XDR

PROACTIVE CYBER-DEFENCE STRATEGIES FOR THE EXTENDED ENTERPRISE

Industry White Paper | February 2022

TABLE OF CONTENTS

PRODUCED BY

CIO Academy Asia

Gerry Chng
Cybersecurity Advisor

TECH PRACTITIONER CONTRIBUTORS

Perry Young
Executive Director, Perimeter & Network Security, Standard Chartered

Abhijit Dasgupta
Global Head - Technology Risk, Control & Governance, ManpowerGroup

TECH EXPERT CONTRIBUTORS

Valerian Rossigneux
Director of Sales Engineering, CrowdStrike

Chris Thomas
Senior Security Consultant, ExtraHop

Lee Dolsen
Chief Architect, Zscaler

Protection Beyond the Endpoint

Today's organisations are facing a deluge of advanced threats such as supply chain attacks and ransomware. Being targeted by such attacks is not a matter of "if" but "when". So, organisations must adopt an assumed breached posture, and focus on how they detect and respond to these threats as quickly as possible. Advanced threats need to be addressed on the inside and dwell time must be minimised.

While organisations are familiar with tools such as Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM), cyber-threats today proliferate through hidden vulnerabilities found in email, endpoint, server, cloud workloads, and networks, many of which are signature-less and go undetected while traversing a corporate network for a long time. In response, Extended Detection and Response (XDR) strategies have emerged to help organisations and their third-party partners stay ahead of cyber-attack from the edge to the core.

An effective XDR cybersecurity strategy weeds out attacks and isolates threats before they cause significant damage. Operating as an ecosystem, it collects, analyses, and makes sense of data feeds from targeted threat detection and response tools to provide greater visibility and to enable more effective detection and response of security incidents. The data that XDR collects encompasses network and firewall traffic, cloud environments and workloads, identity and access, and a wide range of endpoint devices from laptops and workstations to mobile devices and servers, using advanced analytics and automation to detect threats and initiate multi-domain action information from the massive data volumes.

By breaking down the silos between endpoint, network, and the cloud, an XDR strategy utilises advanced technology-driven analytics to expand visibility to the threat landscape, derive high-fidelity intelligence for faster and more effective detection and response.

"In many large organisations, there are a lot of silos as part of the legacy build-up. When an incident hits, the different silos struggle to understand the overall architecture as the design and operations sit in different teams often with different KPIs and measurement. Integration is key and there must be a demonstration of ROI and value to the business."
– Abhijit Dasgupta

The Increase in the Frequency and Impact of Threats

The rapidly changing environment

The last two years have seen organisations accelerating their digitalisation plans in the wake of the Covid-19 pandemic. This has resulted in an increasingly heavy digital reliance, as well as an interconnected but vastly distributed workforce.

In a recent report, the Institute of Electrical and Electronics Engineers (IEEE) reported that 83% of their survey respondents indicated that "Maintaining strong cybersecurity for a hybrid workforce — remote and in-office workers" was a "Somewhat Challenging" or "Very Challenging" task (IEEE 2021).

Traditional security tools that are typically on-premises have a hard time coping with this reality due to lack of visibility and data protection for remote workers. Threat actors have wasted no time in profiteering from this opportunity where the blurring of the traditional boundaries and the rapid change in the technological environment have rendered existing security management policies and controls ineffective.

Rise of eCrime

As highlighted in CrowdStrike's 2021 Global Threat Report, eCrime has become an active and thriving ecosystem where financially motivated entities engage in activities for their financial gains (Crowdstrike 2021). Particularly,

there has been a consistent trend of events leading to a rising eCrime Index (ECX) from December 2020 till the date of that report in February 2021. We have since continued seeing the news headlines in the months in significant ransomware attacks on companies such as Colonial Pipeline, JBS Foods, and Acer just to name a few.

In other similar studies, the Zscaler "ThreatLabZ Ransomware Review: The Advent of Double Extortion" analysed threat telemetry from 150B+ daily transactions and noted a sharp rise in double extortion ransomware attacks since late 2019 (Zscaler, 2021).

