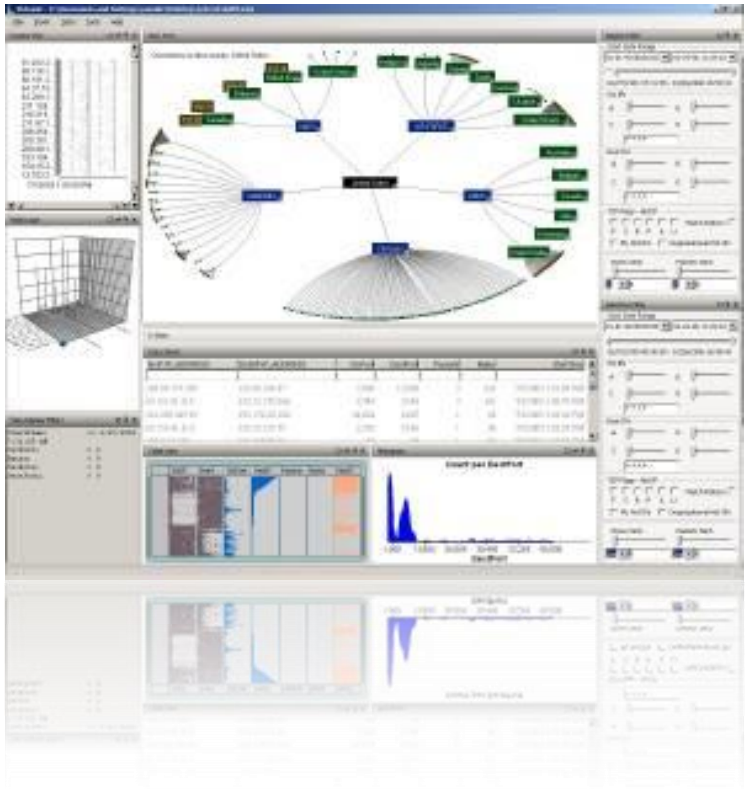
SECURE DECISIONS

A DIVISION OF APPLIED VISIONS, INC.

Enhancing Cyber Operational Decisions

Making Sense of Network Data



Anita D'Amico, Ph.D.
Anita.Damico@SecureDecisions.com
631.759.3909

securedecisions.com
codedx.com
avi.com

About Secure Decisions

Secure Decisions helps you makes sense of data

- Analyze security decision processes
- Build visual analytics to enhance security decision processes and training
- Transition our R&D into operational use

Our expertise starts where automated security sensors and scanners stop

Division of Applied Visions, Inc., which does commercial software development

- 40 people in Northport and Clifton Park, NY
- Secure facilities and security clearances

SecDec Core Competencies

Situational Awareness and Decision Support for cyber operations

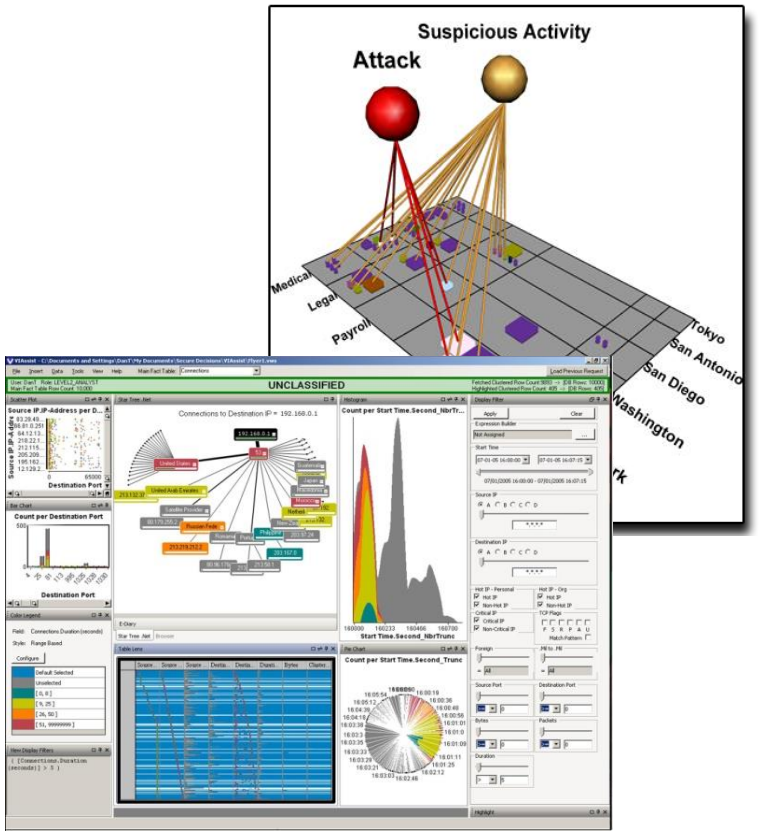
- Analysis of **decision process**
- **Visual analytics** for wired / wireless network data
- **Visualizations** of abstract cyber data
- Visual systems for **CND training**
- **Impact analysis** of cyber events
- **Decision support system** design

