Above. Beyond. Always

Azure Defender for IoT PoC

IOT/OT visibility and unified cyber defence and security operations.

03303 110 840
bc@bridewellconsulting.com
www.bridewellconsulting.com

Document released Q2 2021

Closing the cyber defence gap

Digital transformation continues to drive change and the need for system connectivity across IT and OT environments. The continued growth of convergence across critical national infrastructure introduces a wider attack surface and a need for greater visibility into threats and vulnerabilities across IoT and OT systems.

We understand IoT and OT

Bridewell have a well-established team of consultants who have operated extensively within engineering roles and understand OT environments and the associated challenges that arise across large scale critical infrastructure. During a PoC we assign a blend of consultants, engineers, security analysts and an engagement lead, working closely with the Microsoft wider eco-system when appropriate.

Bridewell's cyber defence services unify Microsoft's leading security technology with skills and services that creates a 360 view of your attack surface to deliver a near real-time threat detection and response capability.

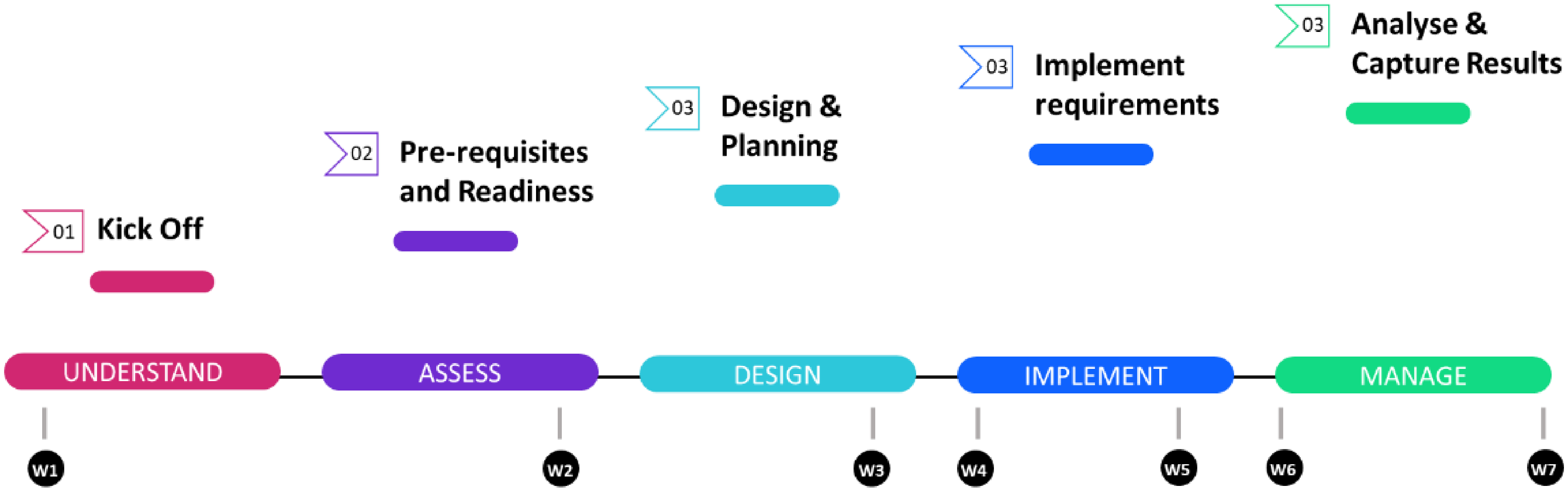
Microsoft Partner
Microsoft

Gold Security
Gold Cloud Platform

Proof of Concept Stages - Timeline

PoC Mission

The aim of Bridewell's PoC is to provide a ***comprehensive insight into the capabilities of Microsoft's enterprise security solutions****, so that informed decisions can be made on the future technology roadmap. We also aim to demonstrate* ***Bridewell's 24x7 managed detection and response*** *capabilities and* ***customer focused*** *approach, so that existing and future clients can experience the* ***added value we provide*** *to enhance and* ***maximise the technology****.*



01 Kick Off

02 Pre-requisites and Readiness

03 Design & Planning

03 Implement requirements

03 Analyse & Capture Results

UNDERSTAND

ASSESS

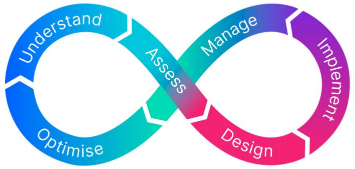
DESIGN

IMPLEMENT

MANAGE

W1 W2 W3 W4 W5 W6 W7

PoC Presentation



Unsure of where to start?

