CASCADE

Joint Cyber Sensor Architecture

[redacted]

Overview

- Project Overview
- Current Status
- Proposed Architecture
- Towards 2015

Project Overview

- Alignment of passive cyber sensor capabilities and architecture in the SIGINT and ITS missions
- Goals
  - Common sensor technology and architecture
  - Address scalability issues in sensor deployments
- Scope
  - Passive sensors and supporting infrastructure are in scope
  - Analytic tools are out of scope
  - Host based capability is out of scope (caveat: passive messaging is in scope)

Our Sensors

SIGINT / ITS

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Photonic Prism

- Monitoring of GC Networks
- Includes:
  - Full-Take Packet Capture
  - Signature Based Detection
  - Anomaly Based Discovery
  - Analytic Environment
  - Oversight Compliance Tools

EONBLUE

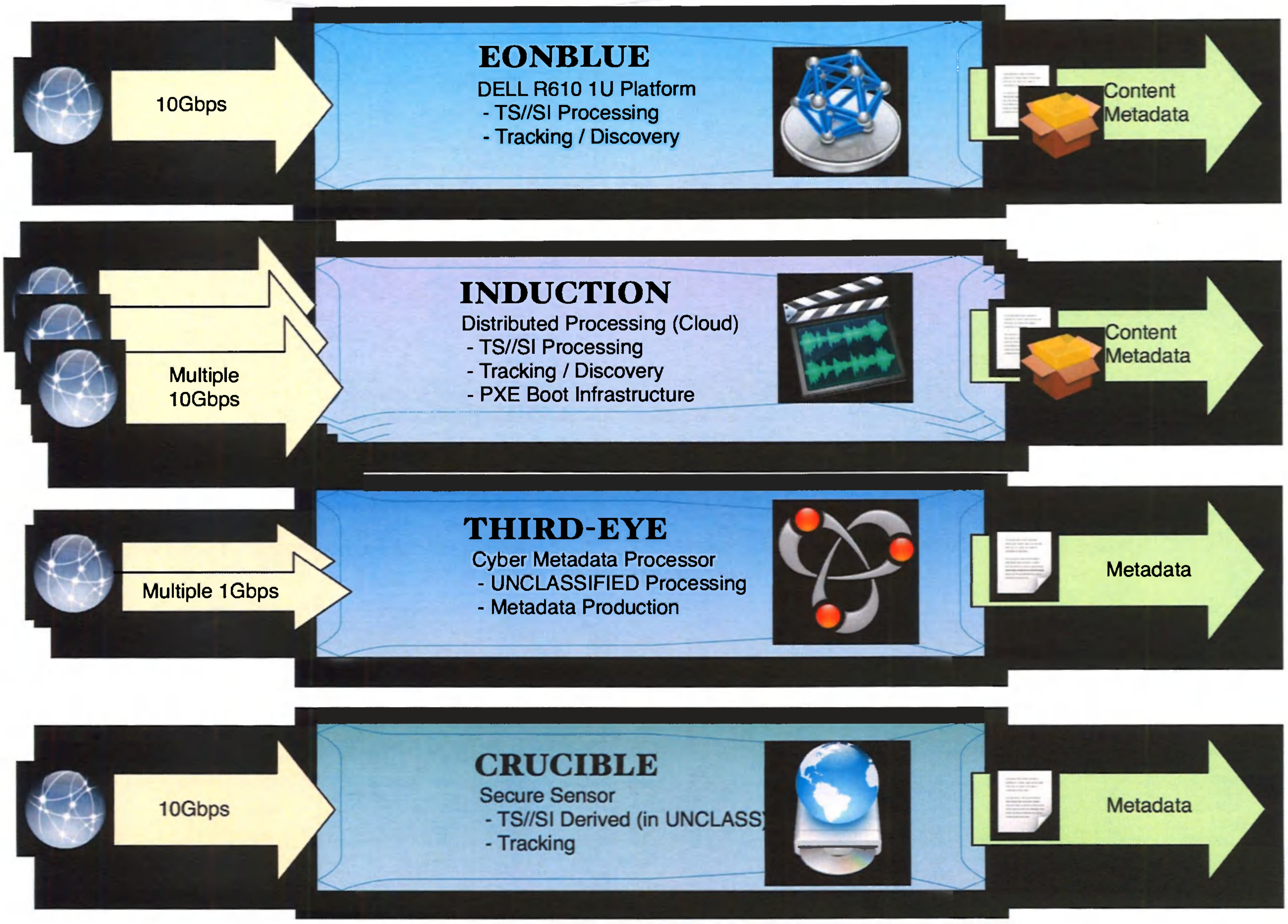
- Monitoring in Passive SIGINT
- Includes:
  - Full-Take (on specific accesses)
  - Signature Based Detection
  - Anomaly Based Discovery
- Additional Functions are offloaded and exist further downstream:
  - Analytic Environment
  - Dataflow / Targeting
  - Oversight and Compliance Tools

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Shades of Blue

Cyber Defence Operations



10Gbps

EONBLUE
DELL R610 1U Platform
- TS//SI Processing
- Tracking / Discovery

Content Metadata

Multiple 10Gbps

INDUCTION
Distributed Processing (Cloud)
- TS//SI Processing
- Tracking / Discovery
- PXE Boot Infrastructure

Content Metadata

Multiple 1Gbps

THIRD-EYE
Cyber Metadata Processor
- UNCLASSIFIED Processing
- Metadata Production

