DECEPTION TECHNOLOGY INCREASED PROTECTION

Honeywell Threat Defense Platform Powered by Acalvio

Honeywell

WHEN YOU DEFEAT THE ATTACK, YOU'RE ON THE RIGHT TRACK

Once primarily thought to be necessary only for entities that need to protect their customers' personal information, defense against cyberattacks is now important for every organization.

When surveyed, a wide variety of businesses in a broad range of industries indicated that threats of attacks on their operational technology platforms – in addition to actual attacks – have increased exponentially in recent years and that protection against these incidents has become an important priority. Deception technology – an active defense strategy rather than simply a passive one – is a powerful weapon against the destructive havoc these invasive strikes can wreak.

Today's deception technology is promoted by many internet security organizations as an additional layer that protects against tenacious attackers without needing to replace defense technology systems that may already be in place. This concept, referred to as defense in depth (DiD), ensures that your business can not only actively defend and survive cyberattacks but also profile and maintain a portfolio of attacker identities to protect against future strikes.

The Honeywell Threat Defense Platform (HTDP) is based on deception and safeguards against unexpected attacks as well as those that can be reasonably anticipated to occur in today's highly interconnected operational technology (OT) environments. Based on historical concepts used in military operations for centuries, HTDP utilizes the formula "Detection Time + Defender Response Time < Attack Time" to seek out and identify attackers and then divert or delay them so that your business has time to determine how best to thwart their attempts and stop them in their tracks.

HTDP includes both deployment and monitoring of your OT systems, providing highly accurate, low-risk protection on an ongoing basis since not all businesses have the ability to keep a high-level information technology crew dedicated to cybersecurity on staff 24/7. Incorporating proprietary techniques in its rapid AI (Artificial Intelligence) response, it deploys decoy assets such as PCs, servers, and OT/IoT devices and is easy to use and scale. Hundreds of decoys can be scaled in within a matter of minutes. The AI also enables the creation of decoys in real time even as attacks are occurring, luring attackers to the protected virtual replica of the organization's network where they're completely off that network and can't go back or get out.

When it comes to adding deception technology to your arsenal of cybersecurity weaponry, don't be deceived by novel approaches with dubious provenance: choose Honeywell, using time-tested techniques for privacy protection.

YOUR ORGANIZATION IS A CYBERATTACK TARGET. YES, YOURS.

1

No business is immune to cyberattacks today. If you have a connection to the internet, you need deception technology protection.

Security risks used to be thought of as being important mostly for financial institutions or other entities involved with safeguarding their customers' personal information. However, as many other industries from data centers and healthcare to transportation hubs and even academic institutions continue to become more internet-connected, OT (operational technology) security risks associated with building systems and processes have become increasingly attractive targets for ransomware and denial of service attacks.

