Webs of Deception: Using the SANS ICS Kill Chain to Flip the Advantage to the Defender

By: Oren Niskin

1.1 Introduction

In their OT Cybersecurity 2023 Year in Review, Dragos identified nation-state actors targeting critical infrastructure [2]. At the same time, businesses are connecting their previously isolated industrial networks to capitalize on the enormous opportunities presented by digitizing the plant floor. As these trends continue, how can small ICS operators defend their industrial processes from adversaries backed by nation-state resources?

"Industrial control systems" (ICS, interchangeably referred to as "Operational Technology," OT) are digital systems that control and automate physical processes and machinery [3]. These include municipal water treatment, electrical generators and distribution substations, chemical manufacturing, oil drilling rigs, ship navigation and machinery, building elevators, and amusement park rides. While traditional information technology cybersecurity programs focus on protecting data confidentiality, integrity, and availability, ICS security focuses on industrial safety and process availability [3].

1.2 Criticality of Small ICS Organizations

Small ICS operations dominate critical infrastructure. Of the 11,128 chemical facilities in the United States, 68% are operated by organizations with fewer than 500 employees [4]. Likewise, the National Association of Manufacturers states that 41% of manufacturing workers are employed in firms with fewer than 500 employees [5]. There are 26,727 "very small" community water systems in the United States, each serving less than 500 customers [6]. The safety of our communities relies on protecting these small industrial sites.

1.3 Hypothesis

Advanced Persistent Threats (APTs) are well-funded, well-trained, and patiently persistent. However, the nature of a small and local ICS operator results in key advantages over a large APT that is thousands of miles away. First, smaller organizations know their users and systems. Second, the owners, operators, and maintainers often live near their industrial facilities. In contrast, the APT must discover and map the target industrial system remotely by relying on a two-dimensional computer screen in a building across the globe– posing a significant challenge to the attacker.

While the APTs may possess all the advantages of capability, time, and money, they are still forced to accomplish specific objectives before achieving their mission. Effective targeted ICS attacks require access to the ICS devices and deep technical knowledge of the system.

This research hypothesizes that small ICS operators can deploy deception techniques to several high-leverage choke points to deceive attackers into revealing their presence earlier in the attack chain. When operating in an industrial environment, this additional response time results in safer and less disruptive response actions.

2 Research Method

2.1 Description of the Lab Environment

A representative architecture of a small industrial organization was developed to test the hypothesis. The lab consisted of an Automation Direct Click Plus Programmable Logic Controller (PLC), a Human Machine Interface (HMI), an engineering workstation (EWS), a pfSense virtual firewall, an Industrial DMZ server, and an Enterprise Domain Controller. The PLC kit was part of the ICS515 course from the SANS Institute. In the SANS ICS515 course, the kit runs a simulated industrial process for the fictional city of Calistoga [8].

An Intel NUC ran VMware Workstation Pro and housed the virtual machines. This lab environment formed a representative secure ICS network architecture based on the IEC62443 standard or Cisco and Rockwell Automation's Converged Plantwide Ethernet (CPwE) design guide [9].

