Bridewell Consulting

Whitepaper

Bridewell CONSULTING
Above. Beyond. Always.

Digital transformation drivers across CNI

Please visit our website at www.bridewellconsulting.com
or call us +44 (0) 3303 II0 940

Whitepaper

Bridewell CONSULTING
Above. Beyond. Always.

Introduction

Digital transformation drivers across CNI

In the UK, we are all reliant upon Critical National Infrastructure (CNI) in our daily lives. CNI providers deliver services such as safe energy and clean water to our homes, enable international trade and travel through transport, put food in our mouths and keep money in the banks. Just like other organisations globally, these industries are going through their own digital transformation journeys. In a world where security risks could put human lives on the line, there are real risks to be managed.

In the UK, we are all reliant upon Critical National Infrastructure (CNI) in our daily lives. CNI providers deliver services such as safe energy and clean water to our homes, enable international trade and travel through transport, put food in our mouths and keep money in the banks. Just like other organisations globally, these industries are going through their own digital transformation journeys. In a world where security risks could put human lives on the line, there are real risks to be managed.

Bridewell works heavily with CNI organisations and has experienced first-hand some of the complex challenges faced across the industry. To develop insight that can be used by our customers and peers, we conducted independent research which involved 250 UK IT and security decision-makers across five key CNI sectors: aviation, chemicals, energy, transport, and water to understand and help them achieve their goals. The full report is available for free below.

Download CNI Report >

One of the things that became clear is that the convergence of IT and Operational Infrastructure (OT) and increased legislative requirements such as the Network and Information Systems (NIS) Regulation is enabling transformation. This is driving a clear need for an integrated approach to cyber security, specifically around threat detection and response. With 94.4% of CNI organisations already embracing cloud for the delivery of OT solutions, this is where an integrated Detection and Response solution, such as the Bridewell Microsoft Sentinel and Defender XDR delivered by a 24x7 Managed Security Partner can offer the protections and skills required. This can also reduce pressure on Cyber Security budgets.

Bridewell
CONSULTING
Above. Beyond. Always.

Context

Access to cloud technologies is changing business models in all sectors, and providers of CNI are also looking for ways to improve service and availability whilst reducing costs and risk. In fact, with 98% of all CNI providers already in the cloud and 56.8% having OT systems connected to or accessible from the internet, we are past the early peak of adoption and racing ahead.

The cloud offers the ability to replace aging infrastructure without the CAPEX required to build systems on premise and enables the adoption of newer application architectures or PaaS (Platform as a Service) solutions that unlock the real value in moving to the cloud. Over 79% of respondents to the research stated that their main OT systems were over five years old and 34% over ten years, highlighting a real need to manage security on aging technology.

The large numbers of geographically diverse pieces of equipment, controls and sensors within the OT environments already necessitates the need for a range of communication services to enable monitoring and process automation. The cessation of analogue services by communication providers and replacement with digital IP systems such as ADSL, 4G and the upcoming 5G are enabling organisations to further increase data-analytics and process automation. This can improve performance and support technology advancements, whilst lowering cost.

As the technologies that are used for IT and OT combine, physical boundaries continue to disappear and the want to distribute monitoring and management of the environments increases, there continues to be a trend to connect and integrate the two worlds, introducing risk and holes where there were previously walls. CNI providers have seen cyber-attacks increase by 50% in the last I2 months, leading to an average of nine attacks per year. 47% of CNI leaders have increased stress levels and it's clear to see why.

We now need to respond to these changes by creating a holistic view of cyber security that provides visibility of the physical OT elements and the ethereal cloud and identity systems. This can be challenging with different owners of IT and OT cyber security within your organisation.

Whitepaper

Bridewell
CONSULTING
Above. Beyond. Always.

OT monitoring challenges

According to our research, OT is still mostly constructed of discrete isolated environments, without accessibility from the Internet or corporate networks. This makes it difficult for threat detection and SOC teams to monitor for indicators of compromise that could allow a response before a security incident occurs CNI organisations are, therefore, presented with a difficult question - Should these environments be made remotely accessible to support proactive security threat detection? Because in doing so, this can expose critical infrastructure to a world of external threats they may not be equipped to defend against. There are solutions to address these concerns. One option could be the use of a data-diode device; a one-way communication device that allows data to be sent out of the network yet has no physical path for threats to ingress into the environment.

