carahsoft

CounterCraft

The Ultimate Guide to Zero Trust & Deception Technology

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASA SEWP V, ITES-SW2 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with CounterCraft, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/countercraftresources

Join Events & Webinars:
carah.io/countercraftevents

Discover Technology Solutions:
carah.io/countercraft

Learn About Procurement:
carah.io/countercraftcontracts

Connect With Our Team:
CounterCraft@carahsoft.com
(571) 591-6290

CounterCraft

Whitepaper

The Ultimate Guide to Zero Trust & Deception Technology

The Ultimate Guide to Zero Trust
& Deception Technology

The ultimate guide to zero trust & deception technology

Zero trust has become one of the biggest buzzwords in the industry today— so much so, that many vendors claim to have a widget that "automagically" implements the zero trust model into an organization. That is simply not true. As Neil MacDonald, VP Analyst at Gartner explains, "Zero trust is a way of thinking, not a specific technology or architecture. It's really about zero implicit trust, as that's what we want to get rid of."

The current environment of cybersecurity threats facing organizations today can be daunting. Organizations have to contend with insider threats, phishing attacks, APTs, hacktivists, script kiddies—the list goes on.

According to the 2024 IBM Cost of a Data Breach Report, the average cost of a data breach rose by 10% compared to the previous year, marking the most significant annual increase since the pandemic[1]. Cybersecurity threats, including ransomware, continue to be a top concern for organizations across industries. In 2023, ransomware attacks surged by more than 200%, with human-operated ransomware campaigns driving much of the increase[2].

Ransomware attacks are a constant threat affecting all sectors. An estimated 2,323 local governments, schools, and healthcare providers were victims of a ransomware attack in 2021[3].

Consider the fact that a data breach costs organizations an average of $4.35 million, and 83% of organizations have experienced more than one data breach[4]. Imagine the business and operational cost such a breach entails. Many affected companies go out of business within six months of an attack, according to insurance company Hiscox[5]. It's no wonder organizations are eager to arm themselves with the latest in cybersecurity tools to help defend against the growing sophistication of cybercriminals.

This also means the adoption of new cybersecurity frameworks, concepts, and models. The zero trust model finds itself at the top of many CISOs' lists as a way to potentially reduce, or even eliminate, cybersecurity attacks.

97%

of companies have zero trust initiatives

80%

increase in three years

$1 M

reduction in the cost of a data breach when implementing zero trust

$60 B

the projected value of the global zero trust market in 2027

[1]Accenture. State of Cybersecurity Resilience 2021.
[2]IBM.Top cybersecurity threats and predictions for 2025.
[3]Emsisoft. The State of Ransomware in the US: Report and Statistics 2021.
[4]ABM Security. Cost of a Data Breach Report 2022.
[5]Hiscox. Hiscox Cyber Readiness Report 2019.

What is zero trust?

According to NIST SP 800-207, “Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated. Zero trust architecture is an end-to-end approach to enterprise resource and data security that encompasses identity (person and nonperson entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure.”

Many vendors consider zero trust as a “cure-all” for all security risks, often believing that merely implementing it will eliminate every security threat magically. However, without sufficient context, zero trust can seem ambiguous and hard to grasp for many — is it a product, a technology, a trend? Research firms like Gartner define Zero Trust Architecture (ZTA) as a solution architecture that replaces implicit trust with continuously assessed risk and adaptive trust levels based on identity and context. It is designed to optimize the organization’s security posture amidst evolving risks.

