



infracritical

2016 ICS Cyber Security Conference, Atlanta, GA, October 24-27, 2016  
Implementing a Publicly-Accessible ICS Event and Incident Database  
Thursday, October 27, 2016

Bob Radvanovsky, CIFI, CISM, CIPS  
rsradvan@infracritical.com

# ***SCIDMARK***

***SCada Incident Database MARKup***

## Reasons for SCIDMARK

- **Several reasons exist for creating database:**
  - **No such database exists that is:**
    - Publicly available
    - FREE of charge (requiring ZERO payment)
    - Provides substantiative and attestable information
    - Completely “open source” (no proprietary info)
    - Provides useful and accessible URLs
    - May be utilized by several public interest groups

## RISI Database

- **There are a few databases, but are limited:**
  - **Repository of Industrial Security Incidents (RISI)**
    - Formerly the “Industrial Security Incidents Database”
    - ISID incepted 2001 by Byes, Lowe and Leversage
    - ISID began at BCIT; discontinued sometime in 2006
    - Resurrected in 2008 by Byres and Fabro
    - Byres Research acquired by ‘exida’ in 2009
    - Security Incidents Organization incepted 2014

# RISI Database (continued)

The RISI database is publicly and freely available.

Web site is: **risidata.com**

The screenshot shows a web browser window displaying the RISI Online Incident Database. The page has a green header with the RISI logo and navigation links for 'The Database', 'About', and 'Contact'. Below the header, the title 'RISI Online Incident Database' is prominently displayed. A search section titled 'Search for an Incident' includes a text input field with the placeholder 'Search the RISI Database' and a green 'SEARCH!' button. Below the search section, it states 'Last Updated: Wed, January 28, 2015'. A table of incident records is shown with columns for Title, Year, Industry Type, Country, and Brief. The table lists five incidents, including the Baku-Tbilisi-Ceyhan Pipeline explosion in 2008 and the German Steel Mill Cyber Attack in 2014.

▲ Title	▲ Year	▲ Industry Type	▲ Country	Brief
Baku-Tbilisi-Ceyhan Pipeline explosion	2008	Petroleum	Turkey	🔍
Iranian Oil Terminal offline after malware attack	2012	Petroleum	Iran	🔍
German Steel Mill Cyber Attack	2014	Metals	Germany	🔍
Russian-Based Dragonfly Group Attacks Energy Industry	2014	Power and Utilities	United States	🔍
U-2 spy plane caused widespread shutdown of U.S. flights: report	2014	Transportation	United States	🔍

# RISI Database (continued)

This is a more detailed description of a specific incident in Olympic, WA (USA) pipeline rupture (gasoline).

3 people dead.  
\$45M tot. damages.

The screenshot shows the RISI database interface. The main header is green with 'RISI' on the left and 'The Database', 'About', and 'Contact' on the right. Below the header is a table of incidents. The incident 'Olympic Pipeline Rupture and Subsequent Fire' is highlighted, and a detailed view is shown in a modal window. A red arrow points from the text on the left to this modal window.

Incident Title	Year	Industry	Country
Oil Company SCADA System Impacted by RF Interference	1989	Petroleum	United States
Blockage of 12 Out Of 13 PLC Systems	2004	Other	Switzerland
Weekly Connection Loss to PLCs	2004	Other	Switzerland
<b>Olympic Pipeline Rupture and Subsequent Fire</b>	1999	Petroleum	United States
Ethernet Network Storm Zaps Multiple PLCs's	2003	Pharmaceutical	United States
UK Air Traffic Control Computers Fail	2002	Transportation	United Kingdom
Errant AntiVirus Definition Brings Down Railway LANs	2005	Transportation	Japan
SCADA Workstation Infected by W32/Korgo Worm	2004	Power and Utilities	United States
Slammer Impacts Offshore Platforms	2003	Petroleum	United States

### Olympic Pipeline Rupture and Subsequent Fire

**Event Year:** 1999      **Reliability:** Confirmed

**Country:** United States

**Industry Type:** Petroleum

**Description:** At about 3:28 pm PDT, a 16 inch diameter steel pipeline ruptured and released about 237,000 gallons of gasoline into a creek that flowed through Whatcom Falls Park in Bellingham, WA. About 1 1/2 hours after the rupture, the gasoline ignited and burned approximately 1 1/2 miles along the creek. (#1)

A number of events led to the rupture of the pipeline. First, was excavation damage done to the pipeline, possibly between 1993 and 1994. Second, was the construction and startup of a new products terminal, where pressure relief valves that were installed, were improperly configured or adjusted. Finally, on the day of the accident, the SCADA system that controllers used to operate the pipeline became unresponsive, (possibly due to the practice of performing database development work on the system while it was being used to operate the pipeline), making it difficult for controllers to analyze pipeline conditions and make timely responses to operational problems. (#1)

# RISI Database (continued)

Only 5 significant fields identified.