Let Bridewell simplify cyber security

No matter where you currently sit on a maturity and adoption curve, Bridewell can deliver consultancy and security managed services that drive your business forward.

Microsoft Security Workshop

Performing a **free** Microsoft Security Workshop allows us to start working collaboratively to understand your business and assess your needs ahead of the next steps across Azure Sentinel and Defender XDR.

Proof of Concept

Taking your key use cases and value points, we will rapidly deploy Azure Defender for IoT to a pilot group for a four-week window.

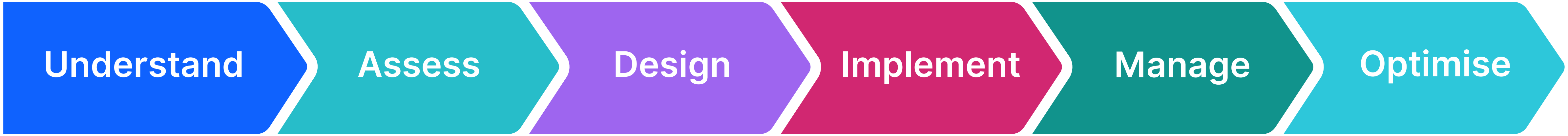
At the end of the PoC, we will report the findings and have the option to scale straight into production.

Managed Detection and Response

Obtain the confidence that you're able to respond to threats 24x7 across Sentinel and Defender XDR by taking a Managed Detection and Response service, backed by Bridewell's industry leading SOC.

Managed Azure Sentinel SIEM

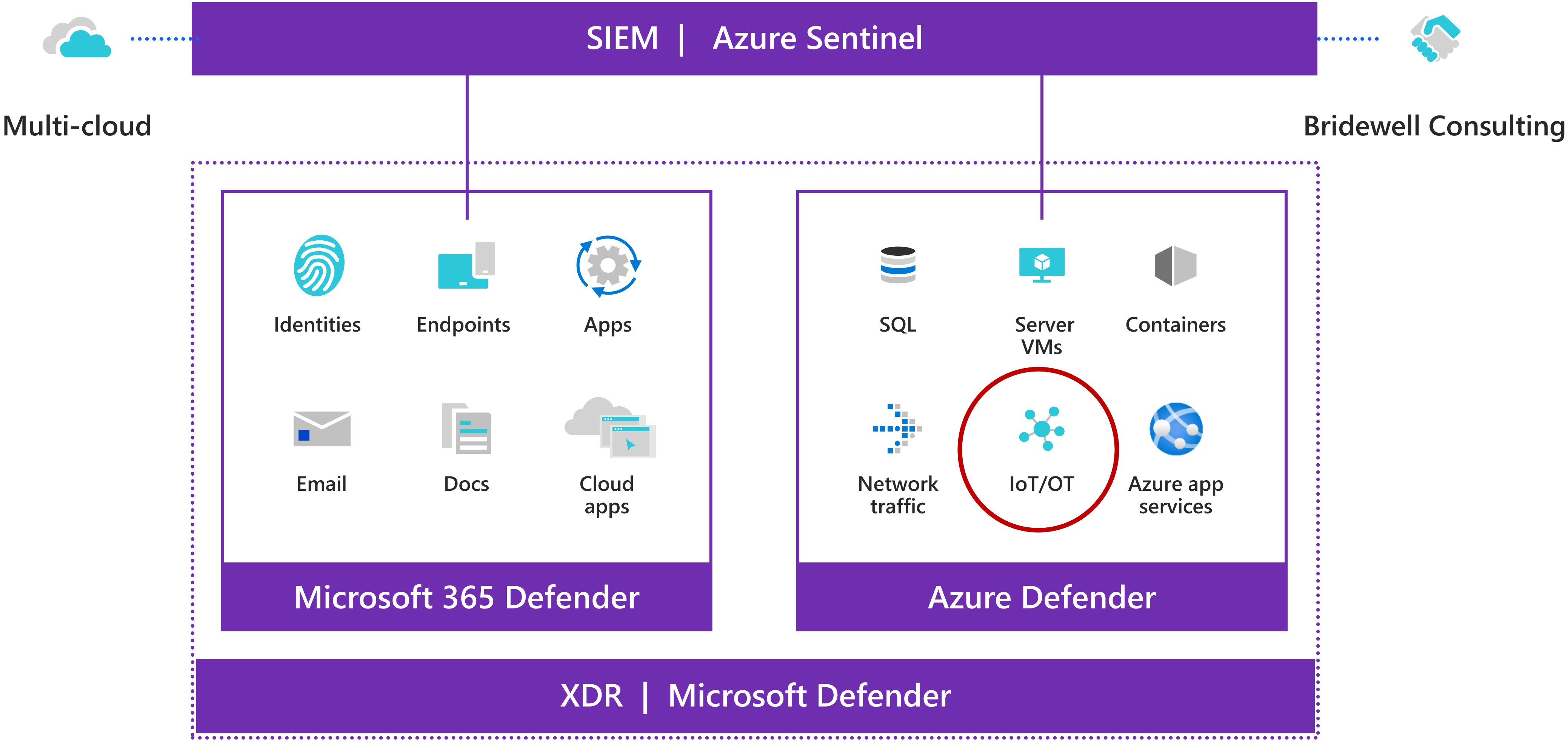
Drive visibility, management, tuning and deliver an ability to respond, 24x7 across your Azure Sentinel SIEM deployment, backed by Bridewell's industry leading SOC.