ExtraHop has also highlighted the importance for a holistic coverage of east-west traffic in an assumed breached posture in a recent blog post (ExtraHop, 2022). Despite all preventative measures, incidents have proven how attackers are able to establish a foothold in the organisation and subsequently move laterally in the blind spots. With the ever expanding cyber attack surface, it is close to impossible for security teams to stay on top of new vulnerabilities and the evolving threat landscape. As such, technology experts have developed sophisticated network traffic monitoring and threat response capabilities more commonly known today as Network Detection & Response (NDR).

Gartner defines NDR as using "non-signature-based techniques (for example, machine learning or other analytical techniques) to detect suspicious traffic on enterprise networks. NDR tools continuously analyse raw traffic and/or flow records to build models that reflect normal network behavior."

An effective NDR capability embedded within the broader XDR strategy helps to illuminate the potential blind spots for a more comprehensive coverage of the threat environment.

These cybersecurity incidents disrupt the business significantly and carry with it reputational, regulatory, and financial losses. There does not seem to be a slowdown, and it has been estimated that such attacks would cost the industry up to $20 billion in 2021 (Global [Re]Insurance 2021). While companies work

hard to put in security measures, the key challenge has been the ability to draw meaningful insights from the volume of data to minimise the mean-time-to-detection (MTTD) and mean-time-to-response (MTTR), two very important metrics to measure how quickly one is able to detect and respond to threats.

Expanding Attack Surface – Beyond Traditional Endpoints

Making Sense of Growing Network Vulnerabilities

The large-scale shift to remote working has driven a big push for more robust endpoint protection, as remote workers access corporate applications and data via their personal computers, mobile phones and even through virtual desktop environments. However, today's enterprise networks are no longer accessed only by such endpoint devices – cloud workloads, SaaS APIs, Virtual Machines and even IoT devices are connected to the network that is often outside of the company's on-premises defensive perimeter.

While sophisticated EDR solutions provide continuous monitoring and deep insights into endpoint activities and do a great job in isolating threats at the network edge, access controls to authorised applications and traffic inspections are not effective in a remote work environment. The siloed nature of telemetry inputs across varying types of endpoints also means that more sophisticated, signature-less threats and Advanced Persistent Threats (APT) could go undetected for long periods of time.

> ***"By leveraging Zero Trust architectures to make the real applications dark, while creating decoys which are easily discoverable, you can obtain high-fidelity alerts when an adversary inadvertently attempts to access the decoys." – Perry Young***

While the industry came up with Security Information and Event Management (SIEM) solutions years ago to address the sprawl of logged data, security teams can easily be overwhelmed by the volume of alerts and siloed nature

of the logs. Clearly, security leaders are looking to leverage true machine intelligence to aid in sifting through the noise to better detect threats and identify root cause.

Increased sophistication

The attack vectors have increased in sophistication and are well-funded activities either by criminal syndicates or state-sponsored actors. Software vulnerabilities remain a key weakness that hackers exploit to gain access to the organisation. While many of the hacks could have been prevented by having a more robust and effective patch management system, there has also been a rise in the availability of zero-day (0day) exploits due to a thriving dark-web market.

Hackers are also shifting to providing "exploit-as-a-service" to maximise their potential returns from the 0day exploits, thereby increasing the overall threat landscape to organisations.

"The use of Active Defence results in less false positives and penalizes the attackers for mistakes made in their operations. It really puts the bad guys in a much more dangerous place because they don't know if the service they are interacting with is real or fake, and puts them in a position where they have to be much more careful." – Lee Dolsen

According to the 2021 CrowdStrike Security Attitude Survey, nearly half (47%) of security professionals believe they can't respond to threats faster is due to too many disparate solutions that don't easily integrate for proper protection and prevention.

Faced with this asymmetry between the attackers and defenders, recent XDR strategies encourage high-fidelity telemetry combined with the use of active defenses to confuse and lure attackers into making mistakes. For example,

Zscaler, which has also recently been recognised as a Leader in the Gartner Magic Quadrant for Security Service Edge (SSE), offers capabilities that enable cyber defenders to create a set of decoys, lures, and honeynets within the cloud environment which engage attackers and allow early detection and remediation. In the next section, we will elaborate on the key pain points by the security operations teams, and how XDR as an emerging strategy holds the promise to minimise this information asymmetry that exists.

