

June, 2016



DARKTRACE ENTERPRISE IMMUNITY

FICTION VS. REALITY


Promote Your Analysts to Black World Global Operators by
Understanding SCADA Vulnerabilities and Insider Threats

Aaron Janssen, Founder
Janssen Technology


DARKTRACE - EXECUTIVE SUMMARY

IOT **ZERO DAY EXPLOIT** **BYOD**
Insiders & Criminals **Advanced Persistent Threat**
Polymorphic Malware **Regulation Compliance**
Training Costs **Performance Bottlenecks**
Budget Cuts **Risk Audits**

DATA ICU REQUIRED
- OpenSSL Heartbleed -




**PHYSICAL
HARDWARE
STATUS OK**



**VIRTUAL
SYSTEMS
COMPROMISED**

***** WARNING *****
**ENTERPRISE ECOMMERCE
CONDITION = CRITICAL**

A CISO's risk management perspective changes frequently, even overnight. You can wake up and find that a zero day exploit has broken your company's ecommerce or a trusted insider has stolen your critical IP.



After Patient Zero has been fully diagnosed, what is the enterprise's GOLD standard of care?

Cyber Triage Protocols

Has Patient Zero been isolated?
 Correct treatment in progress?

Enterprise Immunity Provides Diagnostic Resolution

Darktrace shows who, what, where, when, why and how you have been attacked. Can your organization prevent it again?

DARKTRACE – GLOBAL OPERATORS I

Fiction

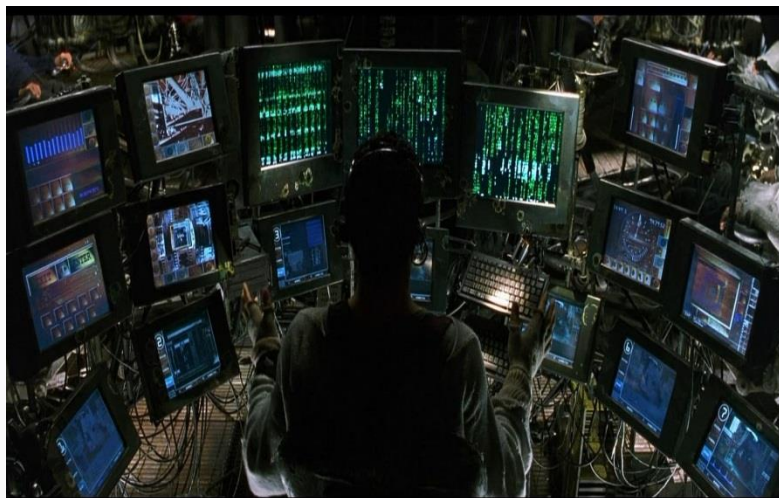
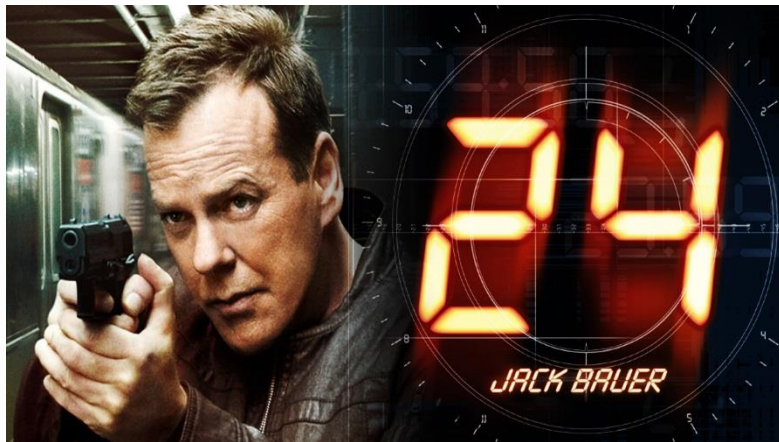
- Most security companies claim they can assist your organization in keeping hackers out of your network.
- Reactive technologies such as signature and heuristic analysis are sufficient to combat today's threats.
- **Even large companies can not economically keep a highly trained incident response team ready to tackle problems in a matter of mins.**

Reality

- Superior visualization speeds response times and facilitates easily customization of data.
- Machine learning systems are continuously reducing errors and improving their accuracy.
- Darktrace has an elite national intelligence trained, cyber incident response 'strike team' that is a major force multiplier.
- Your security analysts can become dark world operators!

