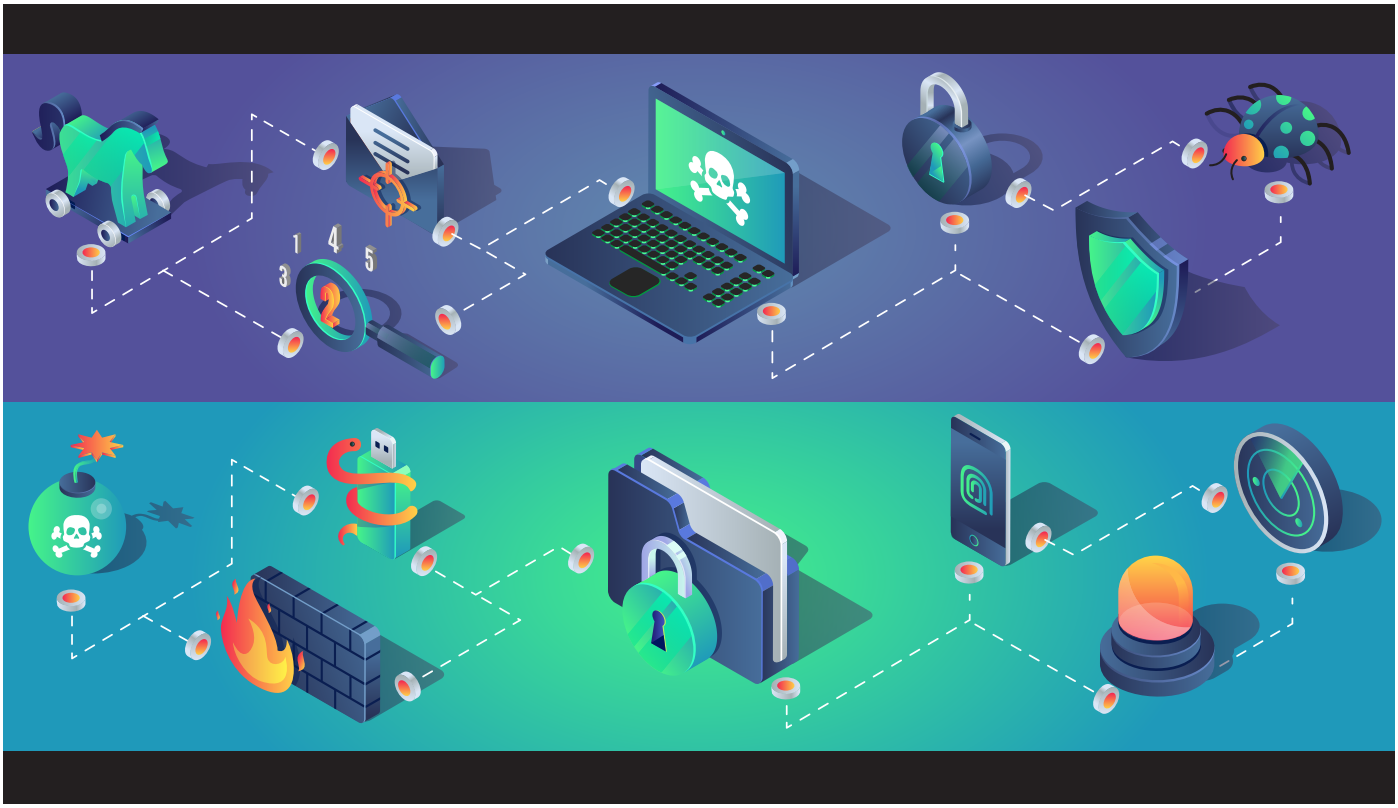
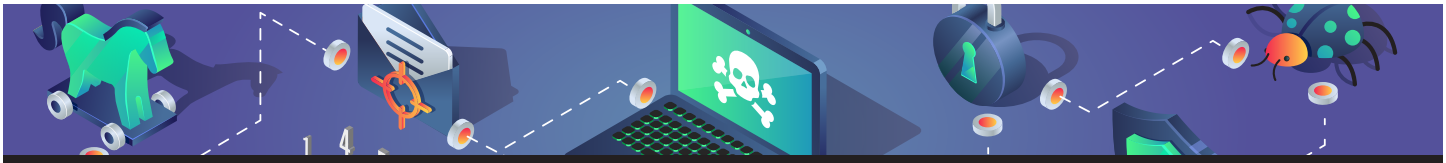
EPRI | ELECTRIC POWER RESEARCH INSTITUTE

