NeMS Enterprise Network Intelligence

TECHNOLOGY SHOWCASE PRESENTATION

HELENA BENTLEY

VP For Business Development

The Problem

- Organizations are suffering from unprecedented breaches of their networks. What's going on?

- You can't secure a network if you don't know what IT is!
  - Computer networks are organic, dynamic, and complex

- Intelligence gaps leave organizations vulnerable to internal and external attacks
  - Putting valuable data, intellectual property, financial performance, and enterprise success at risk

- Networks are not defensible, and people's jobs are greatly impacted as a result

- Upcoming policy will mandate cyber standards for all companies that do business in the State of California

Quellum

Guiding Vision

In a connected world of networks, the bad guys coordinate, collaborate, and share their exploits. The good guys, meanwhile, act locally and don't share enough information to keep pace– so the bad guys are winning. Quellum believes in fighting complex threats with simple strategies:

1. *Make networks defensible*: learn about your network and understand what makes it unique. This is your enterprise network intelligence.

2. *Actively defend your network*: through automation of basic security controls, demonstrated to mitigate up to 80% of everyday security threats

3. *Adopt the bad guys winning strategy*: collaborate, coordinate, and share threat information.

DISCOVER   CHARACTERIZE   MITIGATE

Quellum

Value Proposition

Think of NeMS like a PET/CT scan for your network

At Quellum, we liken your enterprise network to a human body. Just as no two people are exactly alike, networks are dynamic and have individual complexity. Where humans grow, develop, and change organically, every network develops individual topology, settings, and networks.

At critical junctions in the life of your enterprise, don't treat your network body with mediocre health services. Use NeMS—the next generation of cybersecurity network intelligence solutions.

Quellum

The NeMS Advantage

DISCOVER   CHARACTERIZE   MITIGATE

- Automates the most important Critical Security Controls
  - Inventory of authorized and unauthorized Devices (CSC 2)
  - Inventory of authorized and unauthorized software (CSC 2)
  - Continuous vulnerability assessment and remediation (CSC 4)

- Like a continuous PET/CT scan for your network.
  - Uncovers network blind spots
  - Identifies threats evading detection
  - Finds unknown assets needing protection
  - Continuous active and passive monitoring of data traffic
  - Creates most accurate representation of network topology in real time, plus detailed reports on your organization's cybersecurity posture

- Unparalleled technology is faster and more robust than the competition
  - Combines behavioral network algorithms with high-powered network sensors to provide insight more quickly and efficiently than any other single commercial solutions.
  - Pilot feedback indicates that NeMS does the work of at least three other competitor's tools

- You won't even notice it's there– ZERO network interference

Quellum

The Solution: NeMS

Software-based network discovery and characterization tool

- Constructs visual representations of computer network based on observed behavior