DARKTRACE – GLOBAL OPERATORS II

Fiction



Reality



Jim Penrose, EVP

Former Defense Intelligence Senior Level director at NSA (17 years), world expert on insider threats, nominated for Presidential Rank award in 2013



Sir Jonathan Evans KCB

Former Director General of MI5, 33 years experience at UK Security Service, non-executive director of HSBC



Andrew France OBE

Former Deputy Director of Cyber Defence Operations at GCHQ; 30-year government intelligence career

DARKTRACE – NORTH KOREA (THREAT) I

Fiction

- Despite being ruled by a cold war era dictatorial system, Kim Jong-un is a reformer.
- US and EU lead international sanctions are working. \$150 million requested by UN Food Fund. Northern citizens are now up to 3” shorter than their South Korean counterparts.
- **Due to geographic distance, and cultural lockdown North Korea can not threaten 1st world industrialized countries.**

Reality

- North Korea is a country of 25 million people. Frequent starvation even occasional cannibalism have been reported.* 2.5 M died in 1990s
- Most citizens live with severe chronic malnutrition, without electricity or indoor plumbing.
- \$1.3 Billion spent in 2012 on nuclear weapons and ICBMs.
- They hacked SONY Pictures. Estimates of 80 GB to 140 TB.

**[Washington Post Feb,2 2013](#)*

DARKTRACE – NORTH KOREA (CYBER) II

Fiction



Reality



6 (Fiction becomes reality with Sony's 'The Interview')

(Sony Website after being hacked)

DARKTRACE – IRAN, SCADA & STUXNET I

Fiction

- Supervisory Control and Data Acquisition ([SCADA](#)) Systems are secure. **Many still run XP.**
- SCADA is isolated national critical infrastructure such as air traffic control, nuclear power and distribution grids. ([Darktrace has just released a SCADA security product](#))
- The 500 KB Stuxnet worm was ultra-complex, incapable of being weaponized by rogue nations. ([Natanz breakout, oops](#))

Reality

- [CIA World Fact Book](#) notes Iran is a country of over 80 million now with access to new capital.
- Iran is the center of the former Persian Empire with one of the most highly educated populations in the Middle East. 750K STEM Grads @ year.
- In 2010 Iran's nuclear program was the victim of Stuxnet and they are suspected of reverse engineering it for revenge against western assets. US/IL

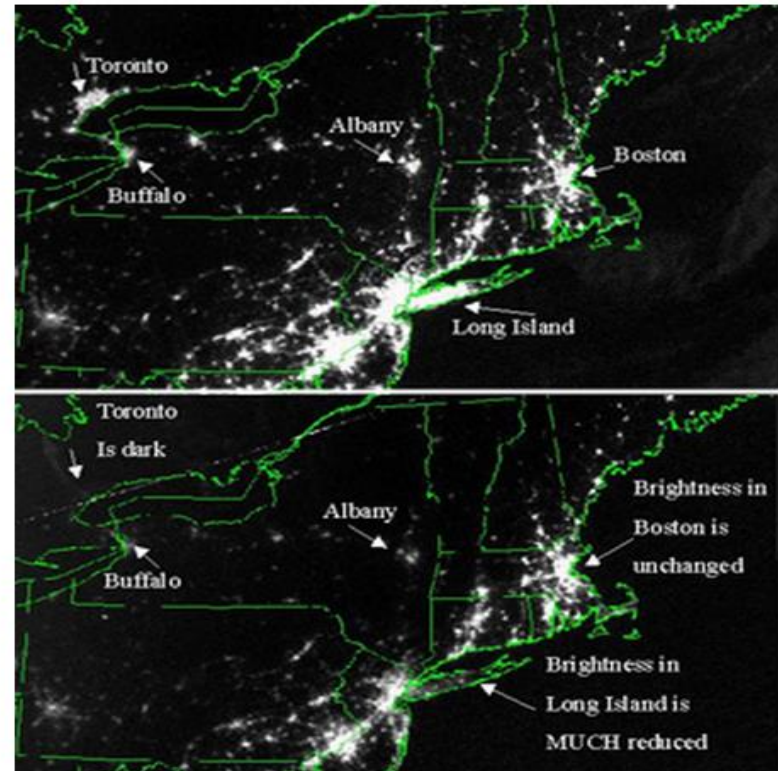
DARKTRACE -IRAN, SCADA AND STUXNET II

Fiction



Figure 3: Former president Ahmadinejad looking at SCADA screens in the control room at Natanz in 2008. The screen facing the photographer shows that two centrifuges are isolated, indicating a defect, but that doesn't prevent the respective cascade from continuing operation (highlighting in red not in the original)

