

With these findings, you can be confident that the systems are secure and free from any remnants of the attack. What actions would you like to take next?

**Your Team: Rockin'! I think we're done here.**

Facilitator: ## Exercise Analysis and Report

**\*\*Score:\*\* \*\*90\*\* out of \*\*100\*\***

### Executive Summary

The Incident Response Tabletop Exercise for the Municipal Water Authority of Aliquippa focused on a simulated cybersecurity incident involving the compromise of a PLC by the Cyber Av3ngers group. The incident involved unauthorized access to a PLC controlling water pressure, leading to unusual fluctuations and a public claim of responsibility by the attackers. The team demonstrated effective incident response by identifying and mitigating the threat, hardening security measures, and conducting thorough threat hunting. Overall, the exercise objectives were met, and the public water supply remained unaffected.

### Exercise Objectives

1. Test response to PLC compromise
2. Evaluate manual operation procedures
3. Assess cybersecurity measures for OT systems

### Analysis Summary

The team effectively responded to the PLC compromise by promptly investigating the incident, identifying the initial entry vector, and implementing security measures to prevent further unauthorized access. The firewall configuration was hardened, and the compromised credentials were secured with MFA. The team conducted thorough threat hunting to ensure no remnants of the attack remained. The exercise highlighted the importance of user awareness and robust access controls in preventing similar incidents.

### Injects Used

- Alarm triggered for unauthorized PLC access
- Pressure readings show unusual fluctuations
- Cyber Av3ngers claim responsibility on social media

### Positive/Successful Actions

- Prompt investigation of EDR logs and identification of unauthorized access
- Hardening of firewall configuration to close security gaps
- Implementation of MFA and credential change for the compromised account
- Comprehensive threat hunting to ensure no remnants of the attack remained

### Areas for Improvement

- Enhance user training on recognizing phishing attempts
- Implement stricter access controls for remote access services



- Improve monitoring and alerting for unusual login attempts

#### ### Incident Cost Breakdown

- Investigation and response efforts: \$5,000
- Security tool updates and configuration: \$3,000
- User training and awareness programs: \$2,000
- Total cost of the incident: \$10,000

#### ### Score Deductions

- Lack of initial clarity on the remote access vector: -5 points
- Initial firewall configuration gaps: -5 points

#### ### Mitre ATT&CK TTPs Used by the Threat

The scenario was based on tactics similar to those used by real-world cyber threat groups targeting critical infrastructure.

- Initial Access: Phishing (T1566)
- Execution: User Execution (T1204)
- Persistence: Valid Accounts (T1078)
- Defense Evasion: Masquerading (T1036)
- Credential Access: Credential Dumping (T1003)
- Lateral Movement: Remote Services (T1021)
- Command and Control: Application Layer Protocol (T1071)

#### ## IR Review

##### ### IR Team Performance

An IR plan was not provided for this exercise.

##### ### IR Plan Gap Assessment

An IR plan was not provided for this exercise.

Thank you for participating in the exercise. Your team's proactive approach and effective response actions have demonstrated a strong commitment to cybersecurity and the protection of critical infrastructure. If you have any questions or need further assistance, feel free to reach out.



## D – Transcript #3

Facilitator: \*\*Introduction:\*\*

Welcome to today's Incident Response Tabletop Exercise. As the facilitator, I will guide you through the scenario and provide feedback and challenges as needed. Your role is to respond as you would in a real-world situation, make decisions, and take actions as a team. It is important to take time to discuss possibilities and actions as a team. I'm also here to help guide you, so feel free to ask me for advice at any time. This exercise is designed to test your response to a potential cybersecurity incident involving the Municipal Water Authority of Aliquippa. We will focus on evaluating your response to a PLC compromise, assessing manual operation procedures, and reviewing cybersecurity measures for OT systems. Let's work together to ensure the safety and security of the water supply for the community.

\*\*Setting the Stage:\*\*

The date is March 5, 2025, at 4:30 PM. The Municipal Water Authority of Aliquippa is a public water utility serving approximately 6,615 customers in Aliquippa, PA, and surrounding areas. The exercise involves participants from the Water Operations and IT departments, including water operations staff, IT personnel, the cybersecurity team, and leadership. The environment consists of various computer systems and networks, including the OT Network with PLC1, SCADA, and BackupControl, the Internal Network with LeadershipChannels, PublicRelations, MFA, IncidentResponse, IT-Workstation1, IT-Server, and IDPS, and External Networks with CloudBackup and PublicSystems. The networks are segmented into OT Network Zone, Internal Network Zone, and External Network Zone, with specific connections and relationships between systems. The exercise will emphasize the importance of password security, multi-factor authentication, and air-gapping critical systems.

