The Secure Decisions Camus system automatically maps relationships between cyber assets and the missions and users that rely on them.

Camus

Cyber Assets to Mission and Users

The Need

Mission Assurance: Mission commanders and planners need visibility into what cyber assets are required, available, and assured

- What devices and applications are needed to accomplish the mission?
- What alternatives allow fight through asset/resource interruption?

Impact Analysis: Network and security operations personnel must assess the operational impact of cyber events such as malicious attacks, unplanned failures, and maintenance outages

- What organizational missions are affected by the asset's loss?
- What other network assets are disrupted by this loss?
- What is the operational impact of this service interruption?

Vulnerability and Risk Analysis: Prioritizing defensive actions, scheduling maintenance, and other proactive measures requires relating cyber information to the missions cyber supports

- What organizational missions rely on devices running the vulnerable OS?
- What critical network assets connect to the vulnerable ones?

There is an inability to relate cyber information to mission

All of these questions could be answered with accurate mapping of cyber assets to the missions, users, and other cyber assets that depend on them. However, current methods for mapping these interdependencies are manually intensive and tedious.

The Solution

Camus is a proof-of-concept for automatically mapping relationships between cyber assets and the missions and users that rely on them. That mapping provides the context needed to prioritize cyber events and assess their impact.

Camus contains a sophisticated and flexible data fusion engine that allows users to build coherent picture from disparate data sources, such as traffic captures and people directories. This comprehensive model of operations reveals relationships between cyber assets and the users and missions that rely on them.

Underlying Camus is a cyber asset-to-mission ontology, developed with a multidisciplinary group of leading subject matter experts and operational practitioners. Semantic web technologies enable populating this ontology with data-driven, measured realtionships between network services, capabilities, users, and missions.

Key Features of Camus

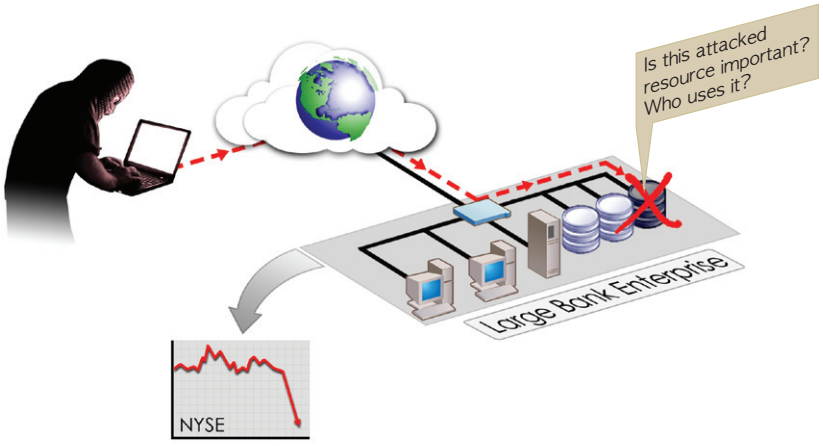
Infer relationships like "depends on", uses, owns, and "member of"

Customizable rules for inferring strength of dependencies

Interface to IDS, SIM, and other security tools to assess impact of attacks

Use existing data sources: no new sensors or agents to deploy

Enterprise partitioning for distributed data processing and greater confidentiality



Camus helps organizations identify real world affects of cyber events

APPLIED VISIONS SecureDecisions DIVISION

Secure Decisions, a division of Applied Visions Inc., performs cyber security research and develops software products for government and commercial customers

camus@securedecisions.com
http://www.securedecisions.com

(631) 759-3988
6 Bayview Avenue
Northport, NY 11768

Camus

Cyber Assets to Mission and Users

Uses

Incident Triage
Incident Response
Network Operations
Mission Planning
Business Continuity Planning
Vulnerability Risk Analysis
Mission Readiness

Questions Camus can help answer:

- ✓ What cyber assets are needed for this mission or task?
- ✓ Are there assets with similar capabilities that can provide resiliency?
- ✓ Which cyber assets should receive prioritized defense or recovery?
- ✓ What missions will be affected by a loss of this cyber asset?
- ✓ Who relies on the failed/attacked asset?
- ✓ What other assets or capabilities depend upon the failed/attacked asset?
- ✓ Who should be notified about this loss?
- ✓ When will an emergency maintenance outage have the least impact to users?

