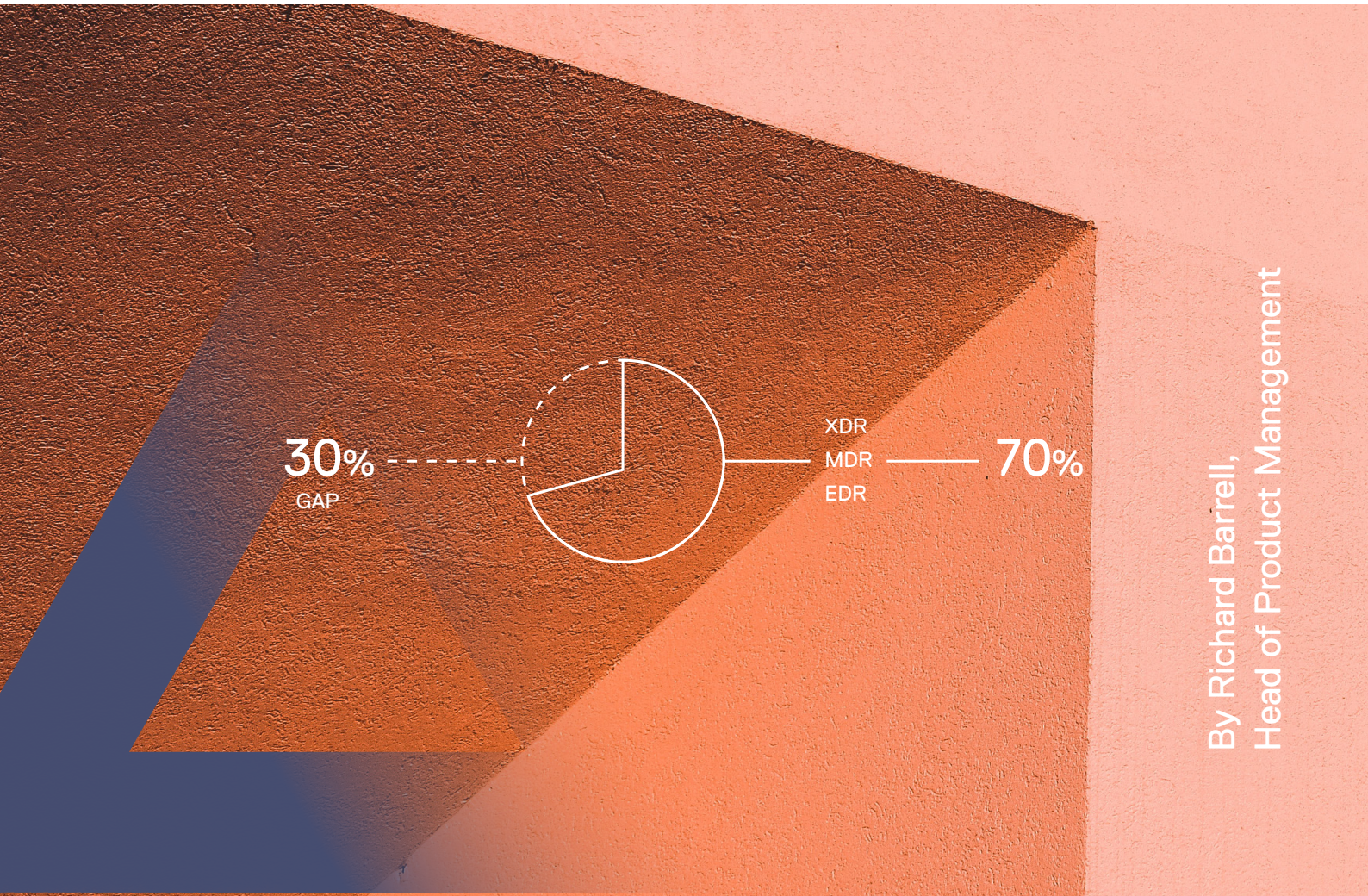
CounterCraft

Whitepaper

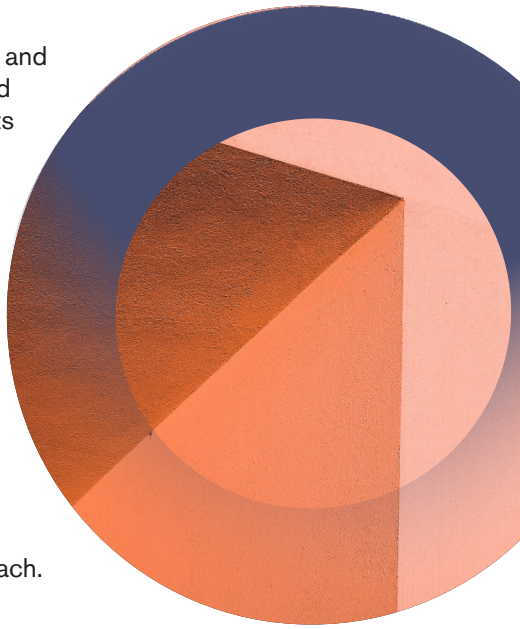
Incorporating Deception into Your XDR Framework