Security Operations Pain Points

Given the dynamics between the attackers and defenders, it is not surprising that the attackers will always be one step ahead using traditional approaches. The readiness of organisations against the increasing threat landscape is also fragmented based on the organisation size and available resources. While smaller organisations naturally struggle with the availability of tools, resources, and the corresponding data, larger organisations struggle with the high volume of false alerts, security components that are not unified, and trying to draw actionable insights from costly investments.

Poor visibility to the security posture

Organisations have shifted from monolithic architectures to composable infrastructures. There is a struggle to obtain visibility to meaningful telemetry, though the challenge is not just about collecting more data, but the right types of data that can be properly normalised and aggregated to provide necessary insights.

Many organisations today rely on siloed solutions, each providing their alerts and dashboards. Often, these lack the sensing capabilities to correlate information across multiple stacks which might provide a clue on a successful attack. To make matters worse, security managers are flooded by false-positive or irrelevant alerts, and under such conditions, it does not take long for analysts to be lulled into the false sense of security or alert fatigue.

Compliance mindset with insufficient emphasis on detection and response

For a long time (and still is at many matured organisations), organisations are driven by the compliance mindset towards Cybersecurity. A negative side effect of this emphasis is the preference of prevention over detection and response. To be clear, we still want to prevent an attack from occurring, but we need to spread our investment to enable us to rapidly detect and respond to attacks when they happen.

In today's 0day-ecosystem, that mindset played to the advantage of the attackers again as we had no means of protecting against 0day vulnerabilities fully, and we are ill-equipped to detect and respond effectively to these successful attacks.

Best-in-class vs. integrated solution

Organisations have also been torn between adopting a best-in-class approach to solution selection, versus investing in an integrated suite of solutions while avoiding vendor lock-in. While the former approach gives greater flexibility for the selection of solutions, it often results in significant efforts to manually integrate the solutions to achieve cross-platform information feeds that provide the much-needed telemetry. The latter might provide better integration at the cost of vendor lock-in or the inability to select a separate third-party component that outperforms the solution within the integrated platform.

Current defenses do not perform well on east-west traffic behavior

Network segmentation is a major component of any cybersecurity strategy today. While several organisations have begun embarking on enterprise-wide Zero-Trust Network Access or similar policy-based network segmentation journeys, many face challenges in keeping their access policies updated. There is a lack of adequate intelligence from network telemetry and user access logs for security teams to identity potential vulnerabilities and weaknesses.

Organisations have made increasing investments into firewall-based access control solutions. While useful, these solutions monitor and block north-south inbound and outbound traffic. A strong ZTNA solution must be one that is tightly integrated with network monitoring tools which has deep visibility into east-west network traffic and include the remote user traffic over the network that the company does not own. Insider threats and APTs have a much greater chance of early detection with insights on suspicious east-west traffic behavior, which then provide valuable inputs for ZTNA policies to be tightened.

In addition, while there are enhanced security components in the form of EDR, blind spots exist within the network environment where such components may not be implemented due to compatibility or operational requirements (e.g. IoT devices, systems without agents, etc.). This has added to the advantage of the hackers as they learn to perform their lateral movements and reconnaissance activities within the blind spots of the environment.

"Visibility is key. You can't have security if you cannot see your assets, especially with the device on many networks today such as IoT, security applications or other vendor applications where you are not allowed to install agents." – Chris Thomas

As such, it is critical for organisations to ensure that their network defenses are able to capture the telemetry created by both managed and unmanaged apps and endpoints, so that cyber breeches through such backdoors have a higher chance of detection. More importantly, organisations must have adequate response protocols automations pre-programmed to automate incident response, alert escalation and isolate infected network systems, endpoints, cloud applications and workloads.

The promise of XDR

An emerging concept coined as Extended Detection and Response (XDR) appeared with the vision to address the challenges highlighted.

