SHARKSEER
Zero Day Net Defense

Ronald Nielson

Technical Director

SHARKSEER

Program Definition: Detects and mitigates **web-based malware** Zero-Day and Advanced Persistent Threats using COTS technology by leveraging, dynamically producing, and enhancing global threat knowledge to rapidly protect the networks.

SHARKSEER

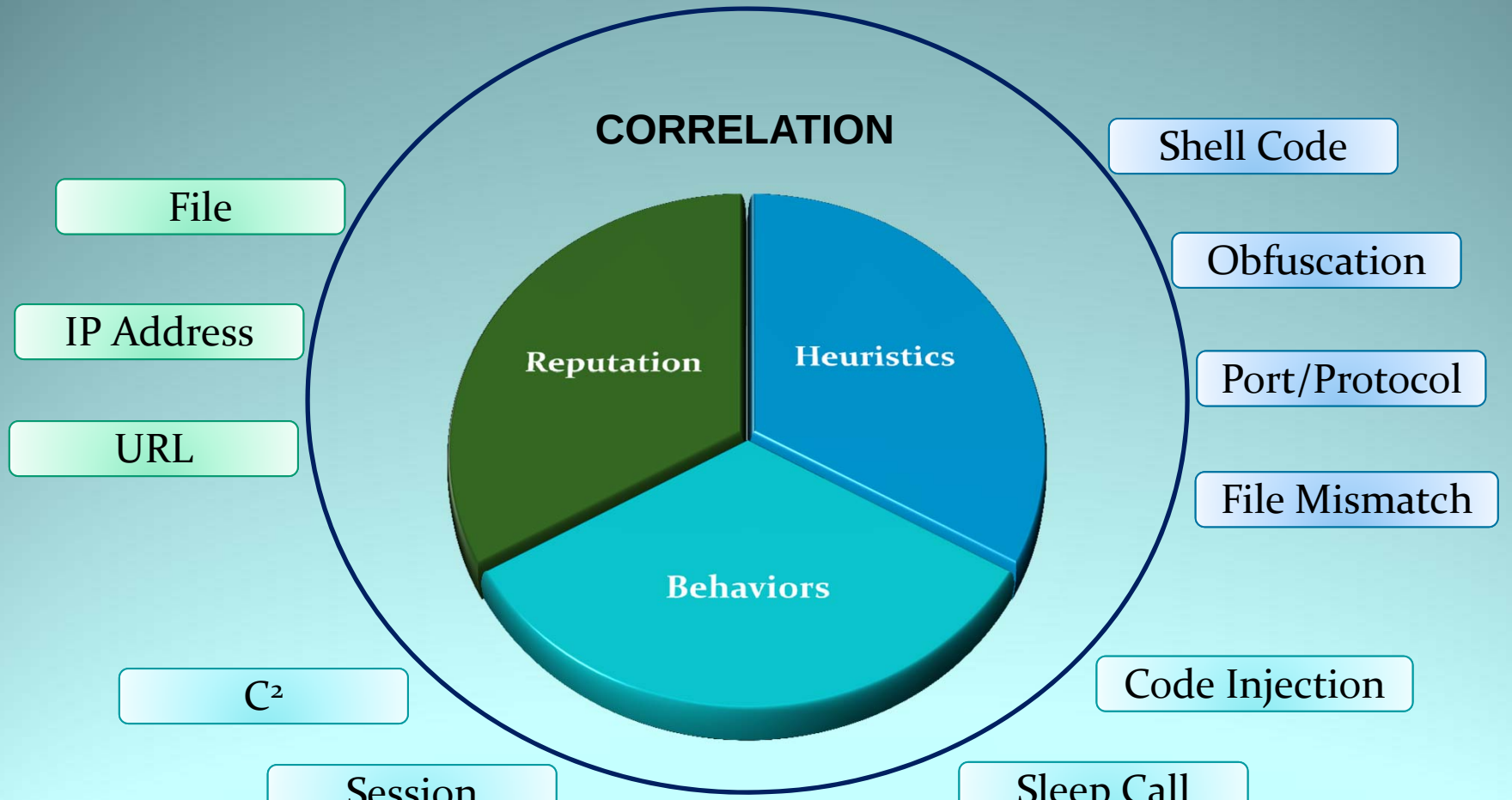
SHARKSEER's GOALS

<u>IAP Protection</u>: Provide highly available and reliable automated sensing and mitigation capabilities to all 10 DOD IAPs. Commercial behavioral and heuristic analytics and threat data enriched with NSA unique knowledge, through automated data analysis processes, form the basis for discovery and mitigation.

