SENSATO
CYBERSECURITY SOLUTIONS

Cybersecurity Myths & Fallacies

John Gomez

About Sensato

2013

Sensato is founded by John Gomez, ex-CTO/President of AllScripts and CTO of WebMD.

2014

Sensato launches its Risk Assessment Workshop program and NIST based Vulnerability Assessment programs.

2015

Sensato creates the first healthcare industry conference on cybersecurity - Hacking Healthcare.
Sensato named one of the Top-500 Most Innovative Cybersecurity Companies in the World

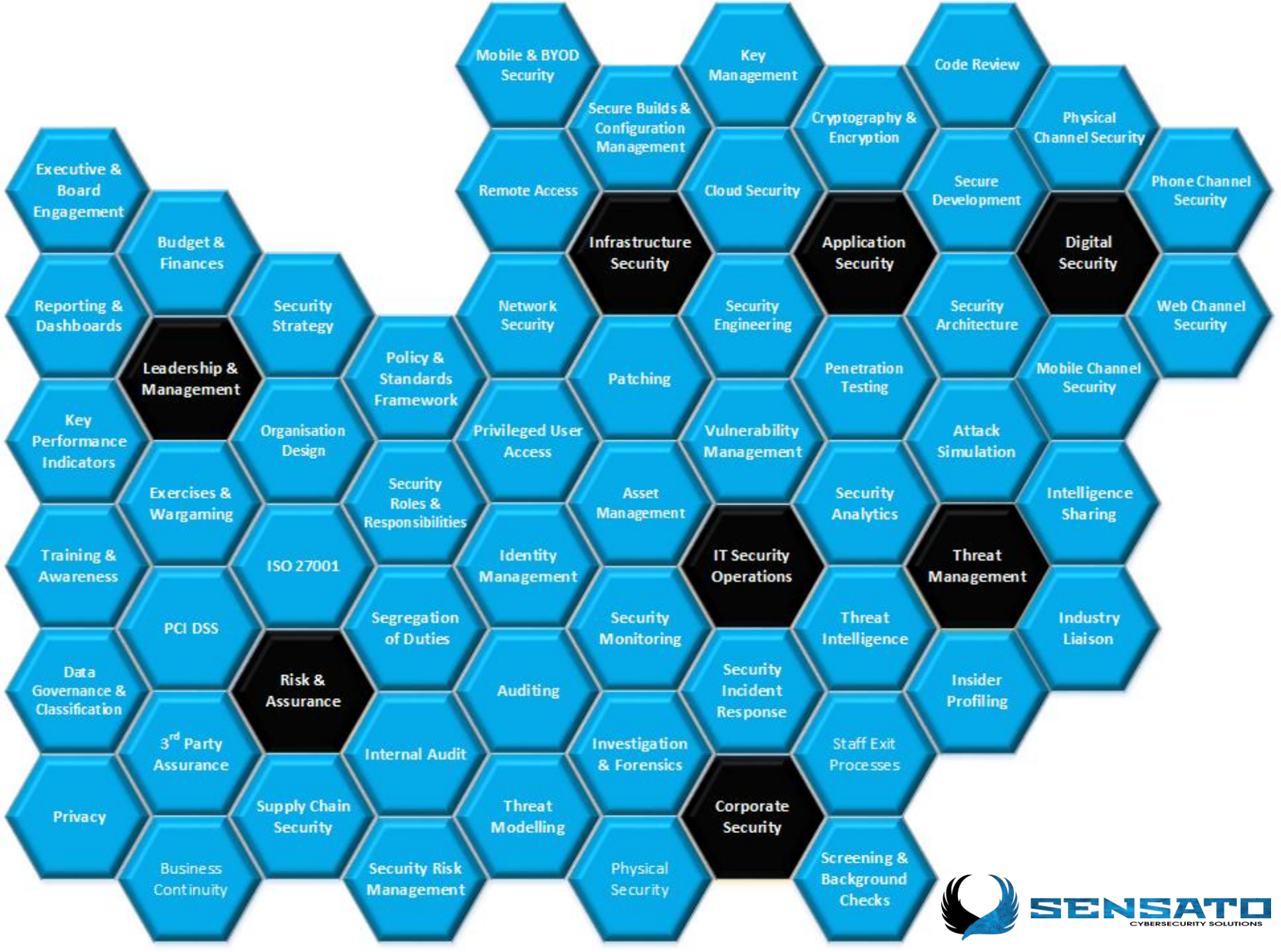
2016

Sensato forms Medical Device Cybersecurity Task Force
Sensato Announces the Sensato Cybersecurity Tactical Operations Center – CTOC
Once again named Top-500
Frost and Sullivan Visionary Leader 2016

CYBERSECURITY 500 WORLD'S HOTTEST SECURITY COMPANIES

CYBERSECURITY TACTICAL OPERATIONS CENTER SENSATO

SENSATO CYBERSECURITY SOLUTIONS



SENSATO
CYBERSECURITY SOLUTIONS

90

Average Password Change Policy Requirement

SENSATO
CYBERSECURITY SOLUTIONS

5 25 63 135

265

295

SENSATO
CYBERSECURITY SOLUTIONS

More Myths

"Changing passwords reduces attackers ability to…"

"If that was encrypted…"

"We passed our audits…so we are…"

"We did an asessement last year…"

"We follow _____ .(NIST, PCI, ISO, DoD)"

"We are _____ certified."

