Power Security & Resilience in OT Systems with CounterCraft

Specific. Actionable. Threat Intelligence
Powered by Deception

Thank you for downloading this CounterCraft Datasheet. Carahsoft is the distributor for CounterCraft Zero Trust solutions available via NASA SEWP V, ITES-SW2, NCPA & OMNIA Partners Company, and other contract vehicles.

To learn how to take the next step toward acquiring CounterCraft's solutions, please check out the following resources and information:

For additional resources:
carah.io/countercraftresources

For upcoming events:
carah.io/countercraftevents

For additional CounterCraft solutions:
carah.io/countercraftresources

For additional Zero Trust solutions:
carah.io/countercraftsolutions

To set up a meeting:
countercraft@carahsoft.com
888.662.2724

To purchase, check out the contract vehicles available for procurement:
carah.io/countercraftcontracts

For more information, contact Carahsoft or our reseller partners:
countercraft@carahsoft.com | 888.662.2724

CounterCraft | carahsoft

/DATASHEET

Power Security & Resilience in OT Systems with CounterCraft

Specific. Actionable. Threat Intelligence
Powered by Deception.

Discover CounterCraft →

Power Security & Resilience in OT Systems with CounterCraft

For many years, industrial systems relied on proprietary protocols and software, which were manually monitored and updated by humans, and had no external connections. As a result, they were not attractive targets for hackers because there was no networked interface to exploit, and there was little to gain or disrupt. However, automation and digitization have made OT systems more attractive to hackers.

Attacks on Operational Technology (OT) are on the rise. These attacks targeting the essential infrastructure and processes that support critical industries such as energy, manufacturing, transportation, and healthcare are carried out by nation states with the intention to cause widespread disruption. By infiltrating OT systems, malicious actors can disrupt operations, cause equipment failures, and even pose risks to public safety. The consequences of such attacks can lead to financial losses, environmental damage, and compromised data integrity among other consequences. Protecting OT systems against cyber threats requires a multi-faceted approach that includes robust cybersecurity solutions that deliver the best threat intelligence, continuous monitoring, and collaboration between IT and OT teams to effectively mitigate risks and safeguard critical infrastructure.

Cyber Physical Systems (CPS) and OT industry verticals are greatly affected by these cyber attacks, with the highest cost per breach in the healthcare industry. However, many other industries suffered from CPS/OT attacks:

Airlines

Four separate attacks causing flight delays for tens of thousands of travelers.

Automotive

14 top automobile manufacturing brands' plants suffered outages causing big production losses.

Mining

Physical operations were impacted in four attacks on metals and mining organizations.

Transportation

Issues with the loading and unloading processes of cargo containers, fuel and bulk oil have been observed in numerous seaports spanning three continents.

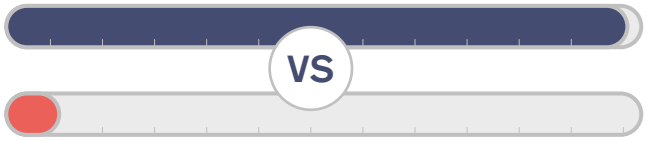
Gartner COOL VENDOR 2021

CPS Category

Attacks on critical infrastructure and physical assets are the main concern for 53% of U.S. businesses.

(Source: Allianz Risk Barometer, 2024)

360 DAYS Competitor deployment



30 DAYS CounterCraft deployment

Gartner predicts by 2025 cyber attackers will have weaponized operational technology environments to successfully harm or kill humans.

(Source: https://www.gartner.com/en/ne…tackers-will-have-we)

Why use CounterCraft

- Specific, actionable threat intelligence driven by deception
- 30-day or less deployment
- Built-in OT use cases
- Supports industry regulatory standards, such as IEC 62443
- Threat intel delivered in real time
- 48 hours average of adversary deflection and isolation

Gartner, Cool Vendors in Cyber-Physical Systems Security: Novel Approaches Enter the Scene, September 2021. The GARTNER COOL VENDOR badge is a trademark and service mark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

The Challenges

Legacy systems

Many ICS/Critical Infrastructure/SCADA/OT systems have been in place for years, and they often run on outdated operating systems and software.

Concerns about software updates

The fear of disturbing equipment that has been operating fine for years, sometimes decades, for a security patch will have a negative impact in production.

IT security practices don't apply

Implementing security controls like anti-virus or host-based intrusion detection on ICS/OT networks or devices can cause system slowdowns or active responses to perceived attacks.

Sophisticated attackers

As stakes get higher, attacks against the industrial sector are increasingly sophisticated.

Insider threats

Insider threats present a substantial danger within OT environments. Whether they are employees or contractors, malicious or negligent, they can deliberately or inadvertently disrupt operations, compromise security, and exfiltrate sensitive data.