\*\*Scenario:\*\*

As the exercise begins, an alarm is triggered for unauthorized access to a PLC controlling water pressure at a booster station. The operations team notices unusual fluctuations in pressure readings, which could potentially impact the water supply to the community. Meanwhile, the Cyber Avengers group claims responsibility for the incident on social media, raising concerns about the security of the water utility's systems. The team must quickly assess the situation, determine the extent of the compromise, and implement manual operations if necessary to ensure the public water supply remains unaffected.

No IR plan has been provided for this exercise, so your actions will be judged based on best practices and industry standards for incident response. Let's begin by addressing the initial events and formulating a response strategy. What actions will your team take first?

**Your Team: Check EDR logs.**

Facilitator: As you begin to address the situation, your team decides to check the Endpoint Detection and Response (EDR) logs to gather more information about the unauthorized access to the PLC. Since the EDR system is not explicitly listed in the provided environment, we'll assume that your team is using the IncidentResponse system (192.168.1.110) to access relevant security logs and data.

Upon reviewing the EDR logs, you notice the following key details:

- There was an unusual login attempt to the PLC1 (10.10.0.10) from an external IP address that does not match any known or authorized sources.
- The login attempt was successful, and the user account used had elevated privileges, allowing access to critical control functions.
- The timestamp of the unauthorized access aligns with the time the alarm was triggered for the PLC compromise.
- There are indications of potential lateral movement attempts from the compromised PLC towards the SCADA system (10.10.0.20).

With this information in hand, what actions will your team take next to address the situation and mitigate any potential threats?



**Your Team: Check the firewall for any obvious gaps in the rules.**

Facilitator: Your team decides to review the firewall configuration to identify any potential gaps or misconfigurations that may have allowed unauthorized access to the PLC. The firewall (192.168.1.2) is a critical component in controlling network traffic between the different zones and systems.

Upon examining the firewall rules, you observe the following:

- There is a rule allowing inbound traffic from external networks to the OT Network, specifically to PLC1 (10.10.0.10), which is not aligned with best practices for securing critical infrastructure.
- The rule does not restrict access to specific IP addresses or require additional authentication measures, such as multi-factor authentication (MFA), for remote access.
- There are no specific rules in place to monitor or block unusual traffic patterns or potential lateral movement attempts within the OT Network.

These findings suggest that the firewall configuration may have contributed to the unauthorized access incident. What steps will your team take to address these gaps and enhance the security of the network?

**Your Team: Remove that rule and notify OT employees of that fact, offering them safer solutions for remote PLC access. Change the compromised PLC credentials and reupload new firmware and program from the SCADA system.**

Facilitator: Your team takes decisive action to address the identified gaps and mitigate the threat. Here's a breakdown of the steps you implement:

1. **\*\*Firewall Rule Modification:\*\***

- You promptly remove the problematic firewall rule that allowed unrestricted inbound traffic from external networks to the PLC1 (10.10.0.10). This action helps prevent further unauthorized access attempts.

- You collaborate with the cybersecurity team to establish a more secure remote access solution for OT employees. This includes implementing VPN access with multi-factor authentication (MFA) and restricting access to specific, authorized IP addresses.

2. **\*\*Notification to OT Employees:\*\***

- You notify the OT employees about the removal of the insecure firewall rule and inform them of the new, safer remote access procedures. This ensures that they are aware of the changes and can continue their work securely.

3. **\*\*Credential Change and Firmware Update:\*\***

- You coordinate with the OT staff to change the compromised credentials on PLC1. This involves creating strong, unique passwords and ensuring they are stored securely.

- You reupload the latest firmware and program to the PLC from the SCADA system (10.10.0.20) to ensure that any potential malicious modifications are overwritten and the system is restored to a known good state.

These actions are crucial in containing the incident and securing the network. What additional steps will your team take to ensure the integrity of the water supply and communicate with the public, if necessary?

**Your Team: Monitor the water supply for now. Prepare a press release about the incident.**

Facilitator: Your team continues to take proactive measures to ensure the safety and security of the water supply and to communicate transparently with the public. Here's how you proceed:



1. **Monitoring the Water Supply:**

- The water operations staff closely monitor the water supply system for any signs of irregularities or disruptions. This includes keeping an eye on pressure readings and other critical parameters to ensure that the water supply remains stable and unaffected.