Much of the detailed info is within the description field.

Could this be used for any level of attestation?

Is this substantive?

The screenshot shows the RISI database interface. The main content area displays a search result for "Olympic Pipeline Rupture and Subsequent Fire". The fields are highlighted with red boxes:

- Event Year: 1999
- Reliability: Confirmed
- Country: United States
- Industry Type: Petroleum

The description field contains the following text:

At about 3:28 pm PDT, a 16 inch diameter steel pipeline ruptured and released about 237,000 gallons of gasoline into a creek that flowed through Whatcom Falls Park in Bellingham, WA. About 1 1/2 hours after the rupture, the gasoline ignited and burned approximately 1 1/2 miles along the creek. (#1)

A number of events led to the rupture of the pipeline. First, was excavation damage done to the pipeline, possibly between 1993 and 1994. Second, was the construction and startup of a new products terminal, where pressure relief valves that were installed, were improperly configured or adjusted. Finally, on the day of the accident, the SCADA system that controllers used to operate the pipeline became unresponsive, (possibly due to the practice of performing database development work on the system while it was being used to operate the pipeline), making it difficult for controllers to analyze pipeline conditions and make timely responses to operational problems. (#1)

A red arrow points from the text "within the description field" to the description field in the screenshot.

Clearly, there are more fields identified.

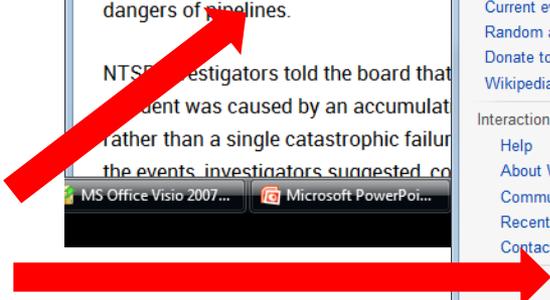
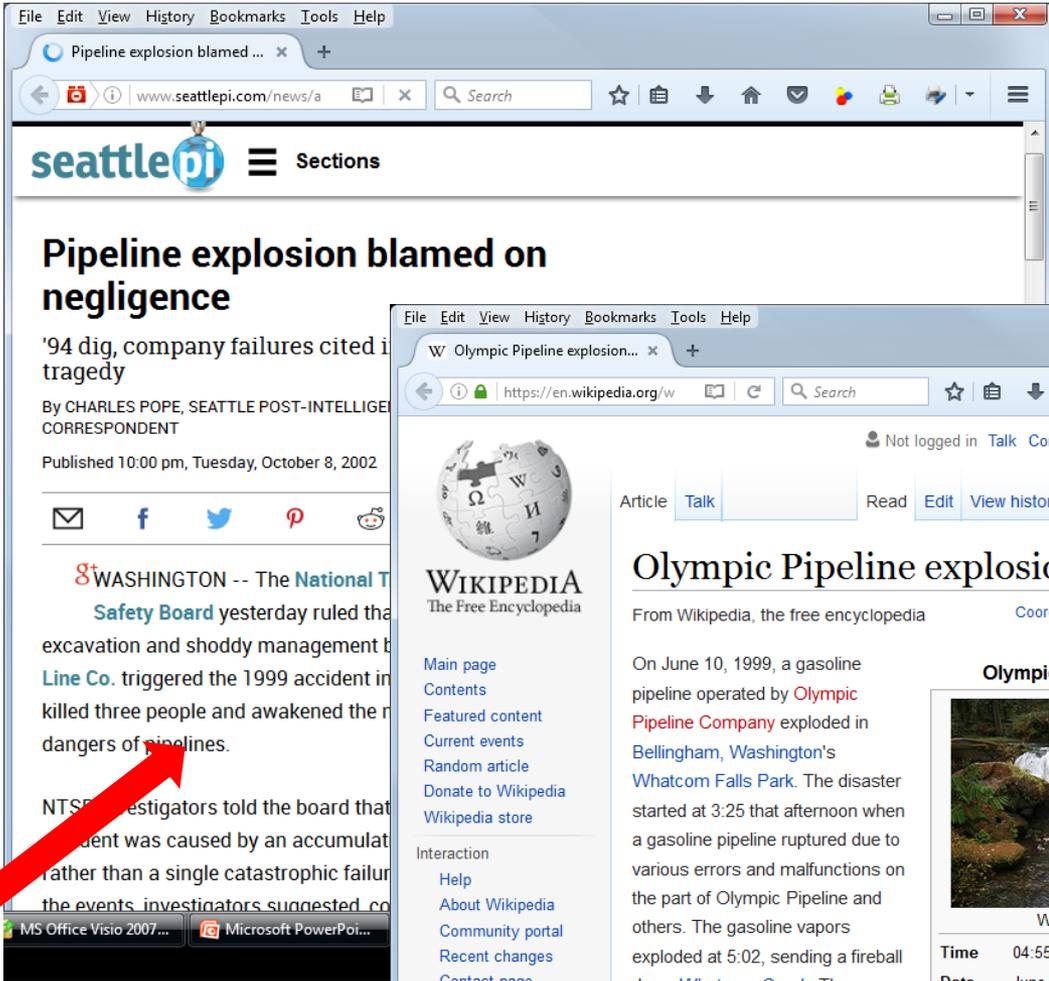
More detailed info, plus source info documents for further referencing.