Gartner defined XDR as a "platform that integrates, correlates and contextualises data and alerts from multiple security prevention, detection and response components. XDR is a cloud-delivered technology comprising multiple point solutions and advanced analytics to correlate alerts from multiple sources into incidents from weaker individual signals to create more accurate detections. It aims to reduce product sprawl, alert fatigue, integration challenges and operational expense, and will appeal to security operations teams that have difficulty managing a best-of-breed solutions portfolio or getting value from a SIEM or SOAR solution." (Gartner 2021a)

While XDR is still at a relatively early stage, there can be great benefits if a collaborative ecosystem can be formed where each partner contributes to part of the broader benefits based on their strength and focus. There is great potential for this XDR strategy to address the challenges highlighted earlier.

Best-of-breed ecosystem providing insights from multiple sources

Today's operating environment is multi-modal and comprises both components and infrastructure across a very wide spectrum of solutions. It is unlikely that a single vendor would have all the security components that would be able to manage all the potential threats across such a diverse landscape, as well as catering to all security management processes from monitoring to triage.

An XDR ecosystem that encourages and permits partners to offer their strength while unifying the threat information and process with end-to-end-visibility can positively enhance the customers' capabilities to deal with today's threat landscape.

Faster, more reliable threat detection

Having access to higher-quality data across different component stacks, XDR platforms allow security managers to identify the origin and extent of the threats more rapidly. Augmented with algorithmic capabilities and automated response playbooks, this makes it easier for teams to shorten the detection

and response windows thereby limiting the amount of damage that could have happened.

> ***"The XDR ecosystem attempts to link together telemetry from endpoint, network, and identity. These can then be further enriched with threat intelligence that brings it to the next level. Who is behind the attack? What is their intended motivation? Do they want to perform extortion, or intend to stay low and slow for a long time?"***
> ***– Valérian Rosigneux***

Most matured organisations embark on proactive and regular threat hunting exercises. Having access to high-quality data across the operating environment benefits the threat hunters as they hunt for clues alluding to the presence of an attacker.

Streamlined and coordinated response

By leveraging high-quality data and AI/ML algorithms, XDR platforms allow security teams to take advantage of pre-planned automated response playbooks to perform the investigation and triage, even though some of the response workflow would span more than one security platform. This allows both consistency and speed in the activities across multiple teams and/or with third-party crisis responders.

Regardless of how algorithms and data can be embedded into such systems, it will never replace the role of the human analyst. Instead, there is potential for the platform to augment the human analyst to perform value-added activities in the investigation and response.

Key characteristics of XDR

There is currently a list of pure-play cybersecurity companies boasting XDR

capabilities as part of their offerings to address this challenge. Obviously, the benefits of unification would be lost if the industry diverges on its own definitions of XDR.

"From an XDR standpoint, it presents to combine the benefits of an SIEM and SOAR platform, and make use of machine learning and Artificial Intelligence to scale out the monitoring and analysis. It becomes too problematic and too much of an administrative burden to correlate the data manually and take the appropriate actions."
– Perry Young

The following are some key characteristics of what a desirable outcome should look like.

EDR at the Core

Every successful XDR solution has its foundation based in EDR. Or as Forrester phrases it in its recent XDR report: "Good XDR lives and dies by the foundation of good EDR." The point is that XDR builds on the principles and processes that EDR first establishes, which XDR then optimises and extends from there.

More tactically, endpoint detections remain the focal point of your XDR capabilities even as they mature. Endpoint detections act as clear markers, and XDR enriches those detections and the response workflows that XDR orchestrates.

Ecosystem - not a single solution

It is quite clear that to address the challenges highlighted above, it is nearly impossible for a single cybersecurity provider to be able to address the entire threat spectrum covering networks, endpoints, hybrid on-premise and cloud infrastructures, AI and machine learning analytics, IoT data collation, event monitoring and orchestration, automated threat response, visualisation and reporting.

As such, while some tech partners may possess multiple capabilities across the stack, a truly successful XDR strategy would require an ecosystem with seamless and coherent collaborations between participating partners.