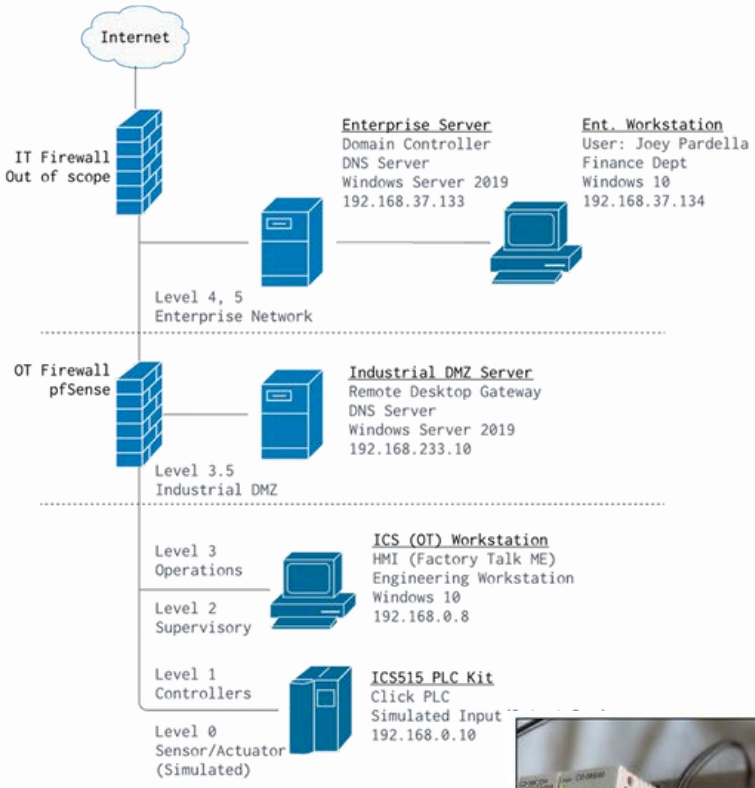

Figure 1: ICS Lab Infrastructure

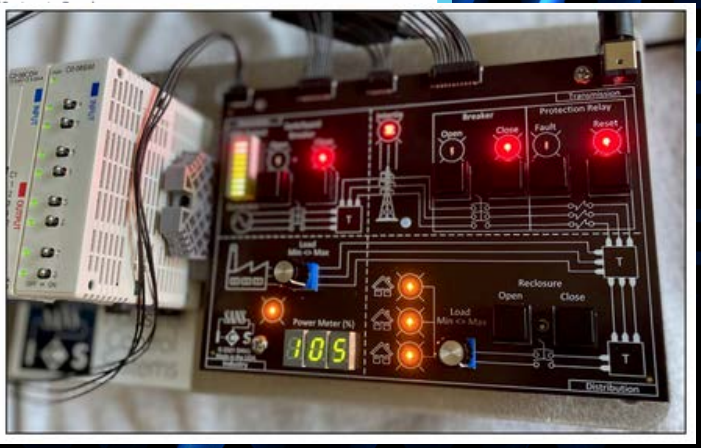

Figure 2: SANS ICS515 Course Kit [8].

2.2 Points of Maximum Leverage

As mentioned, the APT is typically thousands of miles away and has limited knowledge of the defender's ICS network. Drawing on this advantage, the following maximum-leverage points were identified:

1. Pivot from Enterprise (IT) to ICS network. Attackers must first locate and gain access to the ICS to successfully impact the ICS.
2. Exfiltration of technical documentation or data to plan a targeted attack. ICS processes have thousands of values and setpoints. Manipulating the process meaningfully requires deep technical knowledge of the system's configuration and operation.

These points on the ICS attack chain were chosen for two reasons. First, they are common to all ICS attacks. Second, they offer multiple opportunities to detect an ICS-related attack activity before the ICS is accessed.

3 Use of Deception

Cybersecurity defense philosophy has matured over the last three decades in a gradual expansion of defense-in-depth. Network segmentation and firewalls were followed by security monitoring and detection. Despite the increased difficulty, sophisticated attackers could bypass the firewall and avoid detection.

To counter these new sophisticated threats, Lockheed Martin created their Kill Chain. The Lockheed researchers found that attackers follow a sequence of steps to achieve their objective [10]. Equally important, the Lockheed researchers identified six possible "courses of action" available to defenders at each attack step: deny, detect, deceive, disrupt, degrade, and destroy. Splitting the attack into multiple steps and implementing multiple actions at each step offered defenders more opportunities to spot an attack.

Defenders can deploy attractive lures throughout the environment to use the deception course of action. While not useful to a legitimate user, these resources would be attractive to an attacker snooping around the network. If convincing enough, the adversary will interact with the decoy user, file, or system, raising an alert.

Webs of Deception: Using the SANS ICS Kill Chain to Flip the Advantage to the Defender *(cont'd)*

As shown in Figure 3, implementing more "courses of action" created more opportunities to detect the attack. Layering courses of action adds complexity to the attack chain. Each layer adds new opportunities to block or detect the attacker while only adding a small cost to the defender.