SENSATO
CYBERSECURITY SOLUTIONS

New World Order

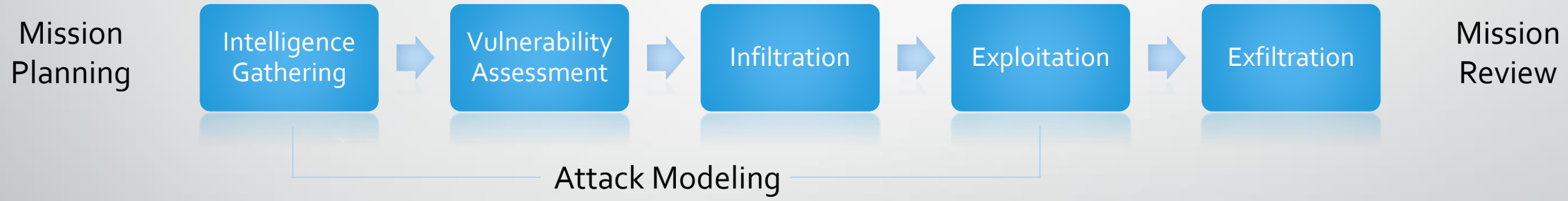
SENSATO
CYBER SECURITY SOLUTIONS

Hackers vs. Attackers

Attacker Motivations

Attacker Type	Motivation	Objectives
Cyber Criminal	Profit – Purely Profit (EAS, RAS)	Theft
Cyber Spy	Nation state – highly sophisticated – highly resourced – think James Bond	Theft
Cyber Terrorist	Ideology	**Death**

The Attacker Methodology



Learning from Anthem

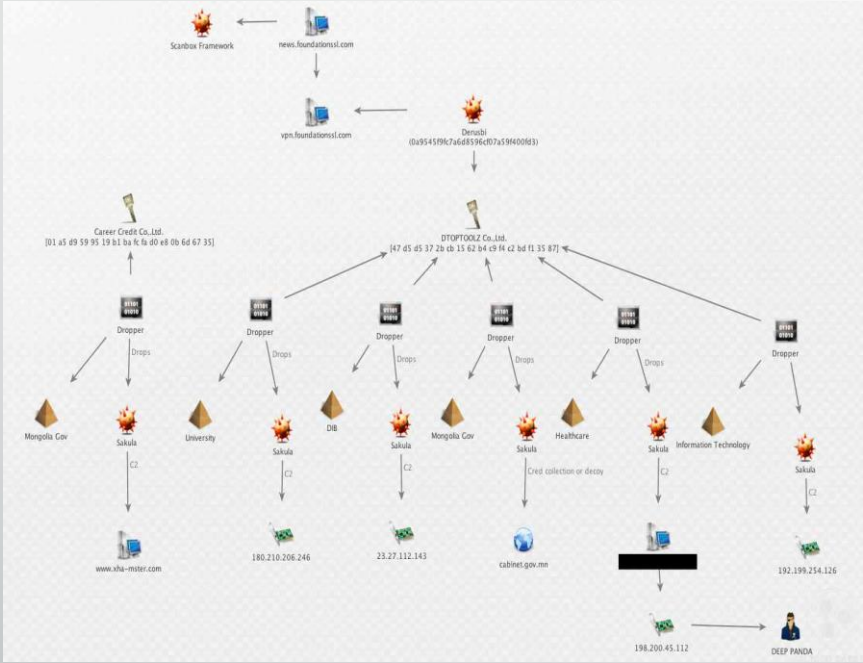
SENSATO
CYBER SECURITY SOLUTIONS

Attribution

- Commonly believed to be part of a broader Chinese Intelligence Group
- Possibly separate, but some evidence suggests it is also known as Axiom, Shell Crew or Group 72. CrowdStrike security team created the name "Deep Panda"
- Highly Polished Organization
- Mature Tactics, Techniques, Practices (TTP)
- Five Year Attack Plan Targeting Key Sectors and Organizations
- Not Financially Motivated
- Possible Human Intelligence Gathering Mission

SENSATO
CYBER SECURITY SOLUTIONS

November 2014



- CrowdStrike publishes a snapshot of the Deep Panda attack framework – known as "Scanbox"
- Scanbox is an extremely intelligent piece of malware that can utilize different payloads.
- Scanbox is executed in a web browser and therefore bypasses detection.
- Scanbox has various plug-ins:
  - Software Recon
  - Browser Plugin
  - Flash Recon
  - SharePoint Recon
  - PDF Recon
  - Chrome Security
  - Java Recon
  - Internal UP Recon
  - JavaScript Key Logger****
- Deep Panda may have authored Derusbi
  - Provides back door access
  - Remote Command and Control

