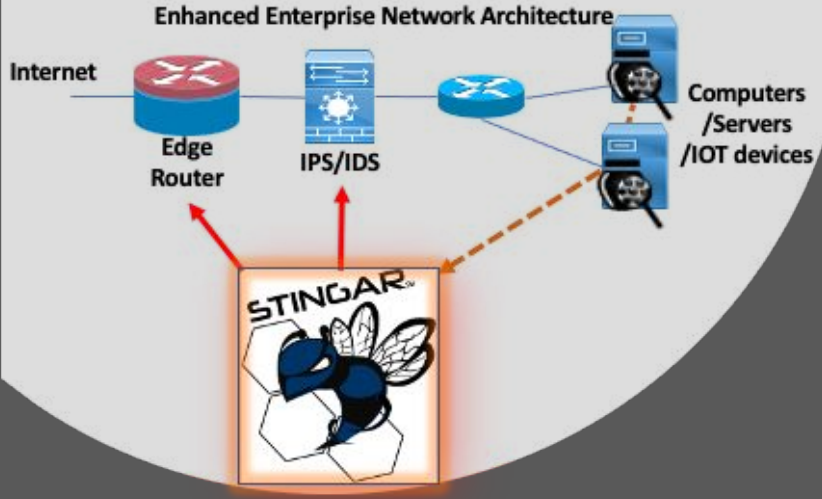

OmniSOC

STINGAR

Shared Threat Intelligence for Network Gatekeeping and Automated Response

Hugh Thomas,
Forewarned, Inc
September 2023



Introducing STINGAR
Security Automation Platform

Shared Threat Intelligence

- Provides real time visibility of cyber attacks
- Shared threat data improves defenses of all partners
- The network effect: Shared data value grows with more users

Network Gatekeeping

- Real time threat blocking at network edge
- Sophisticated "block list" processing avoids false positives

Automated Response

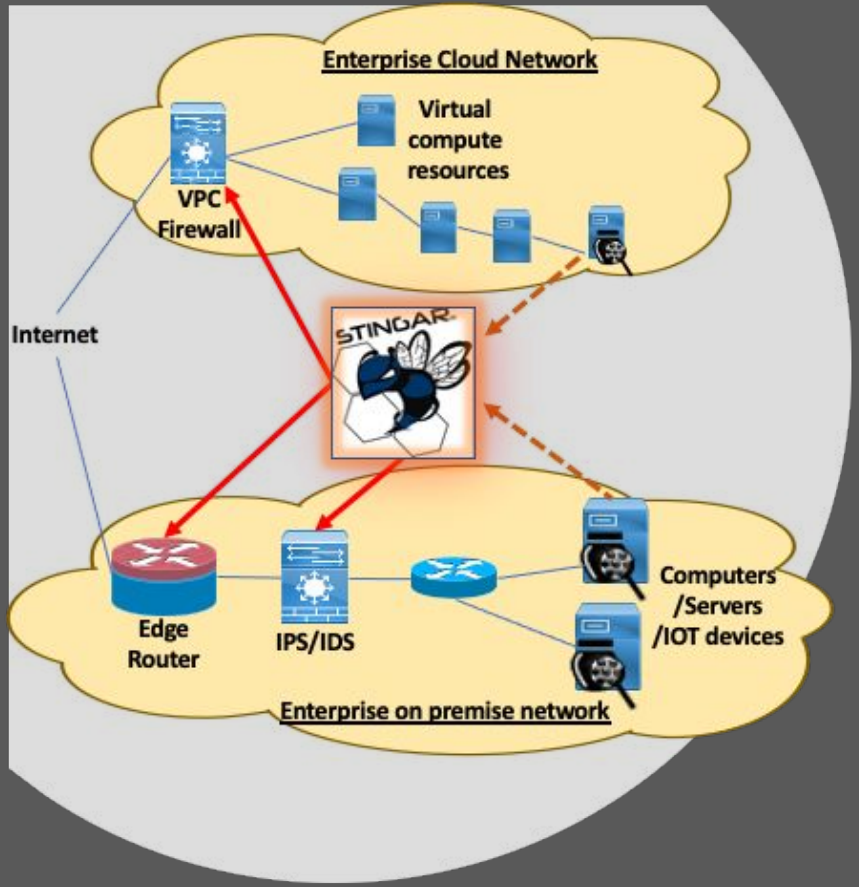
- Provides Automatic Threat detection & Response in real time
- Sub-second response time from intrusion detection to blocking
- Improves quality & utilization of existing network defenses
- Reduces workload of Security/Incident Response Teams
- Saves operating cost$