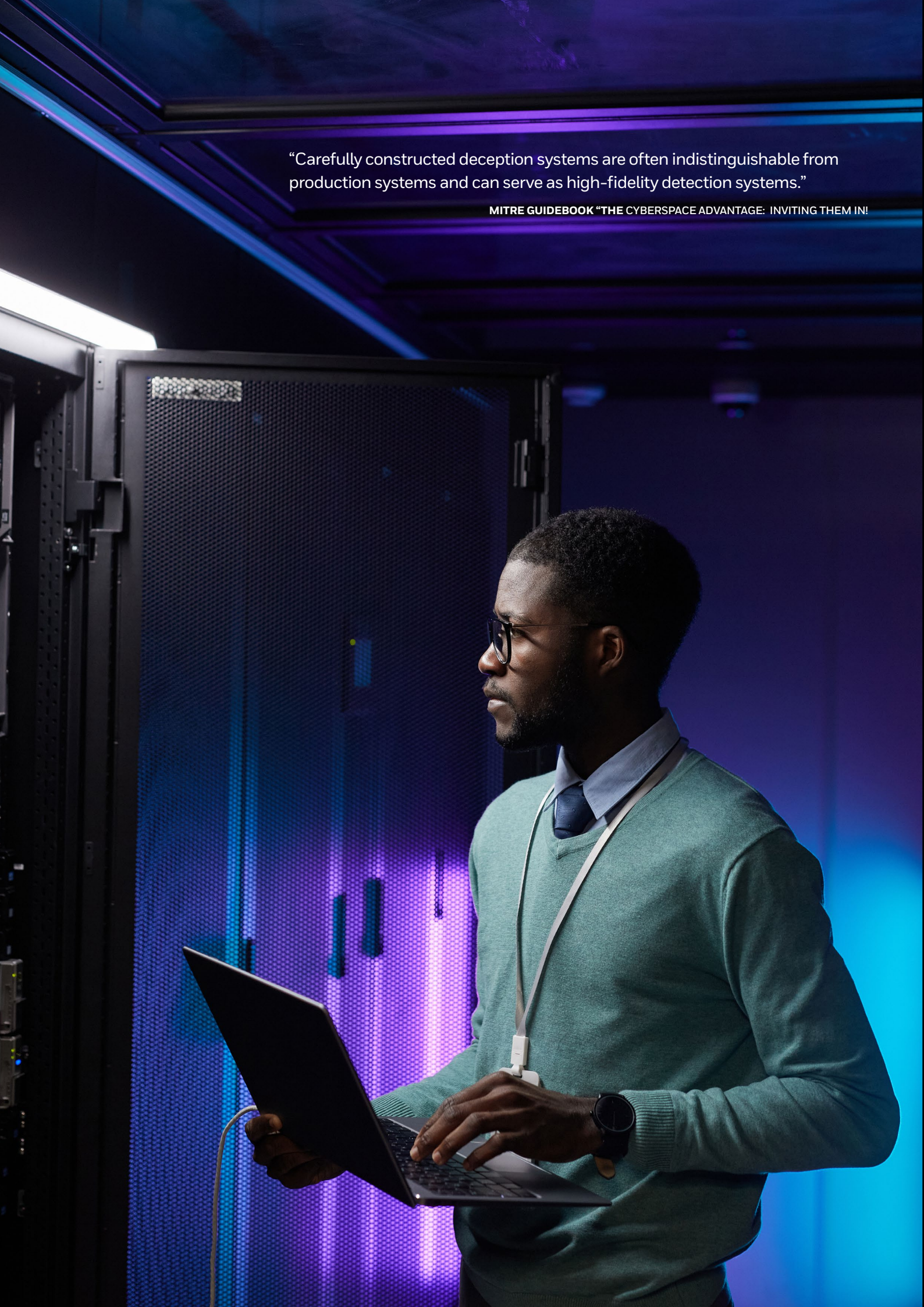
All organizations are vulnerable, and should no longer feel comfortable that they are not susceptible to cyberattack targets: a recent research study by Skybox Security found that 83% of organizations surveyed suffered an operational technology (OT) cyber security breach in the prior 36 months (ITWeb and Skybox Security).

The Honeywell Threat Defense Platform (HTDP) is based on deception, an approach recommended by US government standard bodies because of its ability to detect known and unknown (zero-day) attacks. While the approach is leading-edge, it has roots in straightforward, decades-old strategies to find and defend against adversaries.

More than 60% of incidents at firms with OT platforms last year were against manufacturers, surpassing attacks on financial services vertical market which was 23.2%. Two ransomware groups, Conti and LockBit 2.0, executed more than half of all ransomware attacks on the industrial sector, 70% of which were aimed at manufacturing firms.[1]

Cybersecurity breaches against healthcare entities hit an all-time high in 2021, exposing 45 milliion patients' protected health information (PHI). That is up from 34 million in 2020, and has tripled in just three years, growing from 14 million in 2018. [2]

Oct 2022, the Killnet hacker organization cyberattacked more than a dozen US airports, including Atlanta, LAX, NY LaGuardia, Denver International, Chicago O'Hare, and Phoenix Sky Harbor in retaliation to US support of Ukraine. Public websites were affected but internal airport operations were not impacted. [3]



"Carefully constructed deception systems are often indistinguishable from production systems and can serve as high-fidelity detection systems."

MITRE GUIDEBOOK "THE CYBERSPACE ADVANTAGE: INVITING THEM IN!

DECEPTION HAS BEEN EMPLOYED AS AN ACTIVE DEFENSIVE STRATEGY FOR CENTURIES...BECAUSE IT WORKS

Deception has long been used by the military to lure enemies into combat situations that are advantageous to the deceiver. During WWII, Operation Barclay was a deception by the Allies that turned the tide for the Allied invasion of Sicily in July 1943. The goal was to deceive the Axis powers regarding the location of the Allies throughout the Mediterranean and bogus troop movements, radio traffic, and various other means were deployed to indicate that an invasion was planned through the Balkans rather than Sicily. For further reinforcement of this deception, the British planted faked documents in other locations through military projects known as Operation Mincemeat and Operation Waterfall. The deception was successful: the High Command believed the lie that there were more Allied resources in the eastern Mediterranean, giving the Allied invasion of Sicily the highly effective element of surprise.

While the concept of deception been utilized in the cyber world for some time, it has often been relegated to being thought of as old or low-value technology traps involving "honeypots" or "ping only" decoys. These days, outmoded deception devices like these can be readily bypassed and then allow attackers to stay undetected within the network they've breached to wreak further future havoc. Modern AI-powered deception techniques drive rich interaction with attackers by engaging them in such compelling and realistic ways that they believe that the decoy is genuinely a part of the organization's actual network. As with military operations in the past, an effective deception-based threat defense uses the formula "Detection time + Defender Response Time < Attack Time." Deception finds and then diverts or slows attackers so defenders have more time to act.