SENSATO CYBER SECURITY SOLUTIONS

April 2014

we11point.com

SENSATO
CYBER SECURITY SOLUTIONS

	2014-04-21		2014-04-22
1	Domain Name: WE11POINT.COM	1	Domain Name: WE11POINT.COM
2	Registry Domain ID: 1855543298_DOMAIN_COM-VRSN	2	Registry Domain ID: 1855543298_DOMAIN_COM-VRSN
3	Registrar WHOIS Server: whois.godaddy.com	3	Registrar WHOIS Server: whois.godaddy.com
4	Registrar URL: http://www.godaddy.com	4	Registrar URL: http://www.godaddy.com
5	Update Date: 2014-04-21 03:13:19	5	Update Date: 2014-04-21 03:21:23
6	Creation Date: 2014-04-21 03:13:19	6	Creation Date: 2014-04-21 03:13:19
7	Registrar Registration Expiration Date: 2015-04-21 03:13:19	7	Registrar Registration Expiration Date: 2015-04-21 03:13:19
8	Registrar: GoDaddy.com, LLC	8	Registrar: GoDaddy.com, LLC
9	Registrar IANA ID: 146	9	Registrar IANA ID: 146
10	Registrar Abuse Contact Email: abuse@godaddy.com	10	Registrar Abuse Contact Email: abuse@godaddy.com
11	Registrar Abuse Contact Phone: +1.480-624-2505	11	Registrar Abuse Contact Phone: +1.480-624-2505
12	Domain Status: clientTransferProhibited	12	Domain Status: clientTransferProhibited
13	Domain Status: clientUpdateProhibited	13	Domain Status: clientUpdateProhibited
14	Domain Status: clientRenewProhibited	14	Domain Status: clientRenewProhibited
15	Domain Status: clientDeleteProhibited	15	Domain Status: clientDeleteProhibited
16	Registry Registrant ID:	16	Registry Registrant ID:
17	Registrant Name: wen ben zhou	17	Registrant Name: ad fire
18	Registrant Organization:	18	Registrant Organization:
19	Registrant Street: wen ren zheng fei ren chun 120hao	19	Registrant Street: fdsbcacfdt43
20	Registrant City: xiamen	20	Registrant City: new
21	Registrant State/Province: fu jian	21	Registrant State/Province:
22	Registrant Postal Code: 366115	22	Registrant Postal Code: 366512
23	Registrant Country: China	23	Registrant Country: Cayman Islands
24	Registrant Phone: +86.5925035801	24	Registrant Phone: +65.561235001
25	Registrant Phone Ext:	25	Registrant Phone Ext:
26	Registrant Fax:	26	Registrant Fax:
27	Registrant Fax Ext:	27	Registrant Fax Ext:
28	Registrant Email: e59e@qq.com	28	Registrant Email: admin@we11point.com
29	Registry Admin ID:	29	Registry Admin ID:
30	Admin Name: wen ben zhou	30	Admin Name: ad fire
31	Admin Organization:	31	Admin Organization:

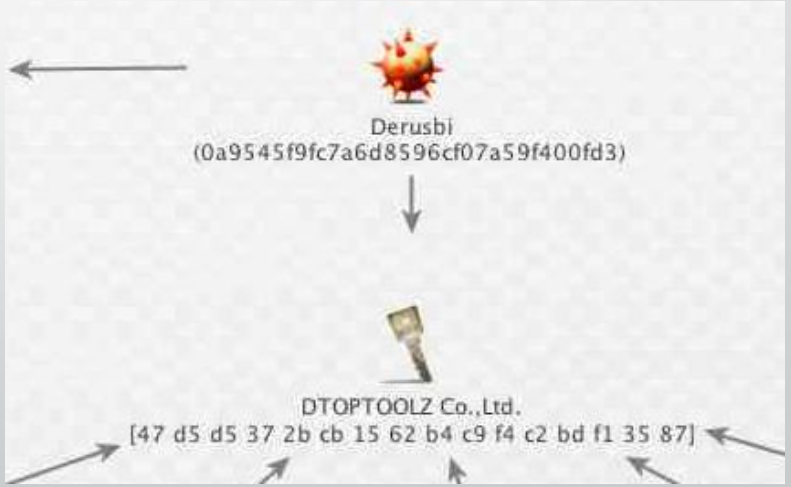

re
Nice to meet you.
We've changed our name from WellPoint to Anthem.

sophistication

- The attacker displayed TTP that is common with highly skilled intelligence agencies.
- If this is part of the attack strategy, then we suspect that they were targeting Anthem well before the attacks launched.
- The Anthem name-change may have created a triggering event to stage the attacks.
- Also registered:
  - myhr.we11point.com
  - hrsolutions.wellpoint.com
  - extcitrix.we11point.com

Citrix Connection

- extcitrix.we11point.com
  - Citrix provides remote access via VPN to employees and *supply chain* partners.
  - Registered April 22, 2014
  - Certificate signed by DTOPToolZ Co. -> Deep Panda



discovery

Anthem discovered the breach inadvertently.

An IT team member noticed someone was logged in with their account at the same time they were logged in…

…it wasn't technology that detected the breach!

Cyber-Terrorism

SENSATO
CYBER SECURITY SOLUTIONS

Cyber levels the worldwide battlefield - we have the largest military - and no citizen will have access to those resources - but access to cyber technologies does provide the same power to the common person as to that of the largest military.

Milware

Milware is a standardized and systemic approach to developing malware. Not all Milware is a weapon - although it can be a weapon. Weaponized code is still in it's infancy and is very immature at this point.

The big issue is that Milware ends up in the wild and hence it becomes a much broader problem, while beyond the targets of the nation state.

Milware In the Wild

There is evidence that Russia is providing legal-protection for illegal cybercriminals in exchange for early access to zero-day exclusivity and advanced penetration tools.

Polymorphic payloads are becoming more powerful and critical. This is a very serious threat and very hard to detect.

ISIS: Hello!

"Put down the chicken bro...and join the jihad!"

SENSATO
CYBER SECURITY SOLUTIONS

THE FANATICS' PROSPECTUS

ANNUAL REPORT: The title reads 'Information', Year 5, and the cover line 'Military operations by ISIS in the Islamic year 1434 (2013) in Iraq'.