Reality



The top image was taken approximately 20 hours before the blackout, and the bottom image was taken approximately 7 hours into the blackout, where you can see, among other changes, that Toronto (upper, left) has gone completely dark. Image Credit: NASA

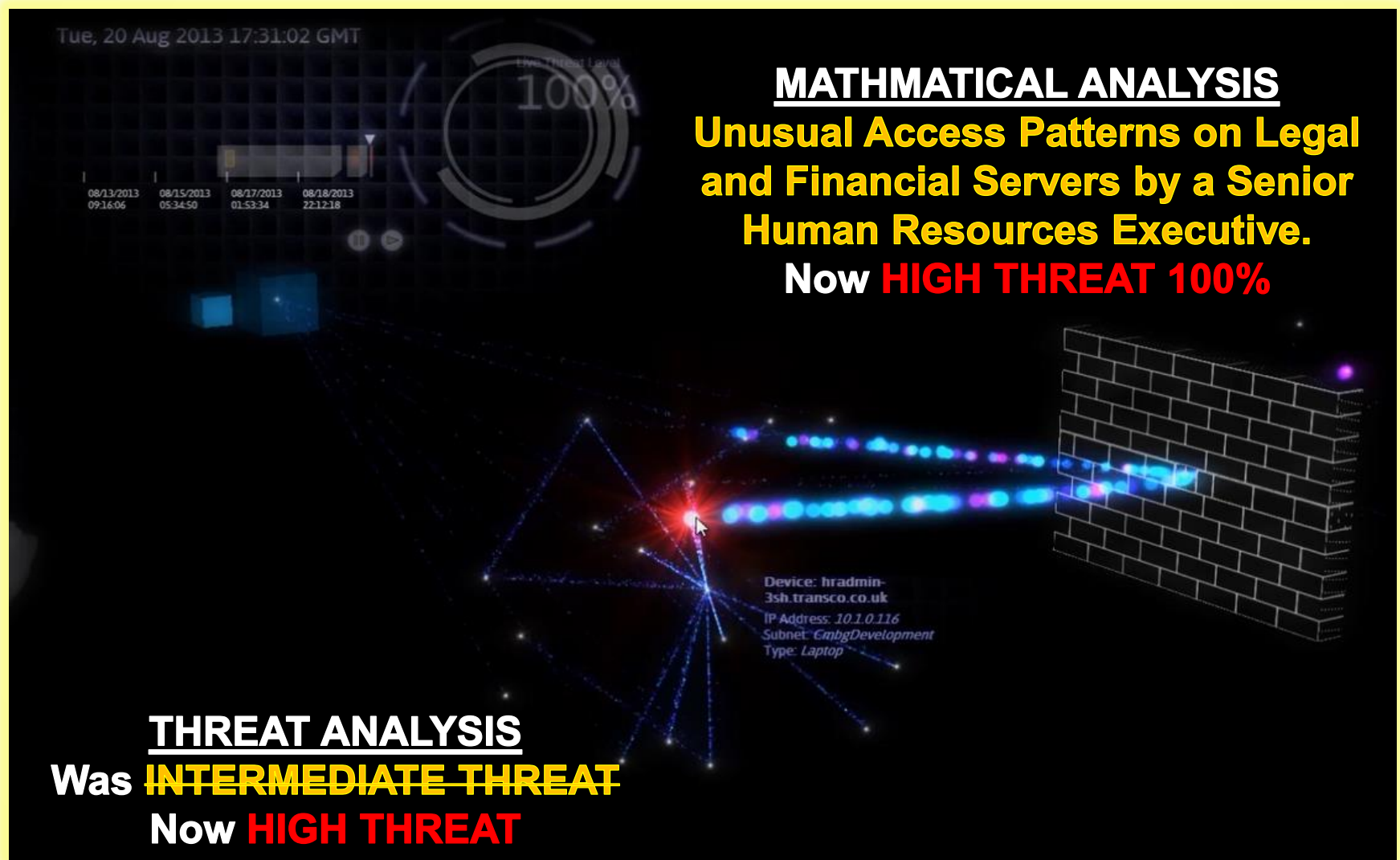
(The Iranians are actually very familiar with SCADA) (US Self-inflicted accident '03)