Could this be used for any level of attestation? **Yes.**

Substantiative? **Yes.**

The screenshot shows the NTSB website with the following content:

- Page Title:** Pipeline Rupture and Release of Gasoline, Olympic Pipeline Company
- Executive Summary:** About 3:28 p.m., Pacific daylight time, on June 10, 1999, a 16-inch-diameter steel pipeline owned by Olympic Pipe Line Company ruptured and released about 237,000 gallons of gasoline into a creek that flowed through Whatcom Falls Park in Bellingham, Washington. About 1 1/2 hours after the rupture, the gasoline ignited and burned approximately 1 1/2 miles along the creek. Two 10-year-old boys and an 18-year-old young man died as a result of the accident. Eight additional injuries were documented. A single-family residence and the city of Bellingham's water treatment plant were severely damaged. As of January 2002, Olympic estimated that total property damages were at least \$45 million.
- Probable Cause:** The Safety Board determines that the probable cause of the June 10, 1999, rupture of the Olympic pipeline in Bellingham, Washington, was:
  - Damage to the pipe by IMCO General Construction, Inc., during the 1994 Dakin-Yew water treatment plant project and Olympic Pipe Line Company's inadequate inspection of IMCO's work during the project.
  - Olympic Pipe Line Company's inaccurate evaluation of in-line pipeline inspection results, which led to the company's decision not to excavate and examine the damaged section of pipe.
  - Olympic Pipe Line Company's failure to test, under approximate operating conditions, all safety devices associated with the Bayview products facility before activating the facility.
  - Olympic Pipe Line Company's failure to investigate and correct the conditions leading to the repeated unintended closing of the Bayview inlet block valve.
  - Olympic Pipe Line Company's practice of performing database development work on the supervisory control and data acquisition system while the system was being used to operate the pipeline, which led to the system's becoming non-responsive at a critical time during pipeline operations.
- Related Information:**
  - Accident Location: Bellingham, WA
  - Accident Date: 6/10/1999
  - Accident ID: DCA99MP008
  - Date Adopted: 10/8/2002
  - NTSB Number: PAR-02-02
  - NTIS Number: PB2002-916502
  - Related Report: PAR-02-02
  - Related Recommendations: P-02-004, P-02-005
  - Related Press Releases:
    - October 03, 2002: NTSB to Hold Public Meeting on 1999 Gasoline Pipeline Rupture
    - October 08, 2002: Determines Probable Cause Of Pipeline Rupture in Bellingham, Washington
  - Related Events
  - Related Investigations
  - More NTSB Links:
    - Investigation Process
    - Data & Stats
    - Accident Reports
    - Most Wanted List



Do these sources qualify as something reliable?

Could this be used for any level of attestation? **No.**

Substantiative? **Maybe.**

But...if combined with an authoritative source? **Then...possibly yes to both.**

[2] http://www.seattlepi.com/news/article/Pipeline-explosion-blamed-on-negligence-1097954.php

[3] https://en.wikipedia.org/wiki/Olympic\_Pipeline\_explosion

## What does this all mean?

- **What is shown is a form of intelligence...**
  - **Aggregated data, from multiple sources, that is publicly, openly, and freely available is called *“open source intelligence”***
    - **No proprietary or confidential information**
    - **No legally-privileged/restricted information**
    - **No information to compromise national security**
    - **No classified (or unverified leaked\* classified) information**