7,681
total of military operations documented

BALANCE SHEET OF OPERATIONS CARRIED OUT BY THE ISLAMIC STATE DURING THE ISLAMIC YEAR 1434 IN IRAQ.

- SUICIDE VEHICLE BOMBS: 78
- CAR/TRUCK BOMBS: 537
- SUICIDE VEST BOMBINGS: 160
- MOTORCYCLE BOMBINGS: 14
- ROADSIDE BOMBS: 4,465
- ARMED ATTACKS (With light, medium and heavy weapons): 336
- ASSASSINATIONS (Using silenced weapons and small arms such as knives): 1,083
- MORTAR ATTACKS: 607
- BOMBING AND BURNING HOUSES AND PLACES OF WORSHIP: 1,015
- CHECKPOINTS SET UP: 30
- SNIPER HITS: 1,047
- CITIES OCCUPIED AND UNBELIEVERS DEALT WITH: 8
- UNBELIEVERS MADE TO REPENT: +100
- PRISONERS FREED: +100
- SHIAS EXPELLED: +100

■ This is a translated version of an infographic that appears in the report

THE WORLD HAS DIVIDED INTO TWO CAMPS

Amirul-Mu'minin said: "O Ummah of Islam, indeed the world today has been divided into two camps and two trenches, with no third camp present:

The camp of Islam and faith, and the camp of kufr (disbelief) and hypocrisy – the camp of the Muslims and the mujahidin everywhere, and the camp of the jews, the crusaders, their allies, and with them the rest of the nations and religions of kufr, all being led by America and Russia, and being mobilized by the jews."

A CALL TO HIJRAH

Amirul-Mu'minin said: "Therefore, rush O Muslims to your state. Yes, it is your state. Rush, because Syria is not for the Syrians, and Iraq is not for the Iraqis.

The earth is Allah's. **{Indeed, the earth belongs to Allah. He causes to inherit it whom He wills of His servants. And the [best] outcome is for the righteous}** [Al-A'raf: 128].

The State is a state for all Muslims. Th land is for the Muslims, all the Muslims O Muslims everywhere, whoeve is capable of performing hijra (emigration) to the Islamic State, the let him do so, because hijrah to th land of Islam is obligatory."

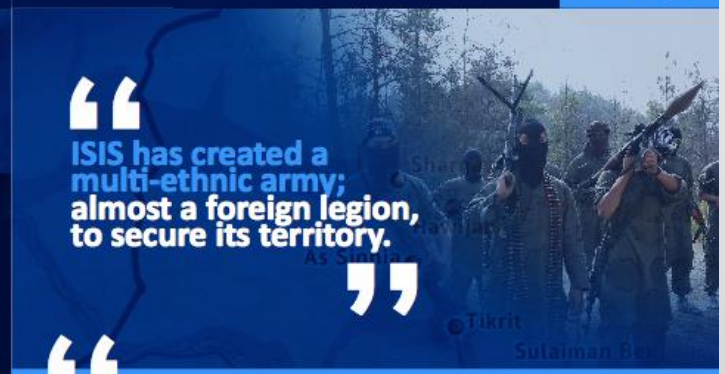
A CALL TO ALL MUSLIM DOCTORS, ENGINEERS, SCHOLARS, AND SPECIALISTS

Amirul-Mu'minin said: "We make a special

THE ISLAMIC STATE IN THE WORDS OF THE ENEMY

Douglas A. Ollivant, former Director for Iraq at the US National Security Council, and Brian Fishman former Director of Research for the Combating Terrorism Center at West Point – two American crusaders – wrote an article titled "The Reality of the Islamic State in Iraq and Syria" a short time before the Islamic State's liberation of Mosul as well as other important cities and towns in Iraq. Here are excerpts from the article.

"Out of the crucible of the Syrian civil war and the discontent in Iraq's Sunni regions, something new is emerging. The Islamic State in Iraq and Syria (ISIS) is no longer a state in name only. It is a physical, if extra-legal, reality on the ground. Unacknowledged by the world community, ISIS has carved a de facto state in the borderlands of Syria and Iraq. Stretching in a long ellipse roughly from al-Raqqah in Syria to Fallujah in Iraq (with many other non-contiguous "islands" of control in both Iraq and Syria), this former Al Qaeda affiliate holds territory, provides limited services, dispenses a form of justice (loosely defined), most definitely has an army, and flies its own flag."



"ISIS has created a multi-ethnic army; almost a foreign legion, to secure its territory."

Finally, this new reality presents a challenge that rises above a mere counter-terrorism problem. ISIS no longer exists in small cells that can be neutralized by missiles or small groups of commandos. It is now a real, if nascent and unrecognized, state actor—**more akin in organization and power to the Taliban of the late 1990s than Al Qaeda.**

"The group does not have safe haven within a state. **It is a de facto state that is a safe haven.**

During the course of the meeting, a number of things were requested from the tribal dignitaries, the most important of which were the following:

- Collecting the zakah and presenting it to the zakah offices located throughout the wilayah
- Preparing lists with the names of orphans, widows and the needy so that zakah and sadaqah can be distributed to them
- Encouraging the youth to join the ranks of the Islamic State
- Turning in any weapon acquired from the regime or the FSA
- Urging those bearing arms against the Islamic State to repent before they are captured

At the conclusion of the gathering, several of the tribal elders and dignitaries in attendance announced their bay'ah to the Islamic State.

More recently, representatives of the Islamic State attended another such meeting of tribal leaders in Wilayat Halab at the generous invitation of the leaders and dignitaries of the tribe of Bu Batush.