Software assurance visualization

Technology transition

Cyber testbed support

Classified portfolio



Current Products Transitioned From R&D

Visualizations to help cyber analysts make sense of massive data, and communicate results

Use:	In-depth incident analysis, historical analysis, watch briefings
Data:	NetFlow, alerts
TRL 9:	Deployed to USCERT In evaluation in intel community
Funding:	IARPA, DHS, AFRL

Use:	Wireless threat and risk analysis, policy compliance, audit reporting
Data:	Wardriving , WIDS
TRL 9:	DoD version downloadable from NRL site; Commercial version available
Funding:	DARPA, AFRL, NRL, DISA

Use:	Triage and analysis of software source code vulnerabilities
Data:	Results of SwA tools
TRL 9:	Info and trial download available at www.codedx.com;
Funding:	DHS

Sample Customers and Partners

Government

Air Force Research Lab
DARPA
DHS
DISA
IARPA
Naval Research Lab
ONR
OSD

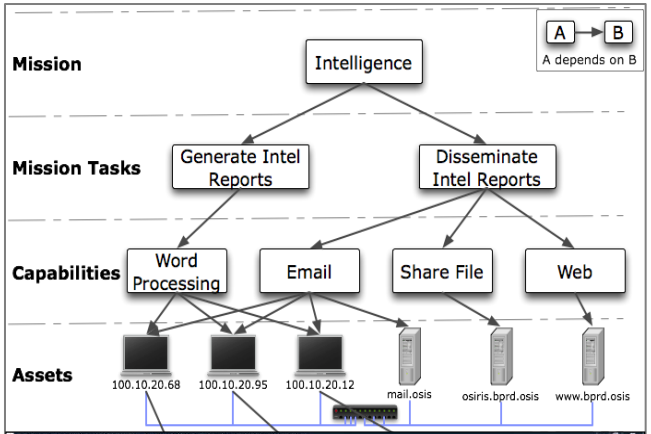
Industry/Academia

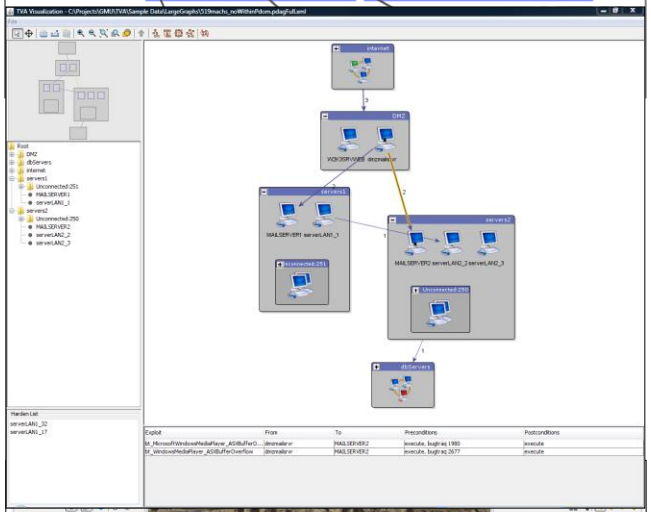
Adventium
Alion
ATC
BAE
General Dynamics
George Mason University
Hopkins Applied Physics Lab
Informatica
ITT
Lockheed Martin
Raytheon
SAIC

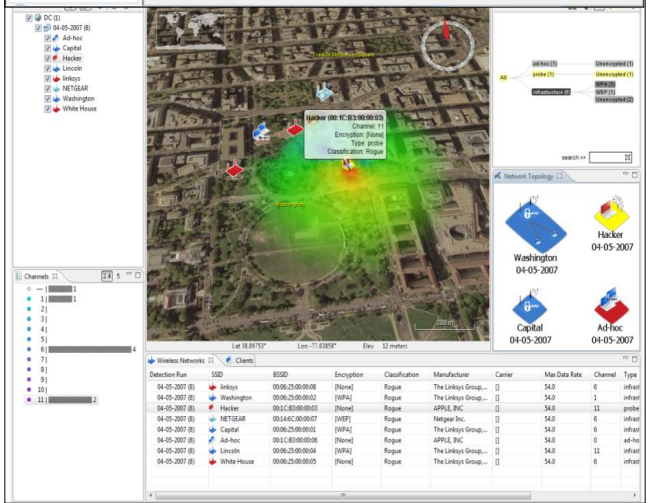
- **Nominated twice by DARPA for *SBIR of the Year***
- **Featured twice as a DARPA Success Story**

SECURE DECISIONS
A DIVISION OF APPLIED VISIONS, INC.