\* ref: Wikileaks, Public Intelligence, Pastebin, GitHub, Cryptome, et. al

## OK...so why SCIDMARK?

- **There are several benefits for this project:**
  - Aggregated data from multiple sources...into ONE source
  - No need to search for all of the sources; most of the research is taken from as many sources as possible
  - Alternative sources for citing in case primary, secondary, tertiary, ... et. al sources become unavailable
  - No need to hunt for relevant, specific information; all relevant information is broken down by 'families'

## Uh...are there any issues?

- **There are several liabilities for this project:**
  - **ONE source can become a highly visible target**
  - **As much as having this database would benefit the ‘good guys’, the ‘bad guys’ would benefit (probably) as much**
  - **Research information at several locations by itself may prove harmless for adversaries; however, combined, this may provide a one-stop ‘grocery store’**
  - **Centralized, aggregated information in one place may be considered a threat to national security**

## Are there any more concerns?

- **Perhaps...a few more:**
  - **IF such a database is considered a threat to national security, it may become a target not only by the ‘bad guys’, but now may become a target by the ‘good guys’**
  - **IF such a database were to be contained, it could become sequestered by classifying the database itself; though this may not happen within the U.S., it may happen elsewhere...**

## Are there any negatives to this project?

- **Yes...there are a few:**
  - Creation of such a database is entirely voluntary
  - Creation of entries within the database is manual, and would be very time consuming
  - Creation of relative or pertinent data may cascade into an almost endless and vicious cycle of creating more data from existing data (data of data of data...or 'metadata'); the question is 'How much is enough?'
  - **ONE VERY BIG NEGATIVE – the word 'cyber incident'**

# OK...so what is a 'cyber incident'?

- ***...more to the point, how many definitions?***
  - NIST Cyber Security Framework (CSF) **does not** define 'incident' or 'cyber incident':
  - DHS Nation Cybersecurity Incident Response Plan (NCIRP) defines 'cyber incident':
    - A cyber incident is defined as an event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.
  - NIST SP 800-53, Rev. 4, App. B, p. B-9 (based on FIPS 200) defines an 'incident' as:
    - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
  - NIST IR 7298, Rev. 2, p. 57 defines 'cyber incident' as:
    - Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See Incident.

# Is there more?

- *...oh, yes...several more...*
  - **CNSSI No. 4009 defines both ‘cyber incident’ and ‘incident’**
    - [‘cyber incident’, p. 22] Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See incident.
    - [‘incident’, p. 35] An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
  - **FIPS 200 defines ‘incident response’, but does not define the word ‘incident’**
  - **NIST IR 7435 mentions ‘incident’, but does not define it**
  - **NIST IR 7621 mentions ‘incident’ and ‘malicious code incident’, but does not define either term**

# BUT WAIT...there's still more!

- ***...oh, yes...now onto the confusing part...***
  - Within NIST IR 7298, Rev. 2, Glossary of Key Information Security Terms, the definition of the word 'incident' can be:
    - ['incident', p. 90; source: NIST SP 800-61] A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
    - ['incident', p. 91; source FIPS 200 and NIST SP 800-53] An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
    - ['incident', p. 91; source CNSSI-4009] An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
  - Just within this document alone, there are THREE definitions for 'incident'
  - ***If you are part of a regulated industry, which one do you use???***

## So what can be done?

- **Right now, the U.S. federal government is focusing their efforts based on the NIST Cyber Security Framework (or “CSF”) document**
- **For PCS environments, the *de facto* document of choice by regulators is NIST SP 800-53\***

\* NOTE: NERC and NEI both reference and include NIST SP 800-53 as part of their cyber security controls

## So...what's the 'big deal'?

- **Definitions are either multiple, or confusing**
  - Definitions focus on *'information'*...instead of *'operation'*
  - Definitions focus on the 'IT Triad':
    - Confidentiality, Integrity, Availability
  - Definitions **DO NOT** focus on the PCS Triad:
    - Safety, Availability, Integrity, Confidentiality

## How would you define ‘cyber incident’?

- ***A ‘cyber incident’ is...***

**“An triggered event or occurrence that either affects, disrupts, or destroys system processes responsible for, or the overall operation itself that, if executed, would impact the physical outcome of one or more functions associated to an infrastructure.”**

Desktop Version

So far, it is still a proof of concept



### Occurrence Information

LOSS OF TELEMETRY W/PUMP [UNIT 41A]

SCID# 2014091401  
ENTITY: FIRST ENERGY CORPORATION  
SEVERITY: CRITICAL COUNTRY: US  
SECTOR: HEALTHCARE/PUBLIC HEALTH  
SUBSECTR: ENERGY/DISTRIBUTION  
Press [LINK](#) for more detailed information.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.