DECEPTION TECHNOLOGY

Emerging Cyber Security Technology for Utilities



October 2019



Executive Summary

Deception technology is a relatively new class of products that change an adopting utility's defense stance from reactive to proactive. Current utility cyber security strategies engage in traditional protect/detect/respond activities for operations technology (OT) environments. This is a reactive defense posture, and even activities such as threat hunting are akin to searching for a needle in a haystack.

Deception tech functions as a powerful magnet. Put one or more magnets anywhere on the haystack, and all needles will find their way to them. This product category also has promise to reduce security vulnerabilities and improve security resource productivity by reducing false-alarm volume and focusing attention on high-confidence alerts.

There are many practical unknowns about the technology in terms of the appropriate design and placement of lures and decoys to deliver high-fidelity alerts. Hands-on experience in deception tech, gained through collaborative research and knowledge sharing, can help utilities understand how to reduce security risks and vulnerabilities in their OT environments and provide practical knowledge to guide these procurement decisions.

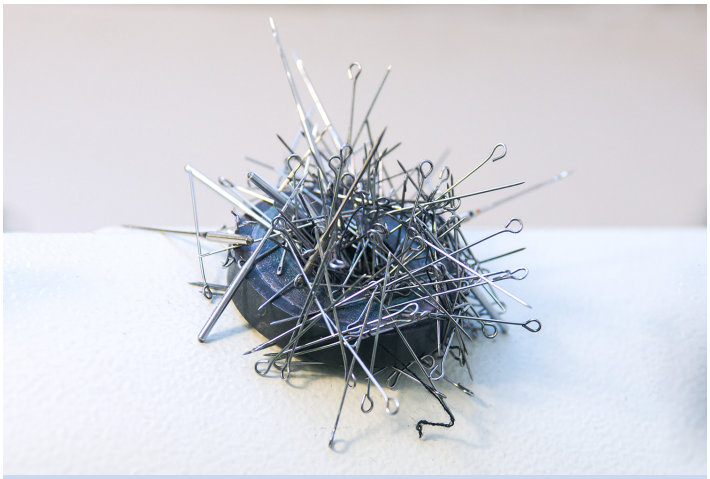


Figure 1 – Deception tech lures and decoys act as magnets to draw attackers away from real assets, applications, and data.

Introduction

Electric utilities face an ever-changing series of threats based on vulnerability exploits, persistent attacks, and inadvertent and malicious compromises of identity and authorizations. While advanced grid initiatives offer many benefits to utilities and their customers, they also expand attack surfaces as new utility components are communications enabled and connected to private and/or public networks.

There is also an extensive list of consequential threat actors intent on inflicting maximum economic and societal harm by compromising the reliability and safety of critical infrastructure like electric grids. The 2015 Ukraine incident is a sobering example of the damage an educated and determined attacker can inflict on grid operations.

Utilities have engaged in a variety of security strategies and tactics to reduce their vulnerabilities to attack. Their cyber security teams have identified and mitigated vulnerabilities, deployed solutions to monitor activity on critical assets, and conducted exercises to test their own cyber defenses. Nevertheless, the consensus is that it is a matter of when, not if, any utility will experience a serious attack with potential to compromise the safe and reliable delivery of electricity.

The Electric Power Research Institute (EPRI) cyber security research programs help utilities understand and mitigate risks in operations technology (OT) environments. EPRI researchers often evaluate new technologies for their applicability to unique utility OT requirements, with their primary focus on production availability of mission-critical assets. These new technologies may first deploy in other business sectors, providing the electric sector with opportunities to examine and investigate them without committing valuable funds.