Key Projects at Secure Decisions



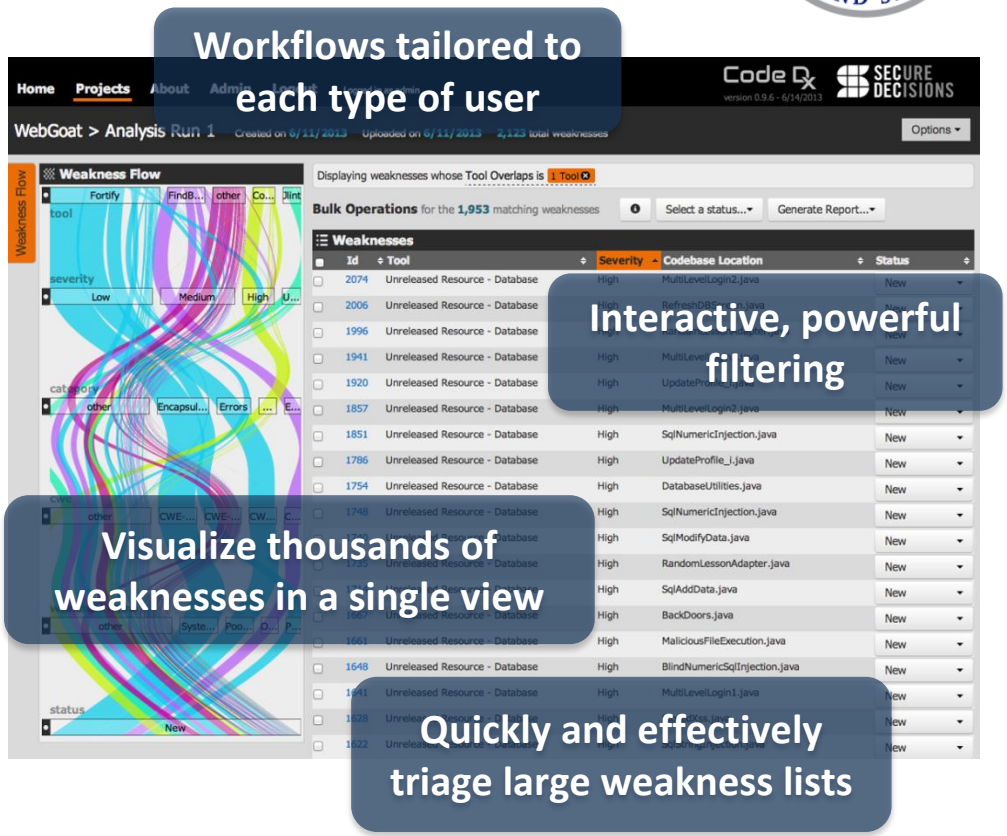




Software assurance visualization

Code Dx: Software Analysis Integration Platform

- Imports and correlates results from multiple SAST tools
- Normalizes results; common severity scale
- Visual analytics to rapidly triage results, remove false positives
- Common UI with custom detail for security analysts, developers, and CISOs
- *Code Dx Bundle* embeds open source SAST tools for use with or without commercial tools
- Affordable for small and medium size businesses



A CWE-friendly application

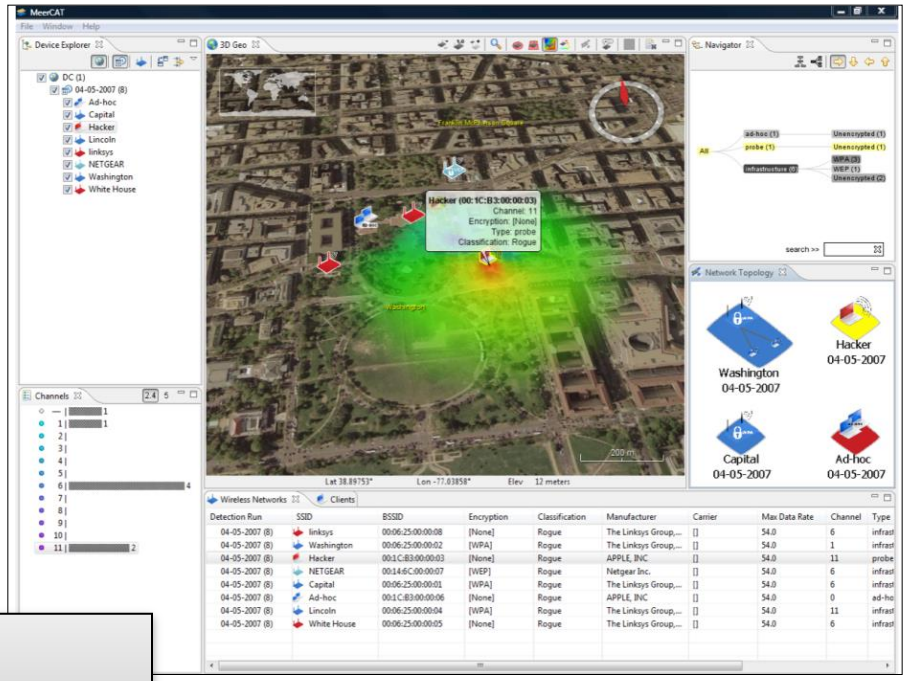
Products that visualize vulnerabilities and suspicious network activity