CARING FOR THE ORPHANS

Wilāyat Ar-Raqqah - Ramadān 19

The Islamic State distributes the share of ghanīmah designated for orphans.

ISIS & Social Media

Monthly Accounts Establish – 27,500 – 45,000

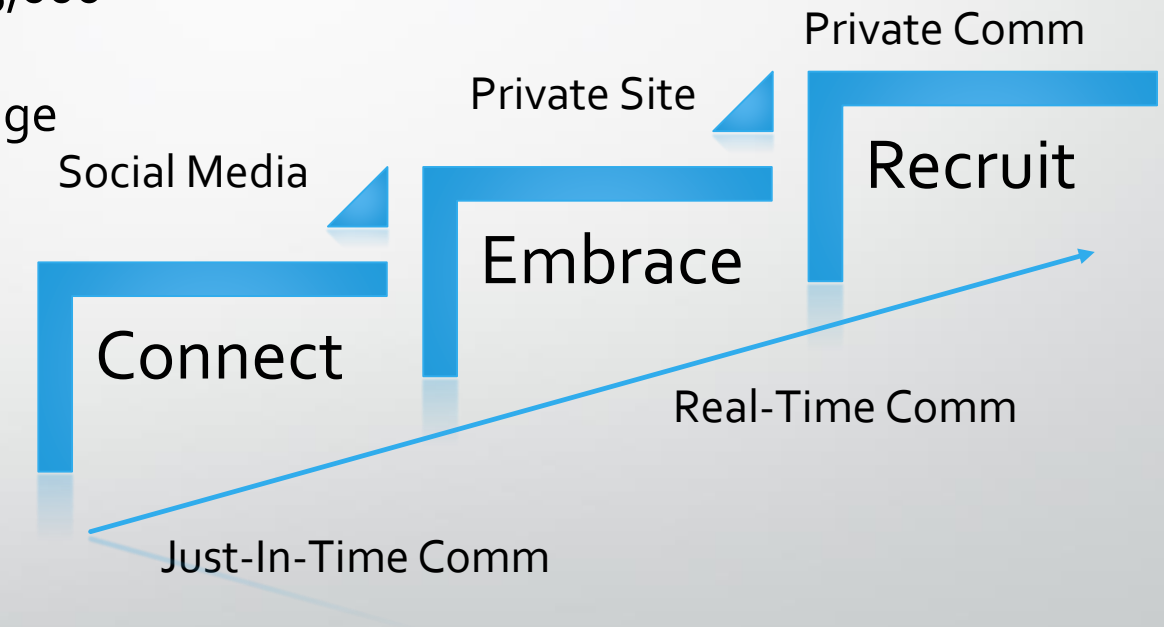
Tweets Sent Per Day – 90,000 on average

Worldwide Distribution Network

PasteBin for Battlefield Summaries

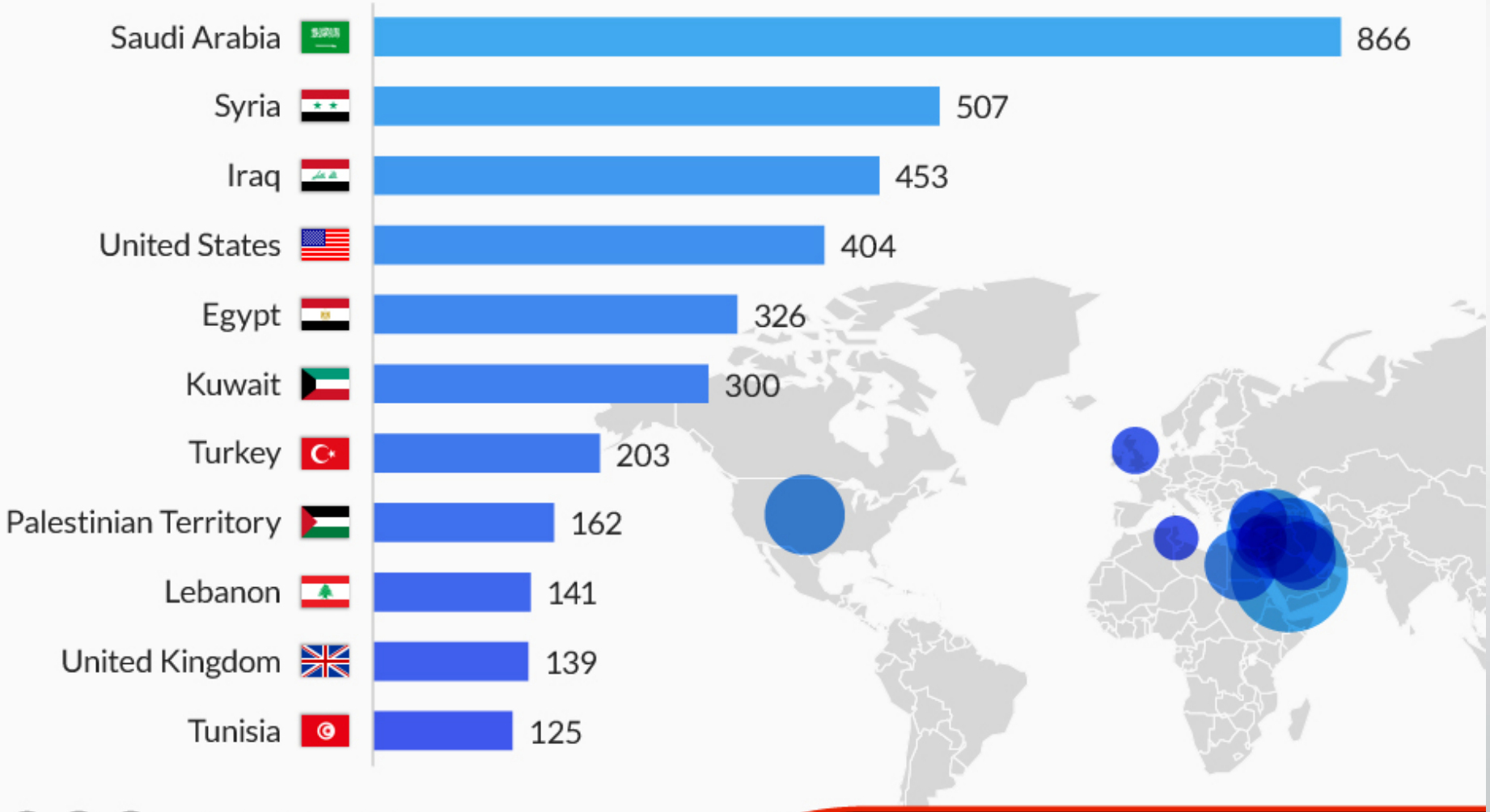
Ask.FM for Interviews and Outreach

SoundCloud for Media



Where are ISIS supporters tweeting from?

Top locations claimed by Twitter users supporting ISIS in 2015 *



* sample size 20,000

@StatistaCharts Source: Brookings Institute

i100 from The INDEPENDENT statista

facebook

Email or Phone

Password

Log In

Keep me logged in

Forgot your password?

Islamic State of Iraq and Al-Sham is on Facebook.

To connect with Islamic State of Iraq and Al-Sham, sign up for Facebook today.

Sign Up Log In

Islamic State of Iraq and Al-Sham

223 likes

Teacher

Flamujt e zinj në kohën e fundit si shenjë përgëzuese për besimtarët, ndërsa brenge për munafikët...

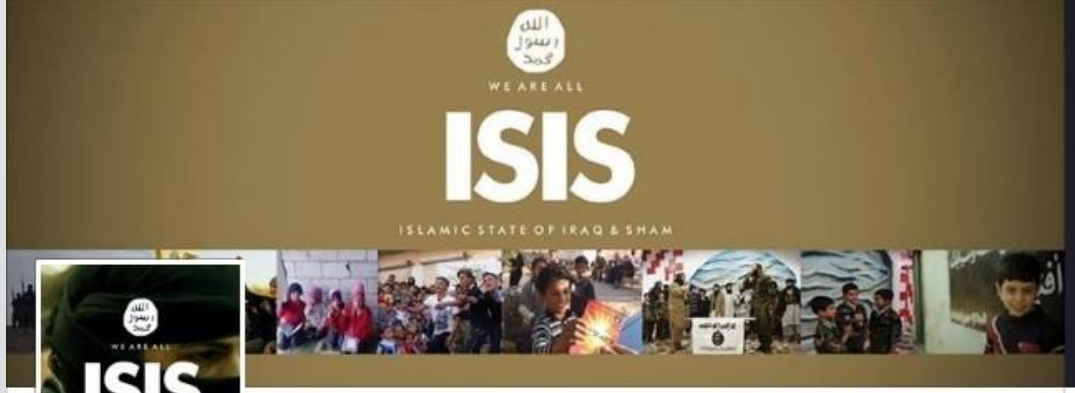
223

About

Photos

Likes

SENSATO
CYBER SECURITY SOLUTIONS



Islamic State
618 likes

Like | Follow | Message

News/Media Website
https://twitter.com/islamicstatee

618

About – Suggest an Edit