The results

Relevant, timely Threat Intelligence improves network security & reduces operating costs

- Removal of bad traffic from enterprise networks
  - Increase in blocks
    - @Duke from ~10M to over 1B blocks per day
  - Reduction of intrusions
    - @Duke >100x increase in blocked intrusion attempts
- Automation with STINGAR reduced SOC workload & lowered operating costs
  - Dramatic reduction in daily IDS alerts (>90%)
  - Realtime shared threat data blocks **>75%** attacks **before** they are detected
  - Enhanced protection against DDoS style attacks
- Installed @ 50+ leading institutions nationwide protecting 1,000,000's users

Improved resilience of Enterprise network and greater return on your overall security investment



STINGAR benefits extend to hybrid/cloud networks

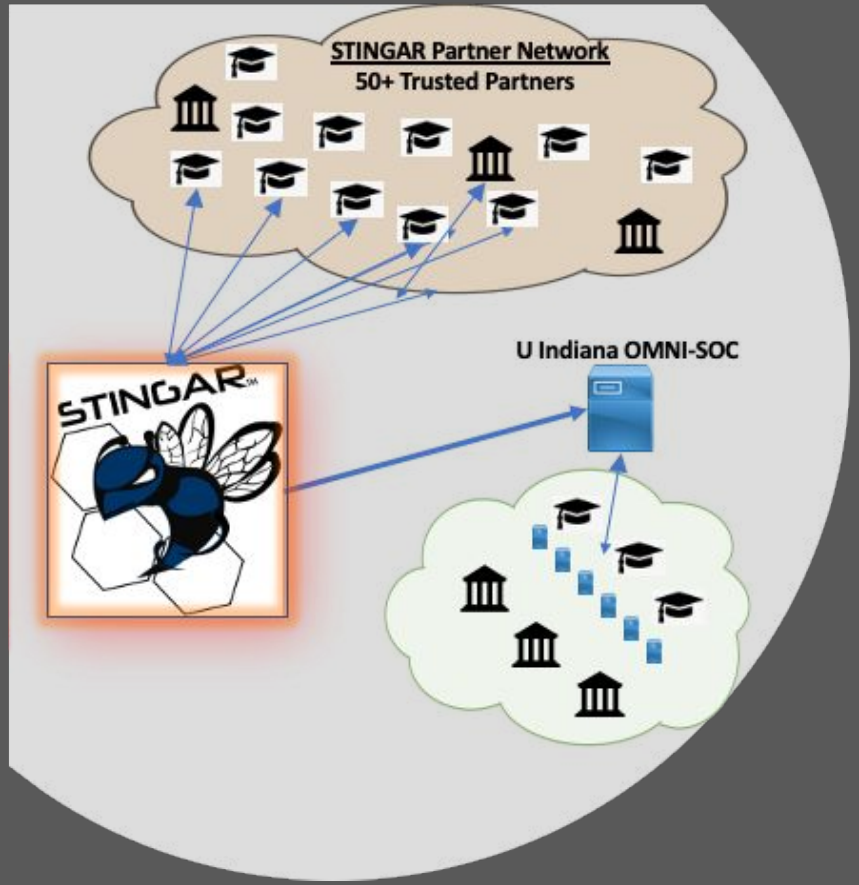
Hybrid network assets increase threat exposure for enterprises

STINGAR's unique software approach protects all network assets

- Improved & consistent Threat Intelligence protection across entire enterprise network infrastructure
- Improved network protection and reduced SOC workload
- Broader sensor footprint
  - Additional benefit by adding more sensors to virtual resources
  - Greater threat visibility and coverage

Trusted Partner Community

- 50+ STINGAR licensees in Higher Education
  - Mature software platform in production since 2016
  - Protecting millions of devices and users daily
  - In use at top Research Universities in USA
- Valuable shared threat intelligence for STINGAR trusted community
  - Large collection of raw Threat Intelligence Data available for research
  - Multiple sponsored research projects underway
  - More members improve overall network intelligence
- Active community of users with support forums, slack channels, regular updates.