<u>Cyber Situational Awareness and Data Sharing</u>: Consume public malware threat data, enrich with NSA unique knowledge and processes. Share with partners through automation systems, for example the SHARKSEER Global Threat Intelligence (GTI) and SPLUNK systems. The data will be shared in real time with stakeholders and network defenders on UNCLASSIFIED, U//FOUO, SECRET, and TOP SECRET networks.

SHARKSEER

What Are We Looking For?



SHARKSEER

SHARKSEER Zero Day Net Defense

PROBLEM
- Current defenses rely heavily on signature based tools
- Signatures are generated after threat is identified
- DAT files are updated manually taking weeks or months

Adversaries Attempt to Send Malicious Content Across Internet

INTERNET

If/When An Adversary Penetrates A Gateway(s), Prevent Outbound Callbacks And/Or Exfiltration

Inbound Malicious Traffic At The Gateways, Components, Host

Shared Global Threat Data Cross Domains

Targeting All Domains

NIPRNET

SECRET

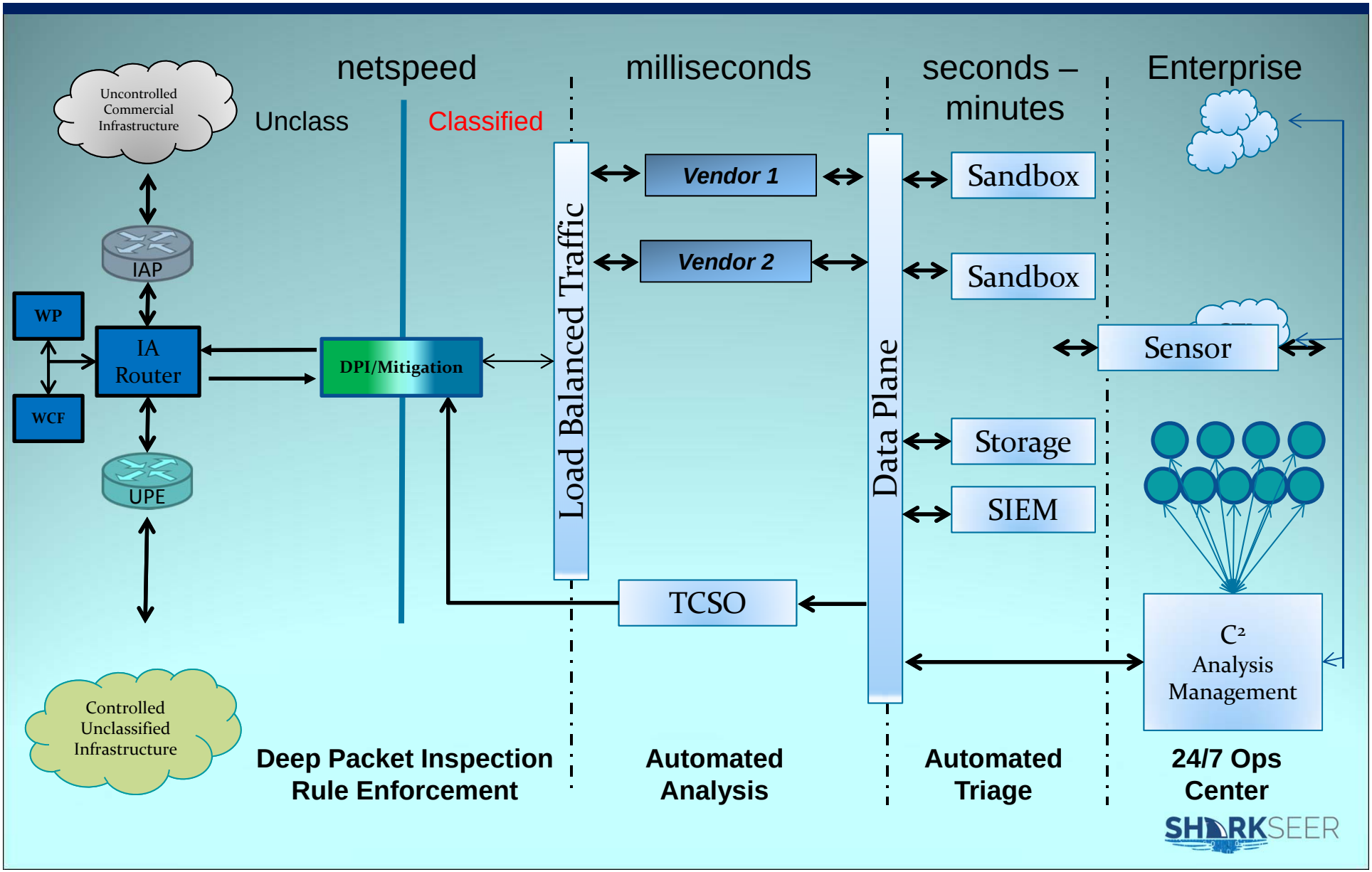
SHARKSEER Operational Space

SOLUTION
- Automate signature updates
- Leverage behavior based and cloud technologies

Unclassified → SECRET → Top Secret

Analysis Cell

SHARKSEER Environment



Tear-Line Reporting

STIX

Unique IP, PII Attribution = Yes
Deep Dive, Full Content Response

Tech - Indicators, Knowledge Repositories, Redacted Content | Mitigation