Unified, threat-focused event analysis and management

With the right security components and visibility, XDR holds a promise to provide a unified approach to managing the threat landscape in two key dimensions. On one dimension, it provides a unification across the different types of infrastructure and endpoint designs that organisations typically have, ranging from endpoints such as IoT devices and workstations to on-premises and cloud security platforms. On the other dimension, it also streamlines the security management process from monitoring and detection to response and remediation.

> ***"XDR is not just about taking all the data and putting it somewhere. That is not going to solve the problem. That is why the XDR Alliance seeks to define what we want to collect, why we need it, and map it to the threat landscape. One day, we hope to be able to threat hunting at scale by querying across the environment regardless of endpoint, network, or cloud workloads."***
> ***– Valérian Rossigneux***

With the unification of the components, processes, and telemetry, there is an opportunity to better leverage algorithms to augment the human analyst performing the monitoring and triage tasks.

Enhanced endpoint visibility and protection

One of the key challenges that XDR tries to address is the sporadic coverage of the environment due to the lack of integration. By pulling together the monitoring capabilities across the diverse types of infrastructure components, it provides more comprehensive coverage of the environment across the

participating solution stack. The information collated from the NDR provides a wealth of information that may not be captured by the endpoints either due to logging levels set or the availability of log agents.

By collating information across the environment, it is also possible to make use of algorithms to boost the signal to noise ratio thereby increasing the chances of picking up an attacker lurking or navigating within the environment with speed and accuracy.

Unified and consistent telemetry across networks, endpoints and cloud workloads

While more work must be done than just collating raw data into a single platform, such unification amongst ecosystem partners offers the opportunity to streamline the types of information logged, and how they are presented. This makes it easier for the XDR platform and downstream processes to embed AI/ML algorithms in the platform or enable self-service extraction of data for bespoke AI algorithms.

"Visibility to the assets is crucial. Without an accurate asset inventory, you can have amazing security solutions but they will not work effectively. The problem is compounded when organizations are starting their migration to the cloud which makes visibility an even more important priority."
– Abhijit Dasgupta

XDR platforms can also incorporate threat intelligence information from partner sources which may include known attack methods, tools, origin, and attack tactics and techniques across multiple attack vectors.

Cloud-native architecture offering greater scalability and agility

As organisations shift more workloads in the cloud infrastructure and achieve

a hybrid setup, the challenges go beyond just gathering insights from on-premises and cloud-hosted infrastructure. The cloud infrastructure offers a uniquely different way to rearchitect the workloads which can introduce a different set of challenges for security monitoring.

An XDR platform with either existing cloud capabilities, or where cloud providers are present as ecosystem partners can allow better integration of cloud capabilities such as infrastructure-as-code (IAC) and policy-as-code (PAC).

Investigation and response

One of the important components of existing security platforms, and more so for XDR platforms, is the ability to shorten the mean-time-to-response. Contextual data presented during the investigation phase helps security analysts to rapidly identify the origin and extent of the damage caused, or the Indicator of Attacks (IoA) even before the system has been impacted. This allows the team to quickly determine the best course of action and is supported by automated response playbooks that aid in the containment and recovery of the environment to a known good state.

This is arguably one of the most important outcomes to achieve cybersecurity resilience in detecting and responding to threat vectors by reducing the MTTD and MTTR.

Essential Components – Modularity & Interoperability is Key!

As the XDR ecosystem will need to comprise multiple solution providers each with their own strengths, modularity and interoperability of the solutions is key for the XDR strategy to work well. Below are some highlights on the essential components.

1. Native Endpoint Visibility and Protection

EDR capabilities such as those delivered by cybersecurity providers such as CrowdStrike, represent a new breed of next-generation cloud-native EDR market players. Compared to established endpoint protection services, CrowdStrike is fully cloud delivered, which means all agent installations, endpoint telemetry monitoring, vulnerability patching and threat remediation and isolation happens fully over the cloud.

EDR capabilities today layer on AI and ML capabilities not only to detect Indicators of Compromise (IoCs) but also leverage context-based intelligence to detect Indicators of Attack (IoAs), allowing security teams to take pre-emptive action against potential threats outside of the corporate network.