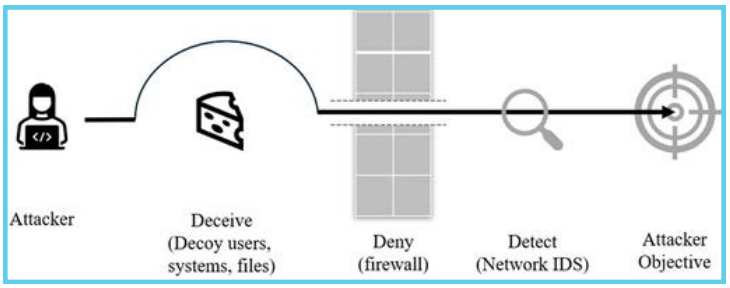

Figure 3: Layering additional "courses of action" from the Cyber Kill Chain.

As an added benefit, even if the attacker detects the deception techniques, the mere knowledge of their presence may slow and deter activity for fear of tripping over a decoy and being detected. This secondary effect can raise the cost of an attack or cause attackers to withdraw [11].

3.1 Deception Prerequisite Recommendation

Before implementing deception as a course of action, ICS defenders should have basic security controls in place. The ICS network should be segmented from the IT network with a firewall. ICS defenders should restrict remote access and require Multifactor Authentication. Next, defenders should monitor ICS network traffic for threats and anomalies. These three ICS practices improve security and operational resilience and form the bedrock of the SANS Five Critical Controls for ICS [12].

Once the ICS network has been segmented, remote access is restricted, and network monitoring deployment has started, defenders can start using deception to complement these controls.

3.1.1 Infrastructure Assumptions

The research assumes:

- The organization has Windows Event Log monitoring and forwarding from workstations and servers to a central location where alerts are generated for the security team.
- The organization uses Active Directory to manage Enterprise IT users and computers.

These precise capabilities are not required. Many alternatives exist to employ the same defense techniques for other Identity Providers, and modern endpoint agents can monitor event logs on the host.

3.2 Decoy 1: Honey OT Jump/Remote Access Hosts

To successfully target an ICS for attack, the adversary must locate and access ICS devices. The first decoy is a jump host that appears to bridge the IT network to the ICS network. Engineering and Maintenance Departments sometimes install a jump host with two separate network cards. One network card connects to the IT network, and the second connects to the ICS network, allowing engineering staff to access the ICS network from their IT workstation. These dual-homed jump hosts are a significant security hole but are also extremely common in ICS deployments. These jump hosts have been used as a quick shortcut for threats to reach OT without detection.

MITRE identifies 36 adversary techniques involving jump hosts in ICS, illustrating their central position in adversary activity. During the 2015 and 2016 Ukraine Electric Power Attacks and the Triton Safety Instrumented System Attack, access to the ICS devices was obtained through jump hosts [13].

If the decoy jump host is convincing, even sophisticated APTs would be tempted to interact with it. A new Windows 10 virtual machine was deployed and joined to the Enterprise IT domain to serve as a decoy jump host. This created a new computer object in Active Directory that APTs will quickly identify upon initial access to the IT network. Figure 4 shows the result of running

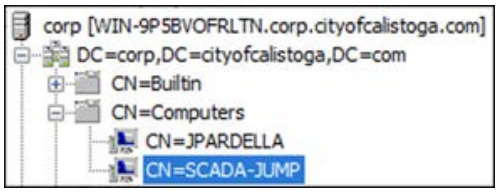

Figure 4: Decoy Jump Host in Active Directory Explorer

Note that a dual-homed jump host residing in the IT network is a poor security practice. The jump host in this example is only a decoy. However, for an attacker targeting ICS systems, this computer object looks extremely attractive.

To make the decoy convincing, the defender must ensure the attributes do not mark the asset as an obvious decoy. As shown in Figure 4, if the system is joined to the domain and never accessed, the lastLogon and loginCount variables will be suspicious. Attackers may also avoid the system if a computer object has a passwordLastSet attribute over 30 days old. Computer passwords in Active Directory are rotated every 30 days by default [14].

isCriticalSystemObject	Boolean	1	FALSE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	11/27/2024 12:51:56 PM
lastLogonTimestamp	Integer8	1	11/27/2024 12:51:50 PM
localPolicyFlags	Integer	1	0
logonCount	Integer	1	2
msDS-SupportedEncryp...	Integer	1	28
name	DirectoryString	1	SCADA-JUMP

Figure 5: lastLogon and logonCount computer attributes in Active Directory.