MeerCAT: Visualization of Cyber Asset Tracks

Visualizes wireless network security

- Physical 2D and 3D **geographic location**
- Logical **network topology** location
- **Communication** patterns
- **Security** status
- **Mission** of cyber assets

MeerCAT

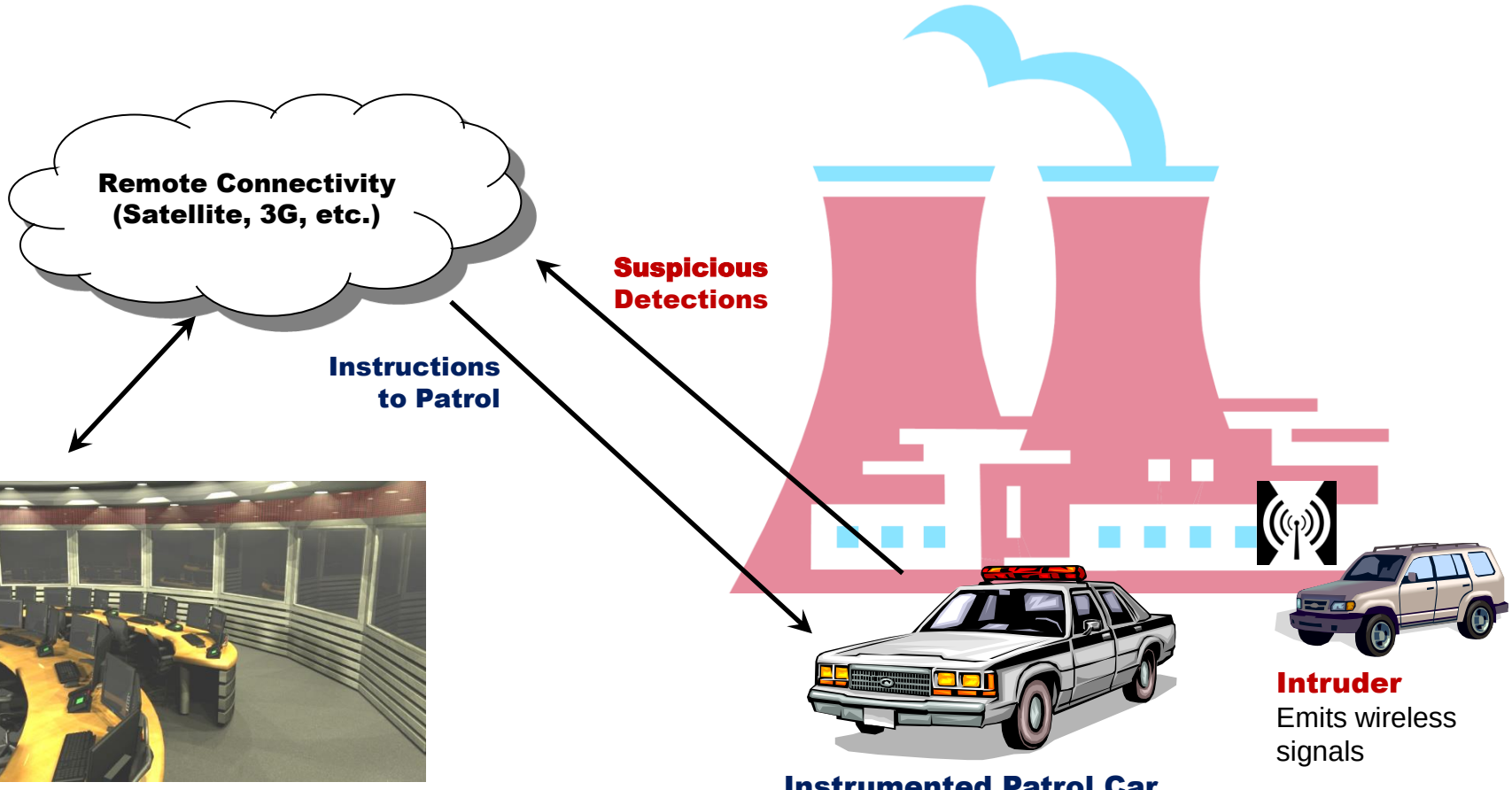


DARPA

An SBIR Phase 2 funded by DARPA

Accredited within DoD's Flying Squirrel Wireless Suite for vulnerability analysts. Featured in DARPA's **SBIR Success Report.**

WildCAT: Wireless Analysis from Patrol Cars



Centralized Monitoring and Analysis
Aggregates and fuses data from multiple facilities.
Provides instruction to field patrols.