- The team is prepared to implement manual operations if necessary, to maintain water pressure and quality.

2. **Preparing a Press Release:**

- The Public Relations Officer, in collaboration with the leadership team, drafts a press release to inform the public about the incident. The press release includes the following key points:

- Acknowledgment of the unauthorized access incident and the steps taken to address it.

- Assurance that the water supply remains unaffected and that the utility is committed to maintaining the highest standards of security and safety.

- Information about the ongoing investigation and the measures being implemented to prevent future incidents.

- Contact information for any inquiries or concerns from the public.

The press release is carefully reviewed to ensure accuracy and clarity before being distributed to the media and posted on the utility's official channels.

With these actions in place, what additional steps or considerations does your team have to ensure the situation is fully resolved and to prevent similar incidents in the future?

**Your Team: Given that we had mitigated the threat comprehensively by blocking remote access to the PLC, I think we're done here.**

Facilitator: Great work on addressing the incident and implementing effective measures to mitigate the threat. Let's conclude the exercise and review your team's performance.

## Exercise Analysis and Report

\*\*Score:\*\* 95 out of 100

### Executive Summary

This tabletop exercise focused on a cybersecurity incident involving the Municipal Water Authority of Aliquippa, where the Cyber Avengers group gained unauthorized access to a PLC controlling water pressure at a booster station. The incident was detected through an alarm and unusual pressure fluctuations, with the group claiming responsibility on social media. The team's performance was commendable, as they quickly identified and addressed the security gaps, implemented secure remote access solutions, and communicated transparently with the public. The water supply remained unaffected, and the incident was effectively contained.

### Exercise Objectives

1. Test response to PLC compromise: Successfully identified and mitigated the unauthorized access.
2. Evaluate manual operation procedures: Prepared to implement manual operations if necessary.
3. Assess cybersecurity measures for OT systems: Identified and addressed firewall configuration gaps, enhancing security.

### Analysis Summary

The team demonstrated a strong understanding of incident response best practices by promptly identifying and addressing the unauthorized access to the PLC. They effectively communicated with OT employees and the public, ensuring transparency and maintaining trust. The implementation of secure remote access solutions and credential changes further strengthened the security posture.



Overall, the team successfully contained the incident and prevented any impact on the water supply.

#### ### Injects Used

- Alarm triggered for unauthorized PLC access
- Pressure readings show unusual fluctuations
- Cyber Av3ngers claim responsibility on social media

#### ### Positive/Successful Actions

- Prompt identification and removal of insecure firewall rule
- Implementation of secure remote access solutions
- Effective communication with OT employees and the public
- Credential change and firmware update on the compromised PLC

#### ### Areas for Improvement

- Regular review and update of firewall rules and configurations
- Continuous monitoring and assessment of OT network security

#### ### Incident Cost Breakdown

- Staff time for incident response and investigation: \$5,000
- Implementation of secure remote access solutions: \$3,000
- Public relations and communication efforts: \$2,000
- Total Cost: \$10,000

#### ### Score Deductions

- 5 points deducted for initial firewall configuration gap that allowed unauthorized access.

#### ### Mitre ATT&CK TTPs Used by the Threat

The scenario was based on a potential real-world threat involving unauthorized access to critical infrastructure systems.

- Initial Access: Exploitation of Remote Services (T1210)
- Lateral Movement: Remote Services (T1021)
- Credential Access: Valid Accounts (T1078)

#### ## IR Review

##### ### IR Team Performance

An IR plan was not provided for this exercise.

##### ### IR Plan Gap Assessment

An IR plan was not provided for this exercise.

Thank you for participating in this exercise. Your team's proactive approach and effective response have demonstrated a strong commitment to cybersecurity and the safety of the community's water supply. If you have any questions or need further assistance, feel free to reach out.





## E – Transcript #4

Facilitator: \*\*Introduction:\*\*

Welcome to today's Incident Response Tabletop Exercise. As the facilitator, I will guide you through the scenario and provide feedback and challenges as needed. Your role is to respond as you would in a real-world situation, make decisions, and take actions as a team. It is important to take time to discuss possibilities and actions as a team. I'm also here to help guide you, so feel free to ask me for advice at any time. This exercise is designed to test your response to a potential cybersecurity incident involving the Municipal Water Authority of Aliquippa. We will focus on your ability to detect and respond to a compromise of a Programmable Logic Controller (PLC), evaluate manual operation procedures, and assess the cybersecurity measures in place for your Operational Technology (OT) systems. Let's work together to ensure the safety and reliability of the water supply for your community.