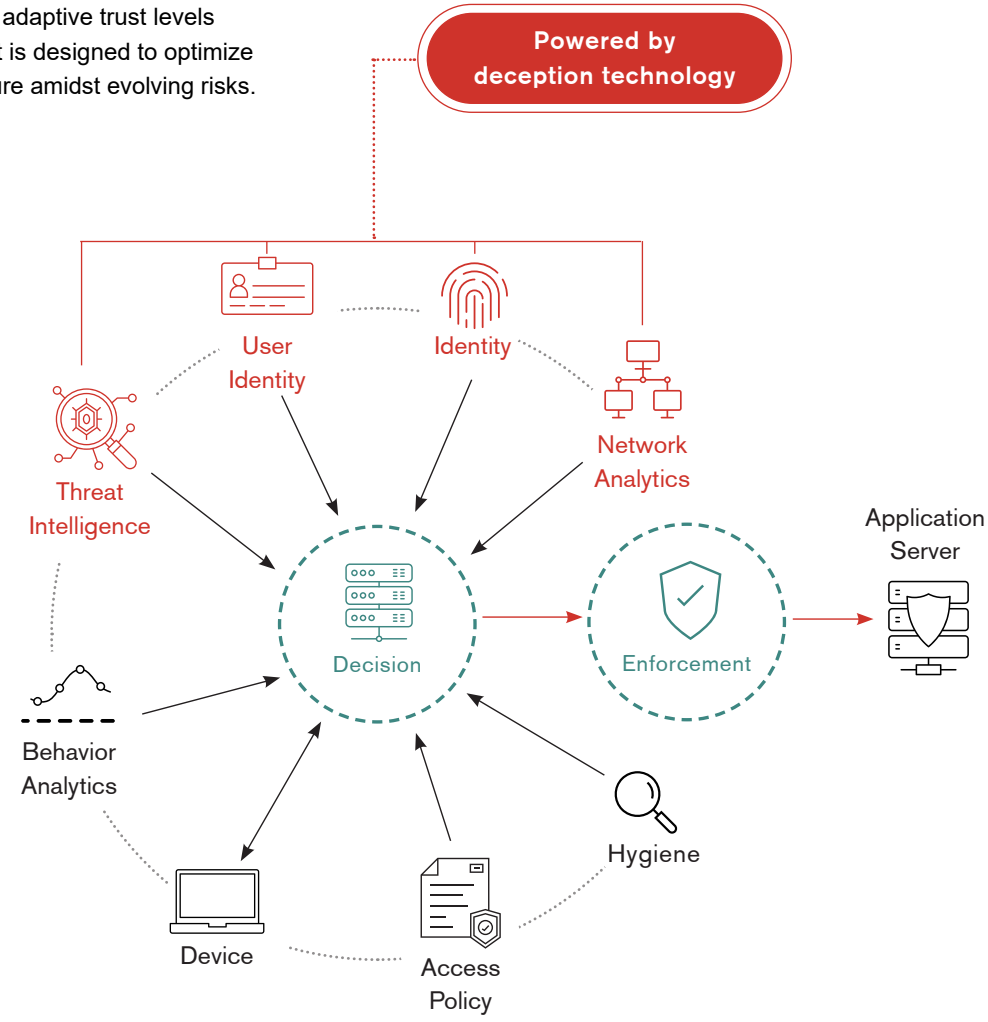
ZTA cannot be bought—it must be built. It’s rarely deployed from scratch, as it uses already deployed technologies within your organization. Implementing and maintaining zero trust is an iterative process. As Gartner states, “Zero trust systematically replaces implicit trust with calculated adaptive trust.”

The zero trust ethos can be summed up by the statement “Never Trust, Always Verify.” However, from a technology perspective, zero trust will always have aspects of multi-factor authentication (MFA), least privilege, segmentation, and IAM (Identity and Access Management) as part of its architecture.

Zero trust architecture

These are the elements that together form an organization’s IT and security architecture. According to CISA, the pillars of Zero Trust Architecture are:

- Identity
- Device
- Data
- Network / environment
- Application workload



The challenges of zero trust

However, as with any framework, model, or concept there are exceptions and gaps. The same is true for the zero trust model. Here are some of the challenges associated with enacting a zero trust model:

/ It's an operational change, and there will be resistance from associates. ZTA limits users—from business users to even administrators—with "just enough" access. This can cause operational issues for various associates, especially administrators, as they lack the permissions needed to perform their usual tasks.