Instrumented Patrol Car
Detects intruder's wireless emissions

WildCAT

APPLIED SCIENCE CENTER FOR HOMELAND SECURITY
Education • Public Safety • Economic Development • Research

VIAssist: Visualization for Information Assurance

Integrates visualization of NetFlow and IDS data

- Multiple **linked** visualizations to see different perspectives
- Don't jump to the most logical conclusion: test hypotheses; see things for various viewpoints
- **Big picture** and **detailed incident** views
- Collaboration and built in **reporting**

Original funding by IARPA and NSA.
Now funded by DHS and AFRL

VIASSIST

Installed at US-CERT
Being prepared for transition to USAF
Under evaluation in IC

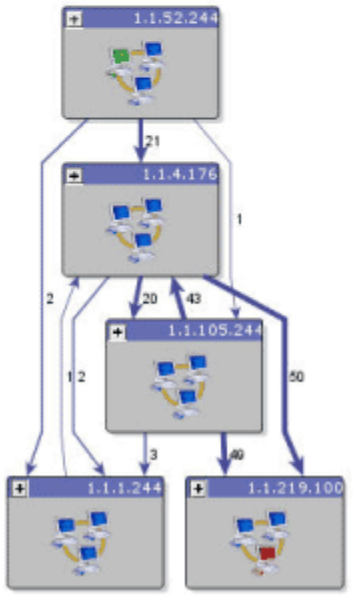
TVA: Topological Vulnerability Assessment

Visualizes attack graphs to understand vulnerability

- Attack paths based on vulnerabilities & topology
- Aggregation to make graphs readable

CAULDRON

Automatically predicts all possible paths of cyber attack within your enterprise.



A collaboration with GMU, for the Department of Homeland Security

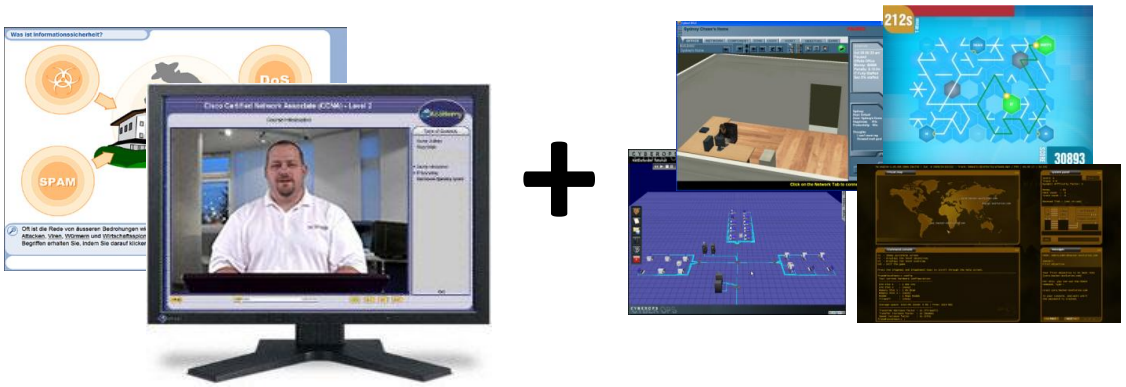
Sold by http://proinfomd.com/

Cyber Security Education

SimBLEND: Game-Based Learning for Net Defense

Blends computer-based training (CBT) with games, visualizations, & simulation to train network defenders

- Harness an existing Learning Management System (LMS) for student tracking and scoring
- Reinforce learning with games



An SBIR Phase 2 funded by AFRL (Mesa, AZ)

CBT + Visuals + Simulations + Games = Better training

Safe Computing Training Courses

Safe computing education for non-technical audiences

- Principles of safe computing
- Work with authorizing institutions for continuing education credits
- Demonstrations of vulnerabilities in typical office environments
- Interactive graphic novels

