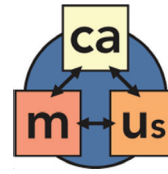


The Secure Decisions Camus system automatically maps relationships between cyber assets and the missions and users that rely on them.



# Camus

Cyber Assets to  
Mission and Users

## The Need

**Impact Analysis:** To assess the impact of a cyber event, whether a malicious attack or maintenance outage, network and security administrators need to know:

- Who relies on the affected asset for their job?
- What organizational missions are affected by the asset's loss?
- What other network services and assets are disrupted by the asset's loss?

**Mission Assurance:** When planning a critical mission or activity that depends on a reliable cyber infrastructure, planners need to know:

- What devices and applications are needed to accomplish the mission?
- What user accounts must be given priority?

**Vulnerability and Risk Analysis:** To assess the risks of vulnerabilities and prioritize their patching, security practitioners need to know:

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

**Currently, these questions are answered by pulling the plug. There is a better way.**

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.

Underlying Camus is a cyber asset-to-mission ontology, developed with a multidisciplinary group of leading subject matter experts and operational practitioners. Using semantic web technologies, Camus discovers the critical relationships between network services, capabilities, users, and missions.

Camus contains a sophisticated and flexible data fusion engine, and uses an ontology-based structure for storage and querying. Disparate data sources, such as traffic captures and people directories, are fused into a comprehensive model that reveals relationships between cyber assets and the users and missions that rely on them.

## Key Features of Camus

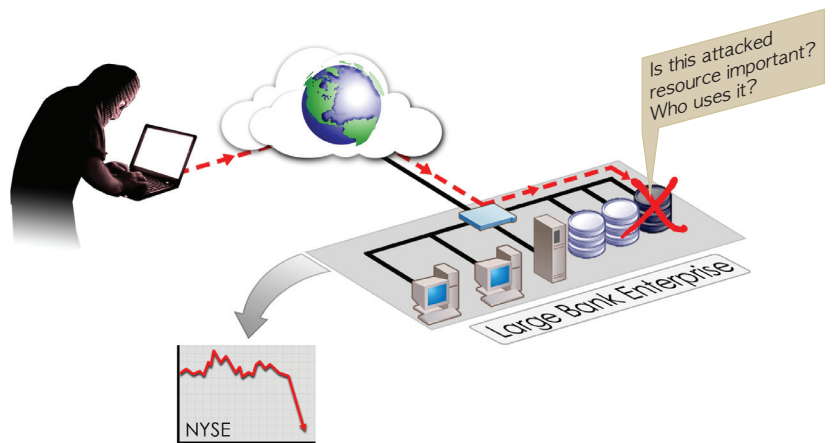
Infer relationships like "depends on", uses, owns, and "member of"

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

## Uses

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

Questions Camus can help answer:

- ✓ Who relies on the failed/attacked asset?
- ✓ What missions do they support?
- ✓ What other assets or capabilities depend upon the failed/attacked asset?
- ✓ Which affected groups need to be alerted by the Incident Response Team?
- ✓ When will an emergency maintenance outage have the least impact to users?
- ✓ During disaster recovery, what mission-critical cyber assets should be recovered first?
- ✓ What assets are required for this task or process?
- ✓ Are there assets with similar capabilities that can provide resiliency?

## Users

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

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

### Situation Awareness

→ See information about dependencies between cyber assets and mission

### Risk Assessment

→ Identify critical assets for vulnerability assessments and single points of failure

### Currency

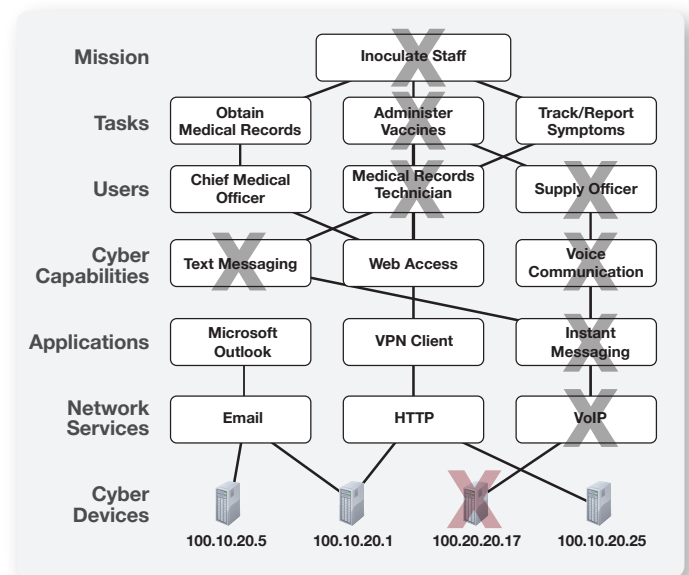
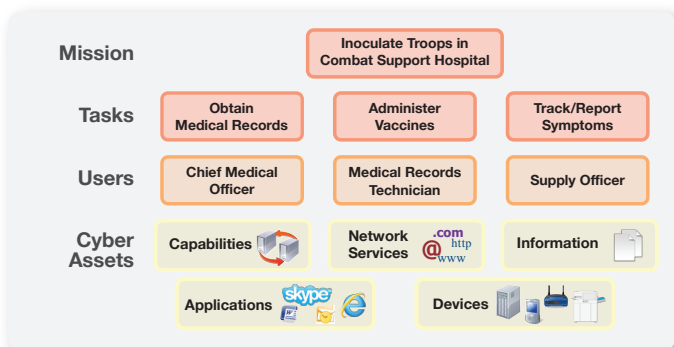
→ Get an up-to-date picture of who uses what assets on your network

### Labor Saving

→ Eliminate manual, time-consuming, tedious mapping of who and what activities are supported by network assets

### Low Maintenance

→ No client software install required



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

**Failed assets have cascading effects on users, services, applications, capabilities, tasks, and missions**

## 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.