/ Per NIST, the zero trust ecosystem is not yet mature enough for widespread adoption.

/ Despite what many vendors claim, there is no single solution that provides all the necessary components.

/ ZTA takes a long time to deploy. MIT Lincoln Laboratory has indicated that it took three to five years to implement zero trust at the companies it has worked with.

/ Few zero trust components available today can be used for all of the various workflows present in an enterprise.

/ Additionally, the zero trust security models assume an attacker is present in the environment and that an non-enterprise-owned environment is no different—or no more trustworthy—than any non enterprise-owned environment.

Working towards achieving zero trust in an organization is a move in the right direction to protect against cyberattacks. However, to truly defend against cybersecurity threats, an organization must take an active defense approach.

How deception supports zero trust

Deception technology is a cybersecurity approach that employs deceptive tactics, such as decoy network environments, honeypots, and breadcrumbs like bogus credentials, to detect malicious actors and gather intelligence about them. Unlike traditional security measures—such as firewalls and endpoint detection systems—deception technology is not limited to defending a perimeter. Instead, it actively identifies illicit activity, even from within an organization. It achieves this by accounting for the attacker's perspective and actions to create an active defense. The ultimate goal of deception is to prevent system damage by delivering better insights and preparation.

Incorporating deception technology within a zero trust architecture creates a powerful defense mechanism that ensures a higher level of security by assuming that threats exist both inside and outside the network perimeter.

ZTA should be structured to incorporate deception-powered threat intelligence related to user breach data as an alert, and respond quickly when malicious activities increase the risk of a user's access.

Deception technology enables an organization to take a proactive cybersecurity stance in conjunction with models like zero trust to create a comprehensive cybersecurity plan. On the following pages you can see how deception technology can complement a zero trust architecture.

Tenets of zero trust

1 All data sources and computing services are considered resources

A network may be composed of multiple classes of devices. A network may also have small footprint devices that send data to aggregators/storage, software as a service (SaaS), systems sending instructions to actuators, and other functions. Also, an enterprise may decide to classify personally owned devices as resources if they can access enterprise-owned resources.

What deception can do

CounterCraft can mirror the assets within your production environment. CounterCraft doesn't emulate environments.

CounterCraft installs on real non-production virtual machines and/or servers to provide credibility.

We have support for essentially all x86 Linux distributions and Microsoft Windows Operating System.

You can create the following assets within our deception environment:

- Servers
- Desktops
- HMI
- Histori
- PLC
- Other asset types include: mobile phones, routers, deception personas, and Windows/Linux servers with no Monitoring Agent installed.

2 All communication is secured regardless of network location

Network location alone does not imply trust. Access requests from assets located on enterprise-owned network infrastructure (e.g., inside a legacy network perimeter) must meet the same security requirements as access requests and communication from any other non-enterprise-owned network. In other words, trust should not be automatically granted based on the device being on enterprise network infrastructure. All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide source authentication.

What deception can do

CounterCraft has a flexible deployment model. CounterCraft can be deployed on-premise within the network, outside the network {DMZ}, and in the cloud.

All communication within the deception environment utilizes SSH connections and TLS encryption.

3

Access to individual enterprise resources is granted on a per-session basis.

Trust in the requester is evaluated before the access is granted. Access should also be granted with the least privileges needed to complete the task. This could mean only “sometime recently” for this particular transaction and may not occur directly before initiating a session or performing a transaction with a resource. However, authentication and authorization to one resource will not automatically grant access to a different resource.

What deception can do

CounterCraft has Role-Based Access Control (RBAC) to ensure that users only have the appropriate amount of privileges within the deception environment.

There are three user accounts: **Administrator**, **Super Architect**, and **Standard**.

User account permissions are further subdivided at the Tenant level into two types of Tenant members: **Tenant Architect** and **Tenant Standard**.