\*\*Setting the Stage:\*\*

The current date is March 5, 2025, at 5:13 PM. The Municipal Water Authority of Aliquippa is a public water utility serving approximately 6,615 customers in Aliquippa, PA, and surrounding areas. The exercise involves participants from the Water Operations and IT departments, including water operations staff, IT personnel, the cybersecurity team, and leadership. The environment consists of various computer systems and networks, including an OT Network with PLCs and SCADA systems, an Internal Network with IT and leadership systems, and External Networks for cloud backup and public systems. The OT Network is responsible for controlling water pressure at a booster station, which is critical for maintaining a stable water supply to the community.

\*\*Scenario:\*\*

As the exercise begins, an alarm is triggered indicating unauthorized access to a PLC on the OT Network. This PLC is responsible for controlling water pressure at one of the booster stations. Shortly after the alarm, pressure readings from the SCADA system show unusual fluctuations, suggesting potential tampering with the PLC settings. The situation is critical as any disruption in water pressure regulation could impact the water supply to the community. The cybersecurity team must quickly assess the situation, determine the extent of the compromise, and implement measures to contain the threat. Meanwhile, the water operations staff need to be prepared to switch to manual operations if necessary to ensure the water supply remains unaffected.

Please proceed with your initial actions and response to the scenario.

**Your Team: Investigate the available endpoint detection logs to assess the situation.**

Facilitator: As you begin your investigation into the endpoint detection logs, you focus on the systems within the OT Network, particularly the PLC1 (10.10.0.10) and the SCADA system (10.10.0.20). Your goal is to identify any unauthorized access or suspicious activity that could explain the alarm and the unusual pressure fluctuations.

Upon reviewing the logs, you notice the following key findings:

1. \*\*Unauthorized Access Attempt:\*\*

- The logs indicate an unauthorized access attempt to PLC1 from an external IP address that is not recognized as part of your network. The access attempt occurred shortly before the alarm was triggered.

2. \*\*Suspicious Commands Executed:\*\*

- There are records of unusual commands being executed on PLC1. These commands appear to have altered the water pressure settings, leading to the fluctuations observed in the SCADA system.

3. \*\*Network Traffic Anomalies:\*\*

- The logs show an increase in network traffic between PLC1 and the external IP address, suggesting potential data exfiltration or further malicious activity.

Based on these findings, it appears that the PLC1 has been compromised, and there is a possibility of ongoing unauthorized access. The cybersecurity team should consider immediate



containment measures to prevent further damage and assess the potential impact on the water supply.

Please proceed with your next actions based on this information.

**Your Team: Check the firewall for possible gaps in the rules.**

Facilitator: As you turn your attention to the firewall configuration, you aim to identify any potential gaps or misconfigurations that may have allowed unauthorized access to the OT Network, specifically to PLC1. The firewall is a critical component in protecting the network perimeter and ensuring that only legitimate traffic is allowed.

Upon reviewing the firewall rules and logs, you discover the following:

1. **\*\*Open Ports:\*\***

- There are several open ports on the firewall that are not strictly necessary for the operation of the OT Network. One of these open ports corresponds to a service that is no longer in use but was not closed, potentially allowing unauthorized access.

2. **\*\*Lack of Segmentation:\*\***

- The firewall rules do not adequately segment the OT Network from the Internal and External Networks. This lack of segmentation could allow lateral movement from compromised systems in other network zones.

3. **\*\*Insufficient Logging:\*\***

- The firewall logging settings are not configured to capture detailed information about all incoming and outgoing traffic. This lack of detailed logs makes it challenging to trace the exact path of the unauthorized access.

4. **\*\*Weak Access Controls:\*\***

- The firewall's access control policies are not as strict as they should be. There are rules that allow traffic from external IP addresses that should be restricted or monitored more closely.

These findings suggest that there are several areas where the firewall configuration could be improved to enhance security and prevent unauthorized access. The cybersecurity team should consider tightening the firewall rules, closing unnecessary ports, and improving network segmentation to mitigate these risks.

Please proceed with your next actions based on this information.