Abstracted, yet actionable data for sharing (Network, Mail, Host)

Machine | Human

Event → Event Response

Team → SME Technical Data Response

Collaborate → Activity/Adversary TTPs & Indicator Response

Ontology (Translation Tool) - Proposed

USG

Real Time
Defense Indicators

<Src IP>1.1.1.1 ← Anonymize

<URL> evil.com
<TTP>Phishing ID 314

<email>subject
<OS> Windows 7, 8
<HASH>d131dd02c5e6eec4

<RegKey>HKEY_CLASSES_ROOT
<SNORT>alert tcp any >...
<INDICATOR>%appdata%
My Docs

Unclass

Real Time
Defense Indicators

<Src IP>1.1.1.1 ← Redact
<dest IP>1.2.3.4
<URL> evil.com
<TTP>Phishing ID 314
<INCIDENT>195730

<email>subject
<OS> Windows 7, 8
<HASH>d131dd02c5e6eec4

<RegKey>HKEY_CLASSES_ROOT
<SNORT>alert tcp any >...
<INDICATOR>%appdata%
My Docs

SECRET

CCMD CNO
Response Actions

<ACTOR>GOLDSTAR ← Sanitize

<Src IP>1.1.1.1
<dest IP>1.2.3.4
<URL> evil.com
<TTP>Phishing ID 314
<INCIDENT>195730
<CAMPAIGN>SHARKATTACK
<email>subject
<OS> Windows 7, 8
<HASH>d131dd02c5e6eec4
<RegKey>HKEY_CLASSES_ROOT
<SNORT>alert tcp any >...
<INDICATOR>%appdata%My Docs

TS

Strategic Nation State
Intelligence

<ACTOR>4125
<SOURCE>INTEL
<Src IP>1.1.1.1
<dest IP>1.2.3.4
<URL> evil.com
<TTP>Phishing ID 314
<INCIDENT>195730
<CAMPAIGN>SHARKATTACK
<email>subject
<OS> Windows 7, 8
<HASH>d131dd02c5e6eec4
<RegKey>HKEY_CLASSES_ROOT
<SNORT>alert tcp any >...
<INDICATOR>%appdata%My Docs