By Richard Barrell,
Head of Product Management

Incorporating Deception into Your XDR Framework: A Game-Changing Approach

Whitepaper



Endpoint, network, and cloud security are a significant concern for today's organizations and have only grown more complex with the institutionalization of hybrid and remote work and the consequent attack surface expansion. The growing number and utilization of products across the security stack marks a need for Extended Detection and Response (XDR) solutions that integrate and centralize visibility and response capabilities, all in one product. XDR also broadens a stack's scope to cover multiple surfaces at once: endpoints, servers, network security devices, cloud workloads, email, and beyond.

XDR provides comprehensive cybersecurity posture, as it integrates various cyber solutions from different sources. But it is also a double-edged sword, as it increases alert fatigue and the probability of receiving alerts from different product vendors at the same time. If not set up correctly, this can result in a multitude of problems for security teams, who don't have the resources to convert hundreds of weak signals from multiple vendors into high-confidence, unified alerts. All it takes is one mistake to open the door to attackers. This whitepaper covers how by incorporating deception technology with XDR frameworks, organizations can identify unknown threats and vulnerabilities from their external and internal surface. A proactive game-changing approach.

The Challenges of XDR

Alert Fatigue

Security infrastructures are constantly under attack. And as we've noted, SOC teams are drowning in alerts coming from their XDR platforms. Security teams put in an enormous amount of hours to investigate, monitor and respond to alerts, a vast majority of which are false positives.

This, in turn, demands either additional skilled resources or improved integration and automation of security tools. The lack of skilled resources is a well-known, industry-wide problem, and organizations are looking for solutions that can automatically contextualize incidents, provide suggested actions, and improve productivity of existing resources frequently using automated playbooks.

Dwell Time Still Too High

According to IBM Security, it took an average of 207 days to identify a breach and 70 days to contain a breach in 2022. That means that, on average, an attacker had nearly seven months inside a network before being cut off. EDR and XDR attempt to shorten that dwell time by detecting and responding to threats quicker. EDR's main strength is detecting and responding to threats at the endpoint level. However, XDR goes beyond that single security layer, securing other critical areas like network and cloud.

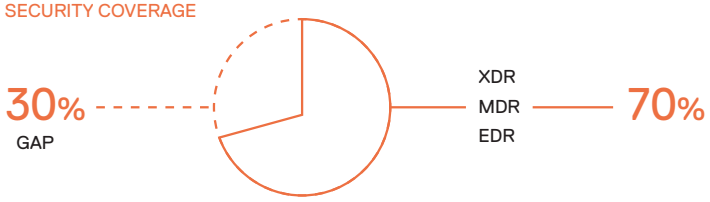
Every incident or compromise requires some form of lateral movement before the threat actor reaches their goal. This is good news for defenders who are able to spot and detect them. The bad news is that lateral movement tends to be relatively easy once threat actors have broken into the network. Dwell time has been largely reduced over the years due to increased deployment of better detection and response tools such as EDR, XDR, SIEM and SOAR tools. But is it enough?

Asset Vulnerabilities

One one hand, threat actors are constantly exploring new, advanced and automated techniques to exploit vulnerabilities and gain access to an organization's network. On the other, security teams are working endlessly to anticipate and stop these vulnerabilities, but most of the time are not able to resolve them immediately. Security teams must previously identify and understand each vulnerability, so they can correctly prioritize the most critical ones and efficiently organize their workloads.

A Limited, Reactive Approach

XDR alone does not meet all needs for long-term use cases beyond incident response, compliance and application and performance monitoring. What's more, XDR is reactive in terms of detection, monitoring and response to attacks. There is no doubt that XDR is currently one of the best cybersecurity tools, which is why Gartner® positions XDR at the peak of the Hype Cycle for Security Operations for 2022, but it is not fully able to anticipate attacks or identify unknown vulnerabilities and new techniques used by threat actors.



XDR needs behavior patterns from previous attacks to be able to automatically detect and respond to future malicious behavior. This is why XDR covers most of common threats and vulnerability issues, but is not yet capable of detecting unknown threats and APTs. This means the security gap left by EDR, MDR and XDR is around 30%.

What is XDR?

According to Gartner®, XDR is “a SaaS-based, vendor-specific, security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed components”. Forrester® describes XDR as an evolution of EDR. XDR ingests data from multiple security products such as EDR, NDR, SIEM and threat intelligence feeds, in order to correlate telemetry data that would otherwise be complicated to find and organize manually. By integrating with these various solutions, XDR also provides the ability to respond to threats either automatically or manually.