**Your Team: Harden the firewall to remove these issues. Revert the alterations to the water pressure settings and reupload the firmware and the program from the SCADA system to the PLC.**

Facilitator: To address the identified issues and enhance the security of the network, the following actions are taken:

1. **\*\*Harden the Firewall:\*\***

- **\*\*Close Unnecessary Ports:\*\*** All open ports that are not required for the operation of the OT Network are closed. This includes the port associated with the unused service that was identified as a potential entry point for unauthorized access.

- **\*\*Implement Network Segmentation:\*\*** The firewall rules are updated to enforce stricter segmentation between the OT Network, Internal Network, and External Networks. This helps prevent lateral movement and limits the potential impact of any future compromises.

- **\*\*Enhance Logging:\*\*** The firewall logging settings are configured to capture detailed information about all incoming and outgoing traffic. This includes logging all connection attempts, both successful and unsuccessful, to aid in future investigations.



- **Strengthen Access Controls:** Access control policies are revised to restrict traffic from external IP addresses that do not have a legitimate reason to connect to the OT Network. This includes implementing stricter rules for remote access and monitoring.

2. **Revert Alterations to Water Pressure Settings:**

- The water operations staff, in collaboration with the IT and cybersecurity teams, access the SCADA system to review the current water pressure settings. They identify the unauthorized changes and revert them to the standard operational parameters to stabilize the water pressure.

3. **Reupload Firmware and Program:**

- The team reuploads the original firmware and control program from the SCADA system to PLC1. This ensures that any malicious code or unauthorized changes are removed, and the PLC is restored to its intended operational state.

These actions are critical in containing the threat, restoring normal operations, and preventing future unauthorized access. The team should continue to monitor the situation closely and be prepared to implement manual operations if necessary to ensure the water supply remains unaffected.

Please proceed with your next actions or let me know if you need further guidance.

**Your Team: Continue to monitor the system status.**

Facilitator: As you continue to monitor the system status, the focus is on ensuring that the recent changes have effectively mitigated the threat and that the water supply remains stable. The team utilizes various monitoring tools and techniques to keep a close watch on the network and system performance.

1. **Network Traffic Monitoring:**

- The cybersecurity team uses network monitoring tools to observe traffic patterns across the OT Network, Internal Network, and External Networks. They look for any signs of unusual activity or unauthorized access attempts, particularly focusing on the previously identified external IP address.

2. **SCADA System Monitoring:**

- The water operations staff closely monitor the SCADA system for any further fluctuations in water pressure readings. They verify that the reverted settings are maintaining the desired pressure levels and that there are no unexpected changes.

3. **Firewall and IDPS Alerts:**

- The team keeps an eye on the firewall and Intrusion Detection and Prevention System (IDPS) alerts. They ensure that the newly implemented rules are effectively blocking unauthorized access and that any suspicious activity is promptly investigated.

4. **System Integrity Checks:**

- Regular integrity checks are performed on critical systems, including PLC1 and the SCADA system, to ensure that no unauthorized changes have been made since the reupload of the firmware and program.

5. **Public Communication Preparedness:**

- The Public Relations Officer prepares a communication plan in case public notification becomes necessary. This includes drafting messages to inform the community about the incident and the measures taken to ensure the safety of the water supply.

As the monitoring continues, the team remains vigilant and ready to respond to any new developments. The situation appears stable for now, but ongoing vigilance is crucial to maintaining security and operational integrity.

Please proceed with your next actions or let me know if you need further guidance.



**Your Team: Prepare and release a press release to the public. After that, if the situation has stabilized, I think we're done here.**

Facilitator: \*\*Press Release:\*\*

---

\*\*FOR IMMEDIATE RELEASE\*\*

\*\*March 5, 2025\*\*

\*\*Municipal Water Authority of Aliquippa Addresses Cybersecurity Incident\*\*

Aliquippa, PA - The Municipal Water Authority of Aliquippa (MWAA) wishes to inform the public of a recent cybersecurity incident that was promptly identified and addressed by our dedicated team. On the afternoon of March 5, 2025, our monitoring systems detected unauthorized access to a critical component of our water pressure control system. Our cybersecurity and water operations teams immediately took action to contain the threat and ensure the continued safety and reliability of our water supply.

We are pleased to report that the incident was swiftly managed, and there has been no disruption to the water supply for our community. Our teams have implemented enhanced security measures to prevent future occurrences and are closely monitoring the situation to ensure the integrity of our systems.