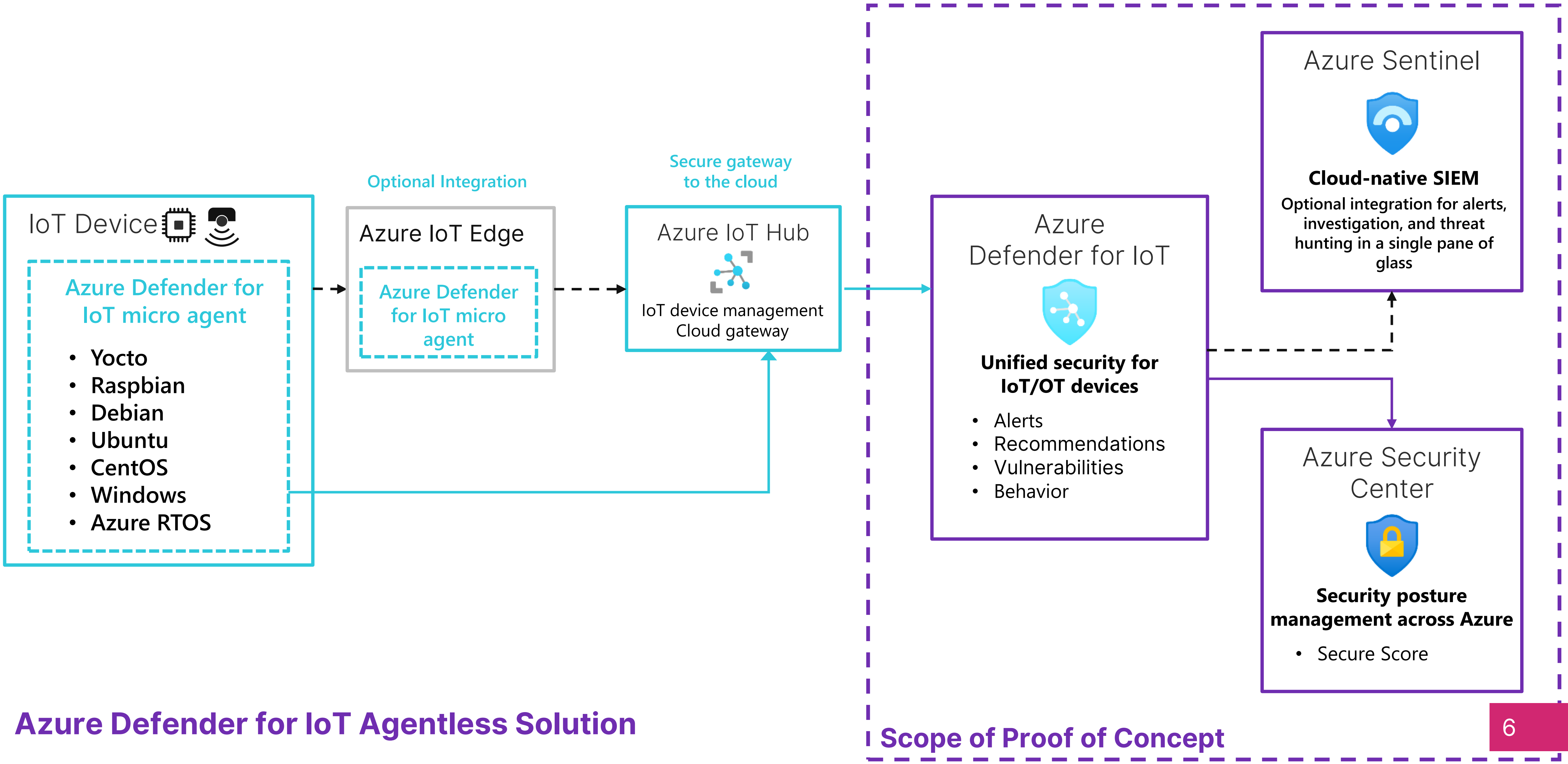
Understand → Assess → Design → Implement → Manage → Optimise

