RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: ANF-F01

HUNTED TO THE HUNTER

CLINTON FIRTH

General Manager, CSC Cybersecurity
Australia & New Zealand
Blog: www.clintonfirth.com
Twitter: @FirthClinton

STEPHEN BRENNAN

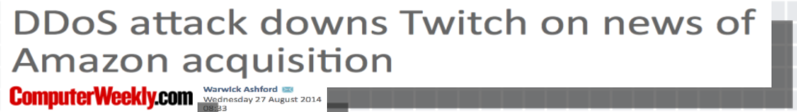
Global Managing Partner, CSC Cybersecurity

Blog: www.csc.com/brennan
Twitter: @StephensLogic

Need for a change

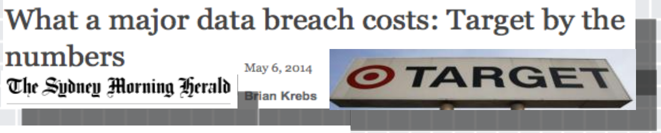
- Exponential attack surface, threat actor growth & evolution
- Current Strategies are ineffective
- Challenge exceeds resources
- Business & clients demand more security form less (budget & friction)
- New Platforms require new (unproven solutions)

We Must Change Our Approach



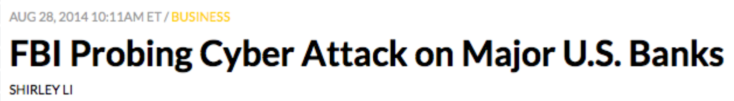
DDoS attack downs Twitch on news of Amazon acquisition

ComputerWeekly.com Warwick Ashford Wednesday 27 August 2014 08:33



What a major data breach costs: Target by the numbers

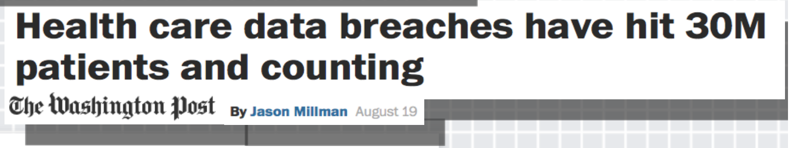
The Sydney Morning Herald May 6, 2014 Brian Krebs



AUG 28, 2014 10:11AM ET / BUSINESS

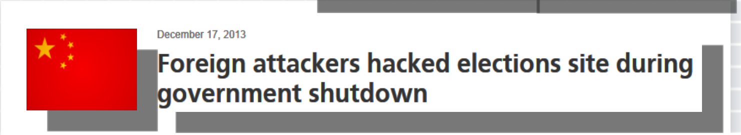
FBI Probing Cyber Attack on Major U.S. Banks

SHIRLEY LI



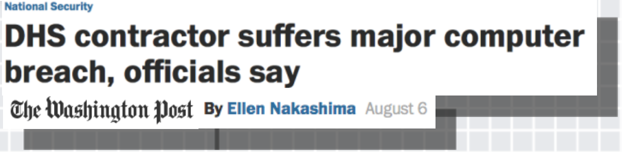
Health care data breaches have hit 30M patients and counting

The Washington Post By Jason Millman August 19



December 17, 2013

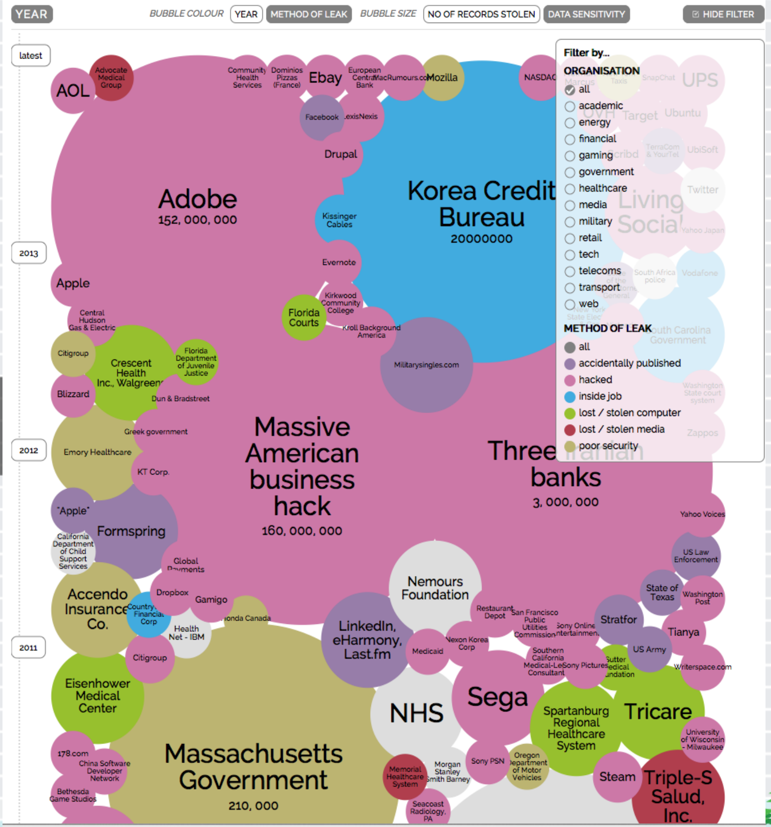
Foreign attackers hacked elections site during government shutdown