User account permissions are further subdivided at the Campaign level into three types of Campaign members: **Manager**, **Operator**, and **Guest**.

4

Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes

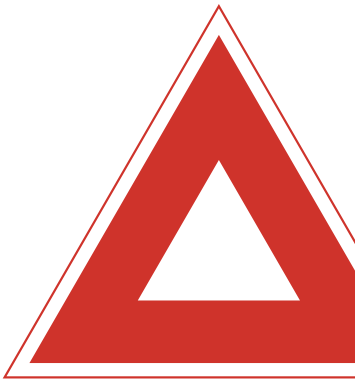
An organization protects resources by defining what resources it has, who its members are (or ability to authenticate users from a federated community), and what access to resources those members need. For zero trust, client identity can include the user account (or service identity) and any associated attributes assigned by the enterprise to that account or artifacts to authenticate automated tasks. Requesting asset state can include device characteristics such as software versions installed, network location, time/date of request, previously observed behavior, and installed credentials. Behavioral attributes include, but are not limited to, automated subject analytics, device analytics, and measured deviations from observed usage patterns. Policy is the set of access rules based on attributes that an organization assigns to a subject, data asset, or application. Environmental attributes may include such factors as requester network location, time, reported active attacks, etc. These rules and attributes are based on the needs of the business process and acceptable level of risk. Resource access and action permission policies can vary based on the sensitivity of the resource/data. Least privilege principles are applied to restrict both visibility and accessibility.

NIST SP 800-207 ZERO TRUST ARCHITECTURE

What deception can do

The CounterCraft platform has a RESTful API to easily integrate with an organization’s IAM solutions to enforce dynamic policies.

Additionally, the CounterCraft platform has role-based Access Control (RBAC) to ensure that users only have the appropriate amount of privileges within the deception environment and easily integrates with an Identity Provider (IdP) or MFA solution via the SAML federation protocol.



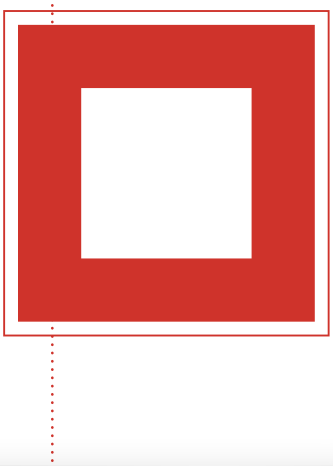
5

The enterprise monitors and measures the integrity and security posture of all owned and associated assets.

No asset is inherently trusted. The enterprise evaluates the security posture of the asset when evaluating a resource request. An enterprise implementing a ZTA should establish a continuous diagnostics and mitigation (CDM) or similar system to monitor the state of devices and applications and should apply patches/fixes as needed. Assets that are discovered to be subverted, have known vulnerabilities, and/or are not managed by the enterprise may be treated differently (including denial of all connections to enterprise resources) than devices owned by or associated with the enterprise that are deemed to be in their most secure state. This may also apply to associated devices (e.g., personally owned devices) that may be allowed to access some resources but not others. This, too, requires a robust monitoring and reporting system in place to provide actionable data about the current state of enterprise resources. enterprise-owned resources.

What deception can do

Assets that are discovered to be subverted, have known vulnerabilities, and/or are not managed can easily be recreated within the CounterCraft deception environment where you can safely and securely gather real-time, actionable tailored threat intelligence on how a bad actor may attack such an environment. Information you can use to shore up your production defenses.



6

All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

This is a constant cycle of obtaining access, scanning and assessing threats, adapting, and continually reevaluating trust in ongoing communication. An enterprise implementing a ZTA would be expected to have Identity, Credential, and Access Management (ICAM) and asset management systems in place. This includes the use of multifactor authentication (MFA) for access to some or all enterprise resources. Continual monitoring with possible reauthentication and reauthorization occurs throughout user transactions, as defined and enforced by policy (e.g., time-based, new resource requested, resource modification, anomalous subject activity detected) that strives to achieve a balance of security, availability, usability, and cost-efficiency.