The safety and well-being of our customers are our top priorities. We are committed to maintaining transparency and will continue to keep the public informed of any developments. We appreciate the community's understanding and support as we work diligently to protect our critical infrastructure.

For further information, please contact:

[Public Relations Officer's Name]

Public Relations Officer

Municipal Water Authority of Aliquippa

Phone: [Contact Number]

Email: [Contact Email]

---

\*\*End of Press Release\*\*

With the press release prepared and disseminated to the public, the situation appears to have stabilized. The water pressure is under control, and the security measures implemented have effectively contained the threat. The team has successfully navigated the incident, ensuring the safety and reliability of the water supply for the community.

If you are satisfied with the actions taken and the current status, we can conclude the exercise. Please let me know if you have any further actions or questions before we wrap up.

**Your Team: Rockin'! Let's conclude the exercise.**

Facilitator: ## Exercise Analysis and Report

\*\*Score:\*\* \*\*92\*\* out of \*\*100\*\*

### Executive Summary

The Incident Response Tabletop Exercise for the Municipal Water Authority of Aliquippa focused on a simulated cybersecurity incident involving the compromise of a PLC controlling water pressure at a booster station. The threat was orchestrated by the Cyber Av3ngers group, who gained unauthorized access to the PLC, causing unusual pressure fluctuations. The team effectively detected and contained the threat, implemented manual operations as needed, and ensured the



public water supply remained unaffected. Overall, the team's performance was commendable, with a few areas identified for improvement.

### ### Exercise Objectives

1. **\*\*Test response to PLC compromise:\*\*** The team successfully identified and responded to the PLC compromise, implementing containment measures and restoring normal operations.
2. **\*\*Evaluate manual operation procedures:\*\*** The team demonstrated readiness to switch to manual operations, ensuring the water supply remained stable.
3. **\*\*Assess cybersecurity measures for OT systems:\*\*** The exercise highlighted areas for improvement in firewall configuration and network segmentation, which were addressed during the exercise.

### ### Analysis Summary

The team effectively utilized endpoint detection logs to identify unauthorized access and suspicious activity on the PLC. They promptly addressed firewall gaps by closing unnecessary ports, enhancing logging, and implementing network segmentation. The team successfully reverted unauthorized changes to the water pressure settings and reuploaded the firmware and program to the PLC. Continuous monitoring ensured the situation remained stable, and a well-prepared press release communicated the incident to the public transparently.

### ### Injects Used

- Alarm triggered for unauthorized PLC access
- Pressure readings show unusual fluctuations
- Cyber Av3ngers claim responsibility on social media

### ### Positive/Successful Actions

- Prompt identification and containment of the PLC compromise
- Effective firewall hardening and network segmentation
- Successful reversion of unauthorized changes to water pressure settings
- Transparent communication with the public through a press release

### ### Areas for Improvement

- Initial firewall configuration had gaps that allowed unauthorized access
- Insufficient logging settings on the firewall
- Lack of network segmentation between OT and other networks

### ### Incident Cost Breakdown

- Investigation and response efforts: \$5,000
- Firewall reconfiguration and security enhancements: \$3,000
- Public relations and communication efforts: \$2,000
- Total Cost: \$10,000

### ### Score Deductions

- Initial firewall configuration gaps: -5 points
- Insufficient logging settings: -3 points

### ### Mitre ATT&CK TTPs Used by the Threat

The scenario was based on a simulated threat similar to real-world cyberattacks targeting critical infrastructure. The initial attack vector involved unauthorized access to a PLC, followed by lateral movement and manipulation of control settings.



- **Initial Access:** T1078 - Valid Accounts
- **Execution:** T1203 - Exploitation for Client Execution
- **Persistence:** T1547 - Boot or Logon Autostart Execution
- **Privilege Escalation:** T1068 - Exploitation for Privilege Escalation
- **Defense Evasion:** T1070 - Indicator Removal on Host
- **Credential Access:** T1555 - Credentials from Password Stores
- **Discovery:** T1018 - Remote System Discovery
- **Lateral Movement:** T1021 - Remote Services
- **Impact:** T1489 - Service Stop

## IR Review

### IR Team Performance

An IR plan was not provided for this exercise.

### IR Plan Gap Assessment

An IR plan was not provided for this exercise.

Thank you for participating in this exercise. Your team's efforts in addressing the simulated incident were commendable, and the insights gained will help strengthen your cybersecurity posture. If you have any questions or need further assistance, please feel free to reach out.