Photos Likes

Highlights

Post | Photo / Video

Write something...

Post

Invite Your Friends to Like This Page — See All

Type a friend's name... Invite

Invite
Invite
Invite

Activity
Recent

Islamic State joined Facebook.

Islamic State shared a link.
8 hours ago

News about Islamic State read there
https://twitter.com/islamicstatee

ISIS news (islamicstatee) on Twitter
twitter.com
The latest from ISIS news (@islamicstatee).

Like · Comment · Share
10 people like this

Islamic State
12 minutes ago

ISIS
ISLAMIC STATE OF IRAQ AND SHAM

الدولة الإسلامية الع
@islamicstatee

41 Photos and videos

TWEETS 87 | PHOTOS/VIDEOS 41 | FOLLOWING 15 | FOLLOWERS 32 | More | Follow

Tweets | Tweets and replies

Retweeted by الدولة الإسلامية الع
AlHayat Media Center @alhayat_en · 1h
Multi-language translations of Sh. Abu Muhammad Al-'Adnani's speech "What Comes To You Of Good Is From Allah"
justpaste.it/ma_asaoak
96 | 27

Retweeted by الدولة الإسلامية الع
ISIS NEWS @isisnews3 · 16m
The Islamic state progressing in #Diyala battles after controlling some of the Safavid army strongholds near Jalolaa
#Iraq #ISIS #ISIL
5 | 6

الدولة الإسلامية الع @islamicstatee · 3h
MESSAGE TO @BarackObama obama
الدولة الإسلامية العراق والشام - FROM ISIS
youtube.com/watch?v=rrf0mm...