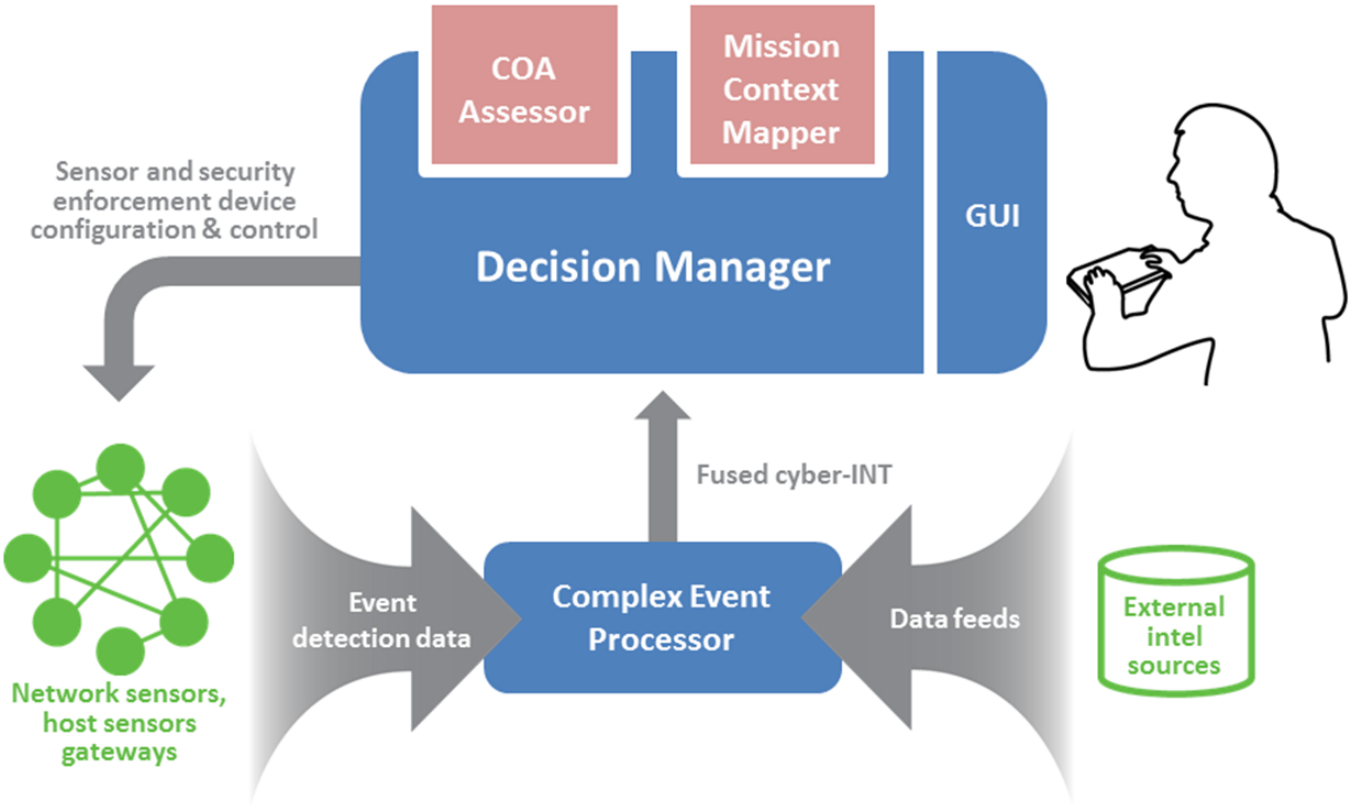
Analytical services and technologies

Deucalion: Cyber Decision Support System

DEUCALION

ONR

Design and develop next generation decision support system for Navy cyber defense