2. Network Detection and Response (NDR)

Security teams can no longer only solely rely on signature-based security tools to detect network security threats that require broader analysis. Signature-based security tools are unable to detect new forms of attacks and do not analyse data from multiple data sources over time to recognize potential threats.

As advanced and stealthy cyber attackers might be, all breeches cross the network in one way or another. The use of machine learning capabilities give organisations the ability the detect subtle anomalies in network activity even from hidden endpoints, unmanaged cloud workloads and foreign IoT devices that other point solutions in the XDR stack may have not been able to detect.

Importantly, NDR plays a crucial role in piecing together the log events from various inputs as any malicious activities beyond a single server will need to traverse the network and these logs can highlight the intent and impact of the attempted attacks. As ExtraHop has described in their blog article (ExtraHop, 2022), this is the "mid game" of the overall kill chain in which the network presents a good opportunity to spot the lateral movements that the threat actors are performing.

3. Cloud-enabled capabilities

On the networking front, remote office users access cloud-based applications and company data remotely through a network service provider, completely by-passing corporate network. Modern cloud-based network security providers like Zscaler, deployed in 150+ data centers around the world, serve as an inline traffic security hub and apply security policies to protect remote users and applications. The cloud network security is an aggregation of numerous security functions including SSL decryption, secure web gateway, DNS security, IPS, sandboxing, inline data leak prevention, and out-of-band CASB, etc.

Most importantly, the Zscaler Zero Trust Exchange implements access control using a concept of application segmentation, linking one authenticated user to only one authorised application in each session. This achieves micro-segmentation at the least privileged level. Since Zscaler is implemented inline between the user device and the application anywhere in the world, the visibility into network traffic becomes very valuable as for the implementation of XDR. Also due to the large amount of traffic telemetry, employing AI and machine learning becomes a necessity to make sense out of these data and translate data into insights.

Many organisations have adopted parts of a ZTNA strategy, often implementing 'best-of-breed' capabilities from independent point providers. While these capabilities do very well on their own, orchestration and integration challenges arise and impede other processes such as incident response automation and data normalisation for forensics and investigation.

For example, multiple alerts coming from different cloud security and isolation do not corroborate threat data and provide insights as to whether these alerts are caused by a single attack from a single threat actor, or represent separate attacks, either from a group of coordinated attackers or from independent perpetrators. With the current shortage of highly skilled cyber talent, a majority of organisations will struggle to build the resources and maturity to build a 'single pane of glass' across the key components within the zero-trust security framework.

For most organisations, Gartner predicts that by 2025, 80% of organisations seeking to procure zero trust security related services will purchase a full-service suite, which Gartner has now defined as the Security Service Edge (SSE) rather than stand-alone cloud access security broker, secure web gateway and ZTNA offerings, up from 15% in 2021.

.4. Security Orchestration and Response (SOAR)

SOAR is a key implementation that allows detection and response teams to perform their triage activities using established playbooks consistently and rapidly. SOAR offers a high level of security automation to quickly isolate infected devices and networks, escalate urgent threats up the right response chain and integrate response processes across different cybersecurity products.

5. Strategic Partnerships needed to integrate NDR with ZTNA Capabilities

ZTNA plays a critical role not only in the prevention of unauthorised access into different segments of the network based on network policies set by security teams, but also serve to prevent malicious actors from freely traversing the network (east-west) should they manage to breach one segment of the network. By making application IPs and URLs invisible, attack surfaces can be eliminated because attacker cannot attach what they cannot see.

New features such as network micro-segmentation and application segmentation are also orchestrated within the ZTNA architecture.

However, Zero Trust policy controls require security policies to be regularly updated based on the permissions rights and changing user profiles within the organisation. Ongoing configuration changes across each layer of the IT stack also mean that overtime, zero trust policies will decay and result in hidden vulnerabilities in policy controls. Network telemetry data provides an almost immutable snapshot of user access activities within the network, as well as data and file transfers patterns between users, endpoints and applications. With AI and ML intelligence, NDR solutions hold great potential to provide meaningful alerts and recommendations

for security teams to detect weaknesses in existing policies and update them proactively before these loopholes get exploited by cyber attackers.