However, before we even consider this, we need to determine if there is useful security data available. Older OT equipment may not generate security events, particularly if they do not have an IP interface and only support serial based communications. The data may also be difficult to extract. An operator interface such as an HMI may log some user data locally, but it may not support any protocols to allow this data to be easily transmitted to a monitoring platform, for example, via syslog.

So these restrictions may give rise to other security monitoring needs to offer the visibility, such as network level analysis. Microsoft's acquisition of CyberX and their integration into Defender for IoT delivers this visibility without changing the existing technology and can offer a way of analysing activity without specifically offering access into the OT environment and devices.

Bridewell
CONSULTING
Above. Beyond. Always.

Bridewell Managed Detection and Response in OT and IT environments

In this section, we will explore how Bridewell's Managed Detection and Response service is designed to address the specific concerns of CNI providers across the UK, whilst they continue to evolve their digital ecosystems.

Let us look at what the Bridewell Managed Detection and Response Service is and why it addresses the issues raised. Traditionally, IT and some OT environments would feed all their log information from servers, firewalls, and network intrusion detection systems (NIDS) into a Security Information and Event Management (SIEM) solution, that would look for rules to be triggered that indicated potentially malicious activities. The problem with this was that the traditional SIEM solutions would generate a lot of noise and offer no enrichment or context into the alerts and as such, created alert fatigue, blindness due to noise and no ability to respond or contain a threat once it had been verified.

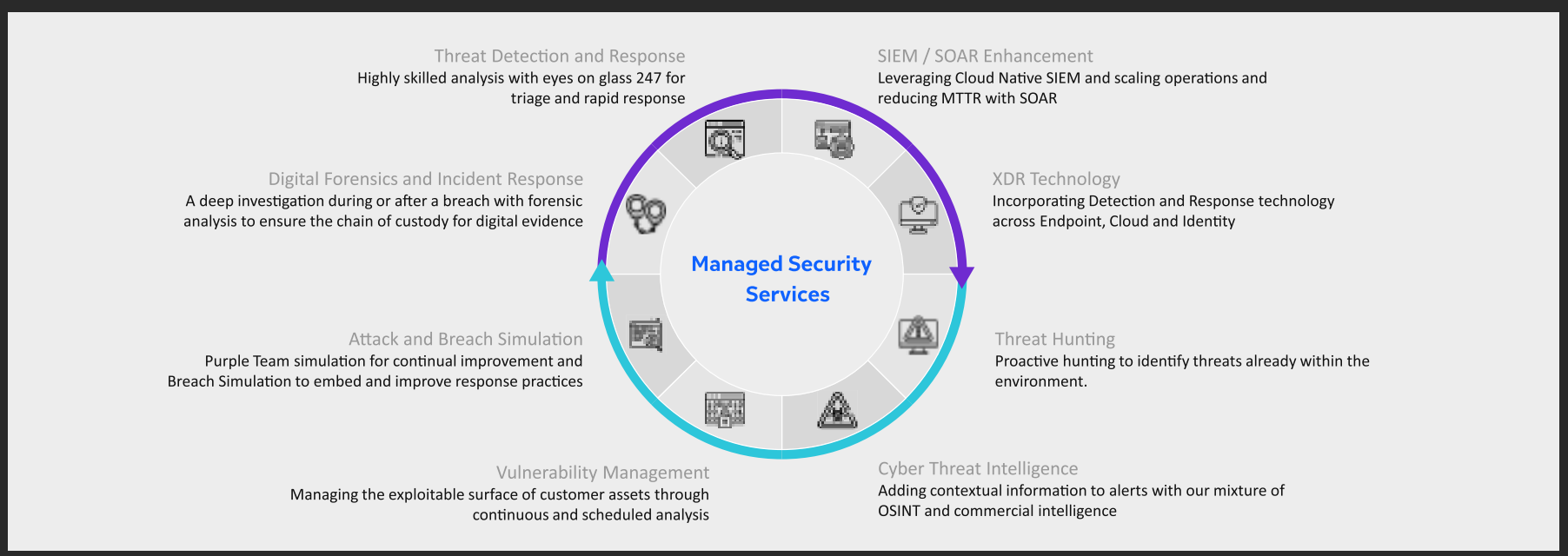
Threat Detection and Response takes this model and extends its use cases into a cloud enabled world. Modern SIEM infrastructures ingest data about user activity and identities from services such as Active Directory to identify patterns and potentially harmful activity from users. They can also ingest data from endpoint protection products, cloud infrastructure across IaaS, PaaS and SaaS to provide a cohesive view of on-premises and physical equipment, as well as the full cloud stack. Cloud leaders are ingesting OT and IoT information into these systems for a very granular and integrated solution for this sector's needs. All of this is tuned with Artificial Intelligence and Machine Learning to filter out noise and share intelligence across a wide audience for protection.