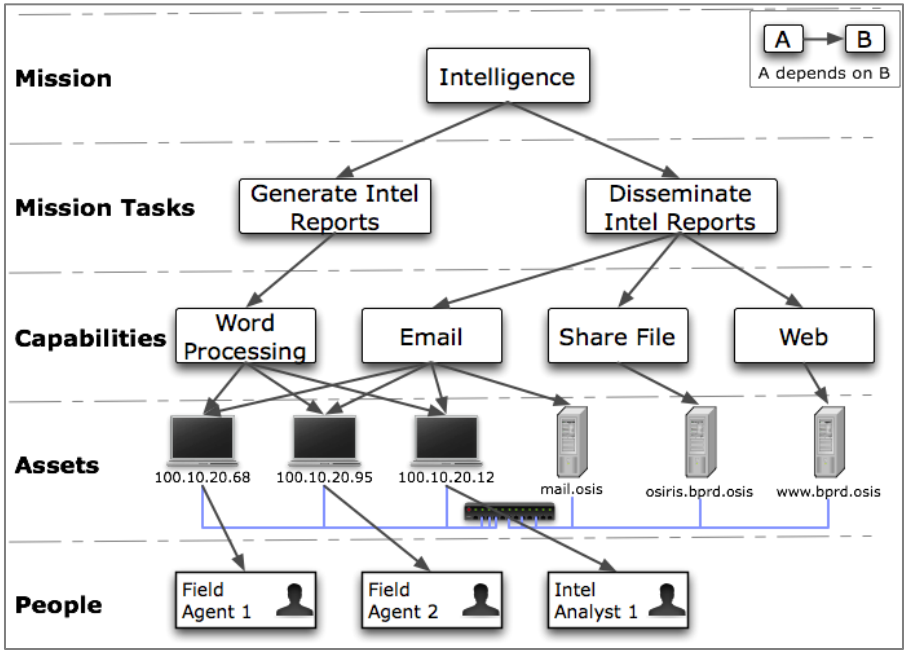


Camus: Mapping Cyber Assets to Missions & Users

Relates cyber attacks to affected missions and users

Current CND ops have poor awareness of how compromised cyber assets affect missions, organizations, and people

- Fuses various network and mission data into a common ontology
- Maps cyber assets to dependent people and operations
- Integrates with security and sensor systems to provide operational information about specific assets

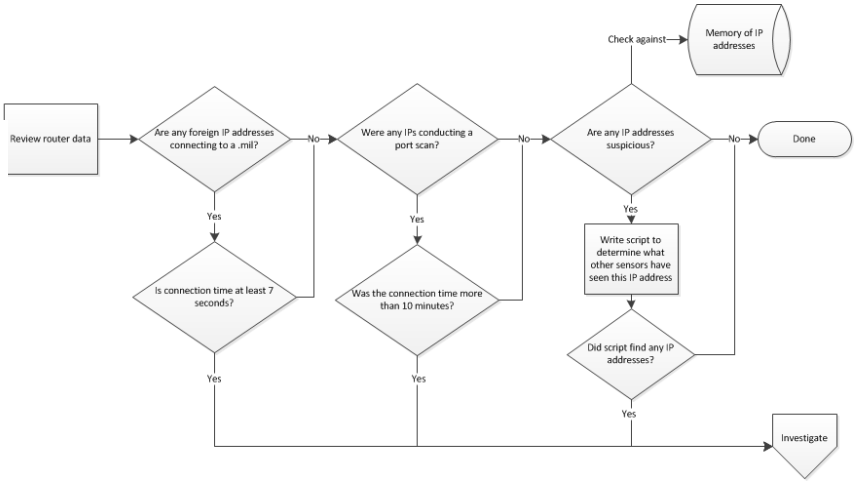


An SBIR Phase 2 funded by OSD through AFRL

NetDemon: Cyber Defense Decision Modeling

Models “as-is” and “idealized” decision processes used in cyber defense

- Analyze current Navy decision process
- Develop scenarios to illustrate future decisions
- Recommend new approach to cyber defense decision-making
- Recommend decision support tools and data



NetDemon

ONR

Test support services and technologies

National Cyber Range

Reconfigurable test range for testing cyber technologies in a high-performance simulated network

Range command and control system to control the execution and monitor the performance of cyber experiments

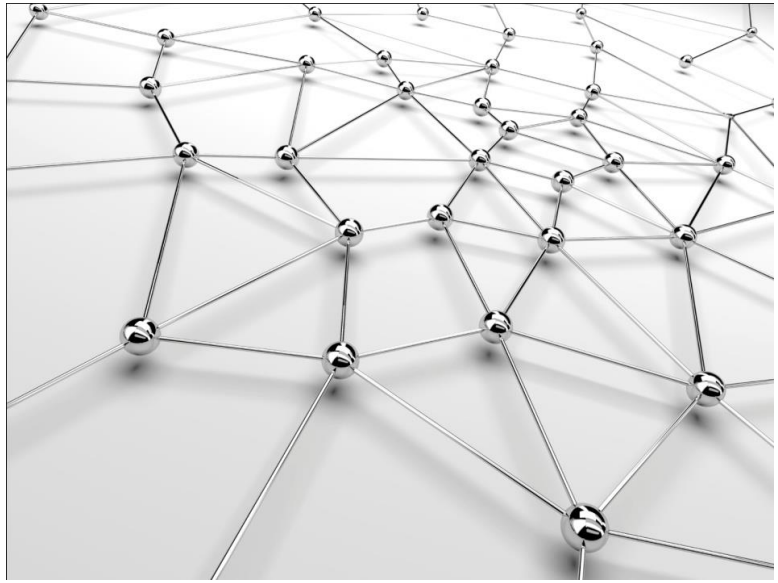
User experience design and implementation for key systems:

Experiment command and control

Design tool

Repository

Gateway



Scalable Network Monitoring Testbed

Testbed for evaluating the performance of new network monitoring algorithms

Developed software to control entire test network:

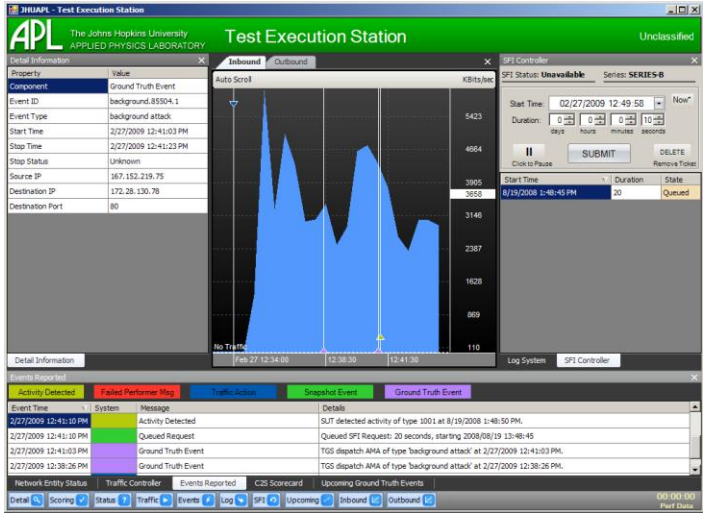
Main C2 System for execution and monitoring of tests

Remote Storage Service controls packet capture from remote locations

C2 System Client/Test Station to display and test control mechanism

Traffic Generation Services for connectivity, control, & status between test controller and traffic generator

Network Management System Services for health and utilization monitoring of the test network



Thought Leadership

VizSec Sponsor and chair of annual symposium for R&D related to visualization for cyber security

Congressional testimony on cyber R&D and education

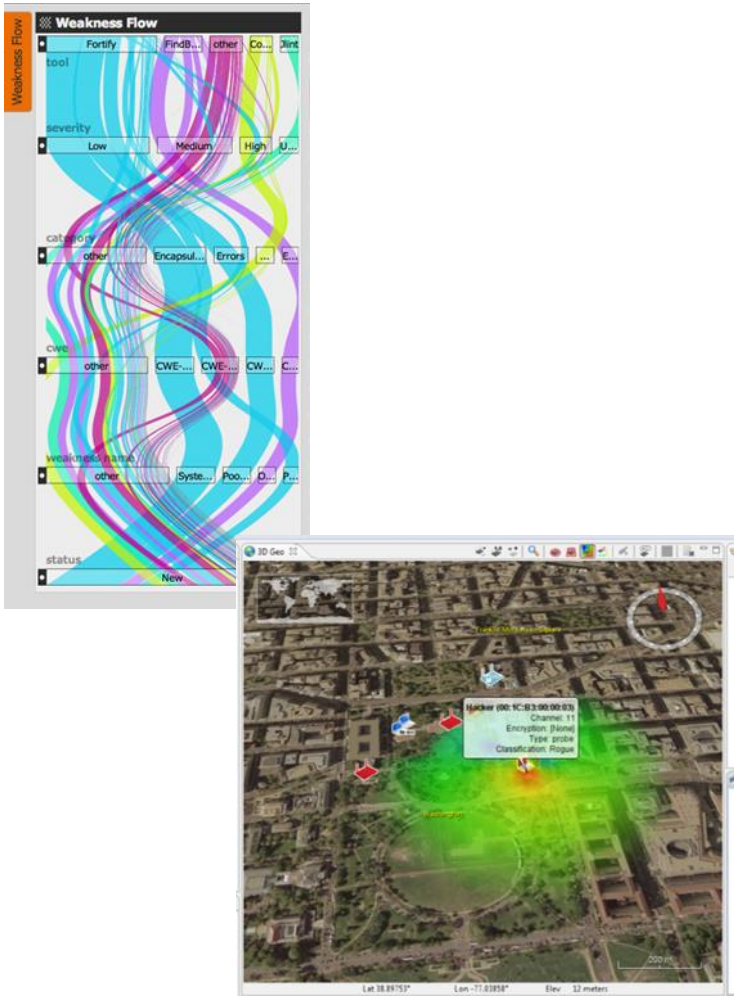
Mission Impact Workshop Conducted by-invitation workshop on mission impact of cyber attacks

Publications in refereed journals and proceedings

Patent for temporal visualizations. Patent-pending wireless security visualization

SECURE DECISIONS

A DIVISION OF APPLIED VISIONS, INC.



Enhancing Cyber Operational Decisions

Making Sense of Network Data

Anita D'Amico, Ph.D.
Anita.Damico@SecureDecisions.com
631.759.3909

SecureDecisions.com
Codedx.com
avi.com