REAL CASE STUDY

The National Electricity Grid Detects OT System Attacks Before Breach

CLIENT: Red Eléctrica	
WHY DECEPTION:	
	/ Ability to deploy in external environments
	/ Ability to collect intel in real time
	/ Full visibility into threat actors' movements
PRODUCT DEPLOYED:	
	/ The Platform
KEY RESULTS:	
	/ Lightning-fast exploit attempt detection and response
	/ Identification of cyber threats targeting Red Eléctrica
	/ Valuable intel on TTPs of attackers
	/ Prioritization of mitigation measures

The Solution

Only by adopting an adversary-centric approach can security professionals truly defend against sophisticated and novel threats targeting OT/CPS.

This is why we have built the deception-powered threat intelligence platform, which can be the first security solution deployed in your OT environment. Even if your OT organization already has a network monitoring solution like Dragos, Nozomi, or Claroty, there is still a need for CounterCraft, thanks to the following capabilities:

30-day (or less) deployment

CounterCraft's speed of deployment is 30 days—on cloud, on premise, hybrid or air gapped. Comparable solutions can take 12 months to deploy, and even in that time only reaching 80% of your network, leaving the typically valuable systems in the remaining 20% vulnerable.

Hardware agnostic and non-intrusive

Our solution is not hardware dependent, unlike other vendors that use physical appliances resulting in a more intrusive, less flexible and scalable approach. They also require full access to the production network environment, creating a more noisy solution with a higher number of false positives.

With CounterCraft, there is:

- / No need to modify the existing ICS/OT network.
- / No need to insert additional inline devices.
- / Quick and safe OT adversary campaign deployment.

Protects production assets

Our technology creates an external environment that provides a containment area for attackers, safe from production assets.

Endless integrations

Our software complements your existing OT network monitoring solution. Our software integrates with just about everyone, including your SIEM, SOAR, XDR, EDR, NDR.

Get the full case study →

What you get with CounterCraft

Specific, actionable threat intelligence powered by deception

From the moment security teams receive a high-fidelity alert from CounterCraft, they know who is targeting their ICS/Critical Infrastructure/SCADA/OT systems, and Level 1-2 Incident Response Analysts have visibility on the one thing they need to do immediately to mitigate risk.

The post exploit threat intelligence provided by CounterCraft is:

- Actionable
- Related to your OT networks
- Delivered in a machine-readable format in real time.

48 hours to mitigate risk

CounterCraft isolates adversaries from the production network, reducing the attack surface and limiting the spread of any potential compromises. On average, we buy companies 48 hours of adversary isolation in a deception environment. This is invaluable time that allows teams to gain situational awareness, thwart the attack, and prevent future intrusions.

Support meeting industry regulatory standards

CounterCraft supports IEC 62443, empowering manufacturing companies to adopt best practices and exceed compliance requirements.

Situational awareness and threat hunting capabilities

With the intel CounterCraft provides, the SOC team can quickly determine whether the adversary's IP or machine name is related to a business-critical situation or a high-risk unauthorized user and can then prioritize the response accordingly.

Not only is CounterCraft able to block IP addresses, but also hashes, powershell scripts and binaries, so security teams can instantly thwart the attack based on MITRE & NIST mitigation controls. CounterCraft also offers threat actor attribution.

Tailored security that works

What makes CounterCraft different is its easy-to-implement decoy representation of your existing infrastructure, covering every security zone of your architecture. This allows for the monitoring of attacks designed specifically to target the current infrastructure.

No noise or false positives

Detection is based on human actions, meaning CounterCraft does not flood your team with false alarms based on signatures or traffic analysis. Alerts that come through are valuable, real-time OT adversary campaigns, and detailed detection TTPs are provided.

Actionable Intel Deliverables

- IP Addresses
- Country of origin
- Domain names
- User agents
- Operating System
- Browser
- Security events: network scans, exploit attempts, etc.
- Usernames and passwords
- Binaries executed
- Commands executed
- New processes created
- Files created
- Network connections created
- Kernel changes
- Users and policy changes
- Security events: network scans, exploit attempts, etc.
- System integrity changes
- Registry changes (Windows)
- Malicious process activity (code injection, remote threads, etc.)