XDR is a tool that collects advanced analytics and transforms alerts from multiple sources into incidents from weaker individual signals to create more accurate detections. It aims to reduce the extensive range of cybersecurity vendor products, alert fatigue, integration challenges and operational expenses.

XDR Solution Highlights

/ Maximizes detection visibility across multiple security levels as it gathers, aggregates and normalizes threat data associated with endpoints, cloud workloads, network infrastructure and email.

/ Uses AI to transform big data from multiple vendor sources - including raw alerts and event data - into meaningful information that leads to better detection capabilities.

/ Provides a single, unified pane of glass for the organization’s entire security ecosystem, drastically reducing multiple independent product catalog.

XDR Solution Benefits

/ The consolidation of multiple data sources into one single interface, reduces the number of tools a security team needs to use and monitor and increases the visibility across the entire infrastructure. This improves security teams productivity and efficiency.

/ Thanks to AI and machine learning, XDR automates responses based on observed behavior within the environment, reducing the stress and fatigue of the security team.

/ The improved visibility and automation XDR provides means security teams have more time to prioritize, analyze and remediate alerts more efficiently.

What is Deception?

“Deception technology is an strategy to supplement an organization’s legitimate technology assets (files, databases, domains, servers, applications, credentials, etc.) with a maze of fake assets (decoys, lures, traps and bait) in an attempt to learn about attackers and misdirect them from the genuine articles. In doing so, the attackers are tempted into interacting with this fictitious environment and reveal themselves, while simultaneously triggering alerts that enable security teams to understand and respond to the attack that is in progress.”

— Gartner

Cyber deception is an active defense technology in which the most sophisticated deception vendors provide real-time actionable adversary intelligence and the capability to manipulate adversary behavior. Organizations using deception take back the advantage, putting threat actors in the defensive position, in part because they no longer know what is real or fake.

Deception Solution Highlights

/ Sophisticated deception vendors allow organizations to create complex digital twins deployed on prem, in the cloud or hybrid, tailored to any organization in a matter of hours.

/ Sophisticated deception vendors allow organizations to create custom fake users, each with a full pattern of life. These personas operate in the deception environment, with realistic behavior and unparalleled hands-on keyboard simulation luring attackers that fall for it.

/ On top of a high-fidelity detection alert, deception can also safely engage the attacker by luring them into a decoy and then sharing the TTPs and IoCs subsequently discovered into the XDR platform.

Deception Benefits

/ Accurate, timely and cost-effective solution. Cybersecurity breaches are active on enterprise networks for an average of 207 days until they are identified. High-fidelity detection combined with deflection and intel collection allows organizations to respond intelligently to attacks, while the attacker is quarantined the deception environment - reducing detection time to minutes or hours instead of weeks and months.

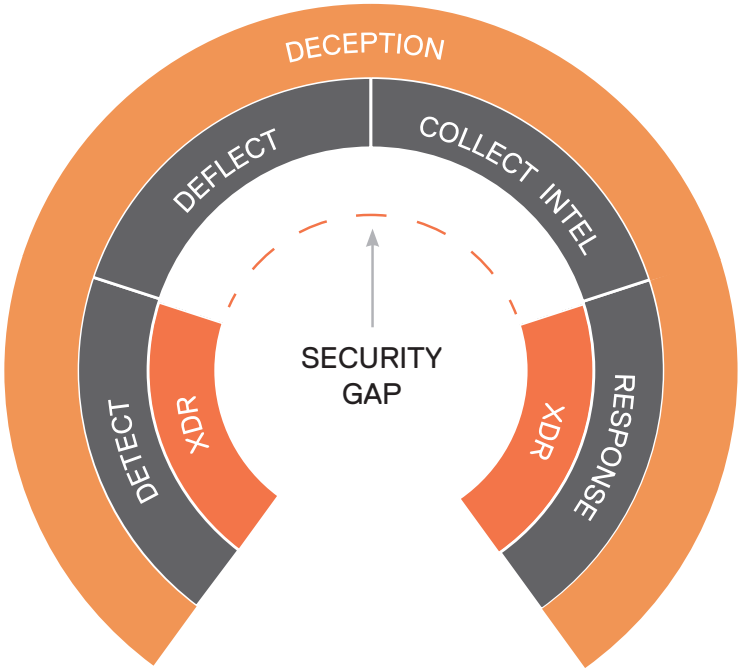
/ Fewer attack surface fissures. By identifying coverage gaps, high-risk vulnerabilities and common misconfigurations in the deception environment with built-in NIST 800-53 matrix and MITRE ATT&CK integrations, the attack surface is protected.

/ Active defense approach. This approach, used inside and outside networks, allows organizations to collect real-time, adversary-generated threat intelligence, providing them a priceless incident response capability that bolsters their entire defense from uncovered TTPs and IoCs.