Unified SecOps

Bridewell CONSULTING



Scope of Deployment



IoT Device

Azure Defender for IoT micro agent

- Yocto
- Raspbian
- Debian
- Ubuntu
- CentOS
- Windows
- Azure RTOS

Optional Integration

Azure IoT Edge

Azure Defender for IoT micro agent

Secure gateway to the cloud

Azure IoT Hub

IoT device management
Cloud gateway

Azure Defender for IoT

Unified security for IoT/OT devices

- Alerts
- Recommendations
- Vulnerabilities
- Behavior

Azure Sentinel

Cloud-native SIEM

Optional integration for alerts, investigation, and threat hunting in a single pane of glass

Azure Security Center

Security posture management across Azure

- Secure Score

Scope of Proof of Concept

Azure Defender for IoT Agentless Solution

Bridewell Engagement Lifecycle

UNDERSTAND

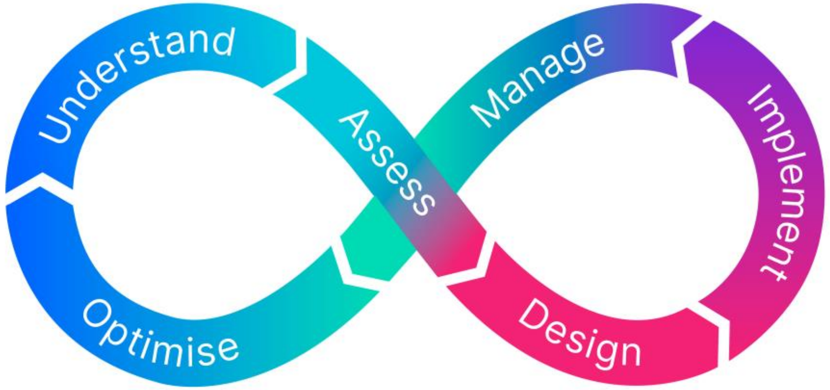
Listen and learn about the customer's business challenges, ambitions, strategic drivers, business goals, culture and desired outcomes

ASSESS

Assess the customer's current position vs a desired state to develop a roadmap for improving cyber security posture and delivering business outcomes

DESIGN

Design solutions, processes and remediation strategies that can enable our clients to implement effective cyber security capabilities and outcomes



OPTIMISE

We have a lean and agile focused approach that is seeking to evolve and optimise the services we deliver, delivering tangible business value to clients

MANAGE

Operate as an extension of our customer's cyber security team, delivering tangible, value added cyber security services on a 24x7 basis

IMPLEMENT

Vast capabilities to implement technical solutions, transformational processes, governance structures, compliance frameworks and migration projects

Proof of Concept Stages - Understand

Kick Off Meetings

*To determine the overall scope of the engagement, capture key considerations and success criteria***.**

