

AIPIO
INTELLIGENCE
CONFERENCE **2019**



FS-ISAC

*Examining
Cyberthreat
Intelligence from a
PPP Perspective*

Scott Ainslie

Regional Director Australia & New Zealand

Pier One, Sydney, Australia

20th August 2019



Traffic Light Protocol (TLP)



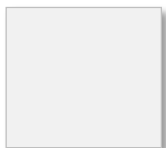
- » **Red:** Restricted to a defined group. Information labeled RED can not be shared with anyone outside of the group



- » **Amber:** May be shared need-to-know with own staff and vendors to mitigate risks. Confidentiality must be contractually assured.



- » **Green:** May be shared with peer organisations and with partners (e.g., vendors, MSSPs, customers). Information in this category can not be shared in public forums



- » **White:** May be shared freely and is subject to standard copyright rules

Context

What is an ISAC?

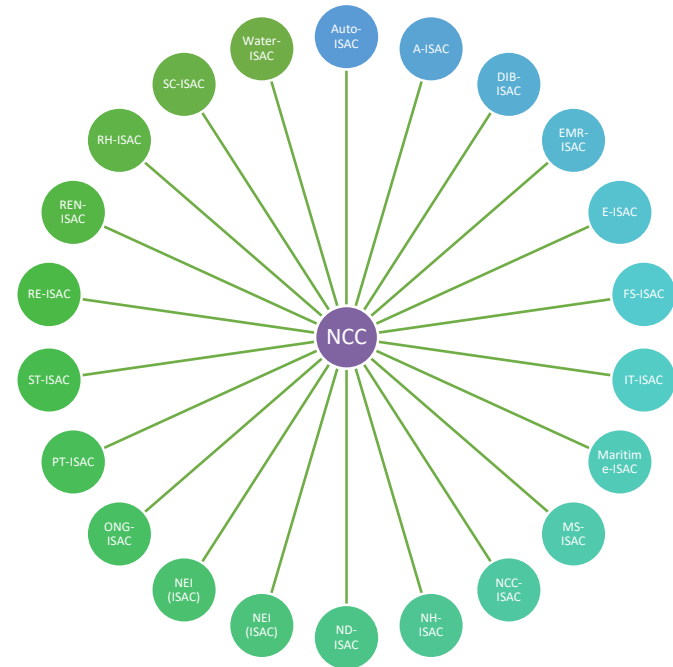


- Information Sharing and Analysis Center
- Created by the Clinton Administration in 1998
- Trusted entities established by Critical Infrastructure Key Resource (CI/KR) owners and operators
- Provides comprehensive sector analysis, aggregation & anonymisation
- All-hazards approach
- Resilience is emphasised through combining cybersecurity and business resilience

ISAC Organisations

- 22 ISAC organisations exist
- Several coexist as ISAO
- Now beyond CII footprint

- Automotive (Auto-ISAC)
- Aviation (A-ISAC)
- Defense Industrial Base (DIB-ISAC)
- Emergency Services (EMR-ISAC)
- Electricity (E-ISAC)
- Financial Services (FS-ISAC)
- Information Technology (IT-ISAC)
- Maritime Security ISAC
- Multi-State ISAC (MS-ISAC)
- Communications ISAC (NCC)
- National Health (NH-ISAC)
- National Defense ISAC
- Nuclear (NEI)
- Oil and Gas (ONG-ISAC)



- Energy Analytic Security Exchange (EASE)
- Public Transit (PT-ISAC)
- Real Estate (RE-ISAC)
- Research & Education (REN-ISAC)
- Retail & Hospitality ISAC (RH-ISAC)
- Supply Chain (SC-ISAC)
- Surface Transportation (ST-ISAC)
- Water ISAC (Water-ISAC)