What deception can do

CounterCraft easily integrates with an IdP or MFA solution via the SAML federation protocol.

Additionally, the user's password is hashed using the PBKDF2 algorithm with a SHA256 hash, a password stretching mechanism recommended by NIST. Users can also protect their accounts by enabling two-factor authentication (2FA) that uses Google Authenticator.

Both users' valid and invalid login attempts are stored with their related information: date, IP address, and user agent.

Users are disabled after a configurable number of invalid login attempts and they can only be enabled by the admin user.

7

The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

An enterprise should collect data about asset security posture, network traffic and access requests, process that data, and use any insight gained to improve policy creation and enforcement. This data can also be used to provide context for access requests from subjects.

What deception can do

Within the CounterCraft deception environment, all security alerts are generated in real-time and can be sent via various communication channels i.e., email, Signal, mobile devices, etc. Additionally, there is out-of-the-box integration with SIEMS and SOAR platforms so that alerts can also be sent in real-time.

All activity within the deception environment is detected, logged, and automatically mapped to the MITRE ATT&CK and ENGAGE framework. It can also be viewed from a native fully customizable dashboard within the platform.

Added benefits of deception technology

As you can see, deception technology is an excellent way to complement the tools an organization is using to enact a zero trust strategy. Cyber deception has many other applications that strengthen security posture and cover ground no other software or technology can. Here are some additional benefits to deception technology:

- Misdirect bad actors away from your valued production assets
- Detect bad actors before they breach your production network
- Discover a dormant adversary and/or insider threat within your production network faster
- Obtain real-time, applicable threat intelligence and behavior analytics (Telemetry, TTPs, and IOCs) on the bad actor to make informed decisions on how to shore up production defenses and remediate the threat
- Gain insight into the tools attackers use to breach a network
- Safely capture and analyze the adversaries' malicious software within a contained environment
- Learn how the adversary avoids detection of other commonly used cybersecurity tools
- Understand what the adversary wants, what they've done so far, and who they are (attribution)

How to meet zero trust architecture standards

The U.S. White House's Office of Management and Budget has mandated that agencies meet specific cybersecurity standards related to a zero trust strategy by the end of Fiscal Year 2024. The goal is to reinforce the U.S. government's defenses against increasingly sophisticated and persistent threat campaigns targeting federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in government. In essence, FY2024 will be ALL about Zero Trust.

The path to zero trust is an incremental process that may take years to implement. However, in the long term, zero trust will enable a more prudent allocation of security investments toward the most critical data and services, across the entire enterprise. Complying with this mandate allows an agency to look at making holistic changes to its cybersecurity architecture and incorporating solutions like CounterCraft to promote a defend forward, proactive approach to warding off cybersecurity threats.

The zero trust roadmap

To understand how deception can help, see the below outline of how CounterCraft's solutions specifically match up to the Department of Defense's (DoD) Zero Trust Roadmap. The mapping below correlates with the DoD's Roadmap, so read on to find out how our capabilities complement DoD's ZTA goals and a guide to follow for the DoD baseline course of action (COA).

/ 1.3.1 - Organizational MFA/IDP

/ 1.5.1 - Organizational Identity Life-Cycle Management

/ 1.5.2 - Enterprise Identity Life-Cycle Management Pt1

- The CounterCraft Platform supports the SAML federation protocol. This allows CounterCraft to seamlessly integrate with MFA or IdP solutions.
- Natively to the CounterCraft Platform user's passwords are hashed using the PBKDF2 algorithm with a SHA256 hash, a password stretching mechanism recommended by NIST. There is a minimum password length requirement of 8 characters.
- Users can also protect their accounts by enabling two-factor authentication (2FA) that uses Google Authenticator.