To detect attacker attempts to access the decoy, defenders can monitor their DNS logs for mention of the decoy's hostname. Since the host has no legitimate purpose, any attempt to access the host should be investigated. The command below continuously monitors the Windows Server DNS log file and returns a result when the string "scada-jump" is seen.

```
PS C:\Users\Administrator> get-content
C:\Windows\System32\dns\dns.log -Wait |
Select-String "scada-jump"
12/11/2024 2:46:49 PM 1280 PACKET
000001E3B969A5A0 UDP Rcv 192.168.37.134
6ef0  Q [0001D  NOERROR] A
(10)scada-
jump(4)corp(15)cityofcalistoga(3)com(0)
```

Webs of Deception: Using the SANS ICS Kill Chain to Flip the Advantage to the Defender *(cont'd)*

The attacker will trigger an alert if any network connection is attempted, including the ping command, Remote Desktop (RDP) connection, and Server Message Block (SMB) file share connection.

3.3 Decoy 2: Honey Files

The second decoy is comprised of fake files that appear to disclose sensitive data about the ICS. The files may appear to describe the industrial process or expose secrets. For example, a file describing a turbine generator's safety limits and another file with an electrical schematic of the generator's safety instrumentation would be valuable information for someone seeking to harm an ICS.

Targeted ICS attacks against a well-engineered system require bypassing the safety limits put in place to protect the industrial process. At the same time, the attackers must avoid detection by hiding the dangerous process state from control room operators. To achieve these two objectives, attackers must manipulate lower-level components of the process in an extremely specific manner.

Industrial processes can contain thousands of variables to manipulate. There are also countless interlocks, alarms, system trips, and fail-safes.

Stuxnet is an example of a targeted ICS attack that succeeded in causing physical damage. To facilitate planning the Stuxnet attack, exact specifications, schematics, and bills of material were exfiltrated from the target organizations using a separate targeted malware called Duqu. The malware searched for specific file types and uploaded them to the attacker's command and control servers [15]. The attackers then used the information in the exfiltrated files to replicate the target control system for Stuxnet's ICS attack development testing, increasing the probability that the complex attack would be successful [16].

ICS defenders can be creative when crafting their web of decoy files. Using the SANS ICS Kill Chain, defenders can place enticing decoy files that appear to offer critical information to the next stage of the attack.

Following John Strand's instructions in his short video "*Honey Files, Canary Tokens, & SIEMS, Oh My!*" an enticing file was created named "Remote Access Procedure.txt." File auditing was then added for "Everyone." This will generate an audit log entry each time the file is accessed, opened, copied, or written to [17].

Turning this setting on for commonly used files would quickly fill the Event Log with audit log entries. However, setting this attribute on a few specific files that legitimate users should not access will create minimal log entries.

Figure 6 shows the audit log entry in the Windows Event Log resulting from when the file was copied to another folder for exfiltration. The small ICS operator can monitor for Windows *EventID 4656* and the filename string using their security monitoring tools.

Since no legitimate user needs to access these files, security teams should investigate any user attempting to access these files. The security team can tune the placement strategy of these files to minimize false positives of people clicking on them by accident or to satisfy curiosity.

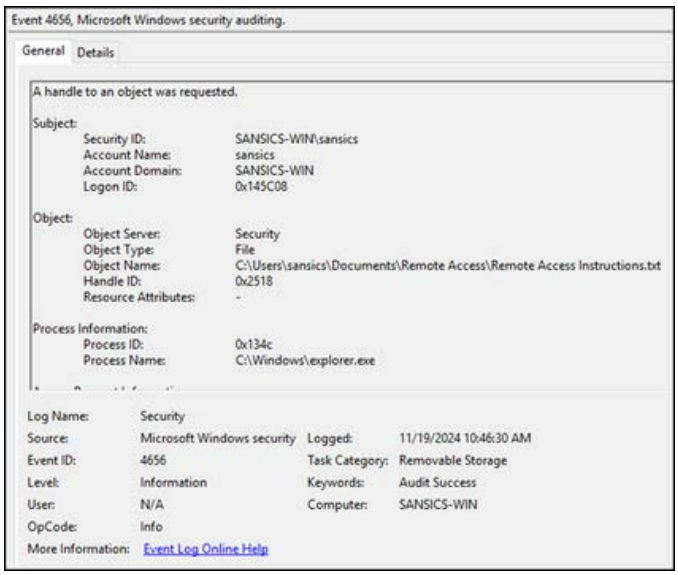

Figure 6: Event Log entry generated when anyone accesses or copies the honey file.