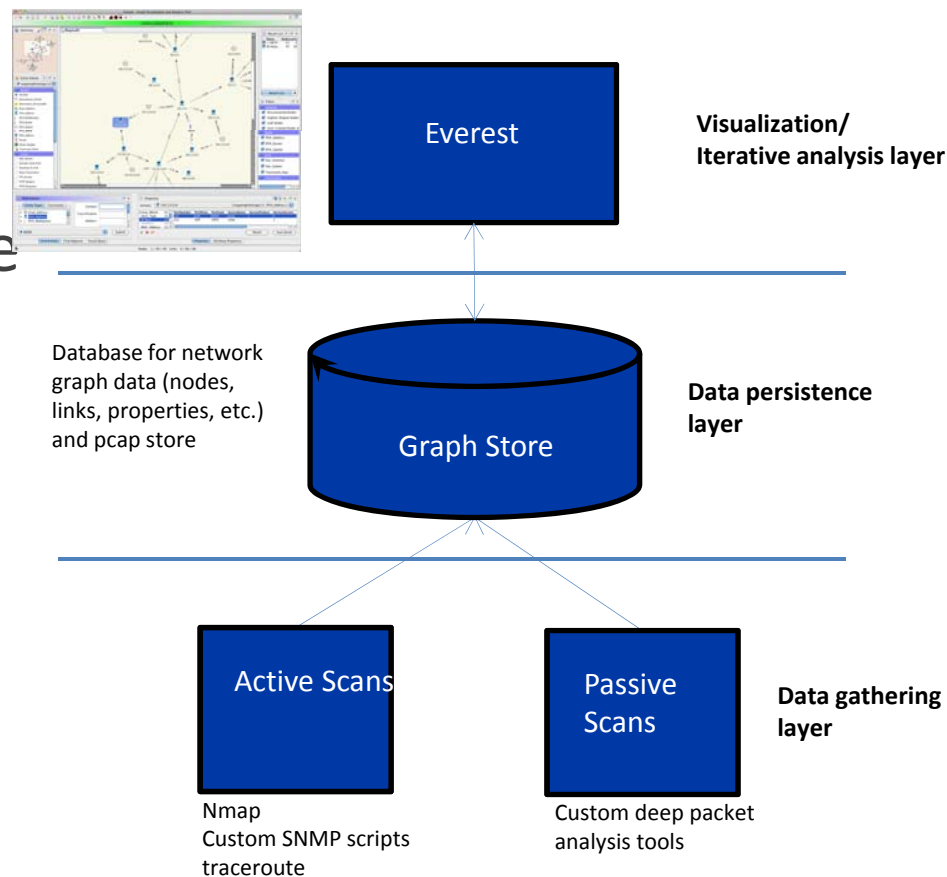- Iteratively visualize, analyze, & explore large dynamic network operations issues
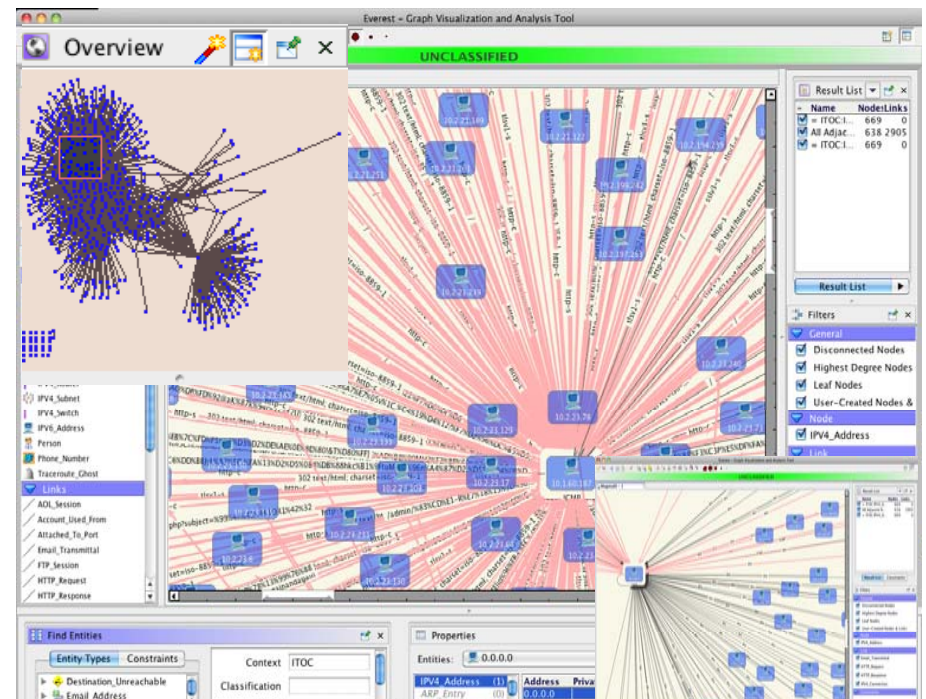
Builds on over 15 years of R&D at **Lawrence Livermore National Labs**

Quellum

The Solution: NeMS

Next generation enterprise network intelligence solution

- Combines intelligent network probes, passive traffic analysis and host discovery

- Constructs OBSERVED network topology and behavior including end hosts and services

Everest — Visualization/ Iterative analysis layer

Database for network graph data (nodes, links, properties, etc.) and pcap store

Graph Store — Data persistence layer

Active Scans — Nmap Custom SNMP scripts traceroute

Passive Scans — Custom deep packet analysis tools — Data gathering layer

System Architecture

Quellum

History

- Builds on 15 years of U.S. Federal **government-funded network analysis and high performance** computing expertise
  - *The NeMS solution is the culmination of millions of dollars in R&D, developed at the Lawrence Livermore National Labs, and fine-tuned over a decade in the most sophisticated cyber labs in the country.*
  - *NeMS is owned and operated Quellum LLC*