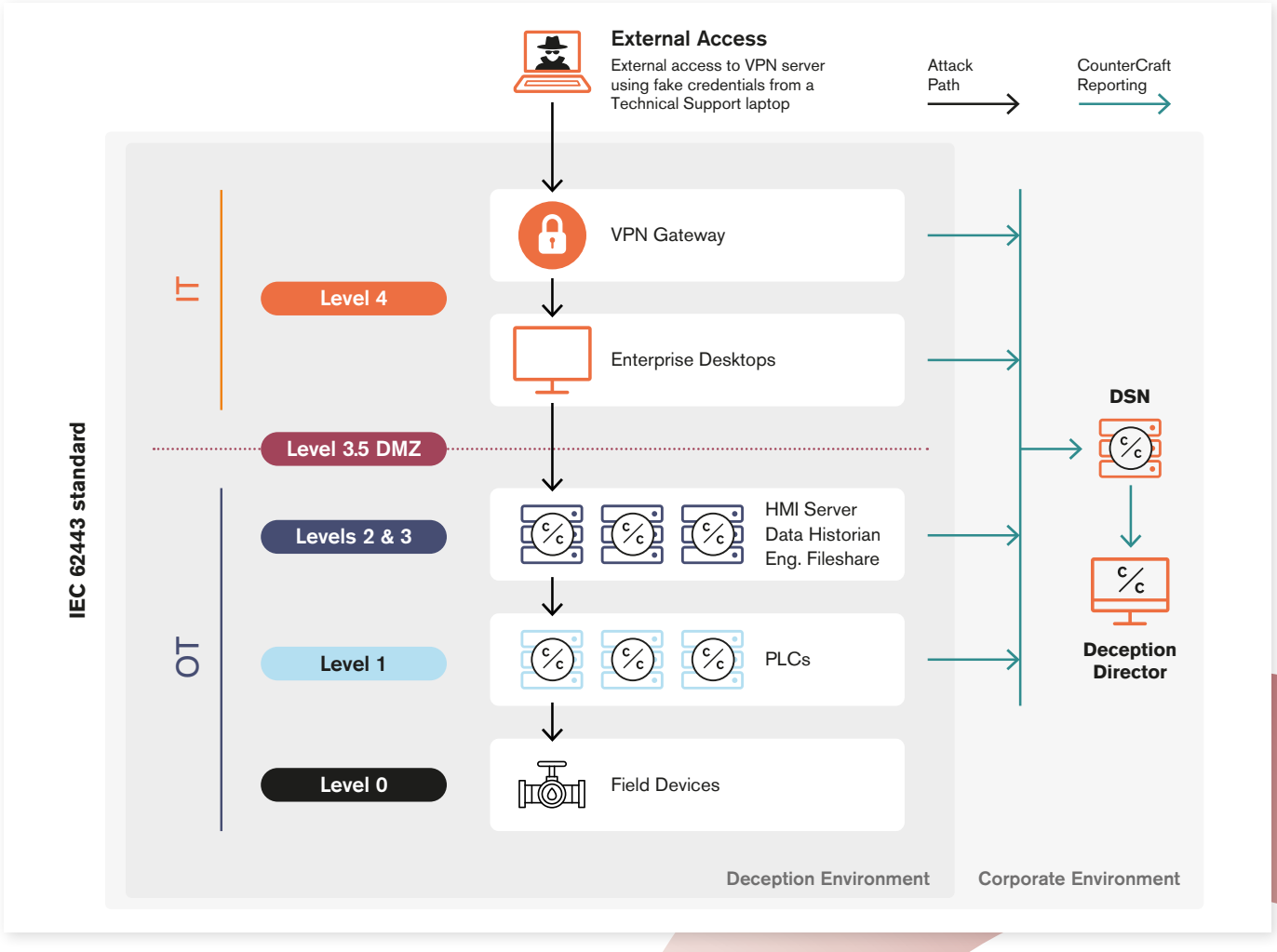
Technical Solution

A SCADA campaign to meet the IEC 62443 standard

CounterCraft's SCADA campaign builds a representation of your existing OT architecture without modifying or requiring access to it. It's deployed completely external to your infrastructure.

The DMZ is particularly important, as real-world experience has shown that most OT attacks start in the Enterprise IT domain (Level 4) and then propagate into the OT network across the IT/OT network boundary. That's why this campaign replicates every level of the customer's OT infrastructure, with a focus on catching attacks in Levels 3, 3.5 and 4.

- Breadcrumbs and engineering workstations in the IT network linked to the ICS/OT environment (level 4)
- IT / OT equipment - deception equipment such as an HMI or Historian (level 2 / 3)
- Emulated PLCs using the CounterCraft "SCADA" Deception Services (level 1 / 2)



About Us

CounterCraft delivers specific, actionable, threat intelligence powered by deception. Our rapidly deployed deception technology redirects adversaries from production to deception environments, capturing relevant threat intelligence in real time, empowering organizations to take action decisively.

Specific. Actionable. Threat Intelligence Powered by Deception.

CounterCraft is an approved cybersecurity supplier by CISA.

Find out more. Request a demo at

countercraftsec.com →