Establishing Cyber SA

SHARKSEER

Commercial Knowledge

NSA Cyber Intel

Partner Cyber Analyst

Supplier

SHARKSEER

Event

PARTNER

Event

Input

(MALWORKS/METAWORKS/CADS)
Automated Community Cyber Analysis Environment

Process

Alerts

Reports

Machine Readable Data

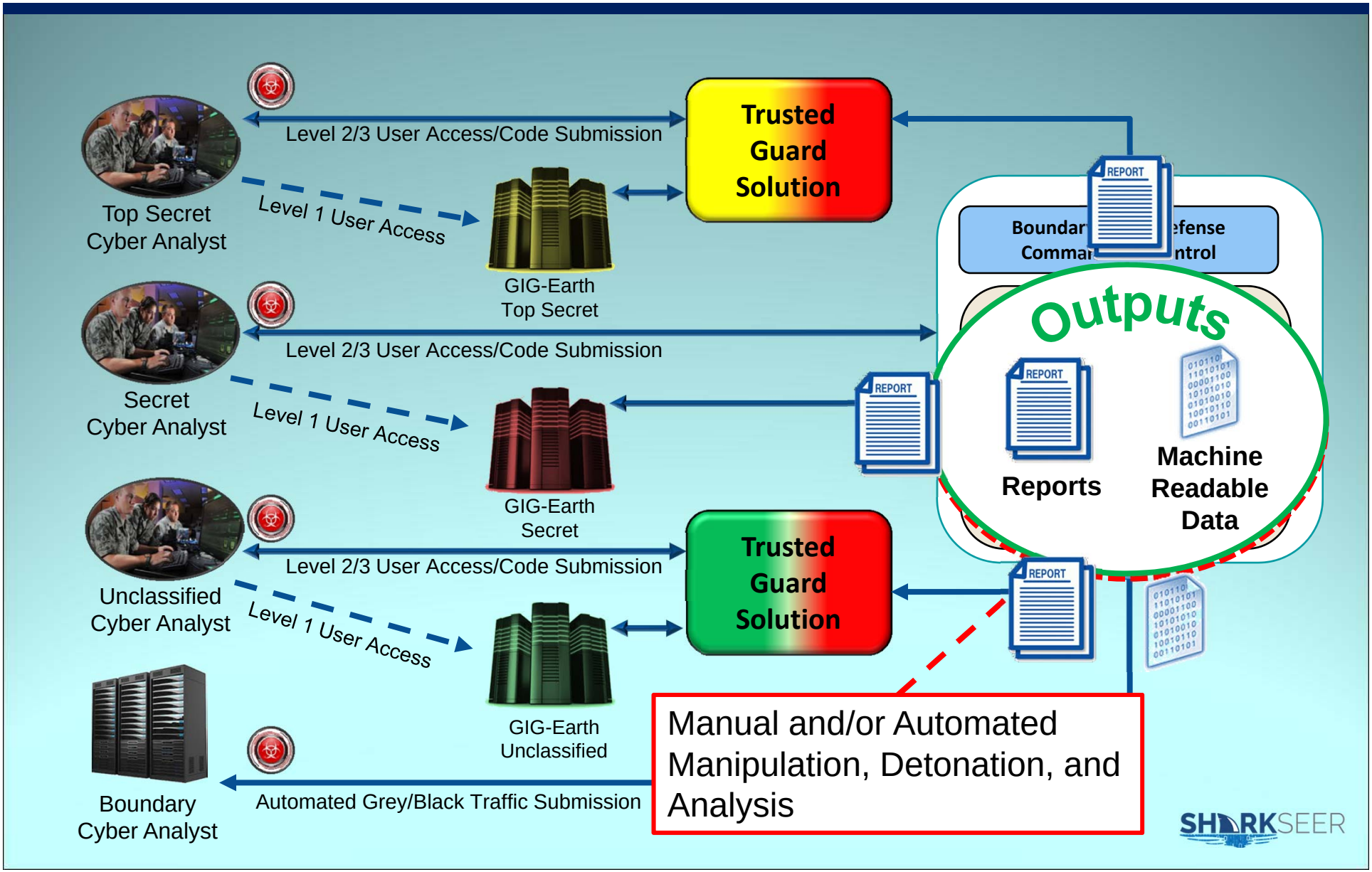
Outputs

Event (Mitigation/Remediation)	Team (Discovery/Authoring)	Cyber SA (Sharing/Dissemination)