- Developed at the Lawrence Livermore National Laboratories, acquired as a Transition to Practice technology with DHS

- Purpose-built to navigate classified, complex networks with a light touch to avoid network interference and detection
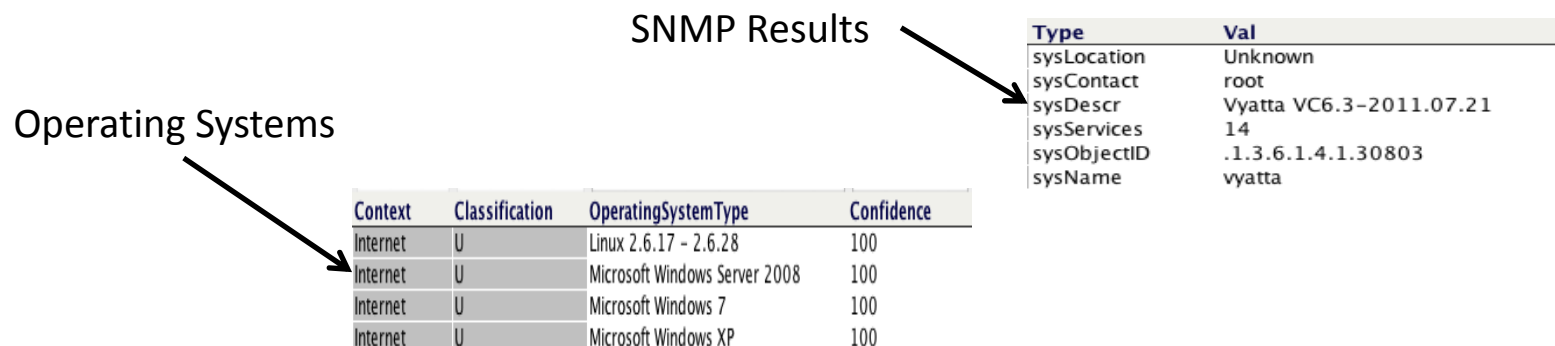
Quellum

Measuring Success: Traction & Validation

- Three successful pilots conducted in high-profile public and private enterprise
  - Library of Congress
  - Cook County (one of the largest hospital system in the U.S.)
  - Large international bank

- Working to solidify 1-2 additional before the end of 2016

- Cyber assessments sell
  - Pilot at international bank led to continued business operations within CGA, Quellum's parent company
  - Quellum senior advisors seeing many requests for assessments–hot market with relatively low barrier to entry

Quellum

Measuring Success: Case Studies

Case #0: Test network validation with ground truth data

- ~6,000 hosts mapped and processed within **20 minutes**

- **100%** of hosts were identified **plus** the **unexpected discovery of an unknown external network connection and a set of network configuration files**

SNMP Results

Type	Val
sysLocation	Unknown
sysContact	root
sysDescr	Vyatta VC6.3–2011.07.21
sysServices	14
sysObjectID	.1.3.6.1.4.1.30803
sysName	vyatta

Operating Systems

| Context	Classification	OperatingSystemType	Confidence
Internet	U	Linux 2.6.17 – 2.6.28	100
Internet	U	Microsoft Windows Server 2008	100
Internet	U	Microsoft Windows 7	100
Internet	U	Microsoft Windows XP	100

Quellum

Measuring Success: Case Studies

Case #1: Operational Enterprise Network

- **22,858 hosts discovered** through combination both passive and active characterization (within 95% of physical inventory performed 18 months prior)

- 11,858 hosts discovered through active mapping

- 4,000 more hosts via passive mapping and 7,000 hosts via SNMP footprinting

Quellum

Measuring Success: Case Studies

Case #2: Virtualized Test Network

- **1-3 hours** for each sequence of virtualized address space (Each network address block contained between 256 and 65,000 hosts)