Bridewell is able to differentiate by understanding the sensitivities surrounding the monitoring of OT environments. We're able to work with CNI providers to understand the threat and risk models associated with their environments and ensure that security event and traffic information is extracted where valuable to reduce the risk from cyber-attacks.

Whitepaper

Bridewell
CONSULTING
Above. Beyond. Always.

Furthermore, they now deliver through the integration with Security Orchestration, Automation and Response (SOAR) technologies, the ability to provide a rapid response for containment, reducing the risk of a major breach. The SOAR solutions are also able to integrate into existing solutions and third-party systems to maximise their value. Wrapping this into an intelligence led, proactive 24x7 security team creates a Managed Detection and Response service that delivers continual protection against financial penalties, regulatory requirements and importantly in some cases, the protection of human life.



Easing regulatory compliance

As a leader in the consultation and implementation of the NIS regulations (Network and Information Systems) for CNI providers, we are experienced in understanding the NCSC Cyber Assurance Framework and good practices needed to meet the regulatory requirements. The implementation of a holistic 24x7 threat detection and response with Bridewell helps support key areas of Objectives B - Protecting against cyber-attack, whilst completely covering the requirements C - Detecting cyber security events, and D - Minimising the impact of cyber security incidents in one package.

Throughout most of this whitepaper, we will be discussing the controls that cover the requirements in section C, but it's also important to cover section D. Bridewell will heavily integrate or own your security incident response and provide a robust Cyber Security Incident Response Team (CSIRT) that is available 24x7 to assist in the response and Digital Forensics led investigations, liaising with the relevant bodies as required. Following an incident, we will run and conduct lessons learnt, share feedback, and identify opportunities for improvement across the whole security architecture.

Bridewell
CONSULTING
Above. Beyond. Always.

Making budgets go further

With only 27% of CNI organisations feeling that their budget is sufficient, leveraging Microsoft's Azure Sentinel and Defender XDR product set, Bridewell can help you achieve a higher return on investment by consolidating security vendors by maximising your existing investment into Microsoft 365 licensing. With Microsoft continuing to grow its market share in office productivity, organisations are investing further into E3 and E5 licensing which have inclusive security services that are not being fully utilised.

Consolidating identity systems, Cloud Access Security Brokers (CASB), phishing and mail protection systems, and endpoint protection products along with a SIEM and SOAR that charge simply on the consumption of logs, there are large amounts of IT and Security budgets that can be saved and focused on the improvement of cyber security or other business initiatives.

Microsoft 365 F3	Windows I0 E5	Microsoft 365 E3	Microsoft 365 E3	Microsoft 365 E5
		EM&S E3	EM&S E5	
Defender Anti Virus	Defender for Endpoint	Defender Anti Virus	Identity Protection	Intune MDM & MAM
Intune MDM & MAM	Vulnerability Mgmt.	Identity Protection	Defender for Identity	Defender for Endpoint
		Intune MDM & MAM	Anti-Phishing	Identity Protection
			Cloud App Security	Defender for Identity
			Privilege Identity Mgr.	Anti-Phishing
				Cloud App Security
				Privilege Identity Mgr.
				Defender for O365
				Compromised User Det.

Enabling Cloud Adoption

Bridewell's vast experience in securing cloud technologies and OT environments makes us a valuable partner in the design and implementation of security solutions, including Threat Detection and Response for your specific use cases, ensuring you can continue your digital transformation and uptake of cloud services, with a further 22% of CNI organisations having plans to connect their OT services to the internet.

Microsoft Defender XDR security technologies provide a holistic approach to detection and response technologies whilst Azure Sentinel can consume event information from any common format to ensure that any legacy or new technologies are covered. Bridewell also can deploy on premise, agentless and passive inspection systems into the OT environment for a disruption free integration of security visibility.

Threat Hunting in OT

Threat Hunting takes a hypothesis led approach to identifying breaches that have evaded other mechanisms or are pre-existing in the system. By taking the hypothesis and working through systems, information and scenarios, analysts and consultants hunt for threats across these estates, without looking into specific tactics, techniques and procedures used to breach these environments. A key benefit to working with Bridewell is our OT and CNI experience. We know that OT environments operate differently, have differing threat models to IT and are sensitive whilst operating under stringent requirements.

