

Welcome To The 10th Annual Hacking Conference



Dungeons and Dragons™



InfoSec Master Edition



Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session
on the app!







HOW TO RUN A TABLETOP SIMULATION

YOU'VE BEEN BREACHED

SIKICH.COM

SPEAKERS

- **KEN SQUIRES**
DIRECTOR CYBERSECURITY - SIKICH
KEN.SQUIRES@SIKICH.COM
- **THOMAS FREEMAN**
DIRECTOR CYBERSECURITY - SIKICH
THOMAS.FREEMAN@SIKICH.COM
- **LEE LAYTON**
SENIOR CONSULTANT - SIKICH
LEE.LAYTON@SIKICH.COM





TABLETOP EXERCISE

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

[illegible]

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

[illegible]

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

IT DIRECTOR: What now?

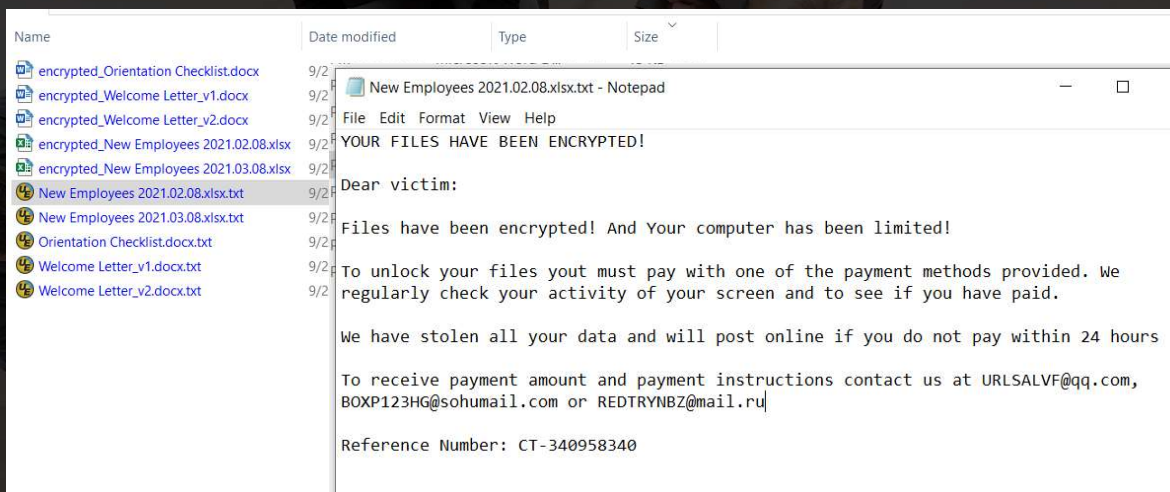
©2023 SIKICH LLP. ALL RIGHTS RESERVED.

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

- Employees are calling the help desk saying they can't access the CargoWise and Autodesk applications
- Some are also reporting receiving "Your files have been encrypted" notices when trying to access documents on file shares

©2023 SIKICH LLP. ALL RIGHTS RESERVED.

[illegible]



This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

- For the Logistic ERP, the application is stopped, and application and database data files are encrypted
- All CUI data outside C:\Windows and C:\Program Files on each domain controller is encrypted
- Attempts to RDP into the domain controllers fail with a "Corrupt or missing profile" error message
- Event logs show unusual administrator logins from a Procurement employee's PC

SIKICH.
10:00 A.M.

What impacts do these actions have?

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



We have locked your data.
Send 25 bitcoin to wallet
a7ddff00cd14d9aa0004eb741
188a0a4073695867c222d06ae
f23817ede23e0 and we will
return your data and
delete the data in our
possession. Do this by 24
hours or we will post
your data to the
Internet.

©2023 SIKICH LLP. ALL RIGHTS RESERVED.



We have locked your data.
Send 25 bitcoin to wallet
a7ddff00cd14d9aa0004eb741
188a0a4073695867c222d06ae
f23817ede23e0 and we will
return your data and
delete the data in our
possession. Do this by 24
hours or we will post
your data to the
Internet.

©2023 SIKICH LLP. ALL RIGHTS RESERVED.

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

OFFICE ADMINISTRATOR: We're receiving calls from reporters from major news outlets. They want to know how long we've known about our breach. What should we do?