National Security

DHS contractor suffers major computer breach, officials say

The Washington Post By Ellen Nakashima August 6

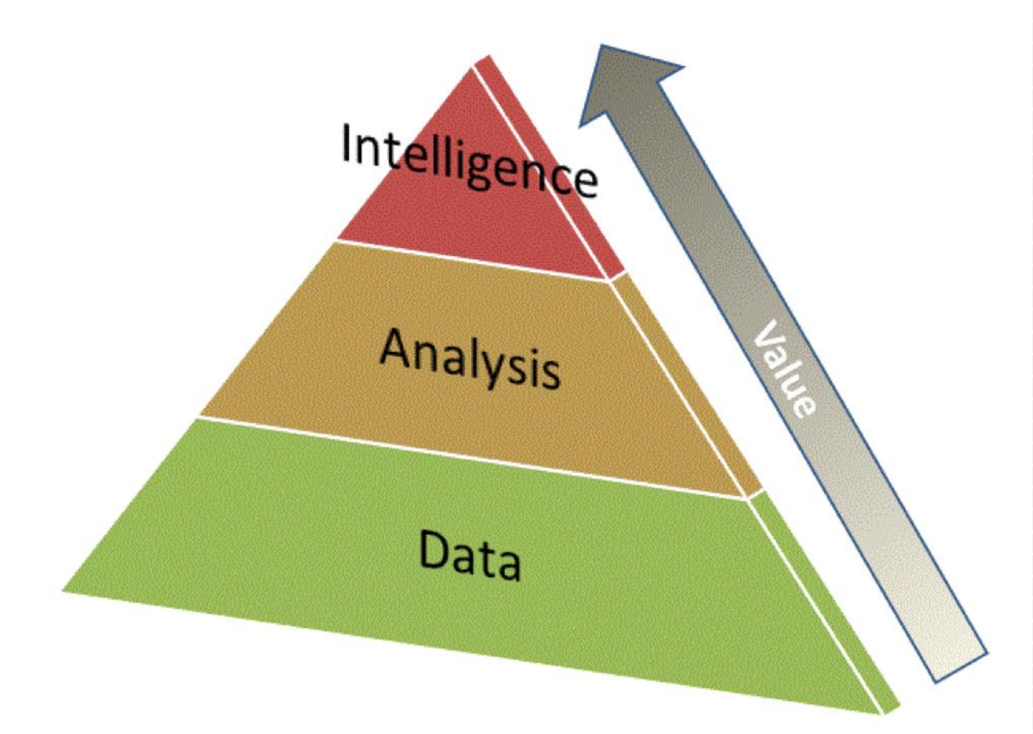


www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

What is Strategic Threat Intelligence?

- Threat actor focus
- Intelligence Analysis
- Collection planning
- Proactive approach

The data within the database — or the threat feed — can be highly useful to the intelligence process. But (and I am not picking nits here) it comprises a data feed, not an intelligence feed (except to marketers).”
Darkreading – Nick Selby



A New Approach to Cyber

"If you know the enemy and know yourself, you need not fear the result of a hundred battles..."