This way, security teams can leverage this intersection point of ZTNA and XDR to proactively strengthen zero trust policies, and similarly, a strong ZTNA architecture plays a complementary role in threat response to quickly and effectively isolate a malicious attacker and quarantine infected endpoints, files and applications in the event of a breech.

What does XDR mean to Cyber Defense Strategies

Cyber defenders are no longer only deterring and detecting attacks. XDR with its key components enable cybersecurity teams to actively seek out potential threats within the network and patch network and cloud vulnerabilities before cyber attackers discover them.

With the blurring of the traditional cybersecurity perimeter, the lowest common denominator to threat defense across the IT environment no longer lies just at the firewall. The new perimeter now is spread across the entire network. Even though attackers may successfully breach perimeter defenses, XDR capabilities today are designed to pick up on the trail of breadcrumbs left behind when attackers traverse the IT network to significantly enhance threat detection success. Breaches can't be stopped but they also hardly cost organisations, it is the resulting disruption of mission-critical services or the loss of critical data that do. CISOs need to pay attention to stopping attacks at the mid-game as attackers move laterally, before the crown jewels are discovered and compromised.

CISOs also should evolve their organisations toward Active Defense, leveraging deception tech such as honey nets to trip cyber attackers. This gives some advantage back to cyber defenders and unlocks precious time for remediation and preventive action. Deception tech, however, will not yield any results when implemented as a standalone solution. It can only

serve its purpose when a strong data feedback loop between NDR and Zero Trust policy engine is already in place.

Conclusion - The future of XDR

The technology is still at the early stages of development. According to Gartner, XDR is currently listed in the Innovation Trigger cycle, which is characterized by an innovation created by a breakthrough and resulting in significant media and industry interest (Gartner 2021b).

While some cybersecurity companies have developed their own vision of XDR and described how their solution meets the expectations of the benefits, some other vendors have taken an ecosystem approach to fulfil the benefits of XDR.

This covers a broad spectrum in the two dimensions that this report has highlighted earlier on infrastructure components and the security management process.

Executed well, this could offer opportunities for organisations to maintain a best-in-class selection of vendors (assuming their solutions can be integrated in a unified manner to the other platforms) while at the same time benefiting from comprehensive coverage of their environment.

The eventual goal should be to gain access to high-quality telemetry across the environment, apply algorithms on the data to augment human analysts, and ultimately to reduce the mean-time-to-detection and achieve rapid response.

REFERENCES

- Crowdstrike. 2021. *"2021 Global Threat Report: Adversary Trends & Analysis." CrowdStrike. https://www.crowdstrike.com/resources/reports/global-threat-report/.*
- CrowdStrike. 2021. *"CrowdXDR Alliance: Extended Detection and Response — United." CrowdStrike. https://www.crowdstrike.com/partners/crowdxdr-alliance/.*
- ExtraHop. 2022. *"IT in the Crosshairs of Modern Ransomware" ExtraHop. https://www.extrahop.com/company/blog/2021/ransomware-gangs-expand-playbook/*
- Gartner. 2021a. *"Hype Cycle for Endpoint Security, 2021." Hype Cycle for Endpoint Security, 2021. https://www.gartner.com/interactive/hc/4004605?*
- Gartner. 2021b. *"Market Guide for Extended Detection and Response." Market Guide for Extended Detection and Response. https://www.gartner.com/document/4007995.*
- Global [Re]Insurance. 2021. *"Ransomware costs to reach $20 billion in 2021." Ransomware costs to reach $20 billion in 2021. https://www.globalreinsurance.com/ransomware-costs-to-reach-20-billion-in-2021/1437206.article.*
- IEEE. 2021. *"The Impact of Tech in 2022 and beyond." The Impact of Tech in 2022 and beyond. https://transmitter.ieee.org/impact-of-technology-2022/.*
- Zscaler. 2021. *"ThreatLabZ Ransomware Review: The Advent of Double Extortion" Zscaler. https://www.zscaler.com/blogs/security-research/threatlabz-ransomware-review-advent-double-extortion.*

For Enquiries, Please Contact:

David Chin
Deputy CEO
CIO Academy Asia
david@cioacademyasia.org