STINGAR's Network Effect

STINGAR's Community generated Threat Intelligence protects all participants

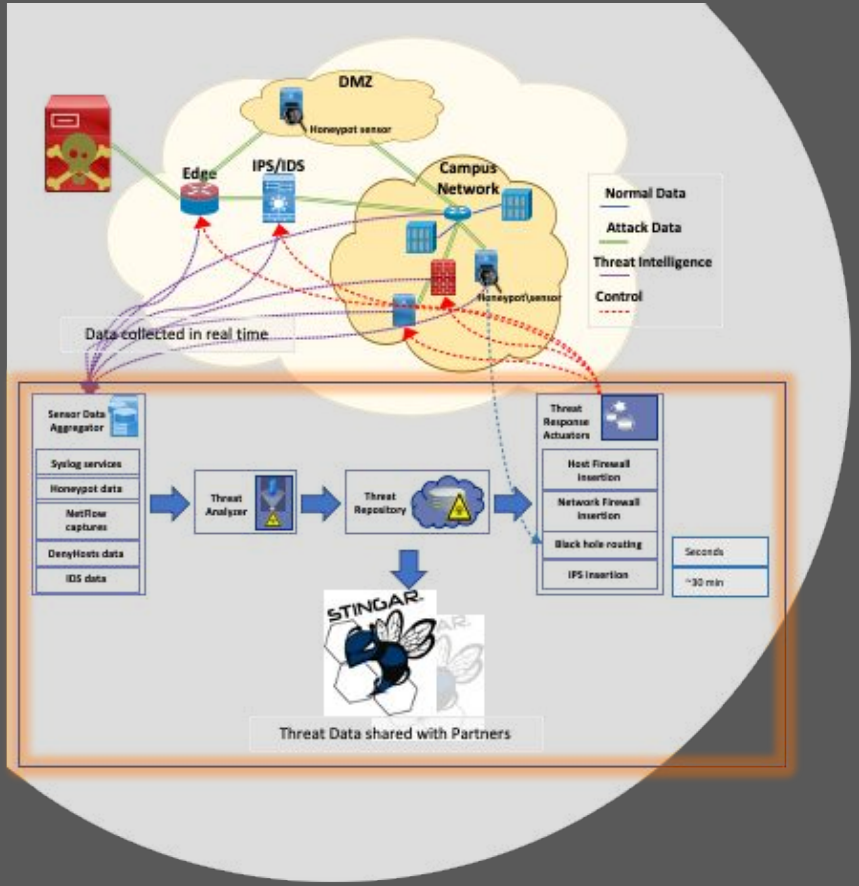
- **STINGAR HigherEd partners providing real time protection for all participants**
- **Threat intel provided via OMNI-SOC for support of HigherEd & Government Research Organizations**
- **>75% attacks blocked on partner institutions before they are detected**
- **Threat Intelligence used for Research & Education**

STINGAR protects your network from the inside

STINGAR provides real time protection for critical infrastructure

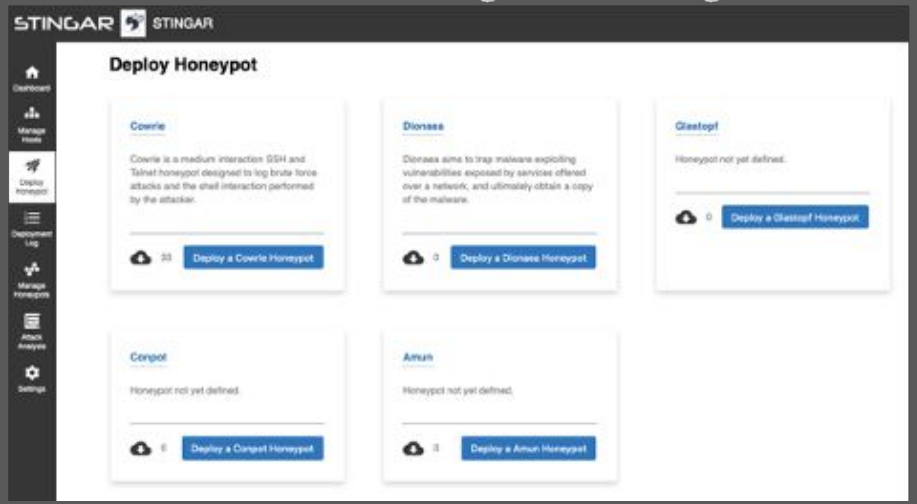
- **STINGAR's custom sensors silently monitor networks from the inside capturing threats 24/7/365**
- **Live threat intel detected from internal sub nets and protected assets**
- **x86 & ARM based sensors on small, low cost (<$50) low power hardware emulating embedded devices, network appliances, etc.**
- **Custom sensors for real time Threat Intelligence for Research, Education, Healthcare, First responders & Defense systems**