Table of Contents

This white paper was prepared by EPRI.

A new potential tool in utility cyber security plans is deception technology. This EPRI white paper examines the state of the art in deception technology, outlines its potentials for utilities, and offers guidance to vendors seeking to supply solutions to electric utilities.

The Basics of Deception Technology

Deception technology is defined as a set of capabilities that:

- Enhance threat detection functions through lures and decoys that serve as early warnings
- Deliver proactive defense functions that misdirect attackers and quarantine or "sandbox" them to discover security vulnerabilities and study attack methods

Deception technologies can be on-premise products or provisioned as services. In this paper we typically refer to the technologies as products, but that is not intended to exclude service options from utility procurement decisions. Deception tech solutions are sometimes compared to "honeypot" solutions, which are commonly deployed within Information Technology (IT) environments in all business sectors, including utilities. A honeypot is a mocked-up version of the real IT environment. It mimics the profiles of attractive assets to lure attackers away from the real systems. To be effective, honeypots need to operate with realistic amounts of data traffic that model typical patterns of activity. For example, if a real email server handles a million emails a day, a honeypot email server that only manages 20,000 emails a day for a limited number of email addresses will look out of place to an experienced hacker. Further, honeypots are static solutions. Unless they are frequently tended with changes in data traffic and patterns of activity, attackers can identify them and avoid them.

One of the primary distinctions between deception tech and honeypots is their degree of real-time, dynamic responsiveness. Honeypots lack true interactivity to engage an attacker and to provide a sandbox environment for safe engagement with attackers. To oversimplify, deception technology could be considered an interactive and intelligently enhanced honeypot. Different deception tech vendors' solutions also have different degrees of interactivity. The more dynamic solutions require more configuration and computing power in order to deploy and create responses and actions similar to those of the real assets, thus deceiving attackers. More dynamic deception tech solutions may mimic a smaller number of virtual systems as a consequence of the "heavier lift" of modeling real conditions.

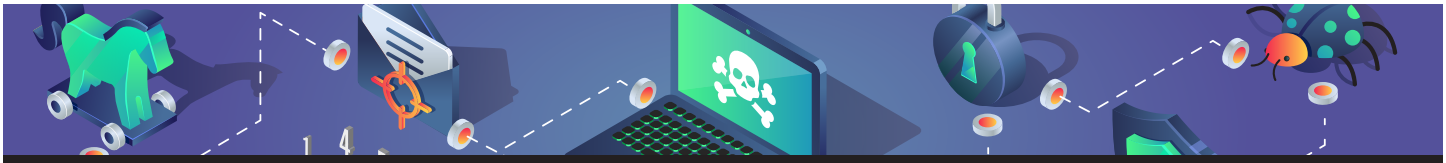
Deception tech is primarily situated in lures and decoys embedded in networks and at endpoints. Deception tech solutions take on an "active defense" role when perimeter defenses are compromised or breached. These solutions can send alarms to existing security operations centers (SOCs) for action. Deception technology alarms are considered "high confidence" within SOC environments that routinely receive hundreds of thousands of alarms daily.

Deception technology consists of the following components:

- **Breadcrumbs**. These are data and applications planted to lead attackers towards lures and decoys. In this document, references to lures include breadcrumbs.
- **Lures**. These are fake Internet Protocol (IP) addresses, servers, or other assets designed and deployed to deliberately lead attackers away from real production environments and into deception artifacts. These are the first line of defense in deception tech.
- **Decoys**. These are assets such as networks or virtual local area networks (LANs) designed and deployed to emulate real environments. Decoys should appear authentic in terms of traffic flow to real systems.

Table 1. Comparison of common characteristics of deception tech and honeypots.