/ 2.7.1 - Implement Endpoint Detection & Response (EDR) Tools and Integrate with C2C

/ 2.7.2 - Implement Extended Detection & Response (XDR) Tools and Integrate with C2C Pt1

- CounterCraft Deception when integrated with XDRs provides high-fidelity alerts that allow organizations to protect legitimate assets early, while the attacker is still in the decoy environment, allowing enterprises to learn from the attacker's TTPs and IoCs.
- CounterCraft Deception adds the ability to deflect and quarantine an adversary while collecting real-time, actionable, and relevant intelligence to enable intelligent response and risk mitigation to the powerful XDR detection and response capability.
- CounterCraft facilitates the Correlation of early detection telemetry provided by deception with other cyber vendor products for maximum coverage, context, and insight.

- Deception provides high-confidence alerts when integrated with XDR, allowing organizations to protect legitimate assets while the attacker is in the deception environment.

  § Note - The CounterCraft Product team is currently working on integrations with leading EDR/NDR/XDR providers.

/ 3.2.1 - Build DevSecOps Software Factory Pt1

/ 3.2.2 - Build DevSecOps Software Factory Pt2

/ 3.3.2 - Vulnerability Management Program Pt1

/ 3.3.3 - Vulnerability Management Program Pt2

- CounterCraft's Deception Platform can identify exploitable vulnerabilities in software used across the corporate network in microservice architectures. This will allow an organization to gain advanced insight into production service weaknesses to enable actionable counterintelligence and observe subsequent threat methodology in highly instrumented decoys.
- The CounterCraft Deception Platform provides file hashes, malicious binaries (if planted by a threat actor), and forensic data, i.e., memory dumps + PCAP files.
- Rules can be configured within the CounterCraft Platform to detect the exploitation of specific CVEs within the deception environment.

/ 4.3.1 - Implement Data Tagging & Classification Tools

/ 4.3.2 - Manual Data Tagging Pt1

/ 5.4.4 - Protect Data In Transit

- All the connections between CounterCraft the web console, Deception Support Node(s) (DSN), and deception Hosts are authenticated and encrypted using digital certificates.
- The agent that resides on the deception hosts communicates with the DSN using TLS 1.3. Clients must authenticate either with client certificates or signed and encrypted tokens. All the traffic is encrypted. All the traffic from the ServerHello message onwards is encrypted. The communication between the Deception Director and the DSN is done via SSH. All the traffic is encrypted. It provides forward secrecy for all connections. All traffic after the SSH server hello is also encrypted.

/ 6.2.2 - Enterprise Integration & Workflow Provisioning Pt1

/ 6.3.1 - Implement Data Tagging & Classification ML Tools

/ 6.5.1 - Response Automation Analysis

/ 6.5.2 - Implement SOAR Tools

/ 6.6.2 - Standardized API Calls & Schemas Pt1

/ 6.6.3 - Standardized API Calls & Schemas Pt2

/ 6.7.1 - Workflow Enrichment Pt1

/ 6.7.2 - Workflow Enrichment Pt2

- CounterCraft addresses active attacker engagement by sending machine-readable intel collected from the deception environment into other security systems i.e. SOAR platforms, so they can be reconfigured instantly to protect assets from the attacker. There is also out-of-the-box integration with several different SIEMS and SOAR platforms so alerts can also be sent in real-time, too.
- The CounterCraft API is a standard REST API that supports basic CRUD operations. Our API has predictable, resource-oriented, URLs and uses HTTP verbs and response codes.
- Automated, conditional, responses to adversary activity can be programmed into each Campaign using Rules. Automated rule sets change the deception environment in real-time by reacting to attacker activity – this engagement aims to prolong the attacker's dwell time in the deception environment to gather more intel and deflect the attacker further away from their aim. Once in the deception environment, the adversary can be manipulated through the use of rules-based adversary manipulation thereby degrading and slowing down the attackers.
- The CounterCraft Deception Platform provides a wealth of information including PCAP, Memory Dump, IOCs, Telemetry, TTPs, file hashes, malicious binaries, and post-breach activity (commands/calls made by threat actors). frameworks and forensic data and post-breach activity.