DECEPTION IS THE CORNERSTONE OF ACTIVE DEFENSE

Deception technology today is more than just an option for OT security. Multiple internet security organizations like the Cybersecurity and Infrastructure Security Agency, the MITRE Corporation and the Center for Internet Security, promote deception-based technology, with general consensus that deception technology should not replace layers of defense already in place; it's an additional layer that defends against determined professional attackers. This concept is called defense in depth (DiD)[4].

Defense in depth is needed since even the most robust defenses eventually fail in the face of a determined attacker with enough talent and resources. Cyber resiliency has evolved to meet this challenge by recognizing that historical cybersecurity approaches based on blocking all intrusions at a network perimeter are insufficient. According to dedicated cybersecurity agencies and research foundations, deploying deception tactics in OT cyber defense as an additional layer can help ensure that a cybersecurity system can withstand and recover from attacks in ways that minimize damage to the defender — including identifying attackers and their tactics for future reference— while also greatly diminishing any benefit to the attacker.*

Thus endorsed, DiD has been adopted by corporations, governments from Federal to municipal, and military branches. It starts with physical security and basic network and PC security (firewalls and switches to segment network traffic) and also incorporates anti-virus and endpoint security running on servers and workstations. A DiD system should also include a combination of physical and software components like backup systems, application white-listing, configuration of the network and components, and physical port protection (USB ports as well as network software communication protocol ports). Honeywell's Threat Defense Platform is designed to monitor and provide automated responses to do just that.

Military DiD tactics from before the days of the Trojan horse to WWII and still today use combinations of fake fence lines and walls, decoy tanks, Potemkin villages, and carefully leaked photos, plans, and documents to push enemies in alternative directions, DiD slows attackers, makes them more cautious to attack in the future, and prevents them from achieving their devious intents.

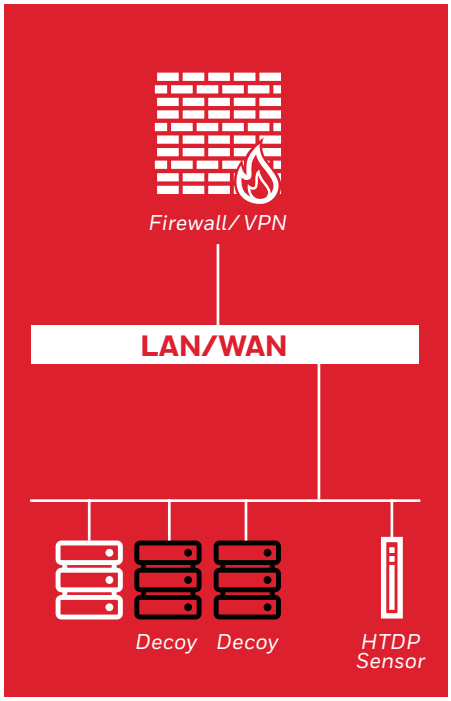
PROVEN STRATEGY, LEADING TECHNOLOGY

2

Based on deception, the Honeywell Threat Defense Platform (HTDP) provides accurate, low-risk internal network threat detection for Operational Technology (OT) environments. The service includes both deployment and ongoing monitoring that frees up internal security team resources, making it well-suited to organizations who need advanced detection but don't have IT specialists dedicated to cybersecurity and don't want to install or operate complex technology.

With proprietary techniques in its rapid AI (Artificial Intelligence) response, the Honeywell Threat Defense Platform deploys decoy assets such as PCs, servers, and OT/IoT devices. It's easy to use and scale as it detects and deflects attackers with specially crafted baits, breadcrumbs, and decoys to trap attacks, even zero-day ones, with precision and speed. Decoys are completely blended, configured by an AI engine that match your systems, interfaces, ports and services for seamless deception by realistically creating a complete virtual replica of the actual network.

Once decoys are in place, HTDP waits for attackers to try to hack into a decoy and quarantines them using patented deception technologies. Once trapped, attackers are rendered harmless and then on your behalf, we can watch and learn from their behaviors to enhance your system's future security. This technique of active defense sets HTDP apart from competitors. The service is optimized for Building Management System environments, making it more effective than alternative technologies. It's everything you need, including expert professional service from a trusted industry leader.



HTDP is a superior approach to threat detection because...

IT'S HIGHLY ACCURATE AND INDEPENDENT OF THREAT SIGNATURE UPDATES

We lure the attackers to come to you, resulting in very low false alerts and high probability of detection as well as handling "zero day" attacks your system hasn't seen before.