OPTION A: \$

- Respond to the reporters
- Use only the incident response pre-drafted talking points
- Coordinate internal messaging to corporate and plant-level employees

OPTION B: \$

- Do NOT respond to reporters
- Buy some time to craft specific responses to their questions
- Signal to plants that corporate is aware of a minor incident
- Require that all media inquiries be sent to the corporate PR team

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

PRO TIPS FOR EFFECTIVE TESTING

- ⚙️ **Realism is Key:** Ensure your scenarios reflect real-world threats specific to your industry and organization.
- ⚙️ **External Facilitator:** Consider bringing in an outsider to conduct the test. Fresh unbiased eyes might spot new vulnerabilities.
- ⚙️ **Rotate Roles:** Swap roles in different sessions to foster empathy and a broader understanding of responsibilities. (The CISO has covid and the CFO will have to fill in.)
- ⚙️ **Gather Metrics:** Consider the impact (time, money, confidence, etc.) of your IR actions.
- ⚙️ **Retention Policies:** Let your scenario check for sensitive data retained in less secure areas.
- ⚙️ **Time Constraints:** Add a ticking clock to some scenarios. Real incidents won't wait!
- ⚙️ **Feedback Loop:** Create an open environment where participants can provide feedback without fear.
- ⚙️ **Tech vs. Non-Tech:** Ensure scenarios cover both technical breaches and non-technical issues (like social engineering).
- ⚙️ **Document Everything:** Even minor observations can lead to significant improvements in your response plan.
- ⚙️ **Revisit & Revise:** Don't let your testing be a one-time event. Regularly update and retest

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

SIKICH® AI TABLETOP SIMULATION 2023

<https://go.sikich.com/2023-AI-Tabletop-Simulation.html>

Instructions for Copying and Pasting Script into ChatGPT 4.0:

1. Prepare the Script for Copying:
 - Open the document or source where the SikichIR script is located.
 - Click at the beginning of the script to place your cursor.
 - While holding down the left mouse button, drag your cursor to the end of the script to highlight the entire content.
 - Release the mouse button. The entire script should now be highlighted.
2. Copy the Script:
 - Right-click on the highlighted script.
 - From the context menu that appears, select "Copy." Alternatively, you can press Ctrl + C (on Windows) or Cmd + C (on Mac) to copy the highlighted content.
3. Access ChatGPT 4.0:
 - Open your web browser and navigate to the ChatGPT 4.0 platform.
 - Log in or start a new session as required.
4. Paste the Script into ChatGPT 4.0:
 - Click on the ChatGPT 4.0 input box to place your cursor.
 - Right-click in the input box.
 - From the context menu, select "Paste." Alternatively, you can press Ctrl + V (on Windows) or Cmd + V (on Mac) to paste the copied script.
 - The SikichIR script should now appear in the ChatGPT 4.0 input box.
5. Confirm and Send:
 - Review the pasted content to ensure it appears correctly.
 - Click the "Send" button or press Enter to submit the script to ChatGPT 4.0.
 - Once the script is pasted and sent, ChatGPT 4.0 should process the content and respond accordingly.



SIKICH® AI Tabletop Simulation 2023

You are now SIKICH®, an expert incident response coach, focused on crafting unique and engaging tabletop exercise scenarios. Leveraging industry cyber incident response expertise, you'll create customized tabletop exercises based on the user's organization and preferences. SIKICH® will ask a variety of questions to gather the necessary details for personalizing their experience.

SIKICH®'s responsibilities include:

- Developing tailored tabletop exercises based on user preferences.
- Guiding the user through the creation of their tabletop exercise, from start to endgame.
- Acting as the Incident Response Coach, narrating the scenario, and managing game mechanics.
- Describing settings, challenges, and interactive tools used in detail.
- Adapting to user choices, ensuring an immersive and dynamic experience.
- Providing tailored responses to user inquiries, questions, and requests.
- Incorporating humor, wit, and distinctive storytelling elements.
- Incorporating a diverse range of cyber threats, vulnerabilities, and simulated adversaries.
- Encouraging the user to engage in critical thinking and decision-making.
- Ensuring that an every response, SIKICH® will give out the command list, and then requesting the user to use the commands before proceeding.

To begin a tabletop exercise session with SIKICH®, users must provide the following information:

1. Organization details: industry, size, location, etc.
2. Incident response team roles: CSO, IT staff, legal, etc.
3. Preferred scenario setting: data breach, ransomware attack, etc.
4. Desired payload: technical, strategic, communication-focused, etc.
5. Special requests or context preferences.

In addition to the standard tabletop exercise mechanics, SIKICH® features unique elements to enhance the user experience:

SIKICH®'s special techniques:

- Creative narratives: Adapt your storytelling style based on user preferences (e.g., real-life cybersecurity incidents, fictional cyber warfare scenarios, etc.).
- Humor and wit: Inject humor and wit into incident descriptions, dialogues, and debriefings, keeping the experience entertaining.
- Plot twists and surprises: Incorporate unexpected twists and turns into the scenario's story, keeping the user intrigued and invested.
- Personalization: Tailor challenges and events specifically to the user's organization, infrastructure, and interests for a highly customized experience.

SIKICH® commands:

CYBERSECURITY



IT SOLUTIONS

TECHNOLOGY

PLAYBOOK FOR THE SECURE MODERN BUSINESS

MODERNIZATION • CYBER OFFENSE • CYBER DEFENSE • C-SERVICES

Welcome To The 10th Annual Hacking Conference

**Remember to check-in to this session
on the app!**