Deception Tech	Honeypot
Emulates data, assets, and networks for proprietary systems	Mimics data, assets, and networks
Includes dynamic interactions and responsiveness to avoid identification as fake	Is static or less capable of realistic interactions
Leverages AI and machine learning to support realistic emulations and appear "lifelike"	Needs frequent manual updates to avoid "fingerprinting" and appear "lifelike"
Plays active defense role that can build knowledge about attacker techniques, tactics, and procedures (TTPs)	Plays reactive defense role that misdirects attackers and alerts organization to intrusion
Operates within the security perimeter	Operates outside the security perimeter



- **Sandbox**. A safe environment where attacker tools like malware can be examined. Deception tech "active defense" capability typically means that the product or service includes a sandbox.

Deception technology products are deployed to detect, analyze, and defend against attacks in real time. They are most effective when tailored to be network specific. By emulating the production environment traffic, they can detect intrusions and alert the network's security team to enact proactive defense measures. Sandbox environments allow security teams to learn about attackers' TTPs, identify vulnerabilities, and plug gaps in defenses.

Deception technologies are used in a number of business sectors, but are traditionally deployed in IT environments, where data integrity is of utmost importance. The financial services sector makes the most publicized use of deception tech, and government agencies are adopters, too. For instance, Sandia National Labs developed a solution called High-Fidelity Adaptive Deception and Emulation System to protect their sensitive nuclear data from advanced persistent threats (APTs) driven by nation-states and other well-organized entities.

Deception tech may be best positioned to detect APTs and zero-day attacks.

Various market forecasts are bullish on growth for deception tech. These forecasts cover all sectors and are not predictors solely for electric utilities. FBR Capital Markets pegs the market to grow to $3 billion by 2019. MarketsandMarkets forecasts market size at $2.09 billion by 2021. There is real promise that deception tech may be best positioned to detect APTs and zero-day attacks, both on the increase for business sectors around the world. However, forecasts also reflect some challenges that may hinder adoption of deception tech. These are:

- Technological complexity of solutions
- Financial justification ambiguities
- Misunderstandings of how to apply these solutions
- Lack of skilled resources to deploy and manage the solutions

Deception Technology Solutions Scan and Analysis

EPRI identified suppliers of deception technology solutions and verified the solutions that are targeted or marketed to industrial control systems (ICS) or OT environments. Some solutions may currently be deployed in utilities, but for sensitivity reasons discussed later, these deployments are not identified. Other suppliers may have OT-oriented solutions or solutions deployed within utilities, but there is no public information available to date that could be used to confirm or validate either point. There are many other vendors with deception technology solutions that focus solely on a specific business sector or are strictly IT network solutions.

As a general rule, deception tech can address different security layers: network security, endpoint security, application security, and data security. This solution scan does not identify whether solutions tackle one or more layers, although a majority of solutions tend to focus on network security.

It is important to note that ICS and utility OT environments have unique conditions. Therefore, EPRI emphasizes that in evaluating any vendor solution, a utility must account for familiarity with supervisory control and data acquisition (SCADA) systems and the high-risk assets in utility networks. Here are the most important distinctions:

- ICS and utility OT systems depend on completely different network protocols than IT systems. The network topology and network traffic will often look different from those of an enterprise space, so ICS or utility OT experience is critical to mislead and deceive a well-educated and motivated attacker seeking to disrupt these systems.
- Embedded systems often look different from enterprise systems as well, and may be more complicated to emulate than simply copying the web page of a back-end system.
- Many utility systems are not designed to be scanned or actively probed, which is the approach taken by some intrusion detection products. In addition, some assets cannot support agents.

Deception technologies have the potential to solve those challenges for utilities, but vendors must have sufficient knowledge of and experience with operational constraints to be effective in utility OT environments.

Each vendor description includes:

- Name of company and link to website
- Name of product
- Use case/experience/interest in ICS and/or utilities
- Technology partners (of interest for data integration)

Acalvio: ShadowPlex. The company identifies applications for ICS environments. The website mentions but does not name a number of partnerships with companies including cloud, network access control (NAC), security information and event management (SIEM), and security orchestration, automation, and response (SOAR) vendors.