### Detection Information

DL: E DT: M DFT: A  
MTD: LE LEM: IDS DER: E  
DDAT: 08/25/2016 DTIM: 1425C \*\* DETECTION  
RDAT: 08/29/2016 RTIM: 1425C \*\* RESPONSE  
RESP: 36 DAYS \*\* RESP IN

DETECTION INFO HERE -- Lorem ipsum dolor sit amet, consectetur adipiscing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.

### Damage Information

OC: Y DAM: Y RCV: Y  
DAMAGE INFO HERE -- Lorem ipsum dolor sit amet, consectetur adipiscing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.  
DAMAGE \$: \$1M  
RECVR \$: \$10M  
RECVR TIME: 6 MONTHS

ADDITIONAL INFO HERE -- Lorem ipsum dolor sit amet, consectetur adipiscing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.

### Web Information

TOP 5 URL LINKS  
L-01: CNN: Finding issues with industrial controls directly connected to the Internet  
L-02: NBC: Is there really a problem with directly connecting devices to the Internet?  
L-03: CNN: Problem with the Internet  
L-04: CNN: Problem with the Internet  
L-05: CNN: Problem with the Internet

### Penetration Information

PT: E PE: CE POE: L POET: H  
PENETRATION INFO HERE -- Lorem ipsum dolor sit amet, consectetur adipiscing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.

### Regulatory Information

RV: Y RFK: N  
REGULATORY INFO HERE -- Lorem ipsum dolor sit amet, consectetur adipiscing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.  
REGULATR: NERC COUNTRY: US  
STATUTE: NERC CIP R6.3, S1.3.4  
STATUTE: NERC CIP R6.3, S1.3.4  
STATUTE: NERC CIP R6.3, S1.3.4  
FINE \$: \$10M  
FINE DATE: 02/01/2018

### Impact Information

OIS: P OIT: LOT ODS: TEMP CAUSE:  
ENV: D ECO: P HUM: NON INCORRECT TELEMETRY  
DESCRIPTION HERE -- Lorem ipsum dolor sit amet, consectetur adipiscing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.  
ODAT: 08/25/2016 OTIM: 1425C \*\* OCCURRENCE  
RDAT: 08/29/2016 RTIM: 1425C \*\* RECOVERY  
EDAT: 08/29/2016 ETIM: 1230C \*\* ENTRY TO DB

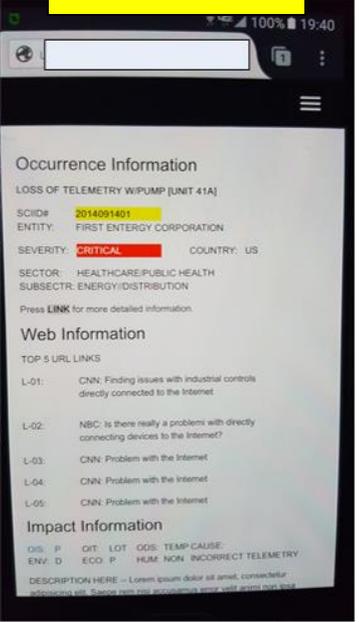
### Attack Information

ATK: Y AT: C AM: SABO AV:  
ATTACK INFO HERE -- Lorem ipsum dolor sit amet, consectetur adipiscing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.

### Legal Information

CV: Y FIN: Y  
LEGAL INFO HERE -- Lorem ipsum dolor sit amet, consectetur adipiscing elit. Saepe rem nisi accusamus error velit animi non ipsa placeat. Recusandae, suscipit, soluta quibusdam accusamus a veniam quaerat eveniet eligendi dolor consectetur.  
LAW ENFR: FBI COL  
STATUTE: 18 USC 1060 (B)(9)(a)  
FINE \$: \$100,000  
FINE DATE: 02/01/2018  
ARST DATE: 02/01/2018  
HEAR DATE: 02/01/2018  
SENT DATE: 02/01/2018  
IMPR DATE: 02/01/2018

Mobile Version



Copyright © Infractical. All rights reserved.

SCIDMARK uses Twitter's Bootstrap v3; works seamlessly on any device

infracritical

PROHIBITED  
BY  
STONEWALLING  
POLITICAL AGENDAS  
SHALLOW PROMISES  
FALLED RESULTS  
BUCKLE UP!

FAILING  
INFRASTRUCTURES  
AHEAD

35  
YEARS

# Questions?

Bob Radvanovsky, (630) 673-7740  
rsradvan@infracritical.com