Customers

SHARKSEER

SHARKSEER Sandbox Environment



Stakeholders & Partnerships

Enhanced Shared Situational Awareness (ESSA)

Comprehensive National Cybersecurity Initiative (CNCI)

SHARKSEER

Power Of Partnership

Cyber Alliances: Collective Defense Becomes Central To Securing Networks, Data - Forbes

Forbes http://onforb.es/1plyuGs

Loren Thompson Contributor

I write about national security, especially its business dimensions.

Opinions expressed by Forbes Contributors are their own.

WASHINGTON 9/19/2014 @ 11:06AM | 3,666 views

Cyber Alliances: Collective Defense Becomes Central To Securing Networks, Data

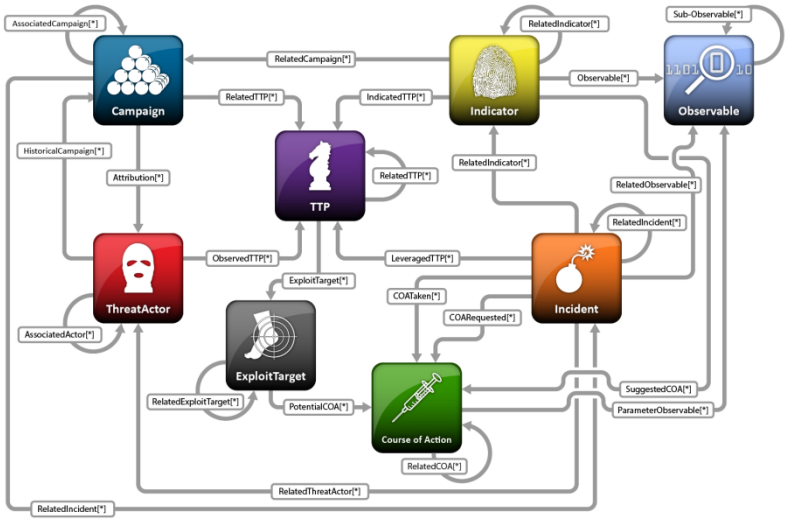
Comment Now

When the North Atlantic Treaty Organization — NATO — wrapped up its summit in Wales earlier this month, the member-states issued a lengthy communique expressing solidarity on major defense challenges. One of the challenges mentioned was cybersecurity. The alliance stated that "cyber defence is part of NATO's core task of collective defence," presenting concerns so severe that they might lead to invocation of Article Five of the North Atlantic Treaty — the article calling on all members to come to the defense of a threatened nation. The communique went on to stress that "strong partnerships play a key role in addressing cyber threats and risks," and committed alliance members to intensified cooperation in pursuit of integrated solutions.

It isn't hard to see why NATO is worried about threats in cyberspace, given Russia's recent use of on-line attacks against Ukraine and other countries in a style of combat that has come to be called "hybrid warfare." However, a

McAfee and Symantec — the nation's two biggest cybersecurity firms — agreed to join a Cyber Threat Alliance founded in May by Fortinet and Palo Alto Networks. The goal of the new consortium, quoting a white paper it issued, is "to disperse threat intelligence on advanced adversaries across all member organizations to raise the overall situational awareness in order to better protect their organizations and their customers."