How Deception Technology Benefits an XDR

The combination of XDR and deception is a great example of how complementary security technologies can extend their value and exponentially increase their effectiveness. Gartner® includes deception technology to be integrated in XDR platforms. Deception is a must have capability to add a greater layer of security, more use cases and threat intelligence.

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.



XDR AND CYBER DECEPTION COVERAGE

XDR and Deception Integration Benefits

/ Deception adds the ability to deflect and quarantine an adversary, while collecting of real-time, actionable and relevant intelligence to enable intelligent response and risk mitigation to the powerful XDR detection and response capability.

/ Correlate 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.

/ Highly automated deployment and management of advanced deception make integration into an XDR a simple task. Sophisticated deception vendors have built use case templates ready to run on the XDR platform. Deception provides XDR with multiple possibilities to identify the gaps in their existing security controls and remediate them.

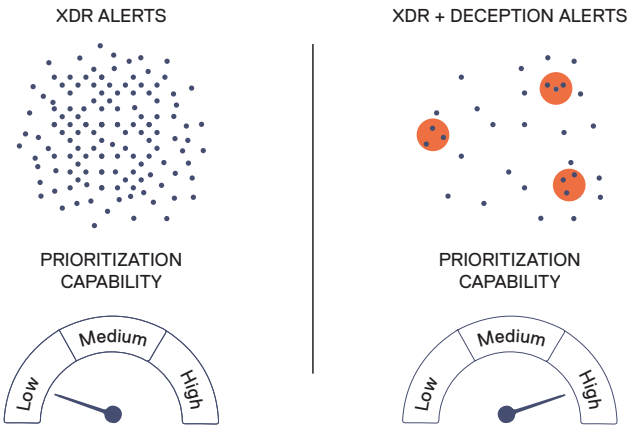
XDR and Deception Use Cases

Proactive Threat Hunting

In addition to early threat detection and unmasking every adversary, proactive threat hunting aims to reduce dwell times and avoid successful attacks. Deception lures attackers into the decoy environment, while SOC, IR and threat hunting teams sit back and quietly observe, gather intelligence, and uncover motives and objectives to finally thwart further activity on production systems. Threat intelligence gathered during threat hunting exercises has proven to be a magnificent addition to security teams and their XDR platforms.

Vulnerability Prioritization

Every organization has vulnerabilities that they are not even aware of. XDR platforms play a crucial role in identifying these vulnerabilities across the entire system. However, XDR's scope can only reach their internal infrastructure ecosystem. Adding deception as a feature to XDRs allows businesses to identify unknown risks and threats tailored to their external and internal attack surface and generate a prioritized list of vulnerabilities mapped into NIST 800-53 matrix and MITRE ATT&CK.



Contextualized Threat Intelligence

Security analysts and incident responder personnel (the SOC team) are constantly using alerts coming from the XDR for triaging threats and automating the appropriate response. However, the extreme alert fatigue that security teams suffer and the lack of resources and personnel often creates more problems. Integrating deception into XDR solutions helps incident response teams and security analysts focus on high-priority alerts that comprise the most significant risks to the organization.

Deception feeds adversary generated contextualized intelligence into XDR solutions with important information and context on IoC and TTPs. A security analyst 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. The data enrichment provided by deception gives the security analyst a complete picture of what happened and why in the event of an incident.

Conclusion

Integrating deception technology with XDR platforms helps organizations take back the advantage. Cyber deception greatly increases the difficulty adversaries have in carrying out their tasks, thanks to digital twins that divert them from the production environment. Once threat actors fall for decoys, they then reveal their entire playbook. Attacks become more costly and time consuming.

Cyber deception can be simple to set up and make it easier for security teams to detect vulnerabilities, thanks to full visibility across their external and internal attack surface. Thanks to the rich telemetry gathered, organizations can respond and strengthen their security posture while the attacker is still in the decoy environment.

Organizations need a consolidated single-pane-of-glass view of their entire security infrastructure. Integrating deception with XDR helps organizations identify unknown threats and vulnerabilities from their external and internal surface. With deception, organizations can engage in active defense and gather rich adversary telemetry useful in multiple use cases. Adversaries have become more sophisticated over the years, but organizations won't fall behind if they implement deception into their security ecosystem. Deception is the only solution that consistently collects adversary intelligence, even from novel threats, to put organizations one step ahead of attackers.

About Us

CounterCraft is a software company that goes beyond detection and response to provide proactive cybersecurity solutions and detect attacks faster for the world's leading organizations. Their premier product, CounterCraft **The Platform**™, consistently stops red teams, spear phishing, ransomware attacks and insider threats. This distributed deception platform is a global leader in active defense, with tooling that provides real-time intelligence and the capability to manipulate adversary behavior.

Find out more. Request a demo at

countercraftsec.com