3.4 Decoy 3: Honey Users or Service Accounts

The third decoy is a fake Enterprise (IT) user in Active Directory who appears to have access to ICS privileges. As discussed, security and operations teams should carefully control remote access into the ICS network. Access should be limited to a designated user group, making it feasible for a small ICS to implement a decoy user account.

MITRE ATT&CK for ICS identifies seven APT campaigns that used valid credentials in ICS attacks, including Ukraine Electric Power Attacks, BlackEnergy, and the Triton attack [13]. Valid credentials are attractive for sophisticated threats since their use is difficult to detect by standard security tools. Once valid user accounts are obtained, the threat does not need a vulnerability or malware-based remote access trojan (RAT) to access the victim. Instead, they can log in using the victim's approved remote access systems.

For example, in the 2015 cyber-attack on Ukraine's power grid, attackers used BlackEnergy malware to breach the external network. Once inside, the attackers stole credentials for a valid user, which they used to move laterally until they were ready to execute their attack [18].

Figure 7 shows IT Active Directory users in the "Engineering" Organizational Unit (OU). A variety of users were created in the IT Active Directory database. One of them, Emmanuel Goldstein, was created as a decoy and joined the "Engineering" OU and the "Remote Access" group.

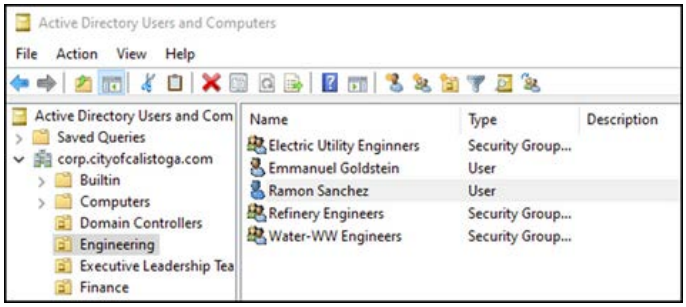

Figure 7: Decoy user embedded in Engineering Organizational Unit (OU).

An APT seeking remote access to the ICS network would be highly tempted to interact with users in a group with ICS privileges. Interacting with the decoy user would result in an alert of attempted unauthorized remote access. However, the user account must be convincing and believable to be an effective lure. For example, the account should not be disabled, the last logon time should be reasonable, and the user should be a member of a convincing group.

As seen in Figure 8, when the attacker attempted to log in as the honey user, *EventID 4625* was created for using an "unknown username or bad password." A successful login, which is also suspicious, raised *EventID 4624*.