- **100%** of remote hosts were identified **and routes were found to** a supposedly secure enclave
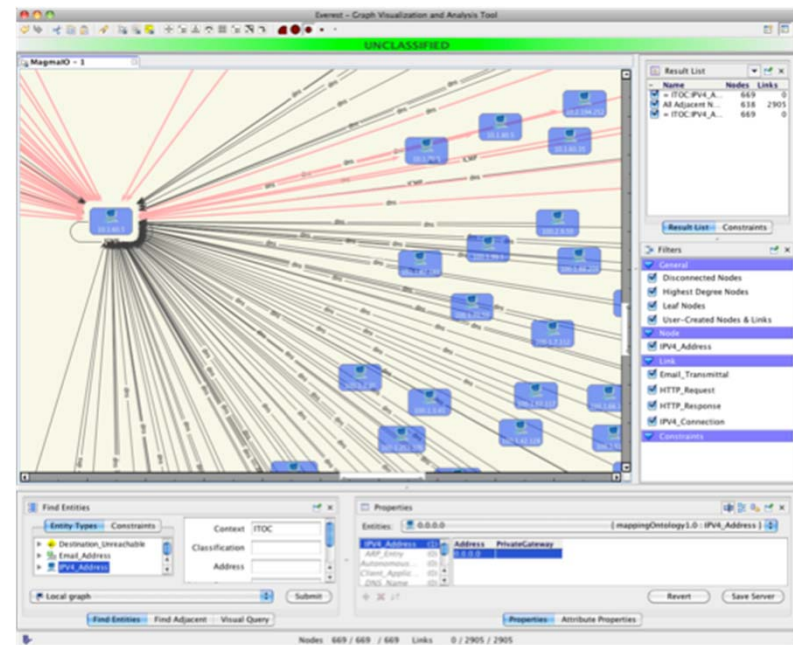
Target Market

The ideal NeMS customer? All of you.

Target markets:
- Channel partners, such as technical consulting firms
  - Sophisticated network analysis to meet demand for cyber assessments as a service. Technical capabilities required to operate create tremendous opportunities for billing.
- Financial industry firms looking to expand
  - Spending expected to increase on average 8.3% annually over next four years, surpassing $100 billion by 2020 from $73 billion in 2016 (Forbes MarketWatch, Oct 2016)
- Cyber insurance providers
  - Annual cyber insurance premiums will more than double over the next four years, growing to about $8 billion in 2020 (Business Insider 2016)

Quellum

Financial Information

- Company stage: angel round
- Previous capital: $300k + self funded
- SaaS revenue model: recurring fee + initial consultation fees
- Narrow focus on cyber assessments and services component
  - Intended to jump start sales– cyber assessment market is hot, and there is a significantly lower barrier to entry by way of CISOs
  - Quellum advantage: established network with high-profile CIO/CISOs

Quellum

Investment Ask

- $1.2M seed round to achieve critical milestones over 9-months

Product

- Engage core technical & product staff
- Establish development infrastructure
- Streamline software & enhance usability
- Engage market to synthesize requirement priorities
- Mature product roadmap

Sales & Marketing

- Engage marketing & sales resources
- Grow pilot engagements, customer pipeline, & channels
- Develop Quellum brand
- Create professional marketing materials
- Validate market and pricing

Quellum

Marketing and Sales Strategy

- The Quellum team is our biggest competitive advantage. Through our founders' decades of experience and relationships in the senior most levels of the corporate and government cybersecurity community, we have a sales and marketing capability that is unparalleled by any of our competitors.
  - In-house marketing expertise means lower cost of new content and outreach

- Through only word of mouth, we have already completed three very successful pilots with marquee institutions: Library of Congress and Cook County, IL (second largest hospital system in the U.S.), and a large international bank.
  - Once those pilots are completed, we will leverage our deep relationships with reporters and influencer with large social media followings to generate attention
  - Leverage founding team's very high profile speaking engagements at the most exclusive cyber events around the world to generate face-to-face meetings with marquee clients

Quellum

Contact Information

For more information on pricing, customizability, and detailed technical information, please contact us below:

Jake Braun, Co-Founder

Jake is Chief Executive Officer of Cambridge Global Advisors (CGA). He has over 15 years of experience in the development and implementation of strategic direction for complex, high profile national security initiatives. He works across technology, intelligence systems and transformational communications programs to develop solutions for clients in both the public and private sectors related to cybersecurity, government data analytics, and immigration.
jakebraun@gmail.com

Helena Bentley, VP for Business Development

Helena is an Account Executive with CGA. She works with cybersecurity clients in the government and private industry spaces to assist in business development and strategic communications.
helena.bentley6@gmail.com

Quellum