">60% of Data Breaches Are Caused By Insider Threats" - Equifax



STINGAR - Cyber Threat Platform

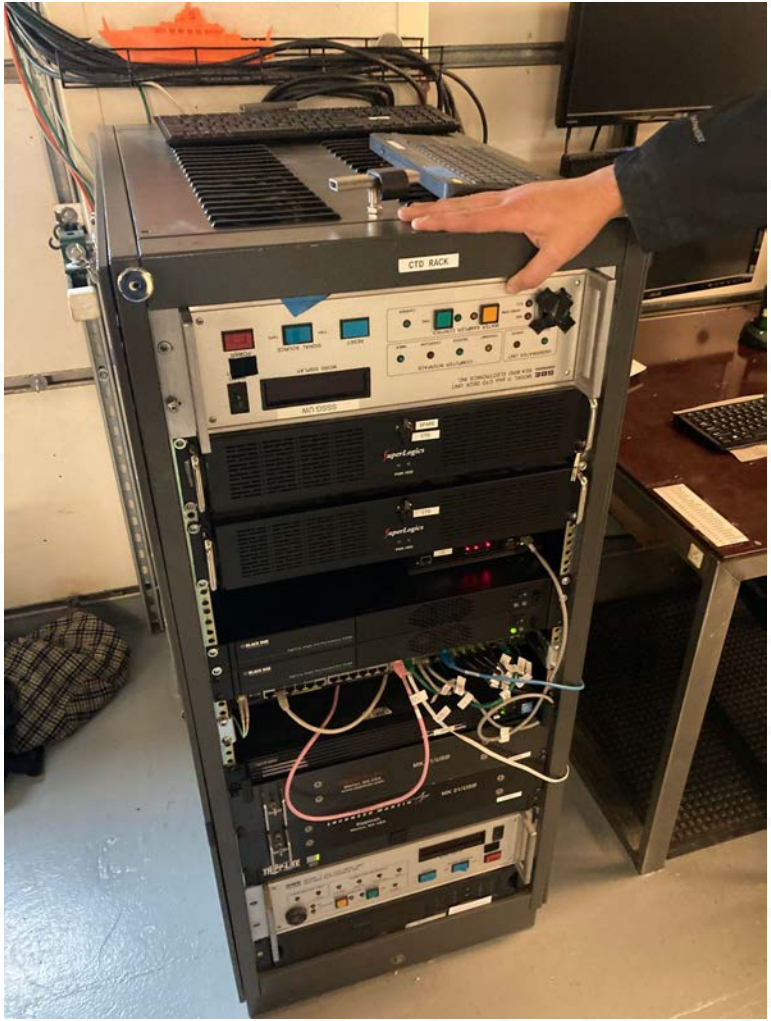
- An Enterprise Software Platform for cyber-threat monitoring & management
  - Simple web based network sensor management
  - Simple to install & virtually zero maintenance
  - Automatic blocking & Network protection
  - Use standalone or integrate with existing SIEM tools