Attivo Networks: ThreatDefend Platform™. The company has an energy utility case study and expresses familiarity with SCADA environments and OT scenarios. The website publicizes a number of partnerships with companies including cloud, NAC, SIEM, and SOAR vendors.

Cymmetria: MazeRunner and ActiveSOC. In early September, the company was acquired by a private equity firm that specializes in turnarounds, which may indicate strategic changes on the horizon. The website notes deception capabilities for SCADA environments. It publicizes a number of partnerships with companies including cloud, threat intel, SIEM, and SOAR vendors.

Illusive Networks: Platform of three products—Attack Surface Manager, Attack Detection System, and Attack Intelligence System. Case studies include manufacturing, but the website provides no specifics on ICS or SCADA familiarity. It indicates partnerships with vendors of several SIEMs and other security products.

Smokescreen: IllusionBLACK. This company has white papers and use cases targeted to SCADA and ICS environments, demonstrating a depth of familiarity with SCADA environments. The website does not mention any partnerships.

TrapX: DeceptionGrid™ 6.3. This company identifies ICS and utilities as two target markets. It partnered with Rockwell and Siemens to create decoys of their industrial controllers. The company has an interesting "deception community" where customers can share countermeasures and custom traps. It has partnerships with SIEM and SOAR vendors.

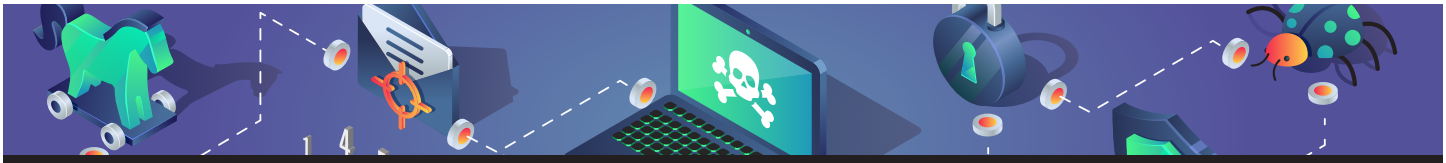
Acalvio and Attivo were interviewed to obtain their perspectives on the applications for utilities. One of these companies has deployed with utilities, although only in the IT environment. Its technologies were designed to address the high-maintenance/high-cost downsides to honeypots. These are EPRI's observations based on vendor discussions, literature and website reviews, and webcast events:

- The utility sector has tremendous promise, but vendor solutions are unproven for utility OT environments.
- Early-adopting utilities must be prepared to help educate vendors on their operations and networks and help develop "data profiles" for typical substation devices and network activity.
- Vendors may have exposure to and/or experience with SCADA and ICS, but in manufacturing environments rather than utility environments.
- There will be a steep learning curve as vendors and utilities determine the best lures and decoys and their best placement in OT networks and assets.
- Procurement decisions must include the infrastructure and labor costs to support the number and type of decoys (passive or interactive).

Utility Deployments of Deception Technology: Dreams and Realities

The utility market is a niche market for vendors creating deception technology solutions that work across a number of business sectors. These are likely to be the larger companies. Those that specialize in ICS and SCADA environments are likely to be smaller companies. Utilities need to take note of this when evaluating solutions.

Utilities are traditionally followers in terms of adoption of new technologies, often tracking the uptake of innovations in other business sectors. Some utilities already deploy deception technologies, such as honeypots and lures, in their IT networks. EPRI spoke with a utility that has selected a deception technology for deployment in its OT environment. It already has deception technology deployed in substations; however, that technology is part of the Windows system, not an OT system emulation. The early learnings from this utility include the following:



- Legacy systems are not equipped to handle advanced solutions like deception technologies. There is a need for improved integration with legacy systems in order to acquire their data in usable formats. There is also a need for sufficient bandwidth or communication speeds from legacy equipment to support the data required for realistic emulation of those systems.
- Funding justifications may be an issue as deception technologies may be interpreted to be duplicative of intrusion detection system (IDS) solutions. There is a need to educate on the distinctions between IDS and deception technology.
- The solution can produce high-fidelity (high-confidence) alerts. If a decoy is in play, there is almost always an attacker at work.