FS-ISAC Mission

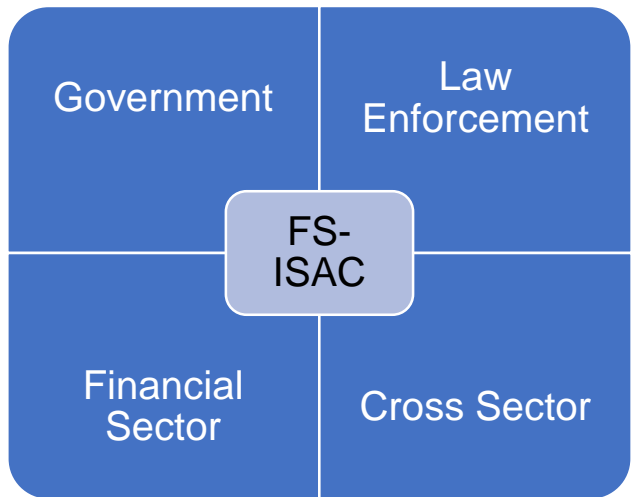
FS-ISAC's mission is to improve the security and resilience of the global financial services sector, including the public's financial life. FS-ISAC empowers voluntary sharing, intelligence, crisis response, exercises and best practices with focused subsidiaries that develop standards and conduct deeper analysis and other forms of collaboration.

- Non profit founded in 1999
- 7,000 members headquartered in 50 countries
- Member driven organisation

FS-ISAC - by the numbers

- » About **7,000** financial institutions
- » **5,000+** *Commercial Banks*
- » **All** *Major Credit Card Companies*
- » **120+** *Registered Broker Dealers*
- » **100+** *Asset Managers*
- » **130+** *Insurance Companies*
- » **42** *Bank Associations*
- » **75** *Alternative Investors*

Private Public Partnerships



- **Goals:**
 - Provide connectivity to public sector for enrichment of data for the membership and possible national defense
 - Provide a channel for public-to-private sector-wide messaging
- **Core Principals:**
 - Sharing with Public Sector Partners **only** occurs with permission of member.
 - Member elects either anonymous or attributed sharing

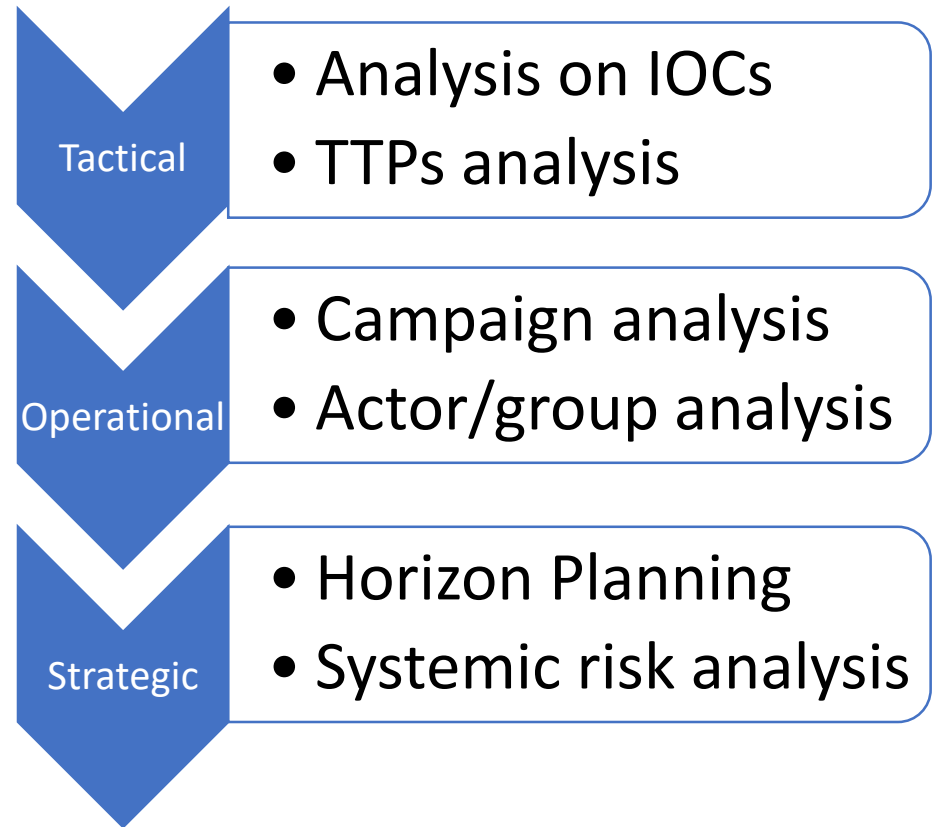
Intelligence

Threat Intelligence & Analysis



Levels of Intelligence Analysis

- Integrated teams vertically and horizontally across the globe
 - Integration allows the building of intelligence without duplication
 - Production addresses needs of multiple tiers of membership
- Full-spectrum analysis (cyber, fraud, physical) for full resilience topics

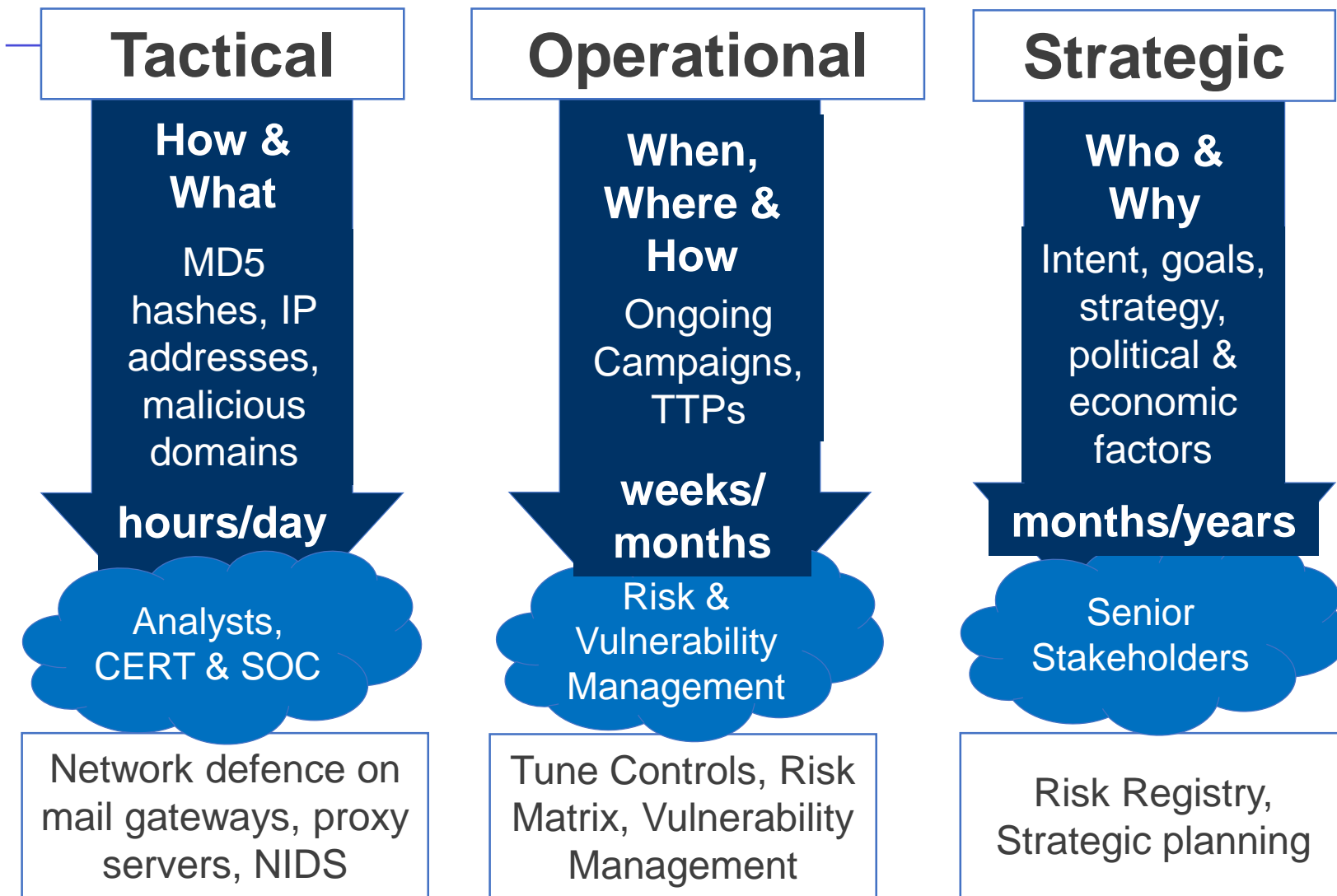


Priority Collection Requirements

- Threat Actors: What are the key and emerging threat actors targeting the financial sector?



Types of Cyberthreat Intelligence

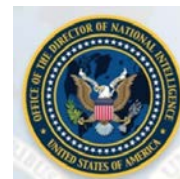


Why FS-ISAC Intelligence?

- The information overload problem
 - A common problem is that users can't consume the flood of emails, alerts and other data coming to them
 - Consolidation is not the only thing that was wanted; members asked for analysis
- The lack of global sector understanding
 - Platform exchange of technical data only told part of the story and not in an authoritative manner
 - Different countries, different sub-sectors, different sizes of members mean that there's a huge scope of stakeholder needs

Attribution

Attribution



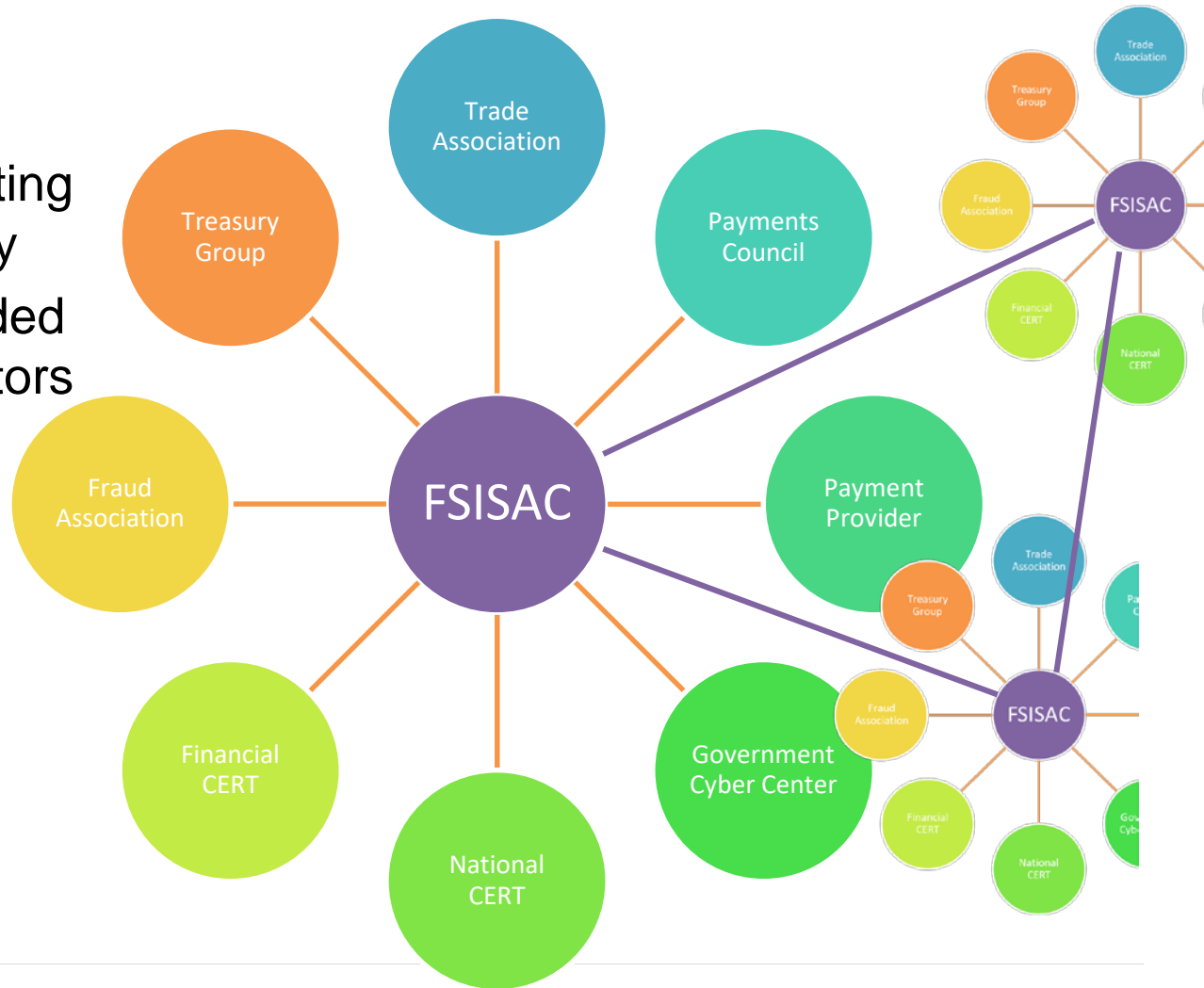
Office of the Director
of National Intelligence

- **Looking for Human Error**
 - Almost all cyber attribution successes have resulted from discovery and exploitation of the attackers' operational security errors
- **Timely Collaboration, Information Sharing, and Documentation.**
 - Attribution efforts benefit from combining the expertise of regional, political, and cybersecurity analysts and the collaboration of network defenders, law enforcement, private cybersecurity firms, and victims
- **Rigorous Analytic Tradecraft**
 - Analysts may start with a set of plausible actors in mind, based on the nature of the cyber incident, the targets, and the context but must be careful to avoid cognitive bias.



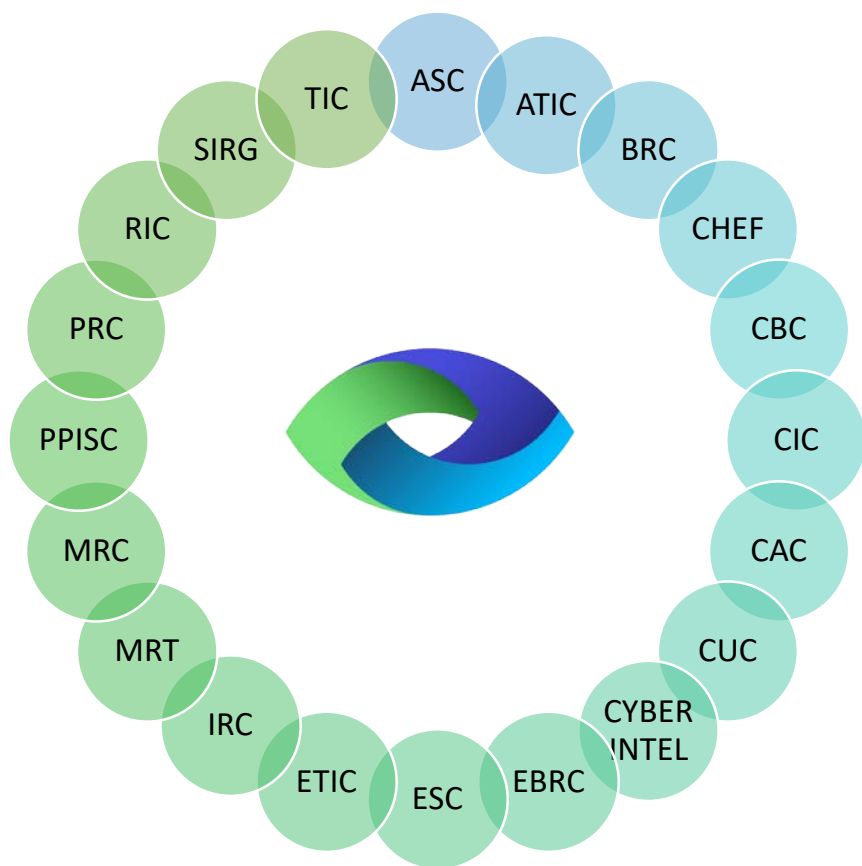
Connecting Trusted Communities

- Integration not competition
 - Plug into the existing network in country
 - Be the link if needed between sub-sectors
- FS-ISAC's network across the world links members together



Trust

Circles of Trust



- » APAC Strategy Committee (ASC)
- » APAC Threat Intelligence Committee (ATIC)
- » Business Resiliency Committee (BRC)
- » Clearing House and Exchange Forum (CHEF)
- » Community Bank Council (CBC)
- » Community Institution Council (CIC)
- » Compliance and Audit Council (CAC)
- » Credit Union Council (CUC)
- » Cyber Intelligence Mail List
- » EMEA Business Resilience Committee (EBRC)
- » EMEA Strategy Committee (ESC)
- » European Threat Intelligence Committee (ETIC)
- » Insurance Risk Council (IRC)
- » Media Response Team (MRT)
- » Mortgage Risk Council (MRC)
- » Payment Processor Information Sharing Council (PPISC)
- » Payments Risk Council (PRC)
- » Retirement Industry Council (RIC)
- » Securities Industry Risk Group (SIRG)
- » Threat Intelligence Committee (TIC)



Source Assessment

- Reliability and Trust

The Admiralty Scale

Reliability

A	Completely reliable
B	Usually reliable
C	Fairly reliable
D	Not usually reliable
E	Unreliable
F	Reliability cannot be judged

Credibility

1	Confirmed by other sources
2	Probably True
3	Possibly True
4	Doubtful
5	Improbable
6	Truth cannot be judged

B

Usually reliable

3

Possibly True

= B3



Source Assessment

- Reliability and Trust

5 x 5 x 5

1.4 Source Evaluation

SOURCE EVALUATION	A Always Reliable	B Mostly Reliable	C Sometimes Reliable	D Unreliable	E Untested Source
----------------------	--------------------------------	--------------------------------	-----------------------------------	------------------------	--------------------------------

1.5 Information/Intelligence Evaluation

INFORMATION/ INTELLIGENCE EVALUATION	1 Known to be true without reservation	2 Known personally to the source but not the person reporting	3 Not known personally to the source, but corroborated	4 Cannot be judged	5 Suspected to be false
--	---	--	---	------------------------------------	--------------------------------------

Dissemination



2.5 Handling Codes

HANDLING CODE	1	2	3	4	5
<p>To be completed by the evaluator on receipt and prior to entry onto the intelligence system</p> <p>To be reviewed on dissemination</p>	<p>Default: Permits dissemination within the UK Police Service AND to other law enforcement agencies as specified</p> <p>[see 5x5x5 guidance]</p>	<p>Permits dissemination to UK non-prosecuting parties</p> <p>[conditions apply see 5x5x5 guidance]</p>	<p>Permits dissemination to (non-EU) foreign law enforcement agencies</p> <p>[conditions apply see 5x5x5 guidance]</p>	<p>Permits dissemination within originating service/ agency only</p> <p>Specify reasons for this and Identify internal recipient(s)</p> <p>A review period should be set</p> <p>[see 5x5x5 guidance]</p>	<p>Permits dissemination but receiving agency to observe conditions as specified</p> <p>[see 5x5x5 guidance on risk assessment]</p>



Summary

- It is still all about HUMINT
- Do not fear big data
- Be aware of and manage bias
- PPP models work - it takes two to tango
- Collaboration & sharing engender trust
- Intelligence is a product – KISS
- Don't brief what you don't believe – stay curious
- Cybersecurity is now an industry pillar reflecting the only real horizontal across all industry verticals.

Questions?

Thank You.

- **Scott Ainslie**
- sainslie@fsisac.com
- +61 421.141.545