IT'S LOW RISK

Deception doesn't require network devices or extra software on OT/IoT devices so it can't cause a service disruption.

IT'S EASY TO DEPLOY AND OPERATE

Our proven-safe cloud-based service handles the deployment, in one day, ongoing operations, and alerts so your facilities and security teams can focus on other tasks.

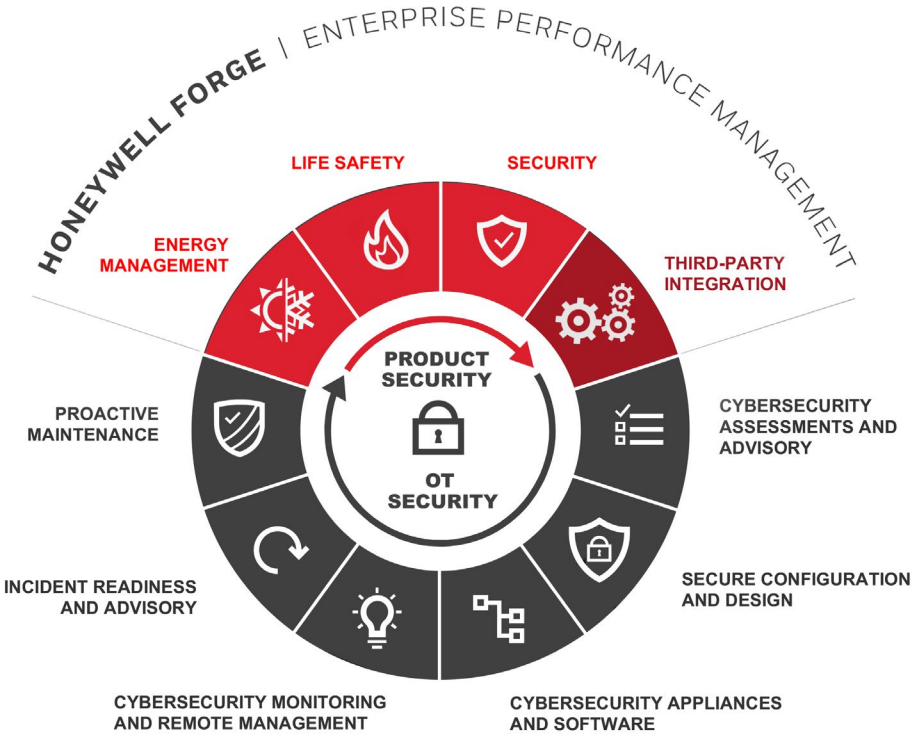
IT'S AUTOMATED

HTDP doesn't rely on human recognition and decisions so attacks are handled faster with less potential damage and lower probability that human error could let an attack continue.

CONCLUSION

DETECT. DECEIVE. DEFLECT. DIVERT.DEFEND.

With decades of OT experience based on even longer expertise in process and building control both as an OEM and service provider, Honeywell's proficiency with OT and IT makes us both a pioneer and leader in cybersecurity. Whether you work in an industrial environment, government, education, healthcare, a transportation hub, data center, commercial bank, or corporate facilities management, the Honeywell Threat Defense Protection Platform can optimize the integrity and security of your systems and let you adopt active defense as a cyber strategy. Contact us now for the state-of-the-art in threat detection...and protection.



Cybersecurity is an integral fabric of Honeywell Business -from products we develop, and third party integrations we enable, to the portfolio of software and services we offer to our clients

REFERENCES

1. DarkReading.com reposted by Security newswire.com, Feb 23, 2022
2. https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people , Feb 2022
3. https://t.me/s/killnet_reservs (list of targeted airports that killnet posted) | CBN News article https://www1.cbn.com/cbnnews/national-security/2022/october/killnet-strikes-again-us-airports-hit-by-cyber-attacks-and-russia-is-the-top-suspect | ABC news - https://abcnews.go.com/Technology/cyberattacks-reported-us-airports/story?id=91287965 | airport tech news - https://www.airport-technology.com/news/dos-cyberattack-airport-websites/ | Spiceworks - https://www.spiceworks.com/it-security/security-general/news/killnet-ddos-attack-us-airports/
4. https://www.mitre.org/news-insights/impact-story/active-defense-using-deception-and-trickery-defeat-cyber-adversaries

*CISA Publication: 2022-2026 STRATEGIC TECHNOLOGY ROADMAP VERSION 4

For more information

https://hwll.co/spx9l1

Honeywell Building Technologies

715 Peachtree St NE

Atlanta, Georgia 30308

www.honeywell.com

Deception Technology Increased Protection | 2022-10-17

THE FUTURE IS WHAT WE MAKE IT

Honeywell