These solutions can be deployed on premise or hosted by the vendor or a managed security service provider (MSSP). Lures and decoys can be widely distributed or sparingly placed to alert on attacks to the systems most vital for reliable grid operations. That implies that there is a price point for almost every utility budget. However, the utilities that are most likely to proceed with some purchase of a deception technology product or service are those that have sufficient internal resources for the training necessary to support this solution. While it is not as time intensive as honeypot maintenance, proper configuration will require a team to identify the lures and decoys, support the build-out of their emulations, and construct the alternate realities of deception technologies. This will be true whether the solution is on premise or hosted by an MSSP.

Utilities that are most likely to be early adopters of deception technologies should have a mature SOC that monitors the OT environment in place. EPRI recommends the integrated security operations center (ISOC) model for holistic monitoring and effective situational awareness. Time and budget will need to be allocated to supporting integration of deception technologies into the SOC. Each utility should measure resource time and volume of alarms on a before-and-after basis to test the hypothesis that deception tech can reduce alarm volume to high-fidelity alarms and thus make resource time much more productive. Therefore, the initial adopters of deception technology will most likely be large utilities that have the work force and budget to invest in the technology and the preparations for it.

Utilities may not be willing to share information about their use of deception tech. There are two schools of thought amongst companies in all business sectors about publicly sharing information on deception technologies. The "don't tell" group sees deception technology as a secret weapon to help identify attacks. This group may have a greater fear of insider threats than of external attackers. The "do tell" group believes publicizing the use of deception tech acts as a deterrent to would-be attackers, just as any home security sign in a front yard warns off burglars.

EPRI's assessment is that the overall vendor offerings are relatively immature when it comes to the details of utility operations. Vendors need time to build their knowledge of the most appropriate lures and decoys for different grid operations. For instance, nuanced knowledge of the differences in data traffic volumes and patterns for transmission SCADA versus distribution SCADA systems is gained by developing realistic emulations to serve as decoys for those systems. Initial utility adopters must be prepared to teach as well as learn in deception tech deployments. The utility could leverage its practical knowledge of utility operations and the OT environment during procurement negotiations. Vendors can utilize the utility's subject matter expertise for product enhancement and improved

configuration and implementation for future engagements.

One of the benefits of deception tech is that it can offer a real-time view of attacker TTPs that in turn may help identify zero-day exploits and APTs. That information is critically valuable to all utilities, not just the one that invested in the deception tech solution. This generates three extremely important questions:

- Is the utility the "owner" of that information, regardless of whether the sandbox is on premise or in the cloud?
- Do utilities that discover attacker TTPs have a responsibility to share that information?
- Are threat intelligence entities prepared to work with the information that may be gained from utilities' deception tech sandboxes?

Utilities are advised to work with their procurement resources and their selected vendor to clearly define roles and responsibilities regarding attack information gained through deployment of deception tech.

Artificial Intelligence and Machine Learning in Deception Technology

Artificial intelligence (AI) is a computer science field focused on creating computers that can perform activities based in human intelligence that include learning, problem solving, and pattern recognition, but often on a far larger data scale than humans can manage. Machine learning is an AI application that enables a computer to automatically learn and improve from experience without additional programming.

Some of the deception tech vendors highlight the interactivity of their decoys based on AI and/or machine learning capabilities. There is no doubt that these are among the sizzliest of technologies, but there are added costs to deploying them. Some discussion of data is found in the companion report, "Data Foundations for Operations Technology Cyber Security Analytics, AI, and other Data-Intensive Applications," but the following discussion summarizes the information relevant to deception tech.

While computing and network costs have decreased, these are still costs to consider if deployment of dynamic or interactive decoys is planned. Ask questions about how many interactive decoys can be supported in a virtual or production environment. Consider the server requirements needed to support interactive decoys. It is very important to establish the ultimate goal of procurement in deception tech. If the goal is to engage an attacker for as long as possible to learn about methods attackers use against network, device, or application vulnerabilities, then interactive decoys may be most suitable. If the goal is to close security gaps by monitoring for attacks that get past the defenses, then more passive decoy technologies that do not have AI or machine learning capabilities may be sufficient.