DARKTRACE – INITIAL PHISHING EXPLOIT

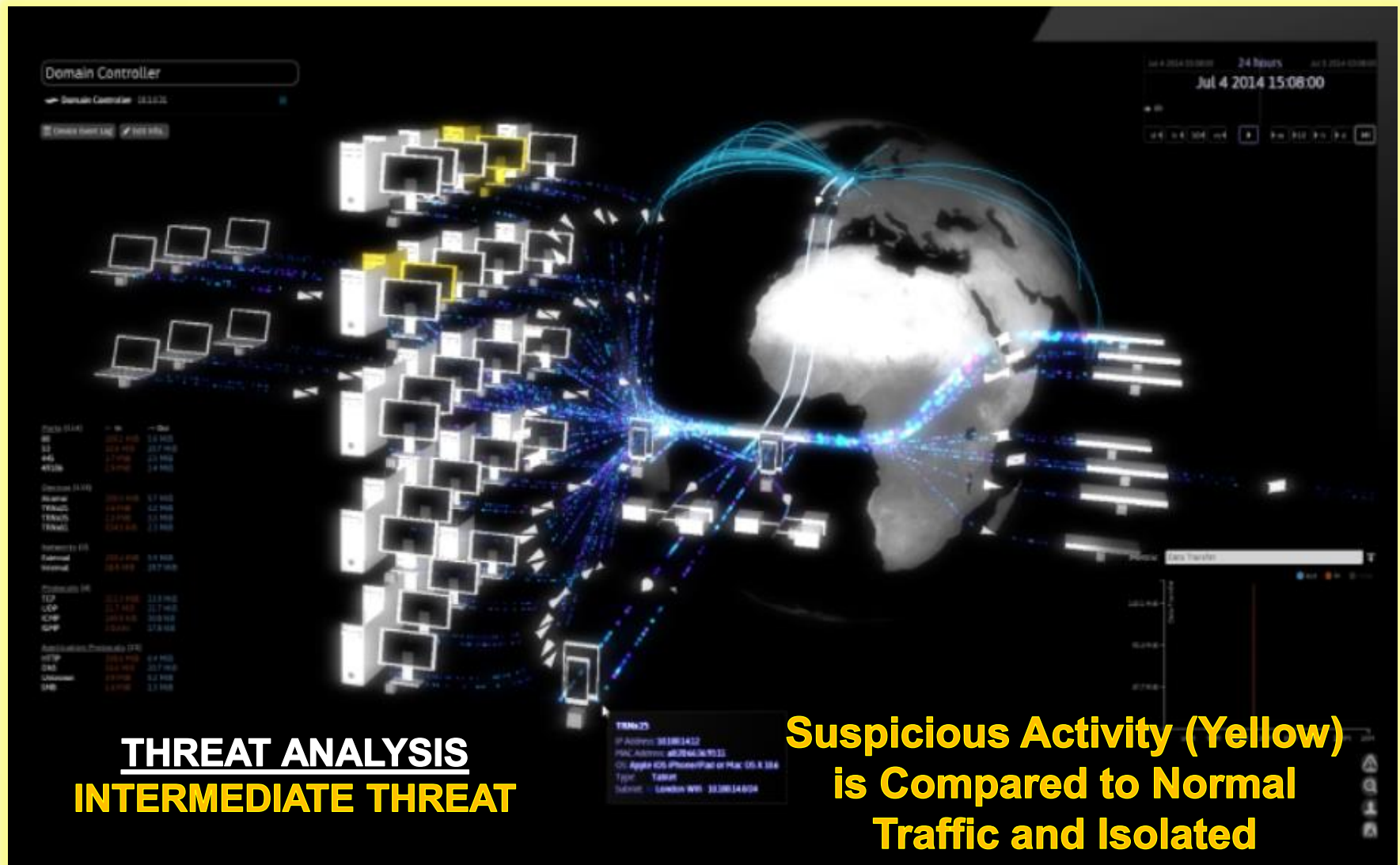
The screenshot displays the Darktrace network visualization interface. At the top left, a search bar contains the IP address '10.1.0.0/24'. Below it, a navigation menu includes 'Home', 'Event Log', 'Edit Info...', and 'Tags'. On the right side, a date and time display shows 'Fri Mar 20' with navigation buttons for 'd', 'h', '10', and 'm'. The main area features a 3D network visualization with nodes and connections in blue and purple. A specific node is highlighted in yellow, and a tooltip provides details: 'buildm2.transco.co.uk', 'Hostname: buildm2.transco.co.uk', 'IP Address: 10.1.0.33 (Wed Mar 18, 17:00:00)', 'Type: Server', and 'Subnet: 10.1.0.0/24'. A globe is visible on the left, and a brick wall structure is on the right.