YouTube

Don't miss any updates from الدولة الإسلامية الع

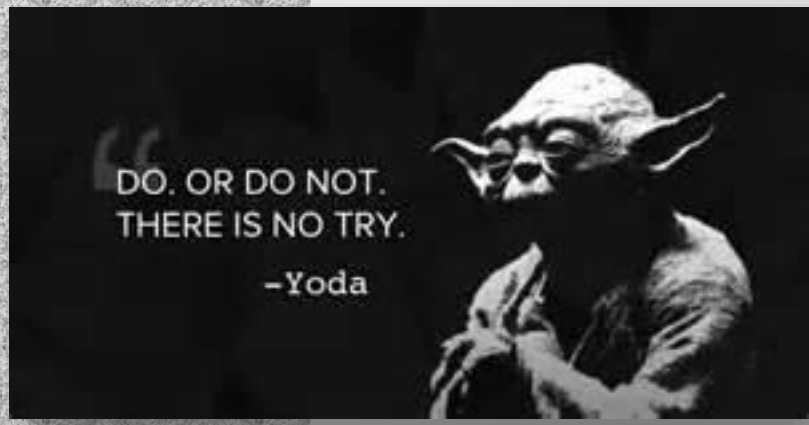
Full name
brabcco
••••••••••
Sign up for Twitter

Worldwide Trends · Change

#WorldCupOpeningCeremony
#inauguracionmundial
Pitbull and JLo
#EmpiezaElMundialYYo
Mr Worldwide
#افتتاح_كأس_العالم
#AberturaDaCopa
Terry Tibbs
Claudia Leite
That Brazilian

© 2014 Twitter About Help Ads info

What To Do



SENSATO
CYBER SECURITY SOLUTIONS

ISIS IT Staff

Cyber-Caliphate Chief Newly Appointed

2014 380 team members

2015 3500+ team members

Dedicated Cybersecurity Team

Dedicated Cyber Caliphate Team

Syrian Electronic Army

Ajax Security Team

Clear Access to Medical Devices

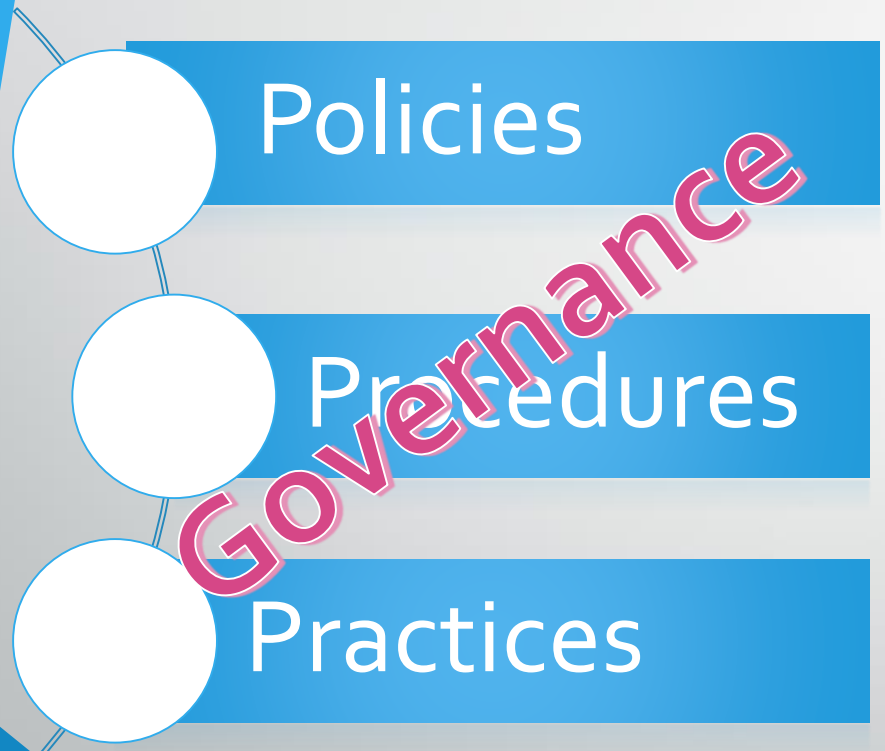
Ideology is not Restricted by International Law or Convention

SENSATO
CYBER SECURITY SOLUTIONS

Keep This In Mind

- You must have *relevant*, *timely* IT Security and Privacy policies that are ***supportive of the current threat landscape***
- You must be able to **demonstrate** that you have **procedures** in place that are based on your policies.
- You must be able to **provide evidence** that you practice your procedures.