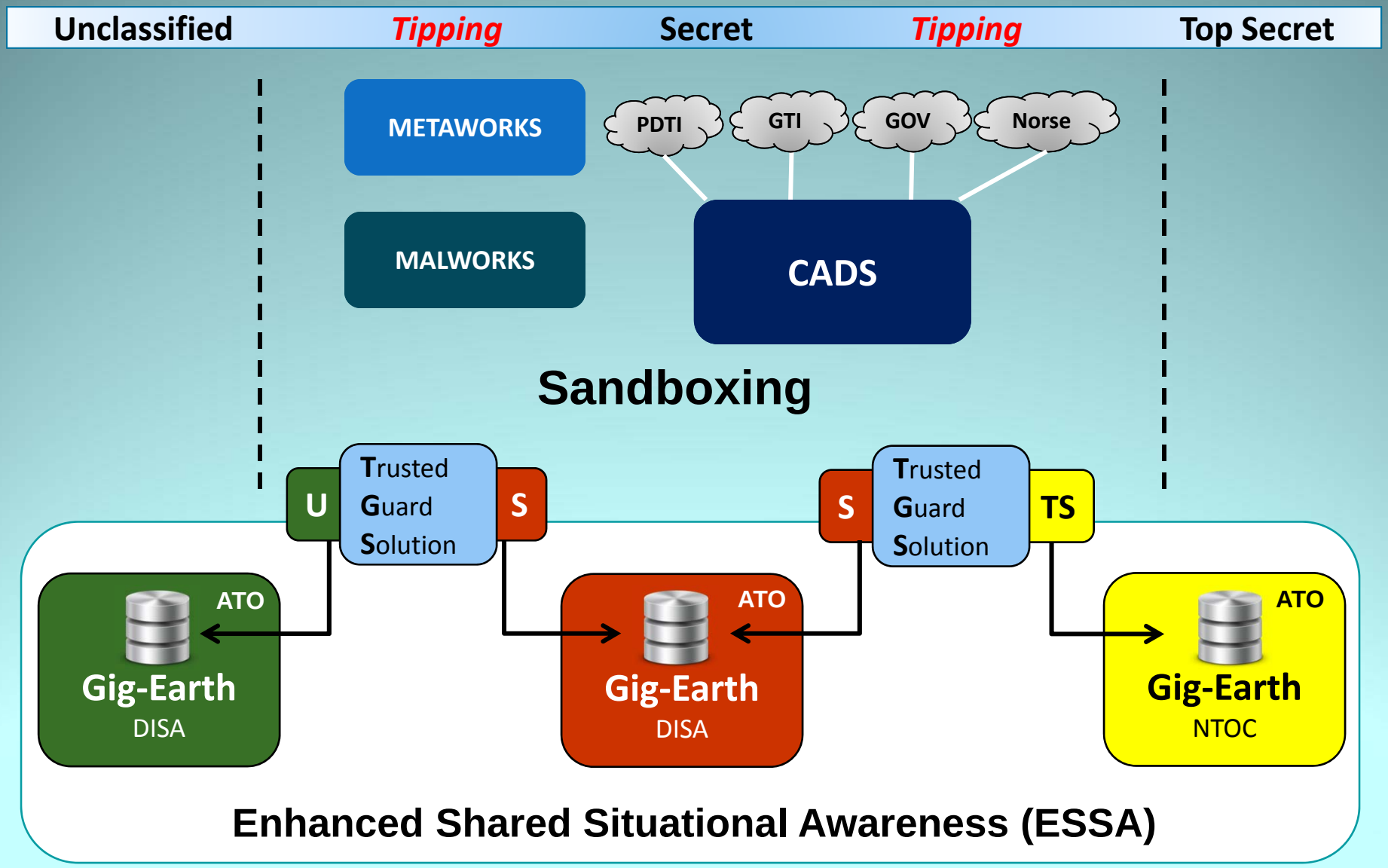
Structured Threat Information eXpression (STIX) v1.1 Architecture



Shared Threat Data

- **STIX - Structured Treat Information eXpression**
- **MAEC –Malware Attribute Enumeration and Characterization**
- **TAXII - Trusted Automated eXchange of Indicator Information**

SHARKSEER Cyber Environment



This document is from the holdings of:

The National Security Archive

Suite 701, Gelman Library, The George Washington University

2130 H Street, NW, Washington, D.C., 20037

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu