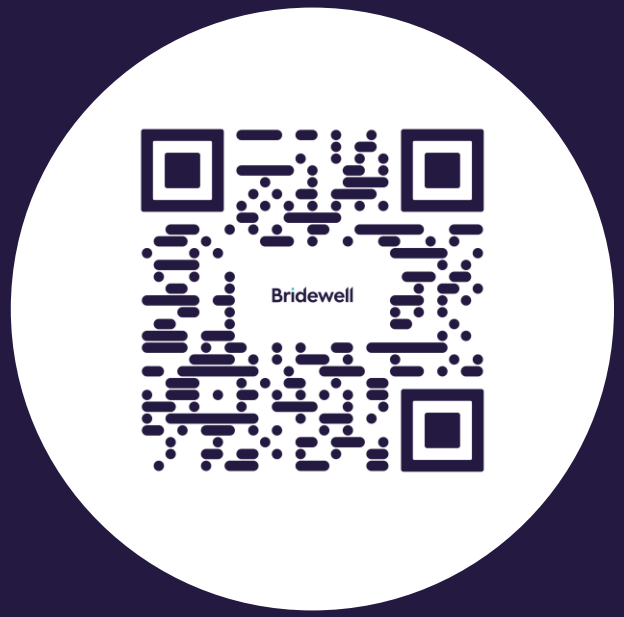


Join us at Slido.com to participate

#795428

Bridewell

HELPING OPERATORS OF CNI TRANSFORM CYBER RESILIENCE THROUGH CYBER THREAT INTELLIGENCE

11th May 2022

Brief
Introduction

Director at Bridewell with responsibility for the Red, Blue and Cyber Threat Intelligence teams.

Martin joined Bridewell in Jan 2021. He is the board member responsible for leading the continued growth and scaling of Bridewell's Managed Security Service portfolio, including Cyber Threat Intelligence, Cyber Defensive and Offensive capabilities.

Martin has nearly 20 years' experience in designing, implementing and leading on secure cloud and networking solutions across on premise, public, private and hybrid cloud services. Prior to joining Bridewell, he was CTO of Timico, a digital infrastructure provider, where he was responsible for strategic direction, digital transformation of the business as well as having ownership of cyber security of the enterprise systems, carrier networks and cloud services.

Martin is passionate about the role cyber security plays in cloud services and transformational projects.

Bridewell

Helping Operators of Critical Infrastructure Transform Cyber Resilience Through Cyber Threat Intelligence

What do I want to achieve in this session?

- Review historic intelligence teachings.
- Have a look at what Cyber Threat Intelligence is.
- Understand the value and alignment to the NIS Regulations.
- Understand the value of gathering and sharing intelligence.

Bridewell

Know your Adversary

The attack on Pearl Harbor was a surprise military strike by the Imperial Japanese Navy Air Service upon the United States against the naval base at Pearl Harbor in Honolulu, Territory of Hawaii, just before 08:00 a.m., on Sunday, December 7, 1941.

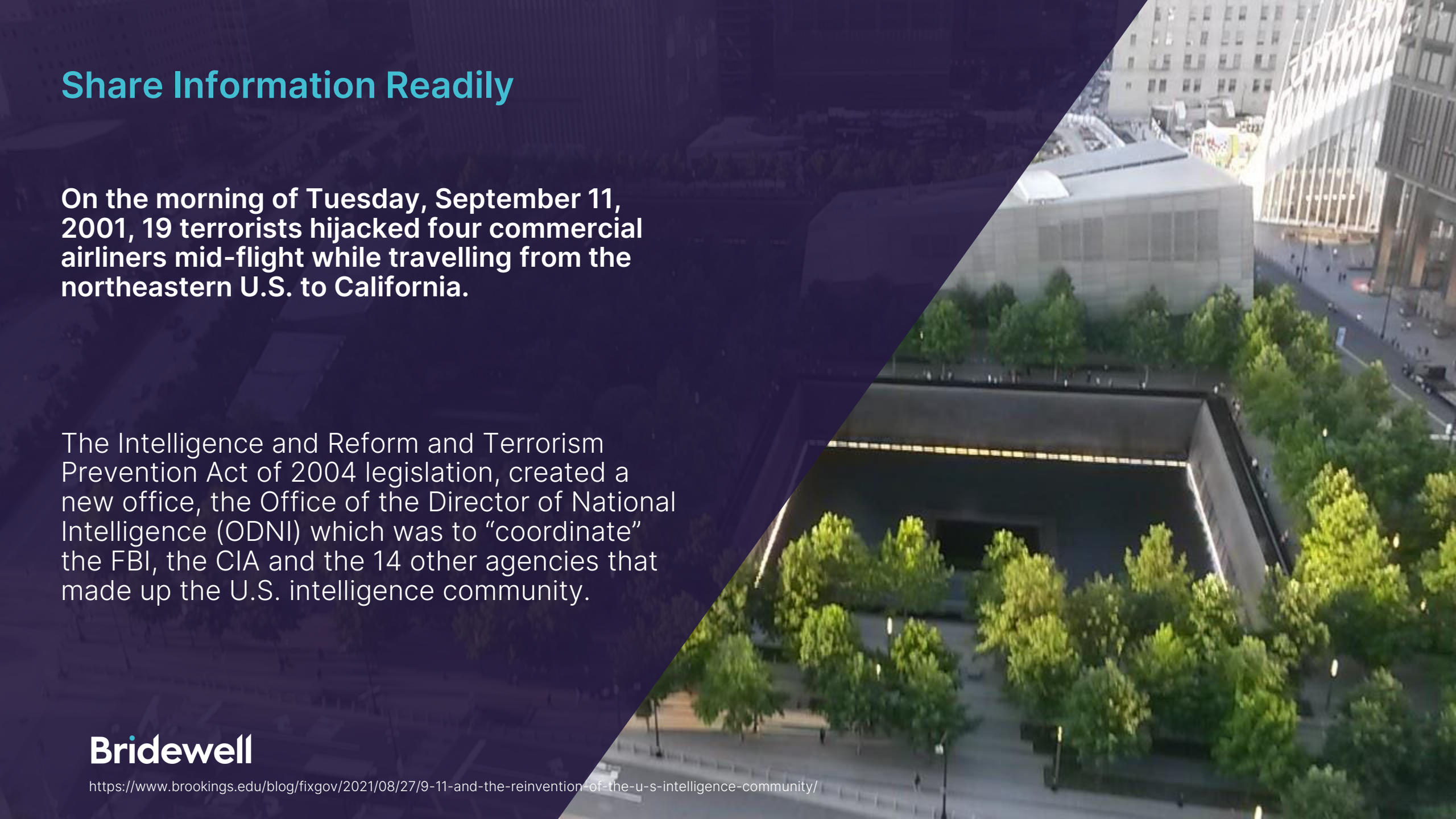
“Intelligence organisations in both the UK and the US had underestimated the Japanese intentions and capabilities and did not imagine that they might be capable of such strategic surprise.” - GCHQ

https://www.gchq.gov.uk/information/did-signals-intelligence-predict-attack-pearl-harbor

Share Information Readily

On the morning of Tuesday, September 11, 2001, 19 terrorists hijacked four commercial airliners mid-flight while travelling from the northeastern U.S. to California.

The Intelligence and Reform and Terrorism Prevention Act of 2004 legislation, created a new office, the Office of the Director of National Intelligence (ODNI) which was to “coordinate” the FBI, the CIA and the 14 other agencies that made up the U.S. intelligence community.



Bridewell

https://www.brookings.edu/blog/fixgov/2021/08/27/9-11-and-the-reinvention-of-the-u-s-intelligence-community/

Change what is shared

March 2022, following the Russian invasion of Ukraine, Ukrainian partners of the Conti Ransomware-as-a-Service provider (Wizard Spider Group) leaked source code and inside information, including details of all active infrastructure.

The distribution of indicators/observables such as IP addresses and hashes hasn't stopped the flow of ransomware attacks by the group since.

The group has rebuilt its infrastructure and , ensuring previous indicators are no longer relevant and is still being successful, with the same TTPs.

Defining Cyber Threat Intelligence

You must understand your organisation before you can understand what constitutes a threat to it.

Truly understanding what constitutes a threat should be a major goal of any organisation and maturing the components will put you “ahead of the curve”.

Analysed information about the hostile intent, capability and opportunity of an adversary.

It is the human that is the threat.

Bridewell

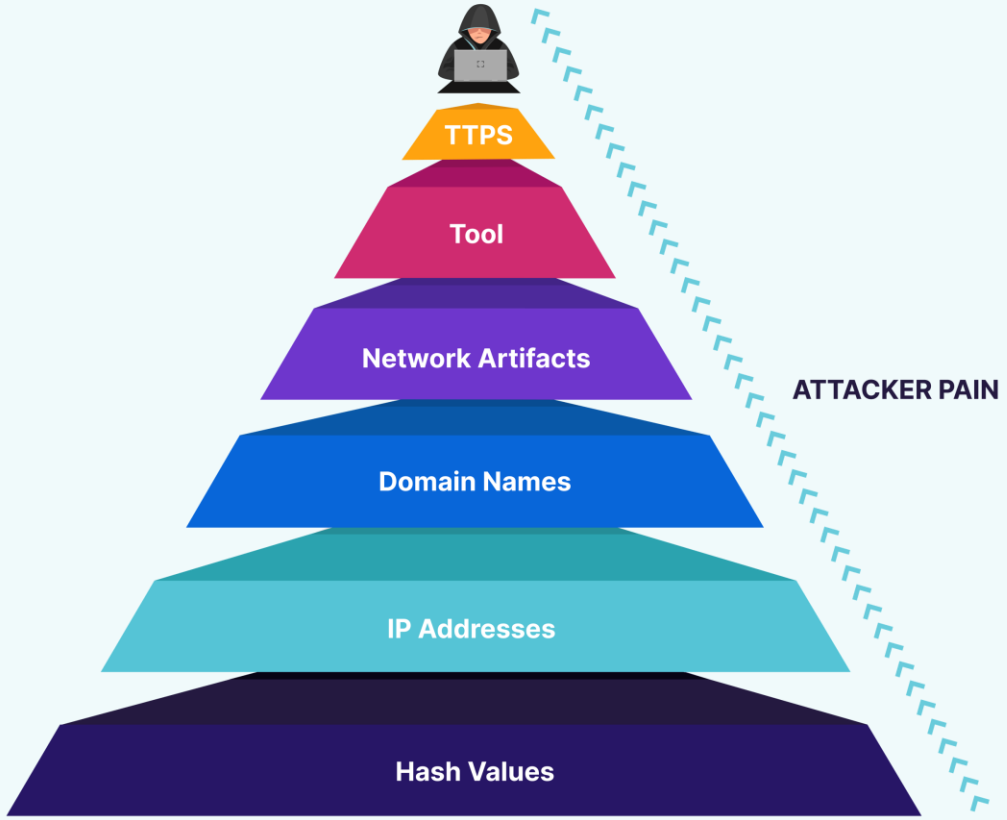
Focus on the Human

Payloads, files, infrastructure and tools can be replaced, with an increasing degree of difficulties, but human behavior is difficult to change.

The “Pyramid of Pain”, developed in 2013 by David J Bianco is a key conceptual model for the effective use of Cyber Threat Intelligence within Cyber Security.

At the bottom of the pyramid are the elements that can easily be changed, with very little annoyance to a threat actor.

Within security operations is it valuable for the planning and deployment of threat detection, aligned to strategic risks and actors, by detecting the tools, techniques and procedures that actors use in campaigns.



Bridewell

Say what you see

Bridewell

slido

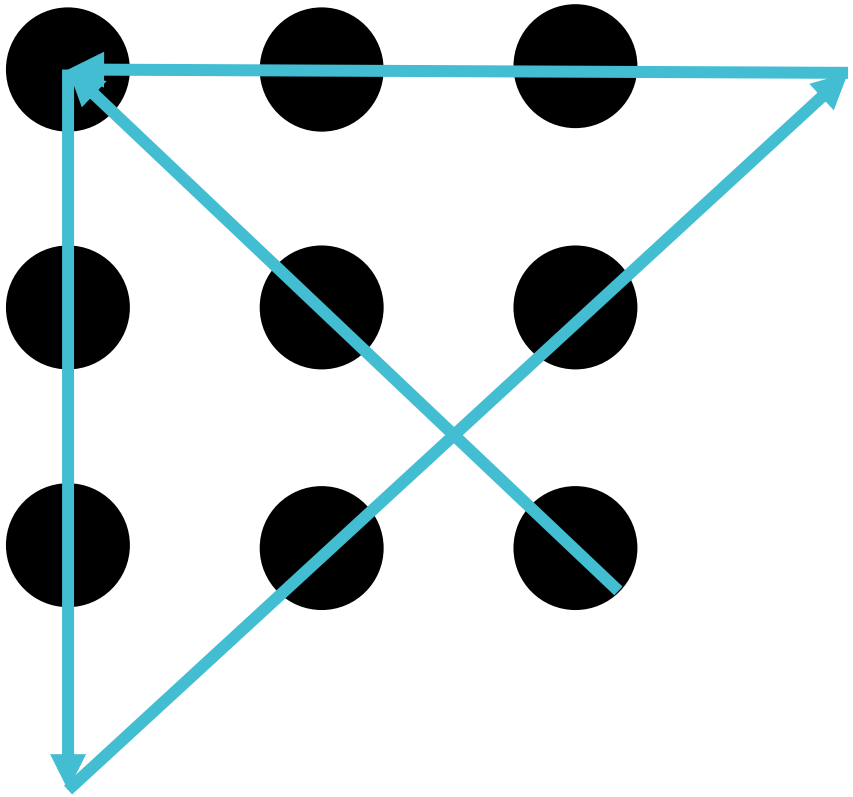
What did the third triangle say?

ⓘ Start presenting to display the poll results on this slide.

Let's look again

Bridewell

“Free Your Mind”



Using just 4 straight lines,
and not taking your pen off the paper,
intersect all nine dots.

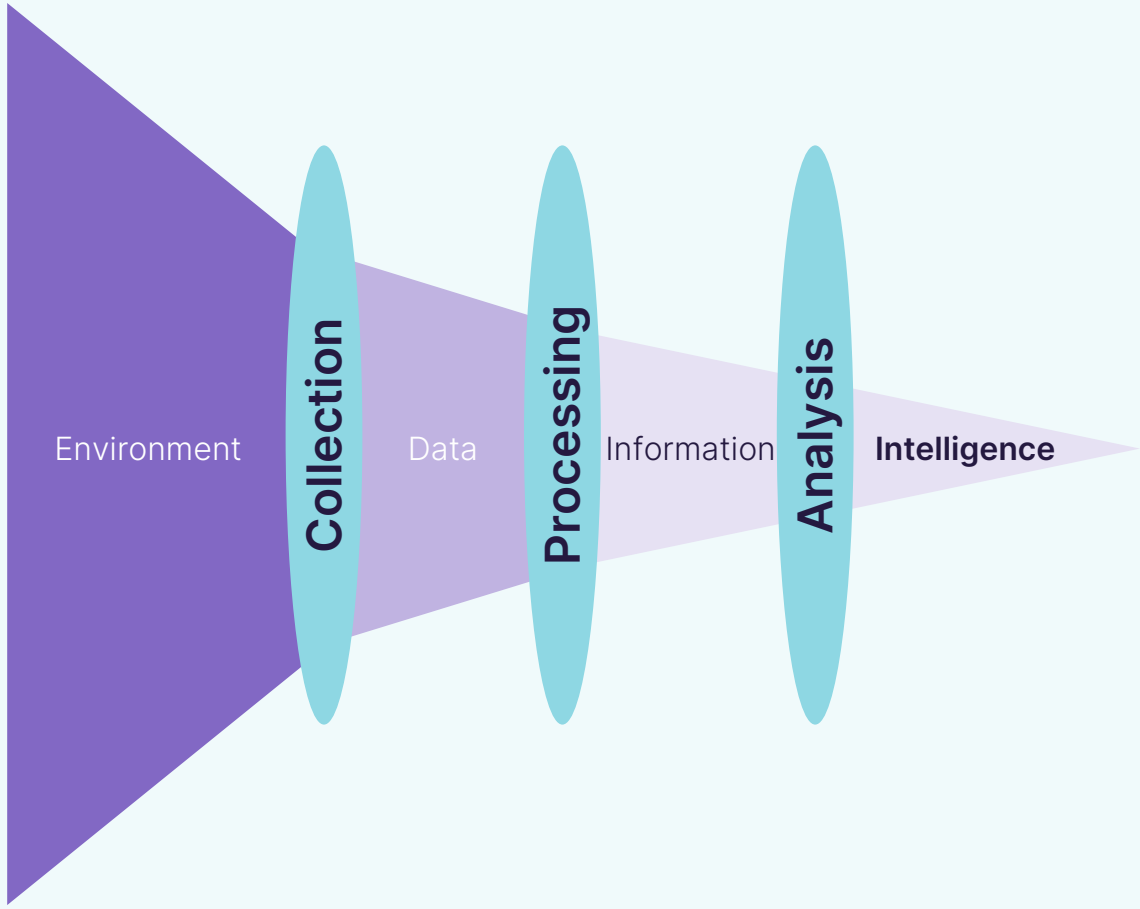
Bridewell

Challenges Turning Data Into Intelligence

“We tend to perceive what we expect to perceive.”

“Once an experienced analyst has the minimum information necessary to make an informed judgment, obtaining additional information generally does not improve the accuracy of his or her estimates. Additional information does, however, lead the analyst to become more confident in the judgment, to the point of overconfidence.”

Good analysts think about “how they think” and use analytical processes to change their perception.



Bridewell

Phycology of Intelligence Analysis - https://www.ialeia.org/docs/Psychology_of_Intelligence_Analysis.pdf

slido

Do you use Cyber Threat Intelligence today?

ⓘ Start presenting to display the poll results on this slide.

slido

Which areas of the NIS Regulations do you use Cyber Threat Intelligence to inform?

ⓘ Start presenting to display the poll results on this slide.

Cyber Threat Intelligence
And The NIS Regulations

Bridewell Research Findings

76%

Of respondents agree or strongly agree that the NIS Regulations have helped organisations improve their Cyber Security posture.

55%

Of respondent's state that they are falling short of the current NIS regulatory requirements.

21%

Of respondent’s stated they had not experienced IT/OT downtime as a result of cyber attacks in the last twelve months.

Bridewell

Soon to be publicly released, please use the QR Code at the end of the presentation.

Bridewell Research Findings

Only 1 in 5 have implemented threat hunting and cyber threat intelligence

Less than half share their threat intelligence with peers

Bridewell

Soon to be publicly released, please use the QR Code at the end of the presentation.

NIS Regulations and the interaction with Cyber Threat Intelligence

As the single point of contact in the UK, the NCSC developed the Cyber Assessment Framework to support operators of critical infrastructure in meeting the NIS regulations. Currently on v3.1, the CAF has the following requirements that need Cyber Threat Intelligence to mature cyber resilience.

Managing Risk

- A1.a Board Direction
- A1.b Decision Making
- A2.a Risk Management Process
- A4.a Supply Chain

Intelligence Reports
Trends
Adversary Database

Protecting Against Cyber-Attacks

- B1.a Policy and Process Development
- B4.d Vulnerability Management

Intelligence Reports
Trends
Adversary Database

Detecting Cyber Security Events

- C1.a Monitoring Coverage
- C1.c Generating Alerts
- C1.d Identifying Security Incidents
- C1.e Monitoring Tools and Skills
- C2.a System Abnormalities for Attack Detection
- C2.b Proactive Attack Discovery

Intelligence Reports
Adversary Database

Threat Intel Feeds

Minimising the Impact of Cyber Security Incidents

- D1.a Response Plan
- D1.c Texting and Exercising
- D2.a Incident Root Cause Analysis
- D2.b Using Incidents to Drive Improvements

Intelligence Reports
Adversary Database

Intelligence Sharing

Inform Decisions With Cyber Threat Intelligence

Strategic, Operational and Tactical

Cyber Threat Intelligence

Strategic Cyber Threat Intelligence

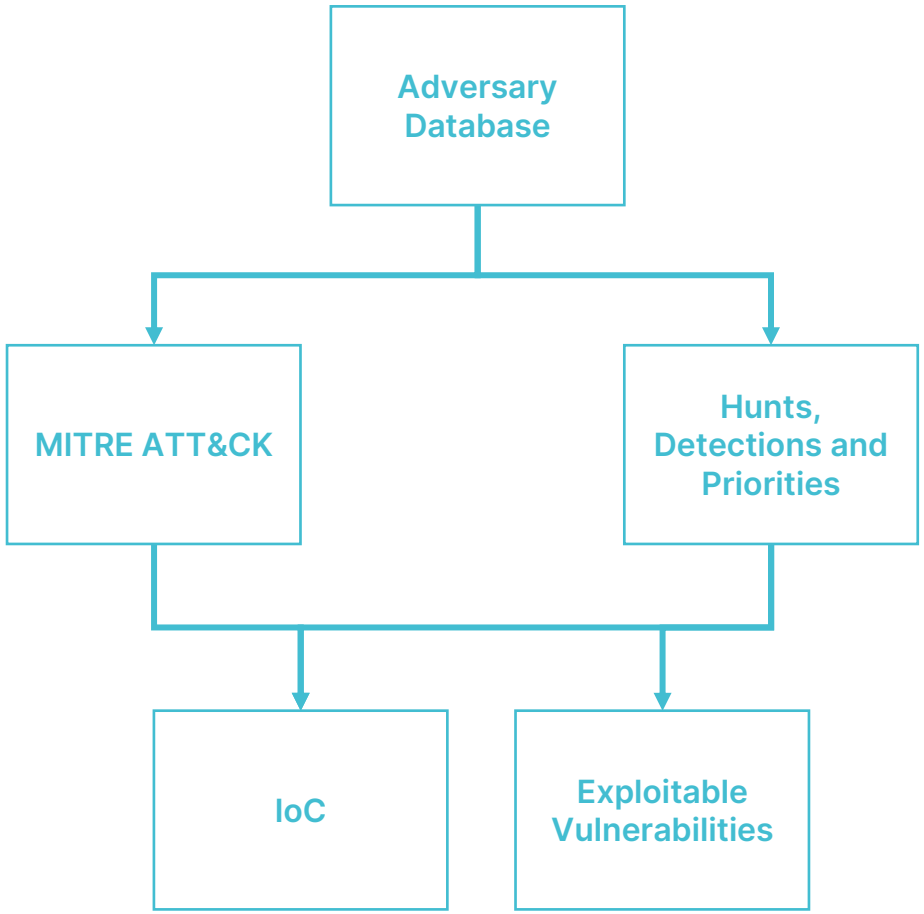
Is focused on future and emerging trends to support longer-term decision making.

Operational Cyber Threat Intelligence

Historical analysis and tracking of capabilities, campaigns and motivations of actors for decisions around perceived and real threats.

Tactical Cyber Threat Intelligence

The link between the threat and technology is used to mitigate active or imminent threats and actors.



Bridewell

Intelligence has a useful lifespan that is dictated by the adversary.

MITRE ATT&CK Framework - Example – Sandworm Team

This threat actor targets industrial control systems, using a tool called Black Energy, associated with electricity and power generation for espionage, denial of service, and data destruction purposes. Some believe that the threat actor is linked to the 2015 compromise of the Ukrainian electrical grid and a distributed denial of service prior to the Russian invasion of Georgia. The most recently released research was the **29th of April 2022**.

Reconnaissance	Resource Dev	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	C & C	Exfiltration	Impact
Vulnerability Scanning	Vulnerabilities	Spearphising Link	PowerShell	Web Shell	Group Policy Modification	Obfuscated Files and Information	OS Credential Dumping	System Network Config Discovery	Remote Desktop Protocol	Keylogging	Proxy	Exfil over C2	Disk Structure Wipe
Search Open Websites / Domains	Domains (Acquire Infrastructure)	Supply Chain Compromise	Unix Shell	Scheduled Task		File Deletion	Credential from Web Browser	File and Directory Discovery		Data from Local System	Web Protocols		Data Encrypted for Impact
Software (Gather victim host info)	Server (Acquire Infrastructure)	Spearphishing Attachment	Exploitation for Client Execution	Kernel Modules and Extensions		Match Legitimate Name or Location	LSASS Memory	System Information Discovery			Fallback Channels		External Defacement
Email Addresses	Malware (Develop Capabilities)	Compromise Software Supply Chain	Inter-Process Communication	Rc.Common		Disable or Modify System Firewall	LSA Secrets	Remote System Discovery			Standard Encoding		Disk Wipe
Employee Names	Social Media Accounts	External Remote Services	Malicious Link	System Firmware		De-obfuscate / Decode files		Domain Account (Account Discovery)			Application Layer Protocol		Endpoint DoS
Domain Properties	Botnet	Valid Accounts	Malicious File			Indicator Removal from Tools		Email Account			Ingress Tool Transfer		Data Destruction
Business Relationships		Trusted Relationships	Visual Basic			Rundll32		Network Sniffing			Protocol Tunneling		
Spearphishing Link		Domain Accounts						System Network Connections Discovery			Asymmetric Cryptography		
Search Victim-Owned Websites								System Owner / User Discovery			Remote Access Software		
											Non-Standard Encoding		

Defenders have to reduce the likelihood of success and detect just one step before exfil and impact to ensure the attack fails to achieve their goals.

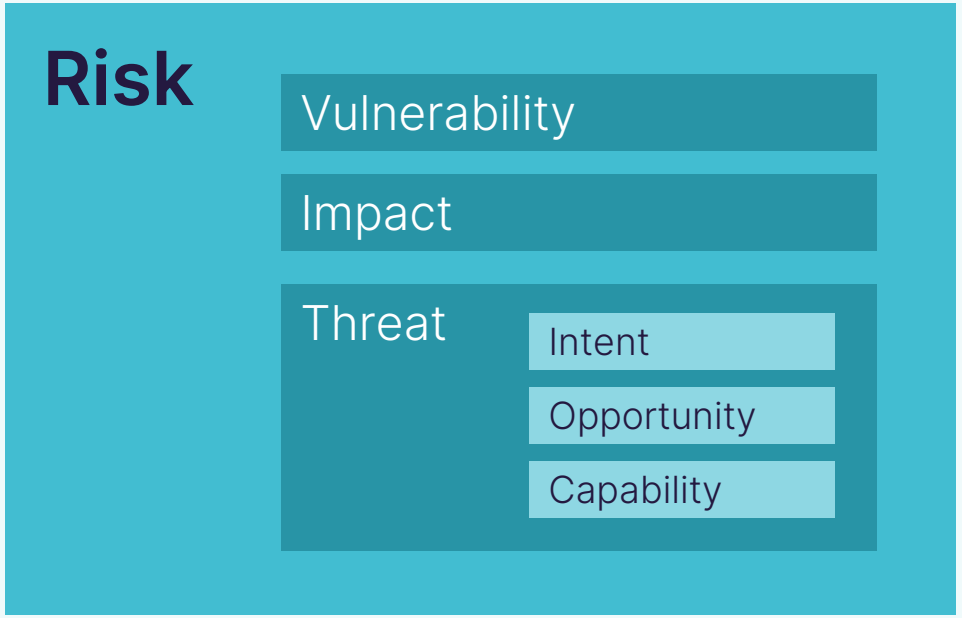
Bridewell

Vulnerability Management

Using Threat Intelligence within the Vulnerability Management Process is key to establishing a Risk Based approach to the mitigation, remediation or acceptance of vulnerabilities.

By understanding the TTP's used by adversaries, including the vulnerabilities being exploited, we can change the priority of remediate based upon threat intelligence.

Importantly, understanding the business impact applies a weight to the risk process to ensure the treatment of risk is aligned to the business.

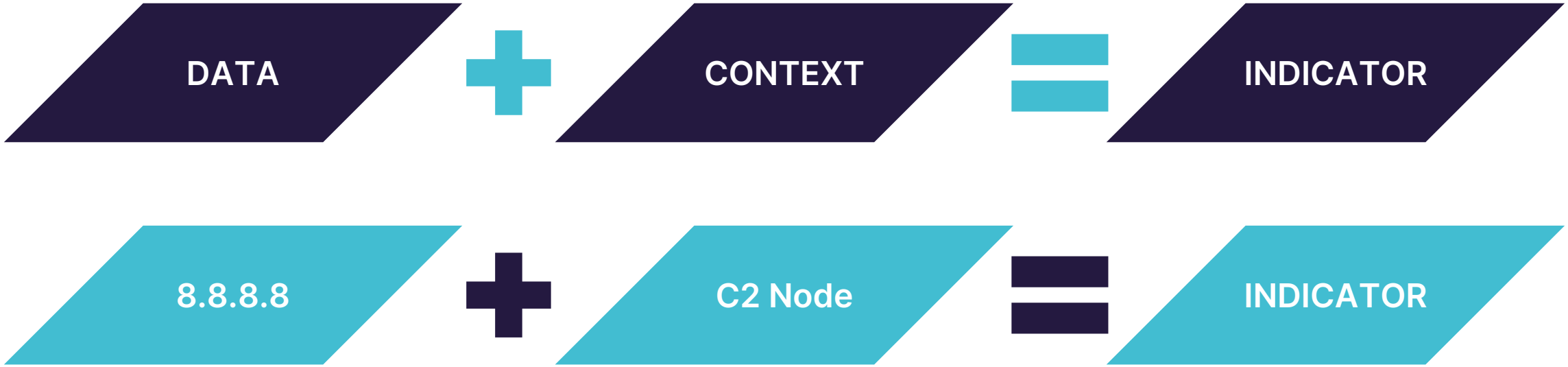


Bridewell

What is an Indicator of Compromise?

A single piece of information is not an indicator, it's a piece of data.

An indicator must indicate something.



Bridewell

OPEN AND TRANSPARENT SHARING OF INTELLIGENCE

Traffic Light Protocol

	When should it be used?	How may it be shared?
 **Red**	TLP: RED is used when information cannot be acted on by additional parties and could lead to misuse.	Recipients may not share TLP:RED information with any parties outside of the original disclosure.
 **Amber**	TLP: Amber is used to where information is shared for action to be taken, but carries privacy, reputation or other sensitive information.	TLP: Amber may only be shared within the organization on a need-to-know basis in order to act on the information.
 **Green**	TLP: Green may be used when sharing information with peers and community groups.	TLP: Green can be shared with peers and partner organisations, but not publicly disclosed.
 **White**	TLP: White may be used when information carries minimal risk of misuse.	TLP: White can be distributed without restriction, subject to copyright.

Bridewell

What to share

From:spoofedemail@spoofedomain.com

To: joebloggs@myutilities.com

Subject: Invoice

Please click the following link to retrieve the invoice for your recent hot tub purchase.

Click Here

User clicks the link which is a direct URL to a silent EXE http://definatelyillegal.com/probablymalware.exe which silently creates a new service called “H4x0r”.

The user clicks again, observes nothing and replies saying sorry, the link seems dead.

One week later during a threat hunt, your analysts identify that Joe Bloggs’ machine, and a few other members of staff is communicating to http://malwareC2.net every hour, like clockwork on port 443.

By performing intrusion analysis, the analyst identifies all activity on the kill chain and prepares to share the information before cleaning up.

Tell me the “observables” and turn them into indicators of compromise.

Bridewell

What to share

Observable	Type	Detection Date	Mitre Tactic	Mitre TTP	Description	Organisation	Submitted by
email[@]spoofedomain[.]com	Email	6/10/2021	Initial Access	T1566.002	On 6/10/2021 “spoofed email[@]spoofedomain[.]com” sent “Invoice” themed emails that included the malicious URL “hxxp://definatelyillegal[.]com/probablymalware[.]exe” [MD5: 32 characters] (T1566.002), which is detected as Trojan.SuperMalware. When executed, “probablymalware[.]exe” [MD5: 32 characters] (T1204.002) creates a Scheduled Task named “H4x0r” (T1543.003) and begins C2 over port 443 to “hxxp://malwareC2[.]net” (T1071.001).	MyUtil	analyst@MyUtil
hxxp://definatelyillegal[.]com	URL	6/10/2021	Execution	T1566.002	As above	MyUtil	analyst@MyUtil
[MD5: 32 characters]	Hash	6/10/2021	Execution	T1204.002	As above	MyUtil	analyst@MyUtil
H4x0r	Process	6/10/2021	Persistence	T1543.003	As above	MyUtil	analyst@MyUtil
hxxp://malwareC2[.]net	URL	6/10/2021	Command and Control	T1071.001	As above	MyUtil	analyst@MyUtil

Intel Sharing – P2P, ISACs and Communities

There are several existing communities within the UK for information sharing, some are more active and bi-directional than others.

- NCSC
  - CiSP
  - MISP Intelligence Sharing Platform
  - Plus, invitation only schemes such as the ICS COI
- Competent Authorities may have working communities
  - Travel – DfT, CAA
  - Electricity and Gas – BEIS, OFGEM
  - Oil – BEIS
  - Digital infrastructure and Digital Service Providers – Ofcom
- Other ISACs (examples)
  - FS-ISAC
  - A-ISAC
  - EE-ISAC

Consider working with your peers to create your own group.

Develop a simple process that makes it easy and ideally visible for all.

Bridewell

https://www.ncsc.gov.uk/blog-post/strength-of-ics-coi-is-the-team

Sharing in the Supply Chain

"Customer/processor agrees to notify the client/controller of any actual or perceived incident/breach within 72 hours..."

Regulators have the greatest success in implementing this because it causes pain for non-compliance. Here's what you can consider.

- Define and share a process that makes it easy and ideally visible for all.
- Audit annually based upon compliance. Introduce it into your supplier assurance frameworks.
- Make if valuable for success.
- Develop incident testing that includes your supply chain to increase awareness and capture lessons learnt.

Bridewell

Summary

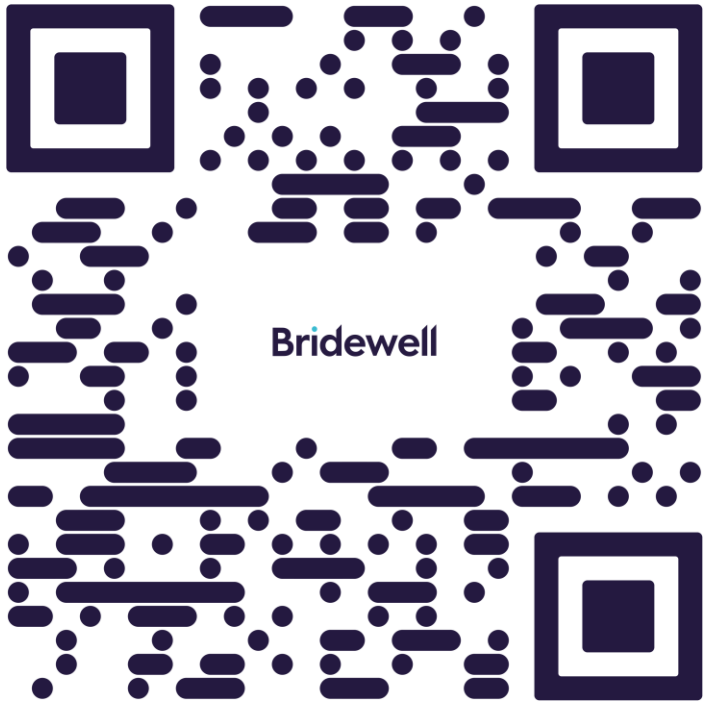
Intelligence sharing need not be complex and restrictive, and it isn't a large leap (or gap) to sharing timely intelligence.

Hopefully through the course of this session, we have shown you the value of threat intelligence, and how cyber threat intelligence can inform decisions throughout cyber security in support of increasing resilience.

Lastly, we hope you have seen that sharing intelligence gathered through bringing intelligence into intrusion analysis can help bolster cyber resilience for your community.

Bridewell

Thank you



To download this presentation and the associated content, please use the link in the QR Code to be directed to the Bridewell website.

- Bridewell CNI Research
- MITRE ATT&CK maps for active threat groups in CNI
- OS Intelligence Sources
- Intelligence Sharing Templates
- This presentation

Bridewell