Keep This In Mind



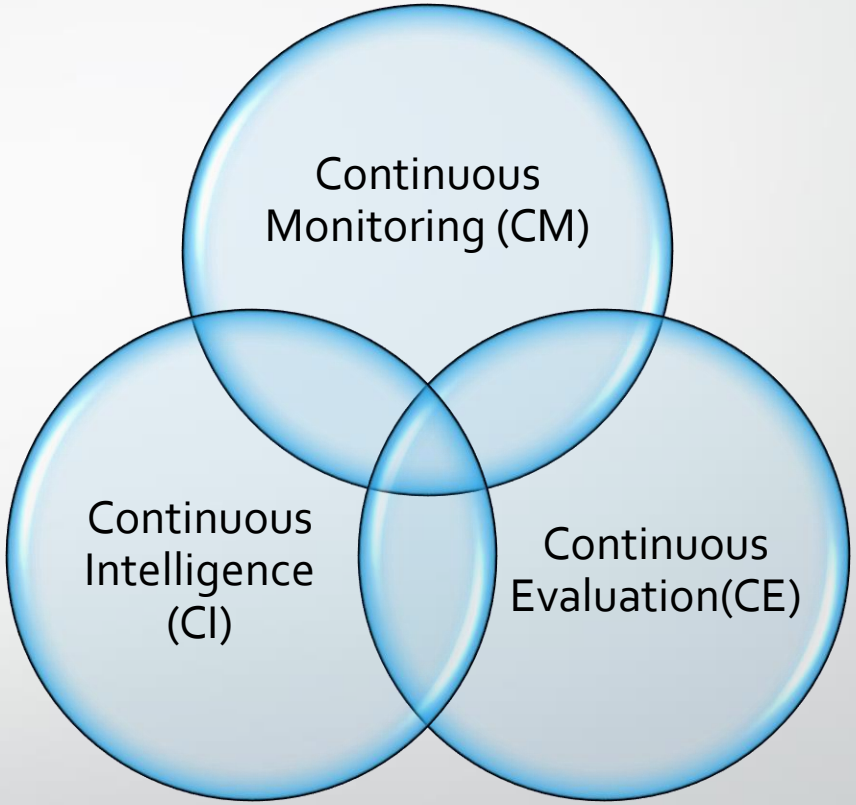
- The **lack of governance calls into question your ability** to show relevance, demonstrate process or provide evidence of practice.
- IT Security **governance vastly reduces risks,** improves readiness and in many ways reduces costs.
- **Governance need not be complicated** – the simpler the better – but it must be:
  - Specific to IT Security
  - Cross-Functional
  - Educated
  - Demonstrable

Level I Readiness

Continuous Monitoring
- Infrastructure Control
- Security Operations Center
- Incident Response
- Containment

Continuous Intelligence
- Timely & Specific
- Actionable
- Acted Upon

Continuous Evaluation
- Risk Assessments (yearly)
- Testing (six months)



SENSATO
CYBER SECURITY SOLUTIONS

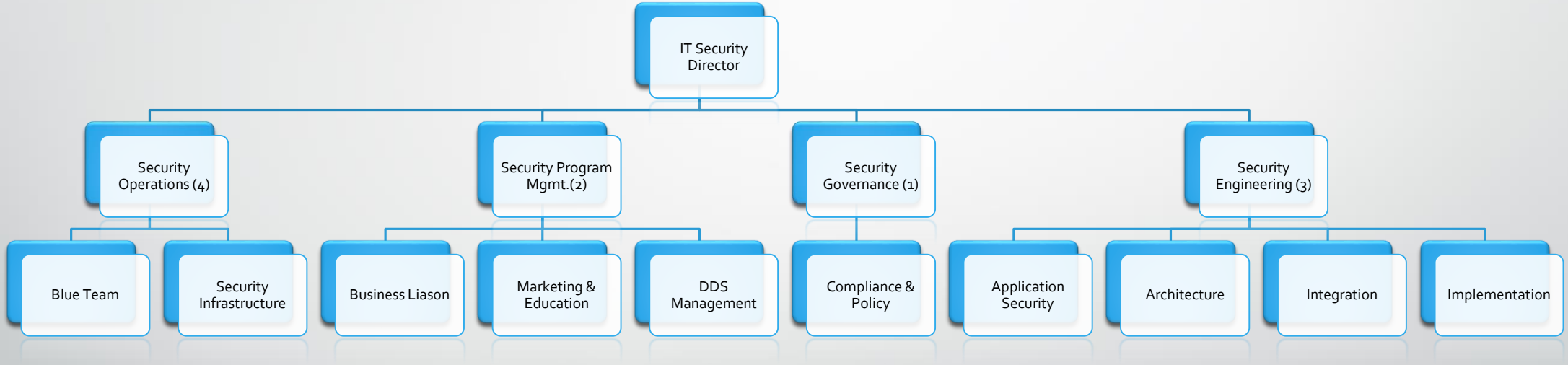
Level II Readiness

Sensato Strategic Imperatives

The top-10 strategic imperatives are designed as a universal score-card. These may not be the ten most important items for your organization, but they are the ten most items we find to be critical to addressing the NIST requirements.

Imperative
Appropriate Access & Controls
Appropriate Qualified IT Security Team
Partner Management
Education Standards
Executive Intimacy
Incident Response Readiness
Monitoring
Old Technology Utilization
Patch Management
Relevant Practices

IT Security Organization Model



Level III Readiness

Cybersecurity Strategic Plan

- 1 & 3 Year Plan
- Mission – Values – Critical Success Factors
- Relevant to Current Threats
- ROI Based
- Acknowledge/Address Weakness & Justify
- DEPLOY **NIST**!!!!

Cybersecurity Data-Driven Security Program

- Establish Measurements
- Establish Review and Evolution Process

Cybersecurity Culture

- View Cybersecurity Holistically
- Marketing & Training
- Commitment to Defense

SENSATO
CYBERSECURITY SOLUTIONS

Sensato Coordinated Risk Scoring (CRS)

Deploy Honey Pots

Attackers Hate These

They have one job – to scream.

Pretty low tech – pretty high return.

They temp and Entice

Too Good to Be True…

If you must…then…

Leave to the End of an attack

Watch for other traffic and activity.

SENSATO
CYBER SECURITY SOLUTIONS

SENSATO
CYBER SECURITY SOLUTIONS

John Gomez
John.gomez@sensato.co

Mike Chirico
Mike.Chirico@sensato.co

www.sensato.co
844.736.7286