/ 7.2.1 - Threat Alerting Pt1

/ 7.2.2 - Threat Alerting Pt2

/ 7.2.4 - Asset ID & Alert Correlation

/ 7.3.1 - Implement Analytics Tools

- Within the CounterCraft Deception Platform, a Tag is a label that can be affixed to different entities in the Console to categorize them.
- There is a pre-existing list of Tags. These are special Tags that the system uses to categorize Events and Objects to assist with their analysis.
- Most Tags are used by the system to automatically categorize MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs). For example, the attack::T1003 Tag will be added to any Events or Objects where the MITRE ATT&CK TTP with an ID of T1003 has been detected.
- Other system Tags include: TOR_NODE Known Tor exit node, VPN: Known VPN exit node (added if you are using an IPABUSE integration), Datacenter: IP address belongs to a known Hosting Provider, Data Center, or Content Delivery Network (added if you are using an IPABUSE integration), Public Proxy: IP address known to act as a Public Proxy (added if you are using an IPABUSE integration), and Web Proxy: IP address known to act as a Web Proxy (added if you are using an IPABUSE integration).

/ 7.5.1 - Cyber Threat Intelligence Program Pt1

/ 7.5.2 - Cyber Threat Intelligence Program Pt2

- Security alerts are generated in real-time and can be sent via email, Telegram, or mobile devices. There is out-of-the-box integration with several different SIEMS and SOAR platforms so alerts can also be sent in real-time, too.
- The CounterCraft Deception Platform provides a wealth of information including PCAP, Memory Dump, IOCs, Telemetry, TTPs, file hashes, malicious binaries, and post-breach activity (commands/calls made by threat actors). We have ~50 out-of-box connectors and a RESTful API that allows us to integrate with various SIEMs in addition to Syslog Servers and CTI tools like VirusTotal.

- The CounterCraft Deception Platform reports in real-time all activity that happens within the deception environment no matter if it's a BOT or APT (human threat actor). All of these events, alerts, notifications, and Threat Intelligence are stored within our platform for a specified amount of time.
- You can use the real-time tailored actionable threat intelligence with context (MITRE ATT&CK/ENGAGE) in addition to the high-level gap analysis information via NIST 800-53 to harden your production defenses.

If your agency is currently working towards implementing zero trust principles into your environment and you want to take this opportunity to implement proactive cybersecurity measures, feel free to reach out to us for more information on how CounterCraft can be a force multiplier to your ZTA strategy. Contact us for a demo today.

Implementing zero trust strategy

The zero trust model, if implemented correctly, can be effective when it comes to protecting against cybersecurity threats. However, it's not the magic bullet many organizations are hoping for.

A mature cybersecurity approach involves incorporating models like zero trust, best-of-breed cybersecurity tools, training, integration, established SOPs + SLAs, and collaboration. It also involves taking a proactive cybersecurity stance instead of the standard reactive one.

To understand how CounterCraft can enhance your zero trust initiative and help your organization take a proactive cybersecurity stance please contact us for a technical briefing.

About us

If you action one thing, make it an alert from CounterCraft.

CounterCraft is a leading provider of deception-powered threat intelligence solutions designed to empower organizations to proactively defend against cyber threats. With CounterCraft, organizations can detect threats early, collect specific, actionable threat intelligence, and stop threats before a breach occurs.

By leveraging advanced deception technology, including digital twins and lateral movement traps, CounterCraft enables real-time threat detection and response, ensuring your valuable data remains protected. Take control of your cybersecurity strategy and equip your SOC team with the tools to defend effectively against modern threats.

Choose CounterCraft for Specific. Actionable. Threat Intelligence powered by deception.

Specific. Actionable.
Threat intelligence
Powered by Deception.

Find out more and request a demo

Get in touch