- Sun Tzu, the
Art of War

Militaries use intelligence

Global cyber war

Threats evolve & calibrate

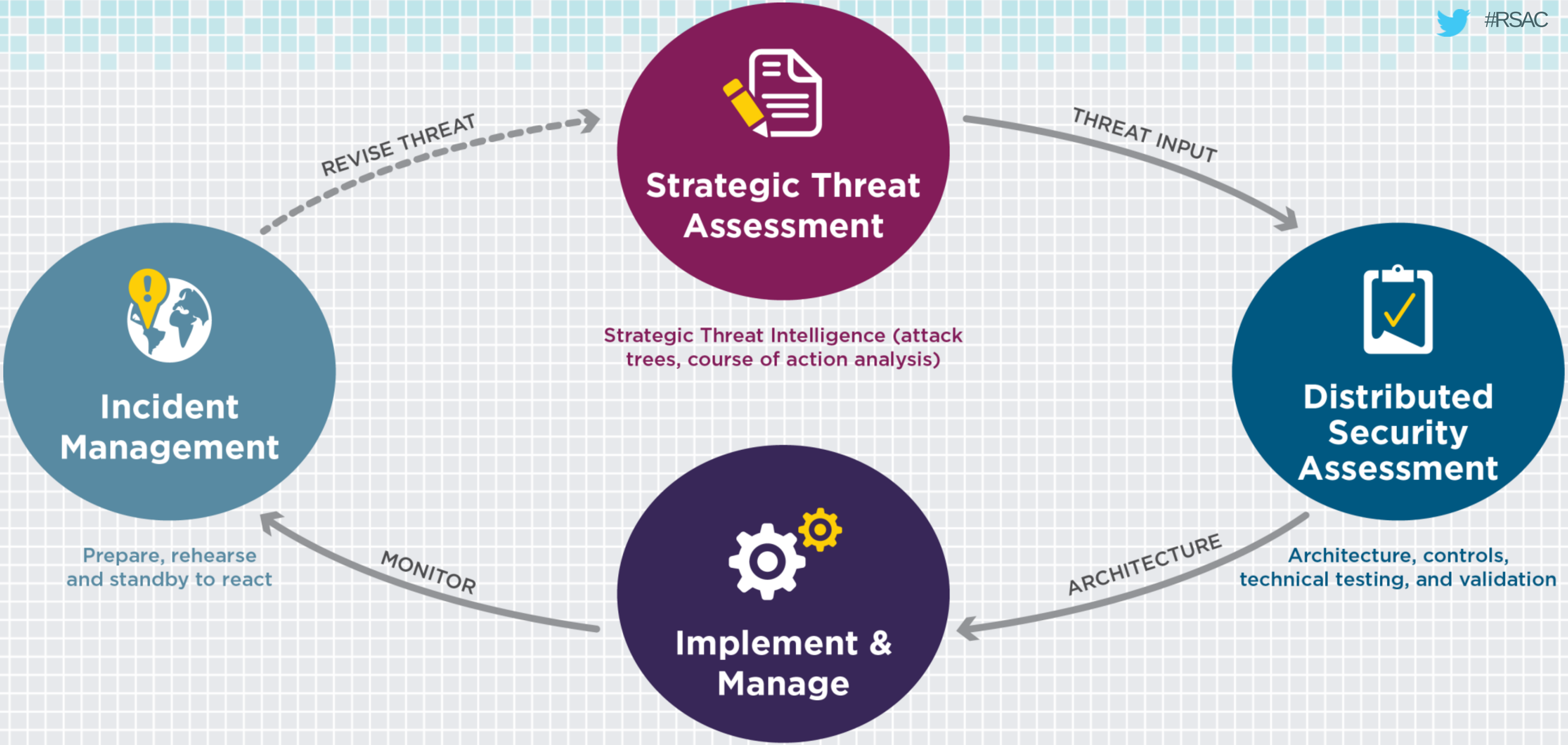
Threats to clients

Business Drivers

- Merger / Acquisition
- Event
- Business Strategy
- Mature compliance
- Service continuity

Technical Drivers

- Disparate Data Sources
- Information Architecture
- Context and Relationships
- Retention and Elastic Search
- Attribution
- New and Emerging Threats
- New Command and Control



Strategic Threat Assessment

Strategic Threat Intelligence (attack trees, course of action analysis)