ENTERPRISE IMMUNE SYSTEM
**Real-Time, Machine Learning,
Security Anomaly Detection**

DARKTRACE – INSTALLATION OF MALWARE



DARKTRACE – LATERAL PROPAGATION



DARKTRACE – COMMAND AND CONTROL



The image displays the Darktrace Command and Control interface. At the top, a search bar shows 'Linux 434' and the system IP 'Linux 434 - 10.100.15.16 - 50465d08693e'. The date and time are 'Mon Feb 2 2015 / 10:23:02'. The main visual is a globe with blue lines representing network connections. A 'Breach Log' window is open, showing a table of unusual activity:

Date	Device / Unusual Activity	Strength
Tue Feb 3 11:09:01	mna-dc1-3 - tranaco.com	Unusual Activity Strength: 72% > 35%
Mon Feb 2 10:23:01	Linux 434	Unusual Activity Strength: 95% > 35%
Mon Feb 2 10:18:01	10.100.17.11	Unusual Activity Strength: 67% > 35%

Below the breach log, the text reads: **THREAT ANALYSIS** and **HIGH THREAT**. On the right, a 'Metric: Connections' graph shows a sharp spike in connections at approximately 10:00, with a red arrow pointing to it. A portrait of Edward Snowden is also visible in the bottom right corner.

These Hacker's Command and Control Servers are Located in Russia, Ukraine, China & North Korea (DPRK)

300+ Machine Learning Metrics Aid in Quickly Deploying Scarce Cyber Teams. Seemingly Innocent Spikes in Traffic are Actually Massive Intellectual Property Thefts Executed by Trusted Employees. Edward Snowden, was a NSA SharePoint Administrator...Who is Yours?

DARKTRACE – DATA EXFILTRATION



DARKTRACE - ATTRIBUTION/RESPONSE

10.100.17.11

Mon Feb 2 2015 / 10:17:32

INSIDER THREAT CONFIRMED
User ID = sue.smith (VP of HR)

***** LEVEL 10 - RISK PROTOCOL ACTIVATED *****
HOST SYSTEM / NETWORK LOCK DOWN INCIDENT -
EMPLOYEE TERMINATION EVENT

SELECT #1 FOR IMMEDIATE (ALPHA TERMINATION) DISCONNECT
SELECT #2 TO MONITOR & COLLECT SECRET SERVICE FORENSIC DATA

Custom Math Models Tune Diagnostics
Packet Filtering, PCAP Replay, REST API

Math / Unusual Connectivity
Math / Device Unusual Activity
Math / Network Profile / Rare connection from source
Math / User Unusual Credential use

DARKTRACE

DARKTRACE – INSIDER THREAT DEBRIEF

The screenshot displays the Darktrace user interface for the host `buildm2.transco.co.uk`. The main window shows a "Model Breach Event Log" for Wednesday, February 4, 2015, at 10:51:37. The log entry is categorized as "Connectivity" and "Math/Unusual", with a description: "5 connections at 12 minute to 23 hour intervals. An unusual time for a connection externally on port 80". The log lists several connection events to `476249.host.cloudfront.com` with various IP addresses.

Overlaid on the interface is a globe with a satellite in orbit, connected to a server rack. A large green text overlay reads: **-- STATUS GREEN -- All Breaches Eliminated INFOSEC Incident Response Team Ready**

At the bottom left, another green text overlay states: **Authorities Notified, PCAPs for Legal Evidence and Reports for Audits are Created Automatically**

At the bottom right, there are two charts: a "Trend Analysis" 3D bar chart showing connection spikes, and a "Connections" bar chart showing a sharp spike in connections at approximately 13:00. The bar chart legend includes "out", "in", and "total".

Thank You!

Aaron Michael Janssen
aaron.janssen@aaronjanssen.com

(760) 707-7730 Mobile



Please visit **AaronJanssen.com** for more details.