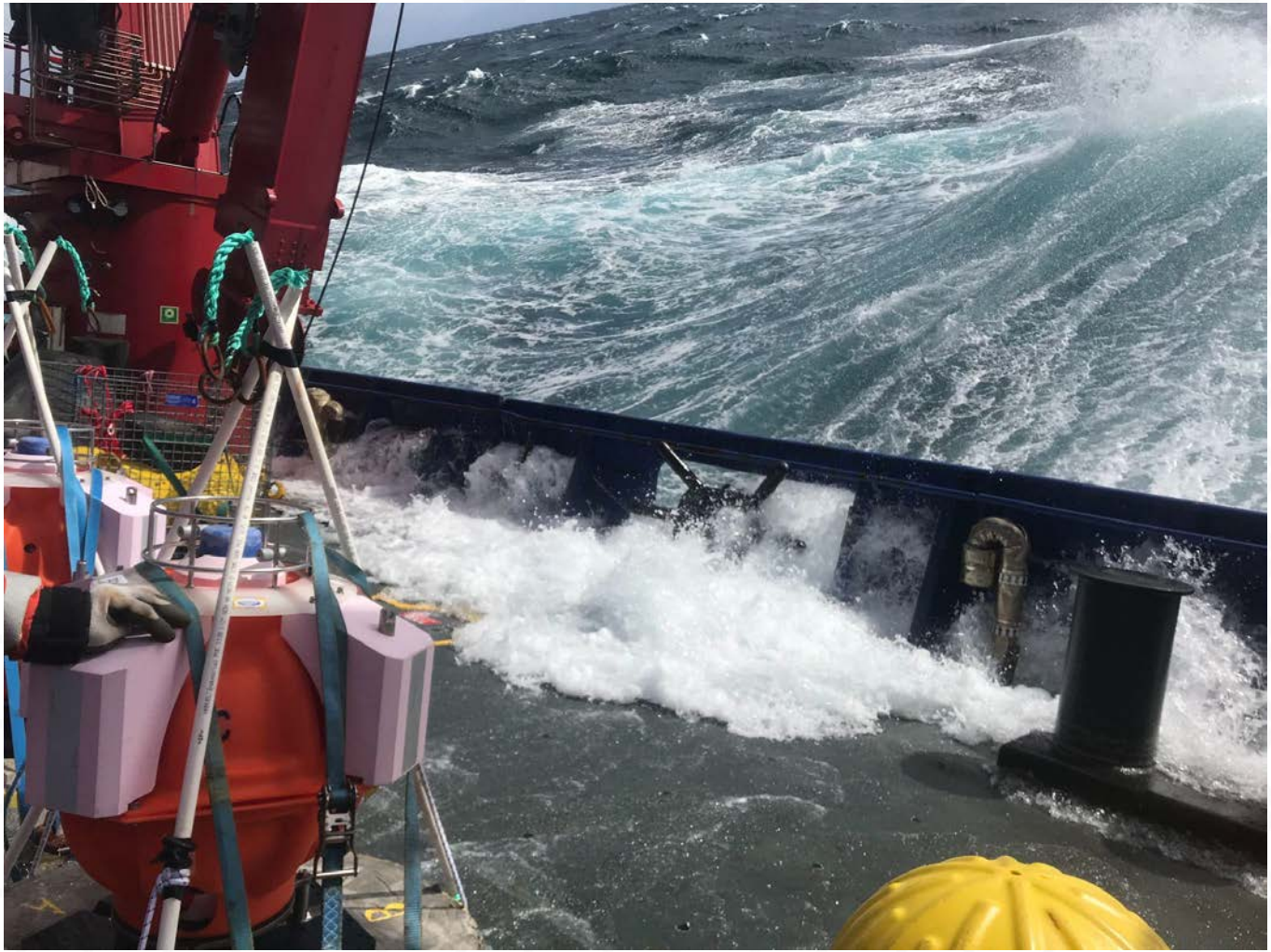



BLUE HERON
Large Lakes Observatory
University of Minnesota Duluth


W


THOMAS G. THOMPSON


CTD RACK



US Academic Research Fleet

14 institutions, 17 vessels, 2 funding agencies.

- No central IT
- New security program
- Lots of infrastructure variety
- Limited tech staff availability

There’s something weird about a distributed organization

14 institutions, 17 vessels, 2 funding agencies. Lots of variety.

- Tech staff capacity
- Little standardization
- Lots of networks
- Tiny internet pipes

Tech Staff

Not all vessels have shore-side IT supporting them.

Marine Techs sailing in the fleet are very busy people.

IT isn’t their primary role.

Bunk space is limited.

Shipboard deployments must be

1. Light-touch for techs
2. Reliable with unreliable internet connectivity
3. Durable, replaceable, or **both**

Light-touch

Once deployed OmniSOC VCS team performs all OS and software maintenance.

- AutoSSH maintains an SSH tunnel to OmniSOC Maintenance Server
- VCS Team then can SSH into Honeypot
- Hardened SSH servers on both ends.
- Authentication is all done locally.

Light-touch

Honeypot data is sent to OmniSOC's STINGARv2 Server using Fluentd protocol.

- Data is secure in transit.
- Honeypot data is cached on the honeypot if not able to report to STINGARv2 server.
- OmniSOC monitors honeypot data.
- Alerts if action is required.

Reliable

Designed to be reliable:

- AutoSSH maintains an SSH tunnel to OmniSOC Maintenance Server
- Flunentd will automatically reconnect to STINGARv2 server if the connection is lost.
- Honeypot data is stored on the honeypot until transmitted to STINGARv2 server.

QUESTIONS ?

For more information please visit :
www.forewarned.io
Or email
info@forewarned.io
Please join our slack channel
https://join.slack.com/t/stingar

Thank you for your interest in STINGAR

Shared Threat Intelligence for Network Gatekeeping and Automated Response

Hugh Thomas,
Forewarned, Inc
September 2023