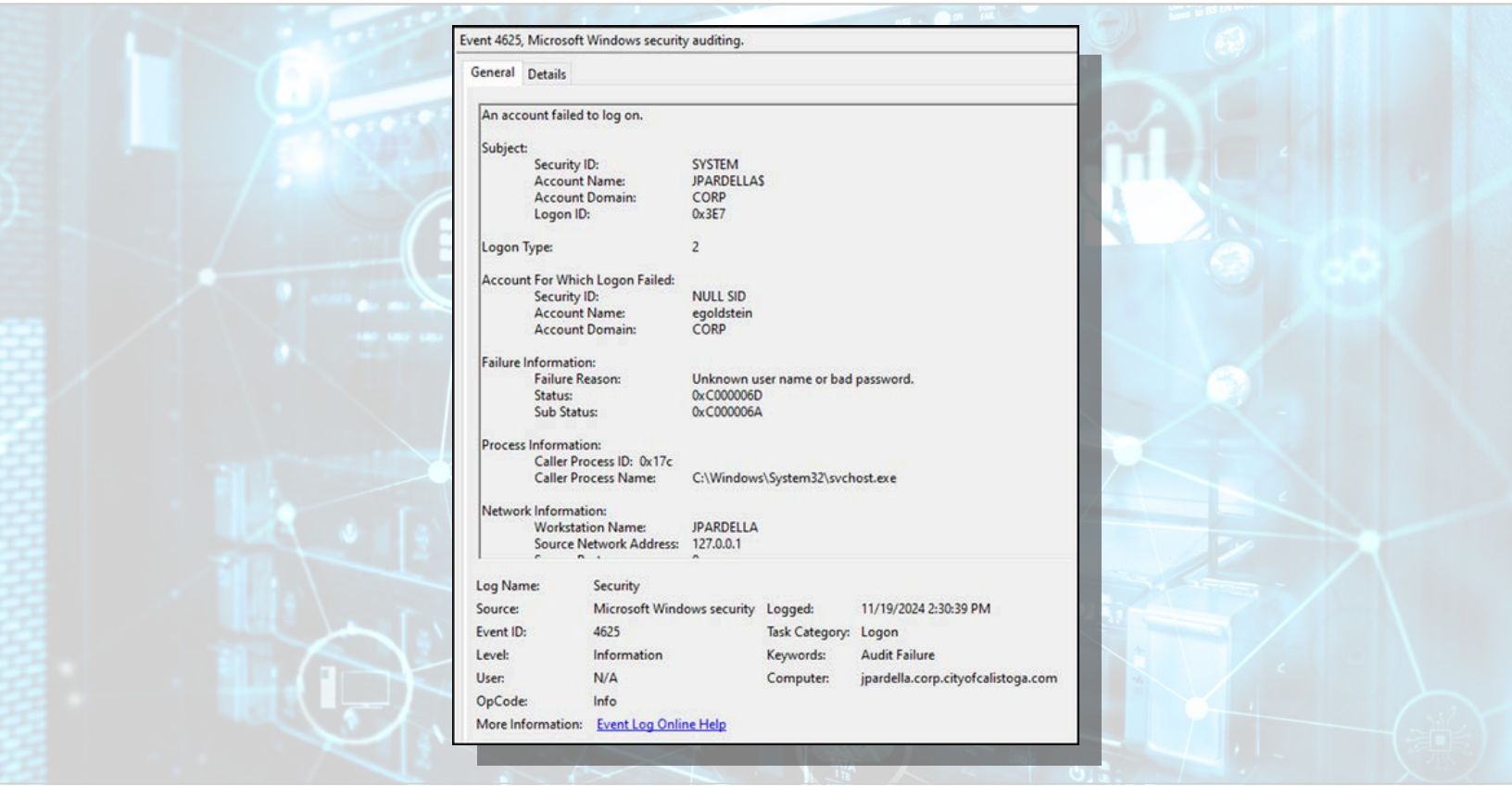

Figure 8: An audit log entry was created for the failed login attempt.

4 Recommendations and Implications

During the research process, several high-leverage opportunities were identified for the defender. These security controls are relatively simple for the defender to deploy and monitor while adding new opportunities to detect the attackers before they can harm the industrial process.

4.1 Incorporate into Security Operations

The detections shown in this research reside in logs on the specific endpoint under attack, like the engineering workstation. The organization should incorporate these logs into its centralized monitoring workflow.

4.2 Incorporate into Security Assessments

Like any security control, deception techniques should be continuously assessed and improved. Incorporating the deceptions into the organization's next penetration test can illuminate which decoys were effective and which were detected as decoys by the adversary. Penetration testers can provide insights into how to make the decoys more enticing or convincing.

4.3 Share with the Community

Lastly, small ICS defenders can increase their leverage against sophisticated threats by combining forces through sector Information Sharing and Analysis Centers (ISACs).Limited sharing of deception strategies across several organizations can multiply detection opportunities, as sophisticated threats often execute campaigns against multiple targets in a sector.

4.4 Implications for Future Research

This paper explored the practical use of deception by defenders of small ICS organizations and identified high-leverage opportunities to even the playing field with the modern APT.

Future research can expand to include additional high-leverage detection opportunities along the Kill Chain. Likewise, future research can include additional courses of action beyond deny, detect, and deceive. The remaining courses of action listed in the Cyber Kill Chain are degrade, disrupt, and destroy. The probability of detecting attacks increases as additional defensive courses of action are employed for each step in the Cyber Kill Chain [10].