Users

Network Operations Staff
CND Analysts
Mission Commanders
Mission Planners
Intrusion Detection Teams
Incident Response Teams
COOP/BCP/DR Planners

Camus provides rich contextual information to existing CND tools such as IDS, SIM, and SEIM systems. It can also be used to provide executives and mission commanders with a dashboard view of cyber-mission readiness.

Key Benefits

Assured Mission Success

→ Use information about dependencies between cyber assets and mission to ensure operational success

Situational Awareness

→ Maintain an up-to-date picture of who uses what assets on your network

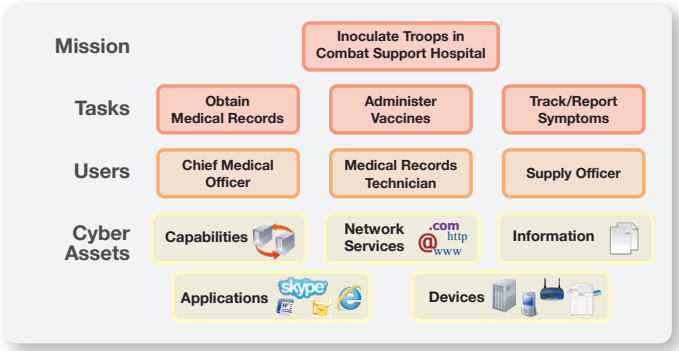
Mitigated Risks

→ Know which assets to defend and maintain

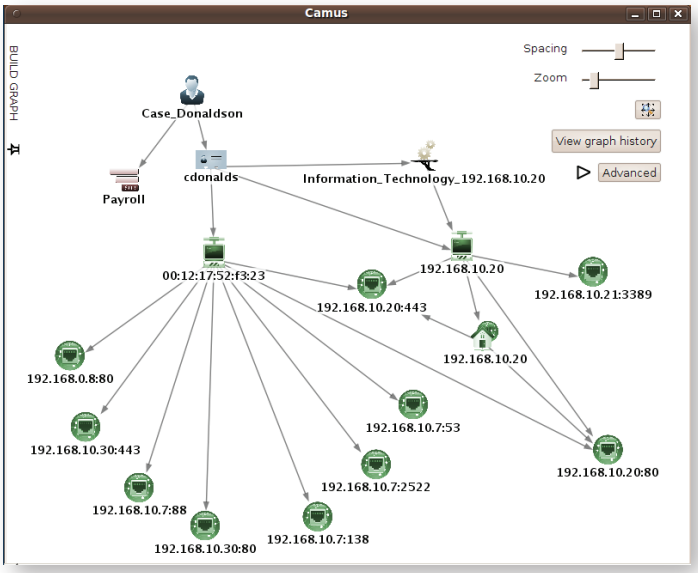
→ Eliminate single points of failure

Saved Time and Labor Costs

→ Eliminate manual, time-consuming, tedious mapping of cyber assets and their use



Mapping missions and users to cyber assets is a critical task for every organization



Users working on tasks rely on service, application, and hardware assets; failures have cascading effects.

System Architecture

Camus is modular; each component can run on a separate host, increasing scalability and performance. The Camus Application Module hosts the application library, web application, and the Camus restlet interface. Other modules include the Semantic Repository Module and the Camus Data Import Module. A Camus API provides integrators with query access to the repository from other systems.

About Camus

Camus was funded by the Office of the Secretary of Defense, and managed by the Air Force Research Laboratory (AFRL) under Phase II SBIR contract FA8750-08-C-0166. SBIR Data Rights (DFARS 252.227-7018, June 1995) apply.

APPLIED VISIONS SecureDecisions DIVISION

Secure Decisions, a division of Applied Visions Inc., performs cyber security research and develops software products for government and commercial customers

camus@securedecisions.com
http://www.securedecisions.com

(631) 759-3988
6 Bayview Avenue
Northport, NY 11768