1. **Product Selections –** Capture what specific Microsoft security technologies will be required to be deployed and configured for the PoC.
2. **Size of Deployment –** Agree the PoC target deployment, which could consist of systems, assets and integration into security operation tools and processes.
3. **Threat Assessment –** Capture areas of concerns, identified threats, utilising frameworks such as MITRE ATT&CK and review any existing use case criteria.
4. **Network Sources –** Agree and capture the network sources required for the PoC to ensure the desired outcomes against the success criteria can be achieved.
5. **Design & Deployment Considerations –** Provide information and guidance on any design and deployment considerations for the PoC.
6. **Access –** Provide instructions on logical access requirements to deliver the PoC and provide client with any pre-requisites needed such as confirmation of security clearance.
7. **Stakeholder Engagement –** Identify and document all key stakeholders for the PoC, their specific requirements and expectations from the PoC.
8. **Success Criteria –** Discuss and agree key milestones, timescales and success criteria that can be used to measure the effectiveness and success of the PoC.

Proof of Concept Stages - Assess

Pre-requisites and PoC Readiness

Work with key stakeholders to ensure technical and administrative pre-requisites are in place to deploy solutions and commence the PoC effectively.

1. **Licensing –** We work directly with our clients and the Microsoft team to review existing licensing, understanding what is available and any trials are activated for the PoC.

2. **Technical Readiness –** Dependent on what tools form part of the PoC, we will ensure the necessary configuration is in place to enable a successful deployment.

3. **Use Case Review –** Assess the feasibility of all use cases captured or develop a standard set of use cases if none are made available, based around common threats.

4. **Client Processes –** Work with our clients to understand their change management processes and any internal governance process that need to be complied with.

5. **Client Resources –** We discuss and identify current resources available for the PoC, including their skill level and experience with the required deployment technologies.

6. **Enterprise Architecture –** Our consultancy team will assess and ensure that the PoC aligns with existing enterprise architecture requirements where applicable.

7. **Future Roadmap –** Our delivery team will assess existing security posture and document any improvements that could be made, beyond the duration or outside the scope of the PoC.

8. **Compliance –** We will assess whether there are any existing or future compliance requirements that need to be met and ensure this is adhered to as part of the PoC.

Proof of Concept Stages - Design

Bridewell CONSULTING

Designing critical success factors of the PoC and for client approval

The Bridewell team of consultants, security analysts and developers will design use cases and key technical requirements.

1 **Delivery Plan –** A documented delivery plan is designed to provide direction to technical and business stakeholders during the PoC.

2 **Change Documentation –** Our assigned delivery team will develop the required change management documentation to ensure products can successfully be deployed for the PoC.

3 **OT Architectural Review–** Engage the client stakeholders to understand the OT landscape and agree a deployment architecture that mitigates deployment risks.

4 **Integration Capabilities –** We often integrate the Microsoft security stack into third party service management solutions and ingest log sources from applications such as Salesforce and Amazon Web Services to unify visibility and detection capabilities.

5 **Automation & Improved UX –** Any agreed automation or additional requirements to improve user experience, such as leveraging Logic Apps and Power Automate will be designed.

6 **Process Design –** We work with clients to design processes around incident detection, response, management and escalation during the PoC.

7 **Custom Reporting –** We leverage API's, Power BI and KQL to deliver custom reporting requirements where required, enabling insight into data produced by Sentinel and other security technologies.

Proof of Concept Stages - Implement

Bridewell CONSULTING

Implementation and enablement of Microsoft's security solutions
Responsible for technical implementation or oversight of the implementation to ensure a successful start to the PoC.

1. **Service Enablement –** We commence the enablement and configuration of key technologies such as Azure Defender for IOT and Azure Sentinel.

2. **Deploy Technologies –** During the PoC a virtual or physical appliance will be deployed with support of the clients technical teams.

3. **Network Analysis –** Agree the scope of analysis and work with the clients teams for deployment of a network SPAN port.

4. **Approved Integrations –** Work with technical and business stakeholders to implement any identified integrations into third party cloud systems.
.

5. **Automation –** Any approved areas of automation as part of the PoC will be implemented by our delivery team to demonstrate the SOAR capability of Azure Sentinel.

6. **Agreed Processes –** Processes for handling alerts, incident management, response and escalation are implemented, following approval of design activity.

7. **Project Delivery –** We deliver an agile and responsive service model and will implement a series of short stand-up sessions and delivery updates through the duration of the PoC.

Proof of Concept Stages – Manage

Management of Azure Defender for IoT during the PoC

Collaborative working with key stakeholders to analyse information, alerts and incidents from Azure Defender for IoT and wider product set.

1. **Azure Sentinel –** We assign a 9 to 5 team to manage the alerts and incidents within Azure Sentinel, informing the client if anything critical is identified during the PoC.

2. **Azure Defender for IoT –** Bridewell will manage the alerts and outputs from all security technologies within the PoC, which differs dependent on client requirements.

3. **Risk and Vulnerability –** Review and analyse the risks and vulnerabilities identified to demonstrate the value of the technology utilised in the PoC.

4. **Delivery Plan –** A project lead will provide weekly updates on progress of the PoC and be available to deal with any queries or requests during the PoC.

5. **PoC Success –** Bridewell take ownership of the PoC and ensure all data is captured to deliver the defined success criteria and presentation of results.

6. **PoC Incident Management –** Bridewell will manage alerts and incidents in accordance with agreed incident management procedures within the scope of the PoC, ensuring any critical issues are dealt with promptly.

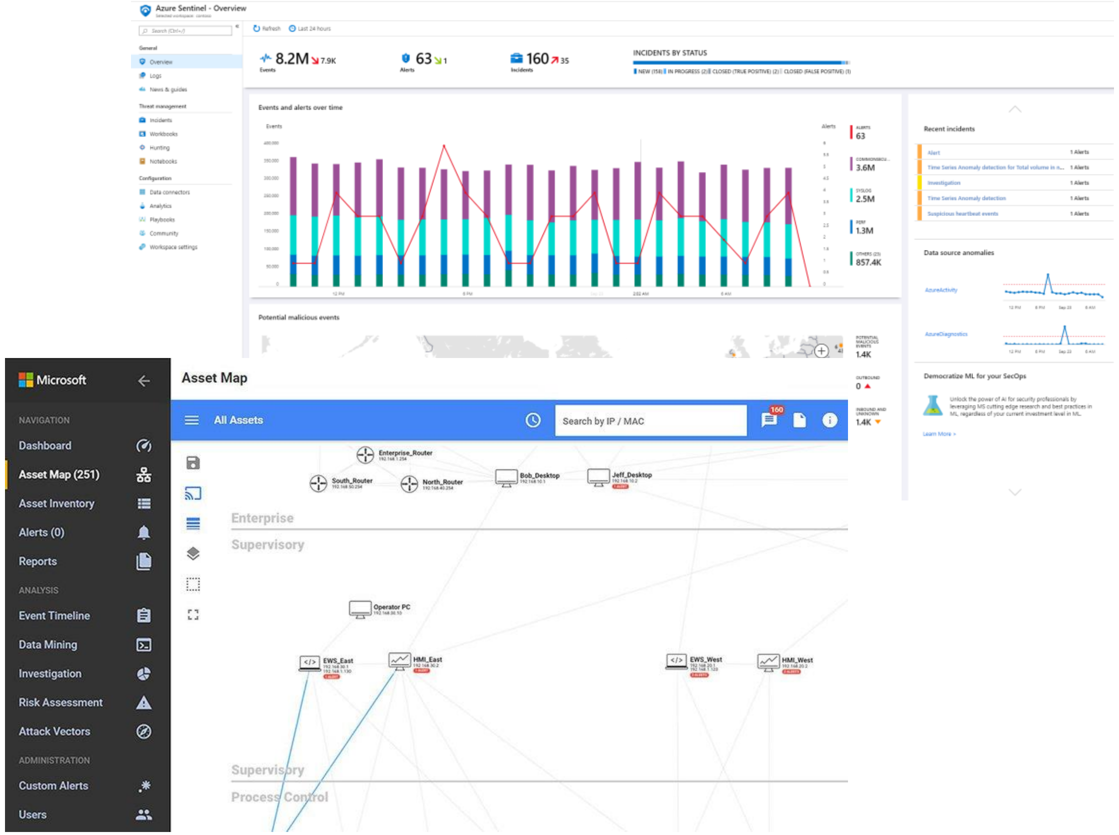
Proof of Concept Stages - Present

PoC Executive Presentation

The outcomes of the PoC are presented to key stakeholders across the organisation in addition to Q&A.

Presentation Areas

- Executive Summary
- Success Criteria
- Asset Review
- Vulnerability Report
- Traffic Behaviour Report
- Security Incident Report



*Includes all pertinent products used in the PoC

**During a PoC, Bridewell's Optimise stage is replaced with Presentation, due to the nature of the engagement.*

End-to-End Cyber Capability

Bridewell Consulting is a leading independent cyber security services provider with a strong reputation and credentials, with fantastic strength and references in Critical National Infrastructure and Financial Services.

Cyber Security

- Compliance Frameworks
- Cloud Security
- Security Architecture
- NCSC Certified Services
- PCI QSA Services
- ASSURE Cyber Audits
- Cyber Security Maturity
- Cyber Security Risk
- ICS/SCADA Cyber Security
- Target Operating Model

Managed Security

- 24x7 Security Monitoring
- 24x7 Managed XDR Services
- Critical National Infrastructure
- Active Threat Hunting
- Cyber Threat Intelligence
- Incident Response
- Digital Forensics
- Vulnerability Management
- SOC Automation
- Purple Team Engagements

Penetration Testing

- Red Team
- Web Application
- IoT and Industrial Control Systems
- Infrastructure
- MITRE ATT&CK Simulation
- Mobile Application
- Cloud Security Assessment
- Source Code Analysis
- SSDLC Advisory
- SecDevOps

Data Privacy

- DPO as a Service
- GDPR Maturity Assessment
- GDPR Gap Analysis
- Breach Response Support
- Programme Leadership
- E-Privacy & PECR Advisory
- Cookie Compliance Mgmt
- OneTrust Implementation
- E-Discovery & SAR Support
- Policy Review & Development

INVESTORS IN PEOPLE | Silver

Gold Microsoft Partner Microsoft

Assured Service Provider in association with National Cyber Security Centre

CREST. | VA | PEN TEST

UK Civil Aviation Authority ASSURE

CYBER ESSENTIALS PLUS

Why Bridewell?

Bridewell CONSULTING

We believe in empowering our clients by knowledge transfer and building strong, trusted relationships.

HIGHLY ACCREDITED

One of the most accredited companies in the UK, Bridewell are trusted advisors across a variety of sectors and are certified by organisations such as the National Cyber Security Centre (NCSC) and CREST.

HOLISTIC DELIVERY CAPABILITY

We provide access to a multi-disciplined team of experts who have referenceable experience of delivering complex migration activities, solution architecture, design and deployment of the technologies.

OPERATE AS AN EXTENSION OF YOUR TEAM

We aim to understand our client's business goals, culture and operating context, so that security operations can be designed to focus on the most prevalent threats and the organisation's business goals.

DEEP DETECTION & RESPONSE EXPERTISE

We combine analysts, consultants, incident responders and security developers to build effective enterprise detection and response capabilities, rated in Azure Top 20 Global Threat Hunters.

AGILE, RESPONSIVE DELIVERY

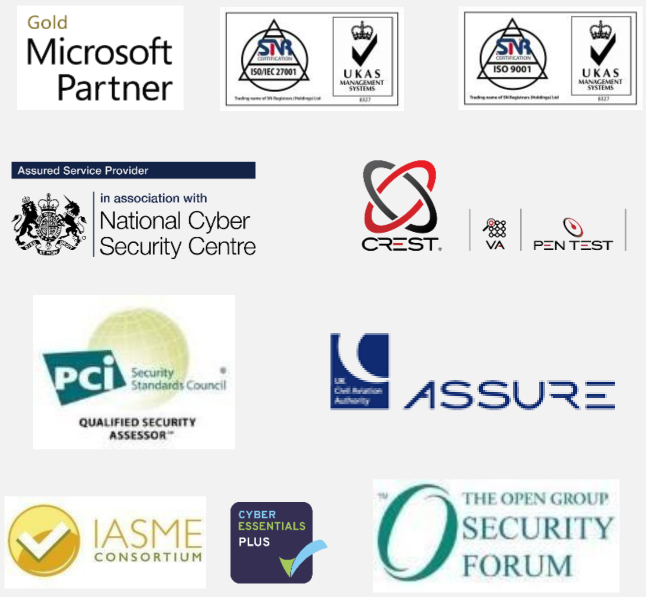
We're able to deliver an enterprise service that is customer focused and built on agile principles and driving real value, seeking to drive automation, integration and deliver efficiencies where possible.

VAST CAPABILITY

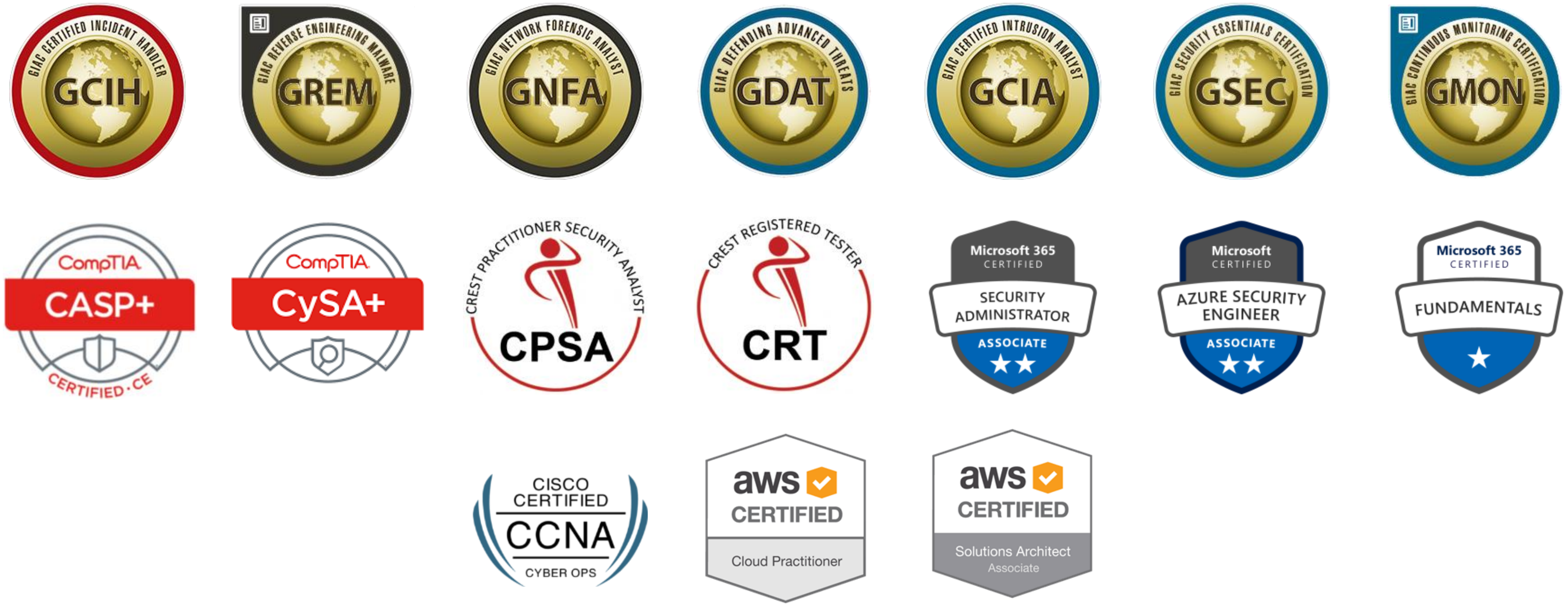
Bridewell has a strong cyber security consultancy and penetration testing practice, which our clients can leverage to conduct purple team assessments and support their compliance requirements.

A Leading Cyber Security Operations Team

As an organisation Bridewell holds leading accreditations from security bodies, making it one of the leading cyber security organisations in the world.


Gold
Microsoft Partner
SNR CERTIFICATION ISO/IEC 27001
UKAS MANAGEMENT SYSTEMS
SNR CERTIFICATION ISO 9001
UKAS MANAGEMENT SYSTEMS
Assured Service Provider
in association with
National Cyber Security Centre
CREST
VA
PEN TEST
PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR
UK Civil Aviation Authority
ASSURE
IASME CONSORTIUM
CYBER ESSENTIALS PLUS
THE OPEN GROUP SECURITY FORUM

Bridewell differentiates our service with the quality of our valued people. We attract, develop and retain some of the leading security skills in the UK, who continually improve and drive our capabilities forward. Below is a view of the skills and accreditations within our SOC alone.



Bridewell CONSULTING

Above. Beyond. Always

Proactive, Cyber Defence Services

03303 110 840
bc@bridewellconsulting.com
www.bridewellconsulting.com

WWW.BRIDEWELLCONSULTING.COM