Observations and Recommendations for Deception Technology Vendors

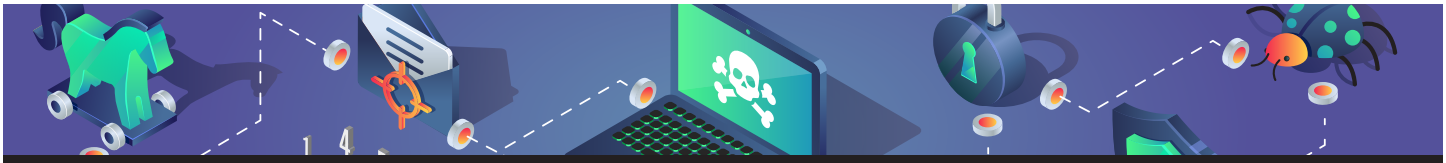
Utilities are risk averse, and that is particularly true regarding cyber security innovations in the OT environment. Utilities prefer proven technologies, but if no utility is willing to adopt an innovation, or (as may be particularly applicable to deception tech) is willing to talk about it, then it becomes exceedingly difficult for vendors to gain credibility with utilities. Here are some observations and recommendations:

- First and foremost, be fully educated on the unique requirements of utilities' OT environments. Understand SCADA systems and utility substation networks and communications. Be prepared to participate in proof-of-concept demonstrations in lab environments that re-create substation conditions.
- Create integrations with the solutions commonly found in utility SOCs and test those integrations upon the release of new versions or upgrades. Use standard, nonproprietary data formats to present data for ISOC reports.
- Make solutions easy to deploy. Utilities do not have piles of cash to expend on operating expenses like consultants.
- Identify the network and computing needs for the solution. More dynamic or interactive emulations have costs. Utilities need to know up front what those will be.
- Seek out partnerships with the leading vendors of critical utility assets to aid in developing "off-the-shelf" network and endpoint decoys that utilities can then customize.

EPRI and Deception Technology Research

There are multiple opportunities for utilities and vendors to work with EPRI to identify and leverage all possible benefits of deception tech.

- EPRI's collaborative research methodology offers a "safe space" for utilities to share knowledge about deception technology deploy-



ments to accelerate learnings and deliver greater benefits to all utilities deploying or planning to deploy these solutions. Building this knowledge may reduce deception tech procurement risks for utilities.

- EPRI has a Cyber Security Research Lab (CSRL) that can re-create several substation environments and evaluate various vendor products. EPRI, in collaboration with utilities and vendors, could set up proof-of-concept demonstrations of solutions to provide hands-on experience with how lures and decoys should be configured to emulate realistic operations.
- The CSRL could be used to help model out various decoy systems, as well as to understand the best places to install deception technology.

- The CSRL also provides a selection of equipment that could be used to help develop decoy systems that mimic those best suited for equipment actually found in a substation.
- EPRI's ongoing research in ISOCs can examine reductions in false-alarm volumes and identify new reporting formats incorporating the high-fidelity alarms produced by deception tech.
- EPRI's ongoing research into threat management can harness actual attack plans harvested from deception tech into future red team/blue team tabletop exercises.
- EPRI researchers could create recommendations for development of lures and decoys and their placement in utility networks for select scenarios such as insider threat or external APTs.
- Deception tech may offer new possibilities for EPRI's metrics research in "protect, detect, and respond" measurements that could be quite impactful for procurement justifications.
- EPRI's research into cyber security training can benefit from improved understanding of the skills that utility security resources need to configure and manage on-premise or hosted deception tech services.

Conclusions and Potential Outcomes for the Future of Deception Technology

Are deception technologies a game-changing solution for utilities? Yes. The shift to zero-trust strategies could presume less investment focused on securing the perimeter and more focused on real-time or near real-time detection of actual attacks. Deception tech also offers the ability to shunt threats to safe environments where utility security resources could study the attackers' tools, techniques, and procedures.

Utilities successfully deploying deception technologies will recognize that these technologies can change their strategies from reactive defense to proactive defense. That will require careful planning to ensure that utilities are prepared to:

- Deploy realistic lures and decoys around what is truly important
- Have a response plan to handle decoy alarms that has been exercised at least at tabletop level
- Develop measures of success for their investment
- Train their cyber security teams to leverage the learnings from failed attacks to reduce vulnerabilities

As with many other innovative technologies, EPRI anticipates that over time procurement of best-of-breed solutions will decline and procurement of integrated systems will take precedence. The reasons for that focus on the complexities of maintaining integrations as vendors release new features and capabilities that may not have backwards compatibility with existing APIs. EPRI also presumes that providers of security platforms will continue to acquire deception tech companies. We expect that legacy SOAR solutions will participate in these acquisition activities, as well as develop their own technologies to address existing customer needs.

Glossary

artificial intelligence (AI). A computer science field focused on creating computers that can perform activities based in human intelligence that include learning, problem solving, and pattern recognition, but often on a far larger data scale than humans can manage.

advanced persistent threat (APT). Ongoing and sophisticated attacks to gain access to a system and probe inside it undetected for a considerable time to inflict maximum damage at some future point.

blue team. A group of resources designated to defend a system to mitigate any discovered cyber security vulnerabilities. It can include networks, devices, and applications.

breadcrumbs. Data and applications planted to lead attackers towards lures and decoys.

Cyber Security Research Lab (CSRL). EPRI's Knoxville lab for cyber security research, development, and demonstrations.

decoys. Assets such as networks or virtual LANs designed and deployed to emulate real environments.

false positives. False alerts and alarms that arrive at SOCs and ISOCs. Both SOCs and ISOCS suffer from high volumes of false alarms.

integrated security operations center (ISOC). Security center that extends SOC responsibilities and capabilities by integrating the OT, physical security, and IT domains into a central monitoring center to improve visibility and situational awareness, coordinate incident response efforts among the domains, and optimize resources.

Information Technology (IT) environment. The systems, devices, applications, and data that support business operations. Specifically for utilities, these include systems such as email, customer service, and human resources applications.

lures. IP addresses, servers, or other assets designed and deployed to deliberately lead attackers away from real production environments and into deception artifacts.

managed security service provider (MSSP). An entity that monitors and/or manages cyber security activities on behalf of another entity. Also known as security-as-a-service.

machine learning. An AI application that enables a computer to automatically learn and improve from experience without additional programming.

operational technology (OT) environment. The systems, devices, applications, and data that support manufacturing operations. Specifically for utilities, these include systems that support the delivery of electricity services, such as SCADA, distribution automation, and volt/var regulation.

red team. A group of resources designated to attack a system to discover cyber security vulnerabilities. It can include networks, devices, and applications.

sandbox. A safe environment where attacker tools like malware can be examined.

security operations center (SOC). A collection of people, processes, and technologies responsible for defending systems—such as a computer network or physical security perimeter—from unauthorized activity through monitoring, detection, analysis, and response and restoration activities.

supervisory control and distribution acquisition (SCADA). A monitoring and control system for industrial applications like electricity generation and delivery that acquires data from a variety of inputs.

true positives. Alerts or alarms that are based on real attacker activity. Deception tech promises high fidelity in alarms, eliminating the false positives generated by current cyber security technologies.

zero-trust strategy. A security model that defaults to not trusting anyone.

zero-day exploit. An attack on a previously unknown vulnerability in a device, application, or network.

EPRI RESOURCES

Christine Hertzog, *Technical Leader, Principal*
650.314.8111, chertzog@epri.com

Cyber Security

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI members represent 90% of the electricity generated and delivered in the United States with international participation extending to 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; Dallas, Texas; Lenox, Mass.; and Washington, D.C.

Together . . . Shaping the Future of Electricity

3002017417 October 2019

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com