Bridewell
CONSULTING
Above. Beyond. Always.

Collaboration between Cyber Threat Intelligence and Physical Security

Bridewell operates an intelligence led Security Operation and we openly share intelligence with our customers and the wider CNI community as part of our standard services. Additionally, Bridewell operates a Cyber Threat Intelligence team that build threat actor profiles and intelligence summaries that can share intelligence with the cyber and physical security teams.

Offering continuous monitoring of your attack surface such as vulnerabilities in internet attached devices allows the prioritisation of remedial activities and physical compensating controls.

Lastly, Dark Web Monitoring and Data Leak Protection can focus activities on the loss of information that can lead to the physical compromise of systems, such as digital blueprints and schematics, all of which work towards strengthening the physical systems as well as cyber.

Red Team Assessments

Although more focused on IT rather than OT assets, you can continue the assessment and improvement of physical security with Red Team Assessments conducted by Bridewell. These take a “gloves off” approach to security testing. Our Red Team (offensive security) consultants will identify and plan entry vectors into a cyber system, including physical security as a point of entry, looking for weaknesses in those systems. Experience in OT environments is essential to understanding the importance of high availability and taking protective measures to identify vulnerabilities whilst ensuring minimal disruption to the environment. When the Red Team establish a possible entrance into the cyber environment, integration of the Red Team with the Blue team (SOC cyber defence) allows us to ensure that the service provides coverage and visibility into the full spectrum of attack vectors attempted by the defensive teams.

Please visit our website at www.bridewellconsulting.com
or call us +44 (0) 3303 II0 940

Bridewell
CONSULTING
Above. Beyond. Always.

Adaptive Security Operations

We appreciate that no two organisations are the same, nor do they have the same levels of maturity in security operation or likely have the same desired operating model. As such, Bridewell offers its Managed Detection and Response (MDR) service as either a completely outsourced model, where we take on responsibility for all security operations and simply become an extension of the OT and IT teams, or we will work to establish a Hybrid SOC operating model where you retain existing skills, knowledge and context within your own teams.

This is commonly seen where organisations want to rapidly mature with an MDR deployment, but then retain escalation and remedial activities in house, leaving the 24x7 functions, incident response, threat hunting and cyber threat intelligence to Bridewell's experienced team.

Bridewell CONSULTING
Above. Beyond. Always.

Rapid Maturity and Safe Deployment

Bridewell's experience working in line with Agile and DevOps methodologies can add value and maturity to security operations in as little as a few weeks. By quickly understanding threats, prioritising activities and use cases, Bridwell's team will deploy your cloud based SIEM and SOAR, integrating your existing Microsoft eco-system within days. This allows for instant visibility of the IT organisation during a period of ingest and tuning before moving onto the other elements of deployment and assimilation. This enables greater confidence in the security levels of the IT systems, reducing the risk of connecting the OT environments to them.

You could go from zero to fully serviced across the cloud and identity elements of your estate, rapidly demonstrating value and security. Across OT, we appreciate rapid change is not always desirable; for example, where the monitoring environment forms any part of sensitive process or safety critical infrastructure. In such circumstances, threat modelling and a more conservative deployment methodology of stepped change is adopted to minimise any risk of disruption.

Next Steps

Throughout this whitepaper we have outlined how implementing Threat Detection and Response with the Microsoft Security Technologies helps address the need to protect IT and OT systems from the growing number of cyber threats as these systems converge.

Ensuring visibility into site level OT traffic and vulnerabilities, the protection and understanding of your cloud and SaaS assets, through to the analysis of user and identity behaviour offers the widest level of protection and response from a single vendor.

With 84% of Critical National Infrastructure organisations unable to fill the current cyber security resource demands, working with a trusted partner such as Bridewell extends the capabilities of the solution using our experience in the CNI space whilst addressing the skills gap.

Working with Bridewell helps to address the major risks for the CNI providers, including the reduction of financial penalties, regulatory action and protecting human lives as key objectives in securing the OT environment. This enables the adoption of a cloud based operating model that drives business success.

Please visit our website at www.bridewellconsulting.com
or call us +44 (0) 3303 II0 940

Bridewell
CONSULTING
Above. Beyond. Always.

Please visit our website at www.bridewellconsulting.com
or call us +44 (0) 3303 110 940