Webs of Deception: Using the SANS ICS Kill Chain to Flip the Advantage to the Defender *(cont'd)*

5 Conclusion

Incorporating deception into an ICS security program creates opportunities to detect ICS attacks early, before the attackers have reached the industrial networks. Basic security controls, like firewalls and secure remote access, combined with deception techniques like honey systems, honey files, and honey users, can flip the advantage from the APT to the ICS defender, reinforcing Rob M. Lee and Michael Assante's declaration that "Defense is doable." [1]

6 References

[1] Rob M. Lee and Michael J. Assante, "The Industrial Control System Cyber Kill Chain," Oct. 2015. Accessed: Apr. 05, 2025. [Online]. Available: https://www.dragos.com/resources/reports/2023-ot-cybersecurity-year-in-executive-summary/
[2] "Dragos 2023 OT cybersecurity year in review executive summary," Feb. 2024.
[3] G. Murray, M. Johnstone, and C. Valli, "The convergence of IT and OT in critical infrastructure," in Australian Information Security Management Conference, Perth: Edith Cowan University, Dec. 2017, pp. 149–155.
[4] Cybersecurity and Infrastructure Security Agency, "Chemical sector profile," 2022. Accessed: Apr. 05, 2025. [Online]. Available: https://www.cisa.gov/resources-tools/resources/chemical-sector-profile
[5] National Association of Manufacturers, "Facts about manufacturing," Apr. 2024. Accessed: Apr. 05, 2025. [Online]. Available: https://nam.org/manufacturing-in-the-united-states/facts-about-manufacturing-expanded/
[6] Center for Sustainable Systems, "U.S. Water Supply and Distribution Factsheet," 2024.
[7] Cybersecurity and Infrastructure Security Agency, "Water and Wastewater Systems." Accessed: Apr. 05, 2025. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/water-and-wastewater-sector
[8] R. M. Lee, "ICS515: ICS Visibility, Detection, and Response," SANS Institute. Accessed: Apr. 05, 2025. [Online]. Available: https://www.sans.org/cyber-security-courses/ics-scada-security-essentials/
[9] Cisco and Rockwell Automation, "Securely traversing IACS data across the Industrial Demilitarized Zone: Design and implementation guide (ENET-TD009C-EN-P)," 2022. Accessed: Apr. 05, 2025. [Online]. Available: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
[10] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," Leading Issues in Information Warfare & Security Research, vol. 1, no. 1, 2011.
[11] E. A. Cranford, C. Gonzalez, P. Aggarwal, M. Tambe, S. Cooney, and C. Lebiere, "Towards a Cognitive Theory of Cyber Deception," Cogn Sci, vol. 45, no. 7, Jul. 2021, doi: 10.1111/cogs.13013.
[12] R. M. Lee and T. Conway, "The five ICS cybersecurity critical controls," Nov. 2022.
[13] MITRE, "ATT&CK, Assets, Jump Host." Accessed: Apr. 05, 2025. [Online]. Available: https://attack.mitre.org/versions/v16/assets/A0012/
[14] V. Pamnani, "Domain member maximum machine account password age - Windows 10," Microsoft Learn.
[15] E. Chien, L. OMurchu, and N. Falliere, "{W32. Duqu}: The Precursor to the Next Stuxnet," in 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET 12), San Jose, Apr. 2012.
[16] W. J. Broad, J. Markoff, and D. E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," New York Times, Jan. 15, 2011. Accessed: Apr. 05, 2025. [Online]. Available: https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html
[17] J. Strand, "Honey Files, Canary Tokens, & SIEMS, Oh My! | John Strand | BHIS Nuggets," Black Hills Information Security. Accessed: Apr. 05, 2025. [Online]. Available: https://www.youtube.com/watch?v=6cs_Z9KDWbo
[18] E-ISAC, R. M. Lee, M. J. Assante, and T. Conway, "Defense use case: Analysis of the cyber attack on the Ukrainian power grid," Washington, DC, Mar. 2016.

About the Author

By: Oren Niskin

Oren Niskin is an industrial cybersecurity expert in Houston with over 20 years of experience from the plant floor to the data center. He has successfully guided manufacturing, maritime, and energy organizations through cybersecurity transformations.