Distributed Security Assessment

Architecture, controls, technical testing, and validation

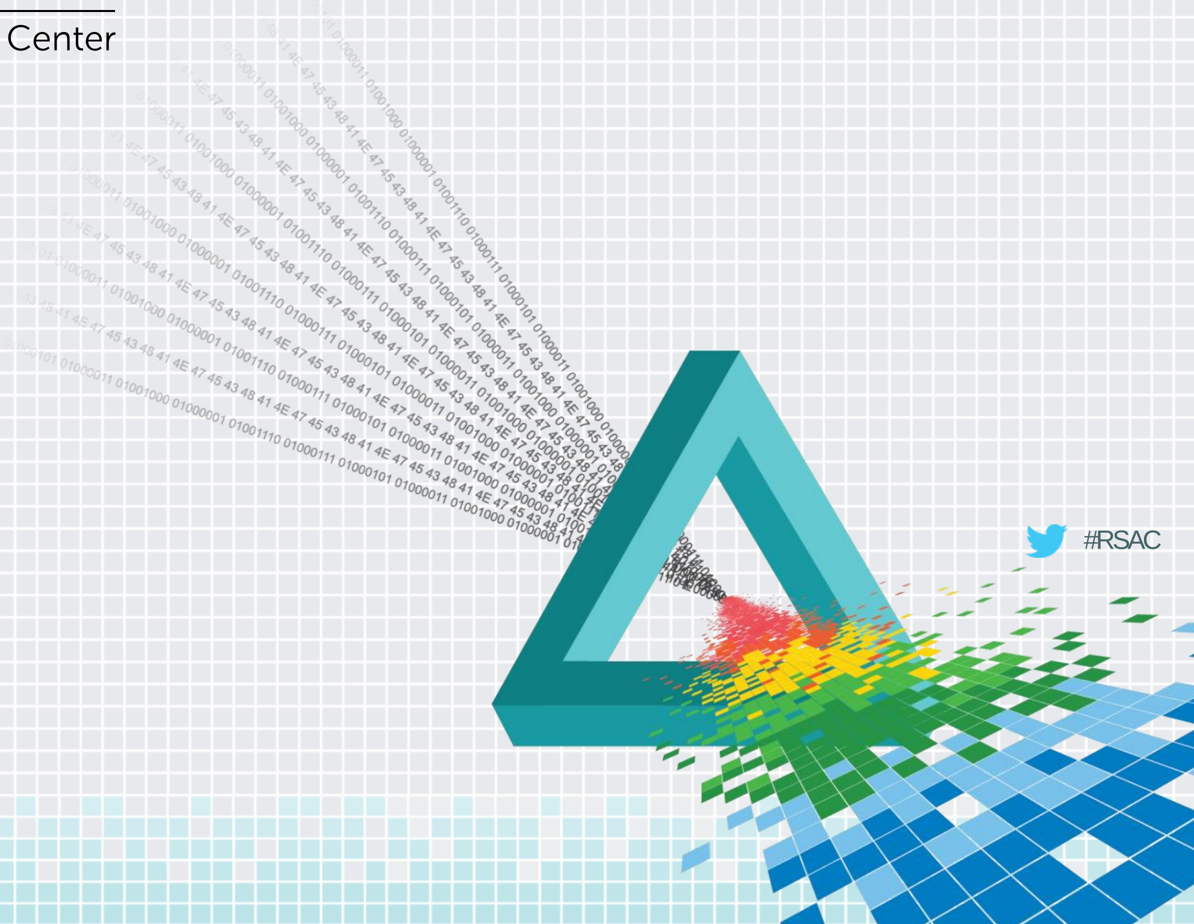
Implement & Manage

Baseline, event monitoring, analysis, threat review, correlation, event management

Incident Management

Prepare, rehearse and standby to react

Strategic Threat Assessment



#RSAC

Strategic Threat Assessment

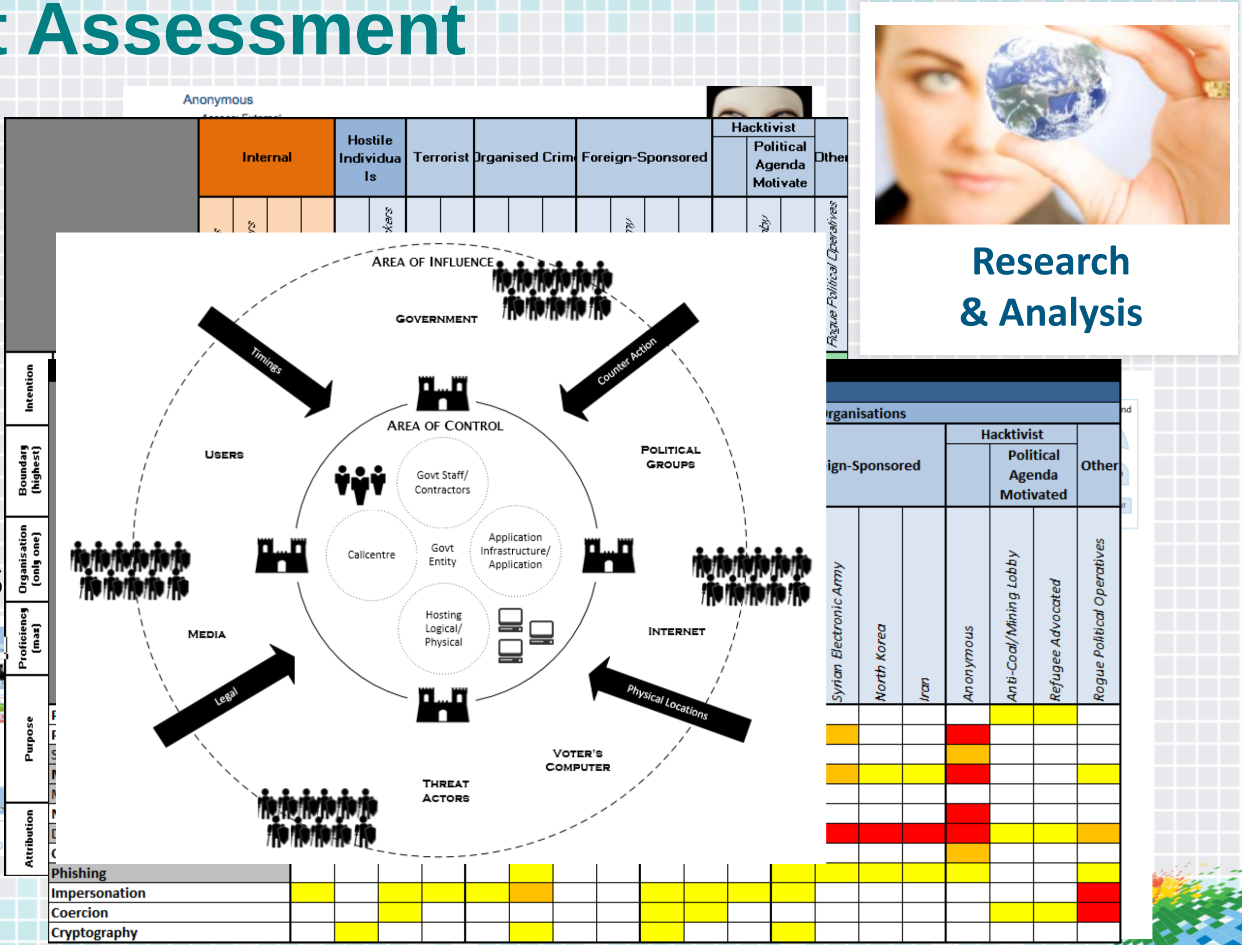
Research & Analysis

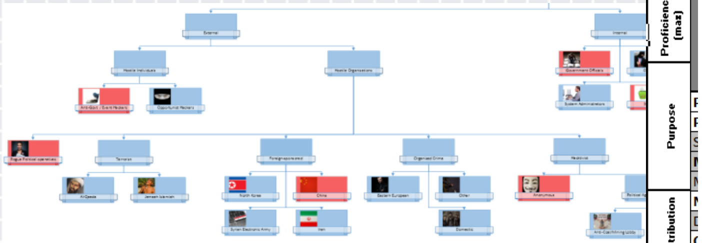
Wargame, Test & Assess

Limited Stealth Operations

Strategic Threat Assessment

- Research Actors
- Attribution
- Attack Trees
- Capability synopsis
- Ecosystem Analysis



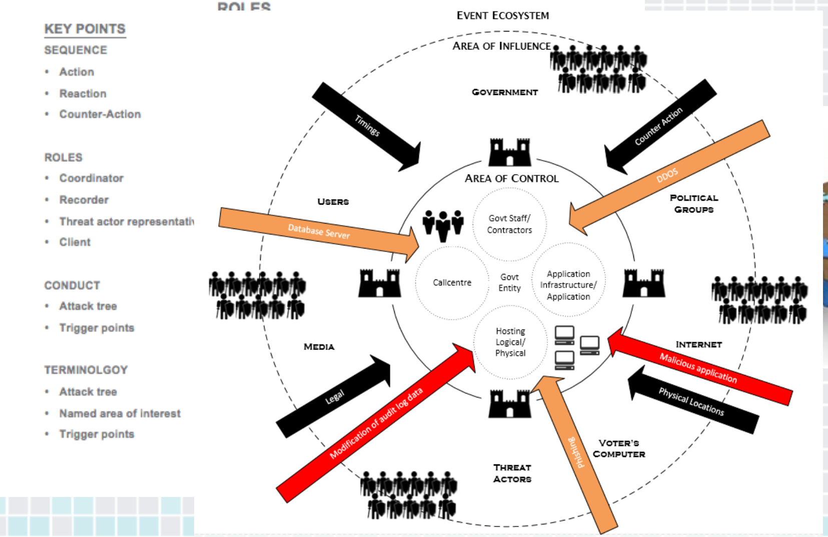


STRATEGIC THREAT ASSESSMENT

- Wargame
  - Specialists
  - Attack tree
  - Action – Reaction – Counteraction
- Threat course of action
  - Wargame analysis
  - Most Dangerous
  - Most Likely

WARGAME

Rules Handout



KEY POINTS

SEQUENCE

- Action
- Reaction
- Counter-Action

ROLES

- Coordinator
- Recorder
- Threat actor representati
- Client

CONDUCT

- Attack tree
- Trigger points

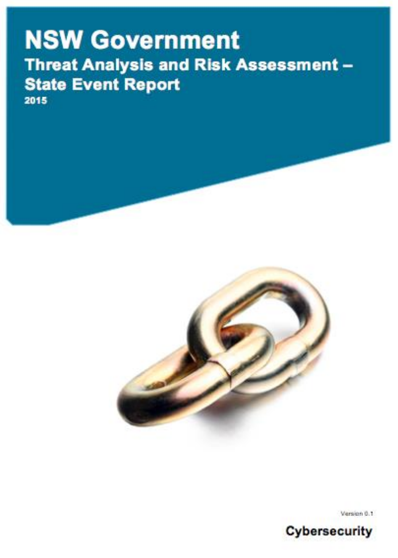
TERMINOLGOY

- Attack tree
- Named area of interest
- Trigger points

Wargame, Test & Assess

Strategic Threat Assessment

- Executive Report
- Intelligence Collection Plan
- Limited Stealth Operations
- Incident Response



NSW Government

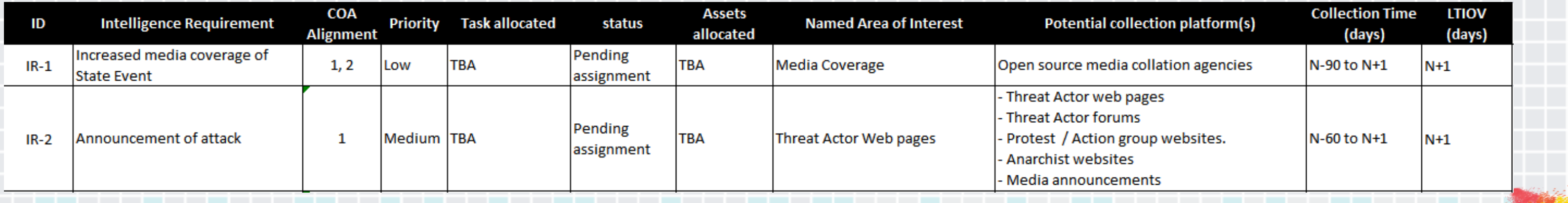
Threat Analysis and Risk Assessment – State Event Report

2015

Version 0.1

Cybersecurity

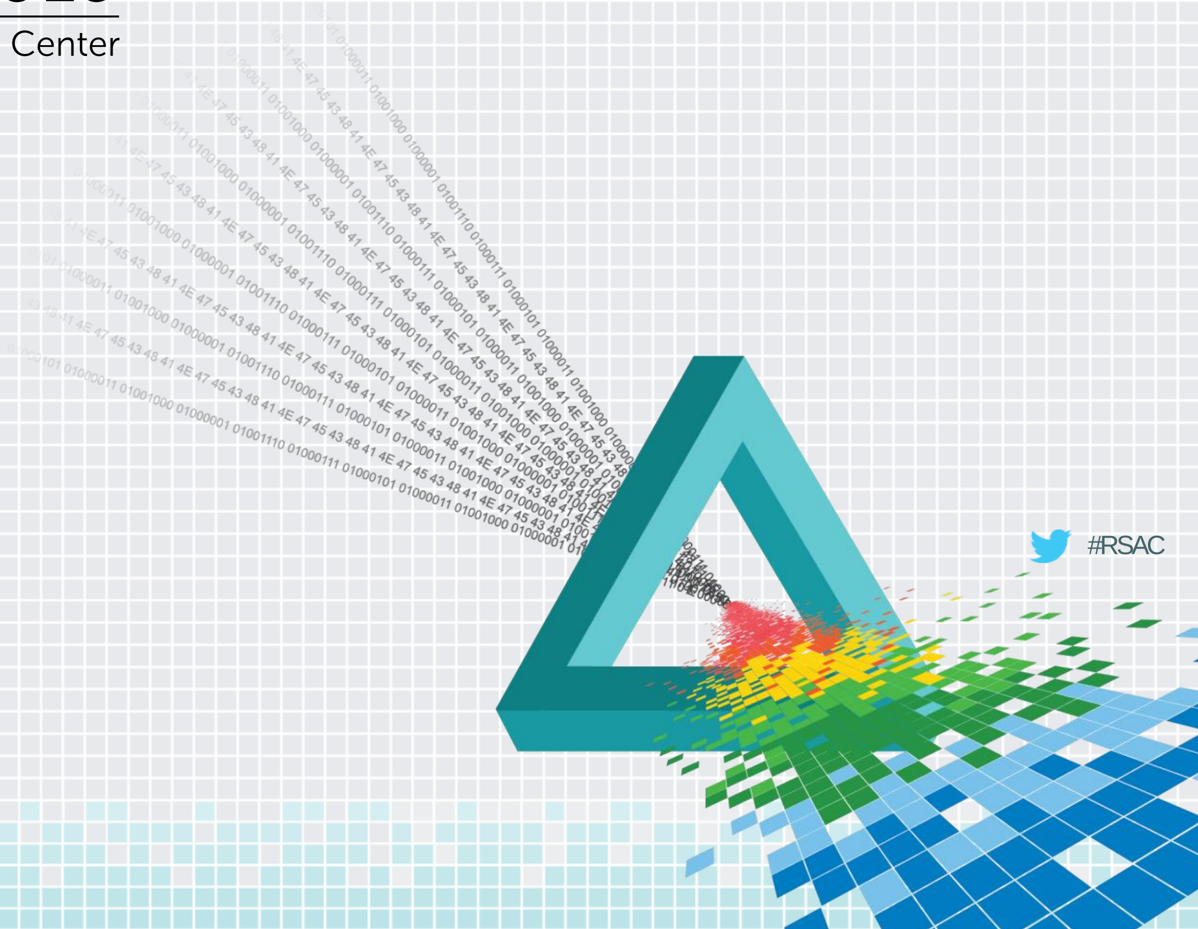
Limited Stealth Operations



ID	Intelligence Requirement	COA Alignment	Priority	Task allocated	status	Assets allocated	Named Area of Interest	Potential collection platform(s)	Collection Time (days)	LTIOV (days)
IR-1	Increased media coverage of State Event	1, 2	Low	TBA	Pending assignment	TBA	Media Coverage	Open source media collation agencies	N-90 to N+1	N+1
IR-2	Announcement of attack	1	Medium	TBA	Pending assignment	TBA	Threat Actor Web pages	- Threat Actor web pages - Threat Actor forums - Protest / Action group websites. - Anarchist websites - Media announcements	N-60 to N+1	N+1

RSAConference2015

San Francisco | April 20-24 | Moscone Center



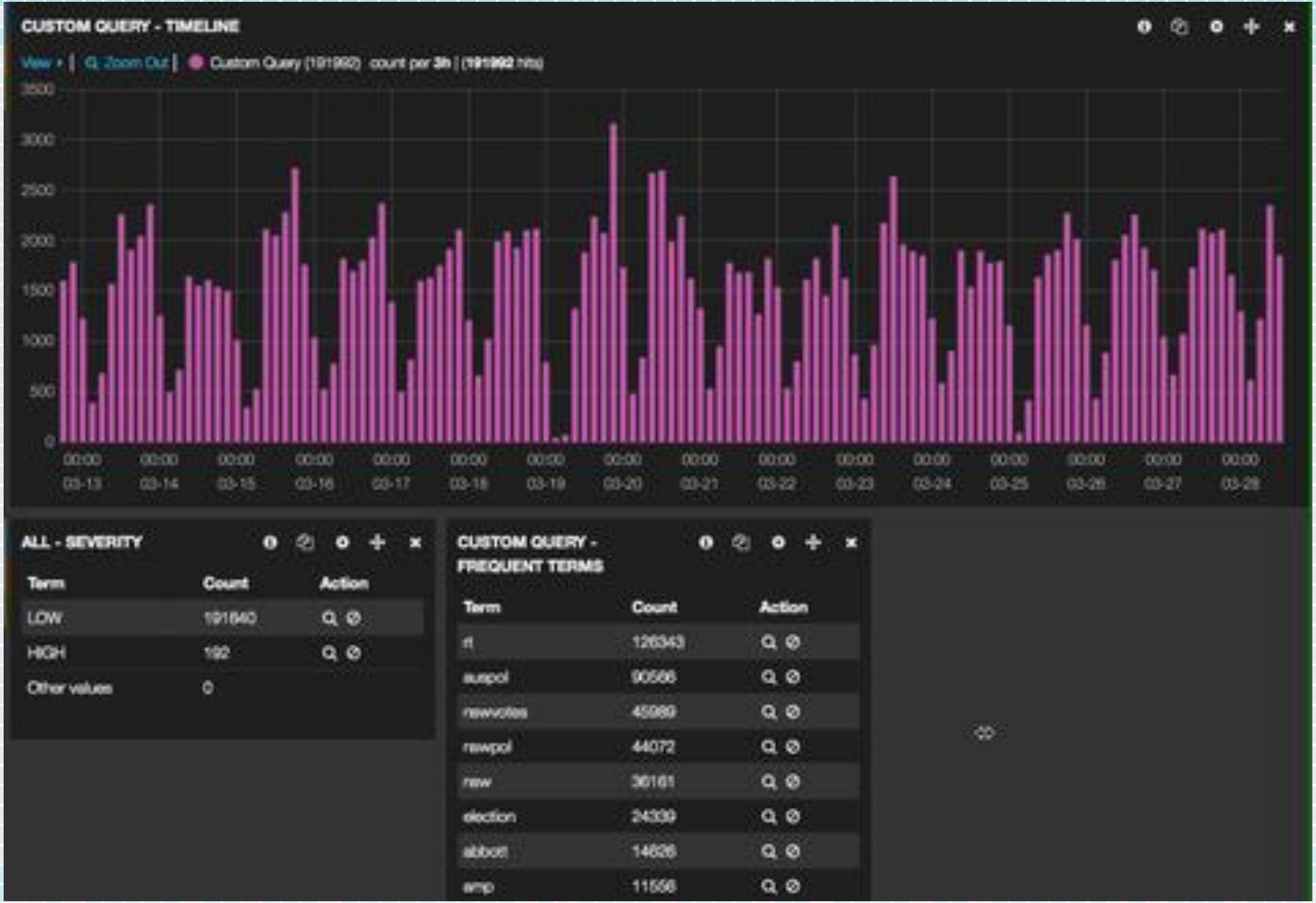
#RSAC

Limited Stealth Operations

Limited Stealth Operations

- Execution of the Intelligence plan
- Predetermined focal points
- Monitor the Threat Actors – Command & Control
- Feed into SOC

Limited Stealth Operations



CUSTOM QUERY - TIMELINE

ALL - SEVERITY

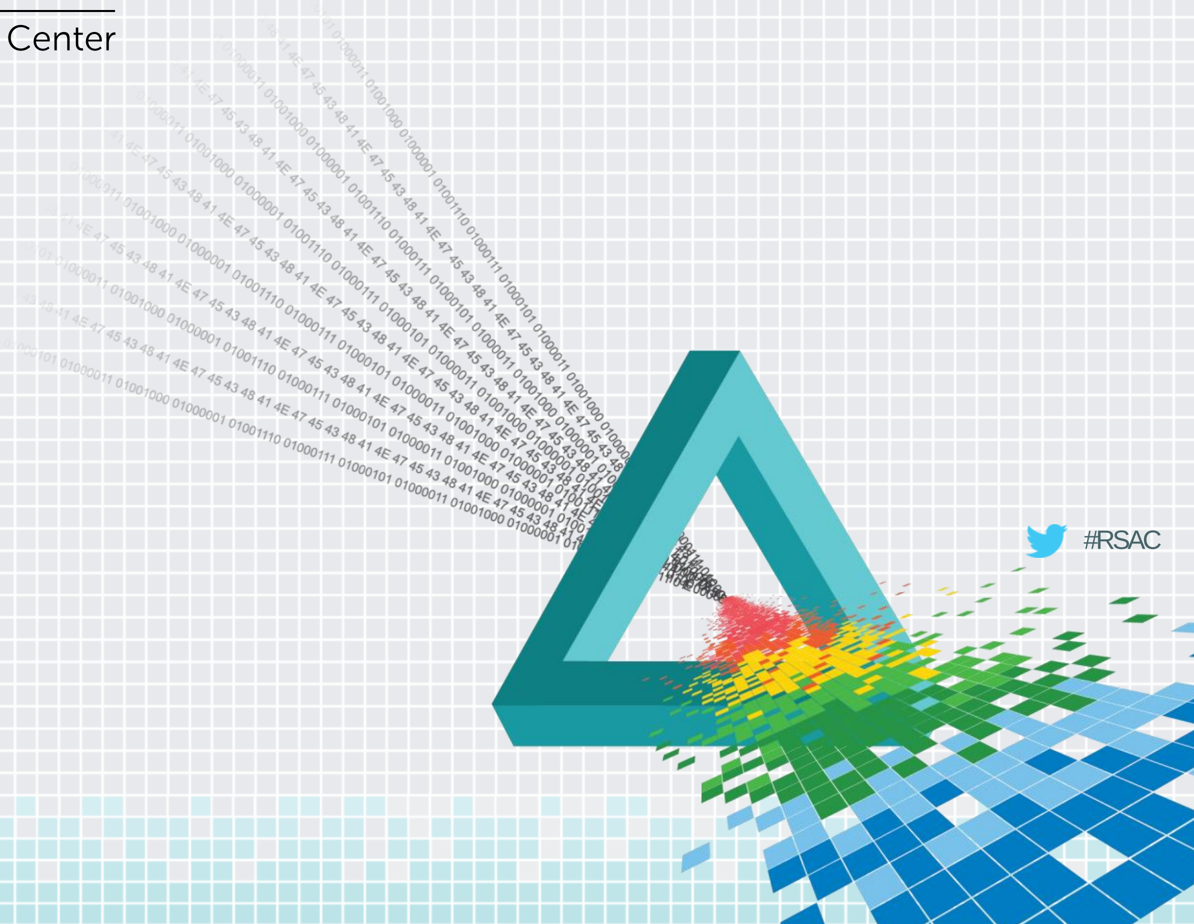
Term	Count	Action
LOW	191840	
HIGH	192	
Other values	0	

CUSTOM QUERY - FREQUENT TERMS

Term	Count	Action
rt	126343	
auspol	90566	
newvotes	45989	
newpol	44072	
new	36161	
election	24339	
abbott	14626	
amp	11556	

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

Summary

Summary

- Compliance is failing
- Unique threat driven approach
- Focus, pragmatic and effective
- Supports business operations
- Turns the tables

Apply Slide

- Think like a Threat Actor
- Research your Threat Actors
- Categorize and prioritize
- Collection plan
- Monitor threat actors