Metadata

10Gbps

CRUCIBLE
Secure Sensor
- TS//SI Derived (in UNCLASS)
- Tracking

Metadata

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Current Status – SIGINT Deployments

- Special Source
  - 100% INDUCTION coverage of main SSO sites + metadata production
  - THIRD-EYE metadata production at select new sites
  - CRUCIBLE deployments to newly emerging sites pre-SCIF environment (survey)
  - Increase in link speeds
- Warranted Collection
  - EONBLUE sensor deployment – full take collection
- FORNSAT
  - Recently upgraded to current EONBLUE code base, leveraging GCHQ CHOKEPOINT solution to integrate with environment (Virtualized)
- Working on SUNWHEEL / SMO
  - CHOKEPOINT system enroute to CASSIOPEIA
  - No SUNWHEEL presence as of yet, plans to leverage CHOKEPOINT capability

Current Status – IT Security Deployments

- Deployment at 3 edge gateway GC departments
  - Dynamic defence is enabled at two of these sites

- Deployment at the main government backbone
  - Dual 10Gbps links (~3Gbps loading)
  - Data volumes continue to increase due to Internet Access Point aggregation

- Currently performing full take and storage of all monitored traffic
  - System performance issues, overall analyst usability issues

Divergence – Sensor Deployments

- While both ITS/SIGINT currently leverage EONBLUE software:
  - The architectures are not aligned
  - Configuration differs greatly
  - Software versions are not standard across programs
  - The full capability of EONBLUE is not being leveraged equally across programs

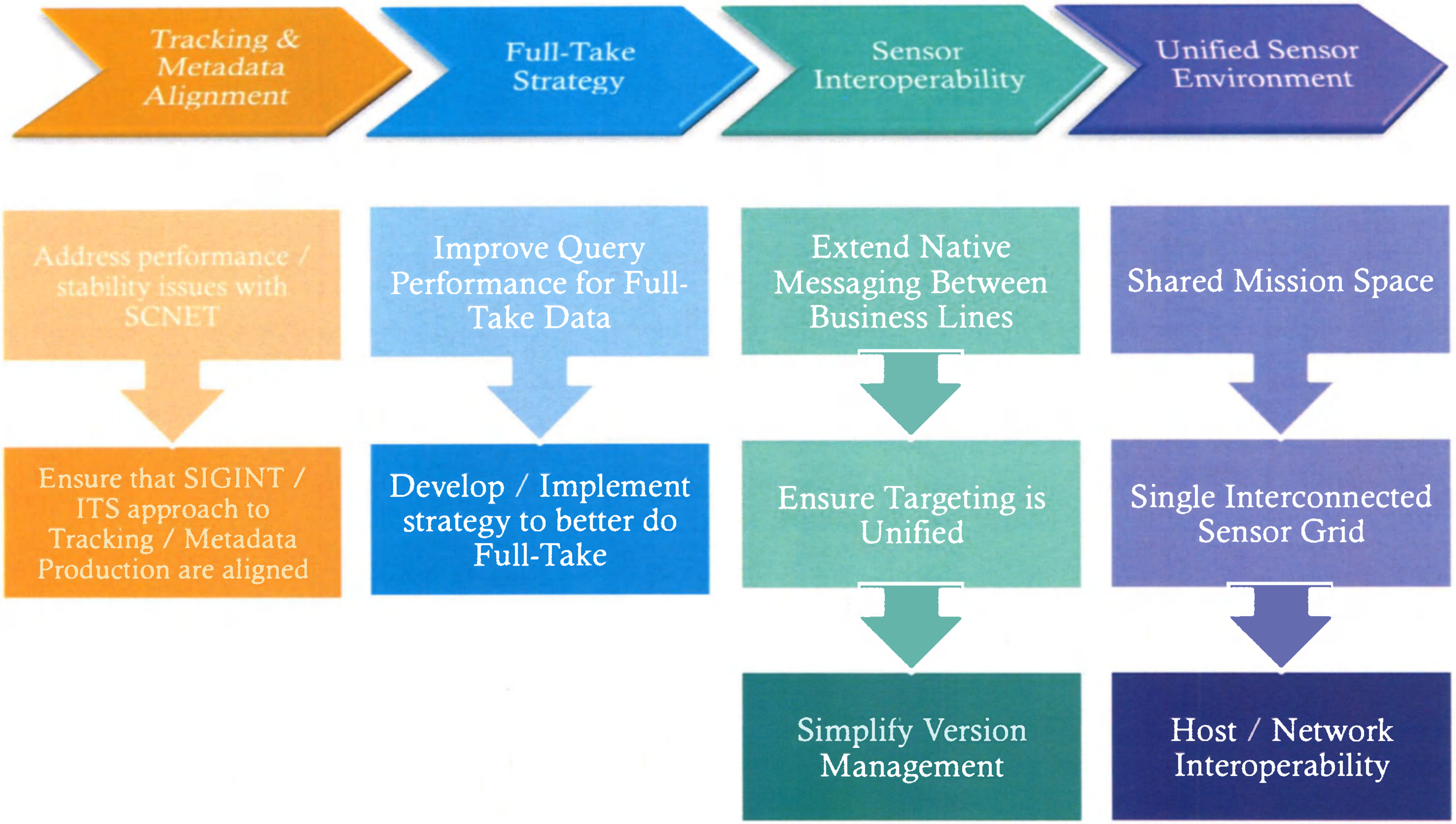
Proposal

CASCADE: A Way Forward

Problem Statement

- Divergence
  - Sensor architectures have diverged between ITS/SIGINT
  - Within each area, versions are not standardized
- Management and Scalability
  - Some configurations will not scale
  - Difficult to manage current sensor environment
  - High cost to grow existing solution (people, HW/SW costs)
- Duplication of Effort
  - Divergence creates duplication of effort
  - Limited resources are not focused on innovation and new challenges

A Phased Approach



Tracking & Metadata Alignment

Address performance / stability issues with SCNET

Ensure that SIGINT / ITS approach to Tracking / Metadata Production are aligned

Full-Take Strategy

Improve Query Performance for Full-Take Data

Develop / Implement strategy to better do Full-Take

Sensor Interoperability

Extend Native Messaging Between Business Lines

Ensure Targeting is Unified

Simplify Version Management

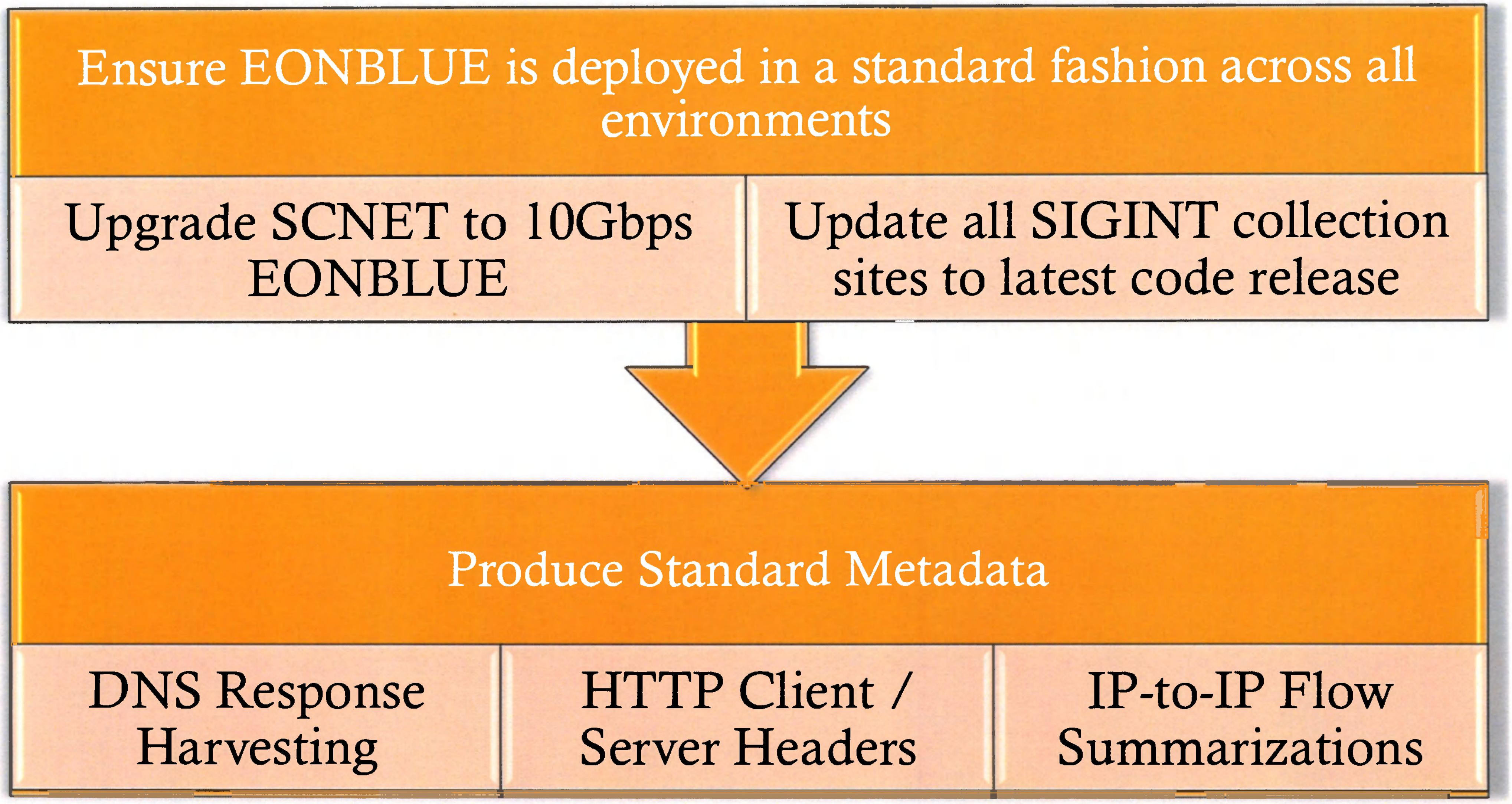
Unified Sensor Environment

Shared Mission Space

Single Interconnected Sensor Grid

Host / Network Interoperability

Tracking and Metadata



Ensure EONBLUE is deployed in a standard fashion across all environments

Upgrade SCNET to 10Gbps EONBLUE

Update all SIGINT collection sites to latest code release

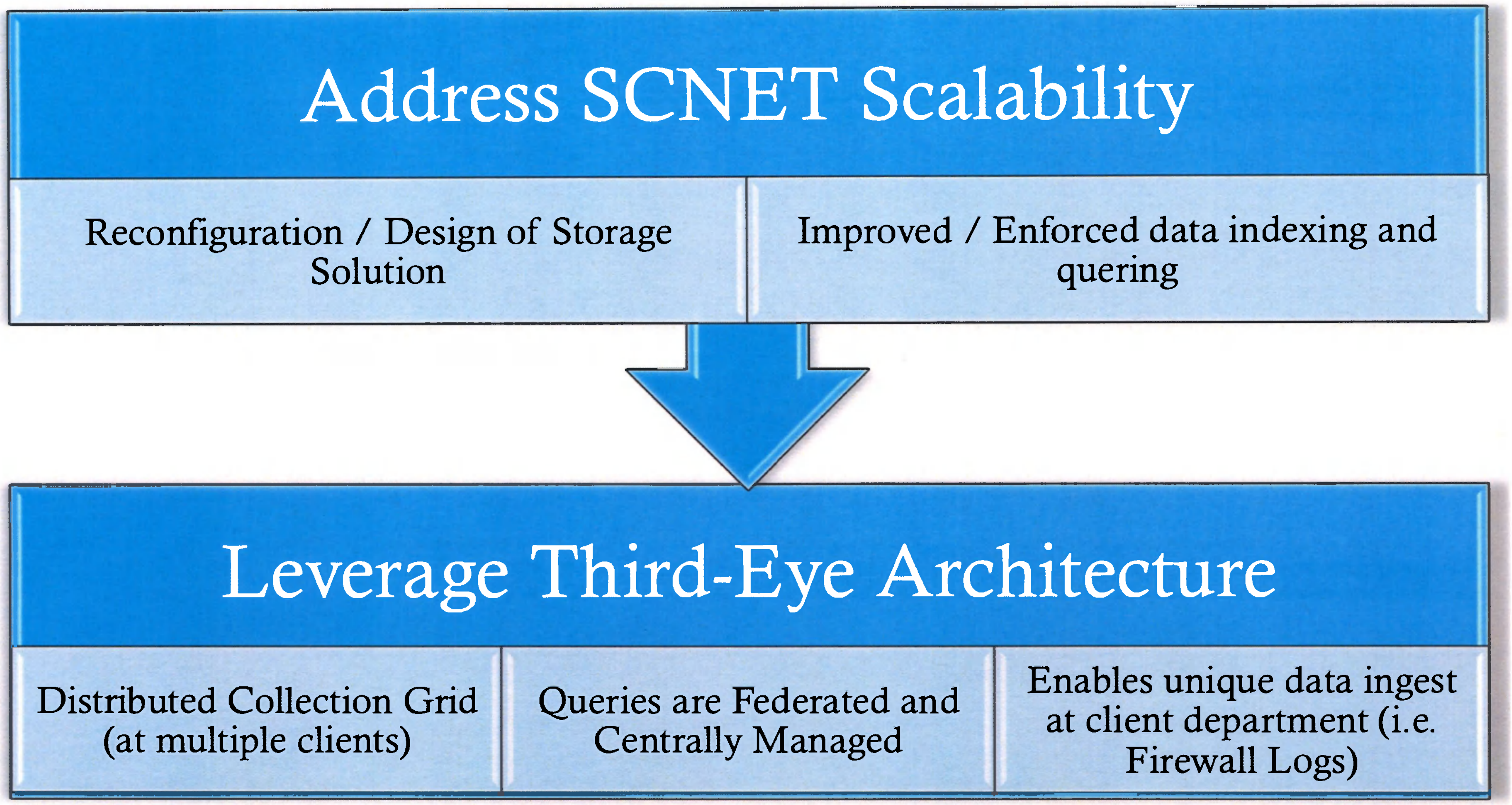
Produce Standard Metadata

DNS Response Harvesting

HTTP Client / Server Headers

IP-to-IP Flow Summarizations

Full-Take Strategy



Address SCNET Scalability

Reconfiguration / Design of Storage Solution

Improved / Enforced data indexing and quering

Leverage Third-Eye Architecture

Distributed Collection Grid (at multiple clients)

Queries are Federated and Centrally Managed

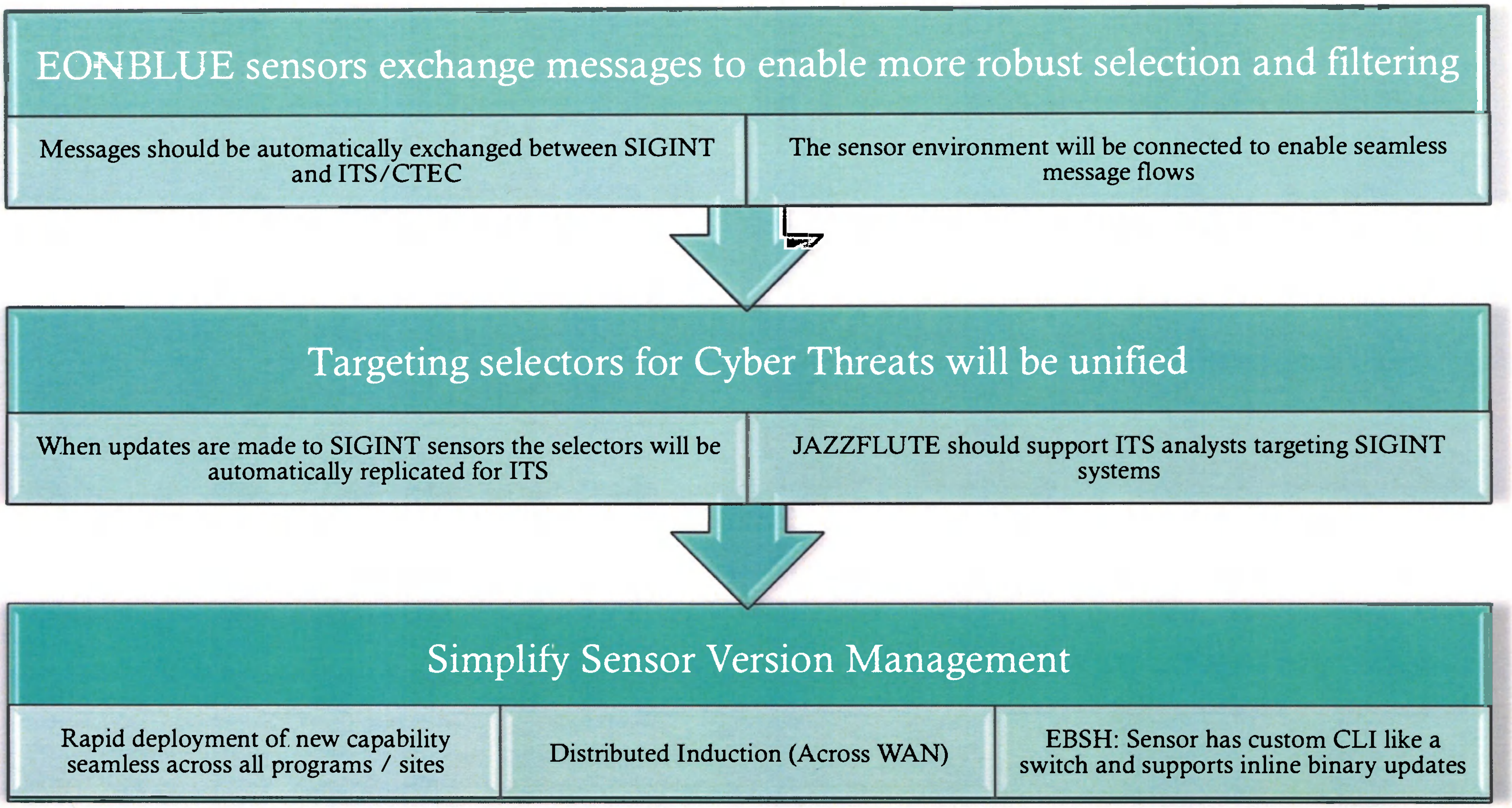
Enables unique data ingest at client department (i.e. Firewall Logs)

Full-Take Strategy

- Benefits
  - Improve Performance
    - Better data indexing techniques
    - Federated queries across multiple systems
  - Reduced Cost (Storage local to client departments)
    - 10,000$ -> 25,000$ per client
    - Re-use of back-end Storage
  - Enable departmental security officers / operators
    - Capability of Third-Eye exceeds what is commercially available

- Cons
  - Requires network connections to each GC Department
  - Requires footprint within each departments datacenter
  - Complexity of distributed processing

Sensor Interoperability



EONBLUE sensors exchange messages to enable more robust selection and filtering

Messages should be automatically exchanged between SIGINT and ITS/CTEC

The sensor environment will be connected to enable seamless message flows

Targeting selectors for Cyber Threats will be unified

When updates are made to SIGINT sensors the selectors will be automatically replicated for ITS

JAZZFLUTE should support ITS analysts targeting SIGINT systems

Simplify Sensor Version Management

Rapid deployment of new capability seamless across all programs / sites

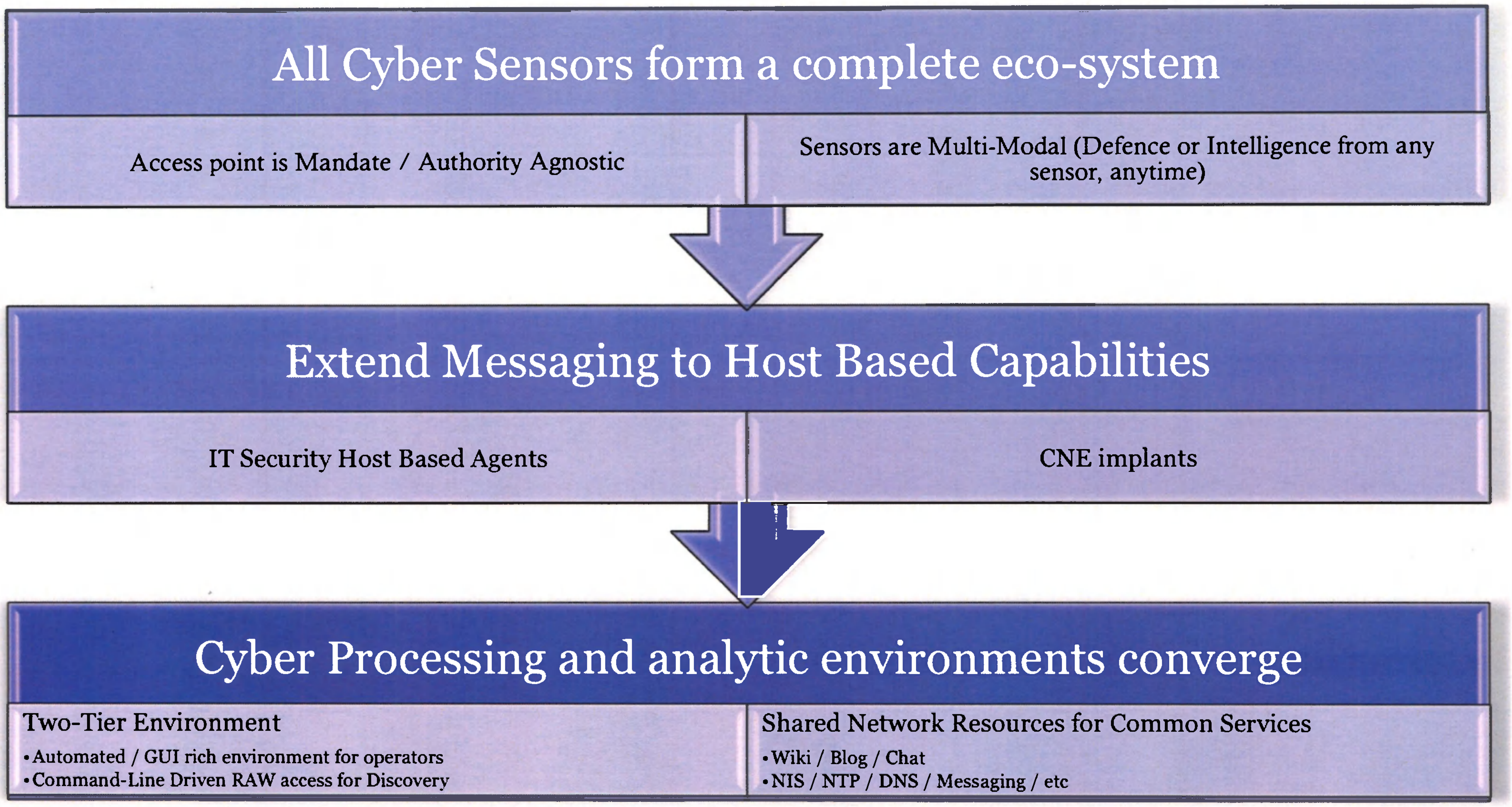
Distributed Induction (Across WAN)

EBSH: Sensor has custom CLI like a switch and supports inline binary updates

Interoperability enables Synchronization

- ITS access to data collected by SIGINT sensors
  - Outputs should be common to enable a common analyst platform
  - Sensor environment should be seamlessly integrated
- Capability remains at cutting-edge
  - Single release for all collection programs in SIGINT, all points of presence, and across both missions
  - Management is simplified for operators, focusing on sensor expansions
  - Standardized OS Versions and Optimizations

Unified Sensor Environment



All Cyber Sensors form a complete eco-system

Access point is Mandate / Authority Agnostic

Sensors are Multi-Modal (Defence or Intelligence from any sensor, anytime)

Extend Messaging to Host Based Capabilities

IT Security Host Based Agents

CNE implants

Cyber Processing and analytic environments converge

Two-Tier Environment

- Automated / GUI rich environment for operators
- Command-Line Driven RAW access for Discovery

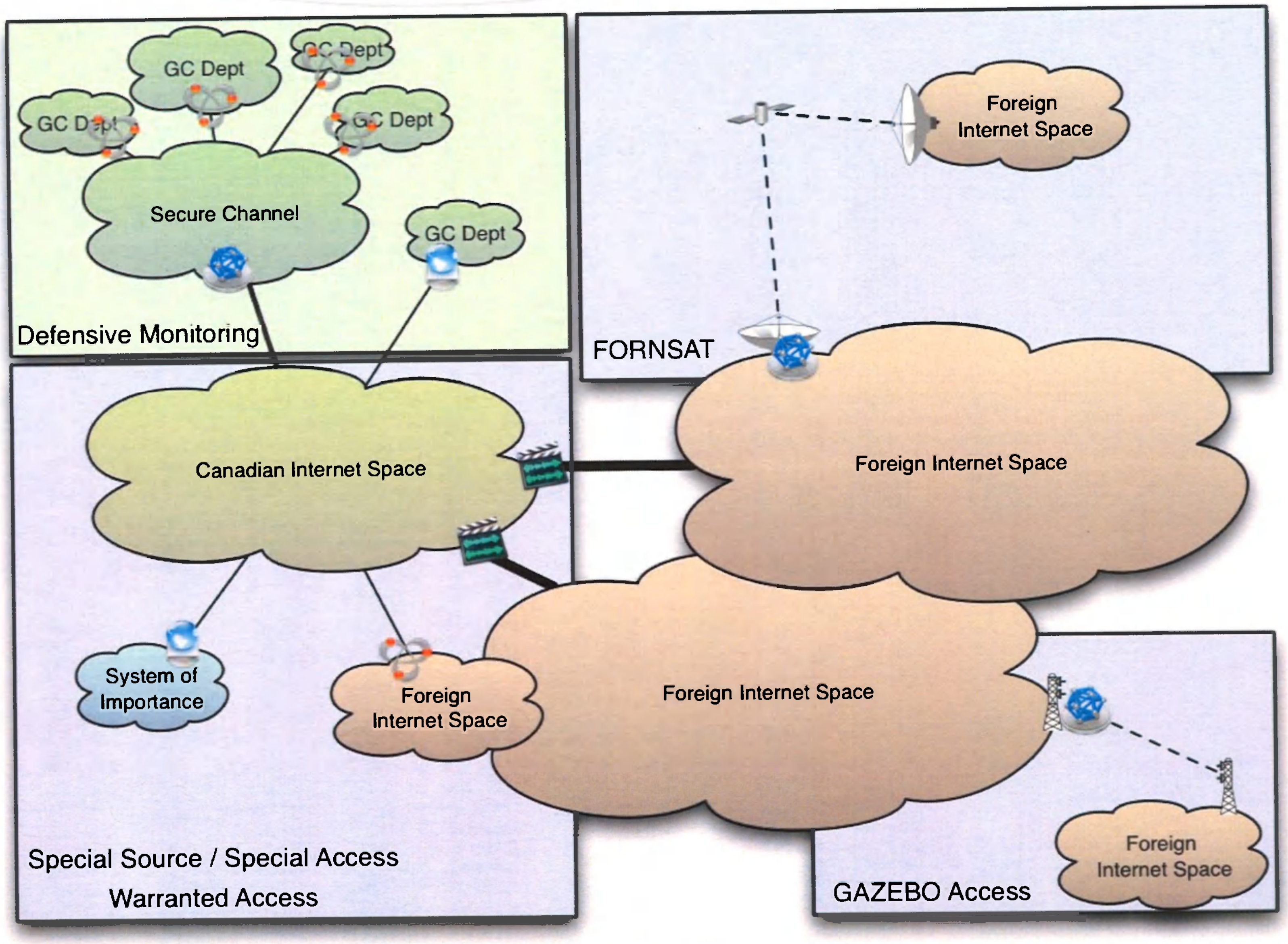
Shared Network Resources for Common Services

- Wiki / Blog / Chat
- NIS / NTP / DNS / Messaging / etc

Synchronized Deployment Strategy

- Where do you deploy sensors to maximize detection capabilities for Foreign Intelligence collection and Network Defence
- Coverage-based deployment considerations – what are the gaps?
  - [redacted]
  - [redacted]
  - [redacted]
- Threat-based deployment considerations – what are the gaps?
  - Based on EPRs
  - Threat trends and forecasting reports
  - Adversary TTPs

Canadian Cyber Sensor Grid



Towards 2015

Beyond sensor unification

CSEC 2015

- Strategic Priorities for CSEC
  - Strengthen "Team CSEC" and Prepare for Our New Facility
  - Adopt Innovative and Agile Business Solutions
  - **Expand Our Access Footprint**
  - **Improve Analytic Tradecraft**
  - Automate Manual Processes
  - **Synchronize the Cryptologic Enterprise for Cyber Security Mission**
  - **Enable "Effects" for Threat Mitigation**

Cyber Sensor in 2015

- **Expand Our Access Footprint**
  - We will increase SPECIAL SOURCE access to include all international gateways accessible from Canada.
  - We will deploy a sensor system that creates a protective grid at multiple layers over Government operations in Canada, and at all classification levels.
- **Improve Analytic Tradecraft**
  - We will equip SIGINT and cyber defence analysts with tools for flexible manipulation and customized analysis of large scale data sets.
  - We will build analytic tradecraft that understands, anticipates, and exploits the methodology of threat agents to provide comprehensive cyber- situational awareness based on multiple sources of cryptologic data.

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Cyber Sensor in 2015

- **Synchronize the Cryptologic Enterprise for the Cyber Security Mission**
  - We will improve how we anticipate, identify, track and mitigate cyber threats on government systems through new concepts of joint operations.
  - We will design and develop joint SIGINT-ITS systems, including common data repositories, joint tasking and analytic systems.
  - We will increase operational capacity by ensuring SIGINT, ITS, and cryptologic partner sensors interoperate seamlessly.
  - We will synchronize and use ITS and SIGINT capabilities and complementary analyses to thwart cyber threats.

- **Enable "Effects" for Threat Mitigation**
  - We will seek the authority to conduct a wide spectrum of Effects operations in support of our mandates.
  - We will build the technical infrastructure, policy architecture and tradecraft necessary to conduct Effects operations.
  - We will further integrate ITS and SIGINT authorities and operations to leverage common sensors, systems and capabilities necessary for active and expanded dynamic cyber defence measures.

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

The Network Is The Sensor

Principles

Security needs to be transparent to the user in order to be effective

Security is a right for all Canadians
- Federal Government
- Municipal / Provincial Gov
- Critical Infrastructure
- Industry
- The Citizen

End-Users should incur little cost for security

IT Assets should be distributed

Access is mandate / authority agnostic

Goals

Detect threats as they enter our national networks, not at the Gateway

Identify Exfiltration, Command and Control, anywhere in our national networks

The network is your defence for all infrastructure

Rationale

We can't keep pace with our adversary

Gateway / Device / End-Node protection is not sufficient (essential, yes)

Rather than plugging one hole at a time, build better layered defence

Principles Explained

- Security is Transparent
  - If security inhibits functionality, or interferes with user experience it will be bypassed
- Security is a right
  - Attempting to protect everybody with end-node / gateway defenses is not feasible.
- IT Assets should be distributed
  - We run an open market, network providers will compete to provide access
  - Consolidated gateways creates single points of failure
  - Cost / Redundancy considerations

Goals

- Detection before attack hits target
  - If we wish to enable defence we must have intelligence to know when attacks enter our national infrastructure
- Identify Exfiltration / Command and Control
  - Some attacks will slip through or can't be seen (i.e. shaping)
  - Exploit our temporal advantage - aggressively pursue these implants as they will communicate 'home' for instruction
- The Network IS your Defence
  - In some cases, in cooperation with our partners we can affect change at the CORE of the Internet on detection:
    - Modify traffic routes
    - Silently discard malicious traffic (hygiene filtering)
    - Insert payload to disrupt adversaries

Rationale

- Keeping pace with the Adversary
  - From the time a malicious PDF is opened, till SEEDSPHERE has interactive control of a workstation is <3 minutes
  - There are countless malicious actors (state, crime, generic malware)
- Gateway / End-Node Defence by itself is insufficient
  - It is only one part of the problem
  - Over 600,000 Apps in the iTunes Appstore (How do you secure that?)
  - Defence in Depth includes network monitoring, and network interaction
- Build better Defence
  - Our current MO is to resolve one incident at a time
  - Automate the defence through a robust network capable of not only detection, but manipulation of malicious traffic

What does it Mean?

- EONBLUE will be integrated into the Network
  - Monitoring Government of Canada
  - Monitoring Core Infrastructure (Special Source) extending the reach to view national infrastructure
  - Monitoring foreign Internet Space
- EONBLUE will enable defensive operations
  - Through robust communication with host-based capabilities
  - Through direct manipulation of network communications
  - Through interaction with Teleco infrastructure to affect change

Food for Thought

Changing the way we think

Changing the way we think

- Tipping and Cueing
  - If the purpose is to enable defence of national infrastructure it becomes unnecessary in a 5-eyes context
    - We have full visibility of our national infrastructure
    - The chance of ‘beating’ the internet for latency of an attack is minimal
    - The network will perform the filtering
  - What if instead T&C enables intelligence collection (Cyber Session Collection)?

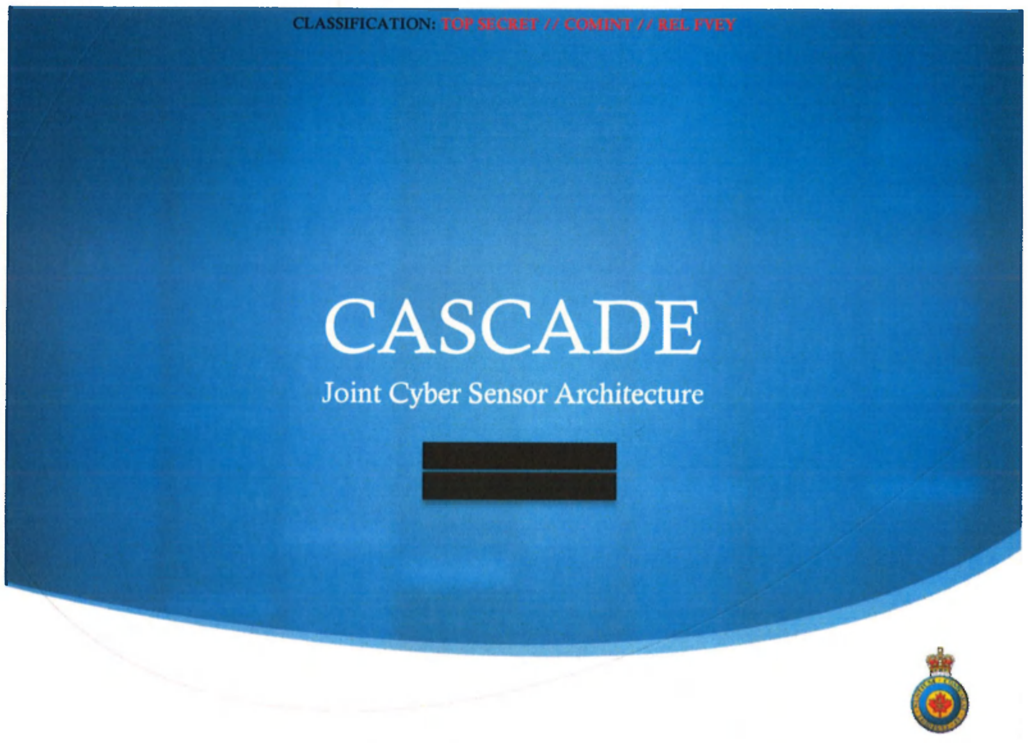
- Targeting and Tasking
  - We all share common targets and we will all target using our national capability the cyber threats we know about
  - No need for 2nd party tasking / targeting requests. Instead expose cyber information across the community
  - What if instead we focus on analytic collaboration and knowledge transfer
    - TEXPRO information, federated repositories (malware/traffic), etc

Changing the way we think

- Foreign SIGINT Intercept
  - Becomes the ‘hunting ground’ for discovery of new threats
  - Enables attribution and counter-intelligence reporting
  - Defence is taken care of by ‘The Network’
  - Mobile Platforms are the next frontier, what is their implication on Cyber?
- Domestic Defence
  - We will exhaust the treasury deploying network appliances to perform dynamic defence
  - The same capabilities will be integrated into the CORE of the Internet
  - Defence in Depth through complimentary capabilities on end-nodes, at the gateway, and in the core of the Internet.

Conclusion

- CASCADE
  - The harmonization of ITS/SIGINT Sensor capabilities
  - Lays the foundation for long-term integration of Cyber within the Cryptologic Enterprise
- Towards 2015
  - The Network is the Sensor
    - Defence, Mitigation, Intelligence all formed from a single comprehensive network creating a perimeter around Canada
    - Extending our reach through 5-eyes partnerships to ensure mutual defence of national assets.



CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

CASCADE

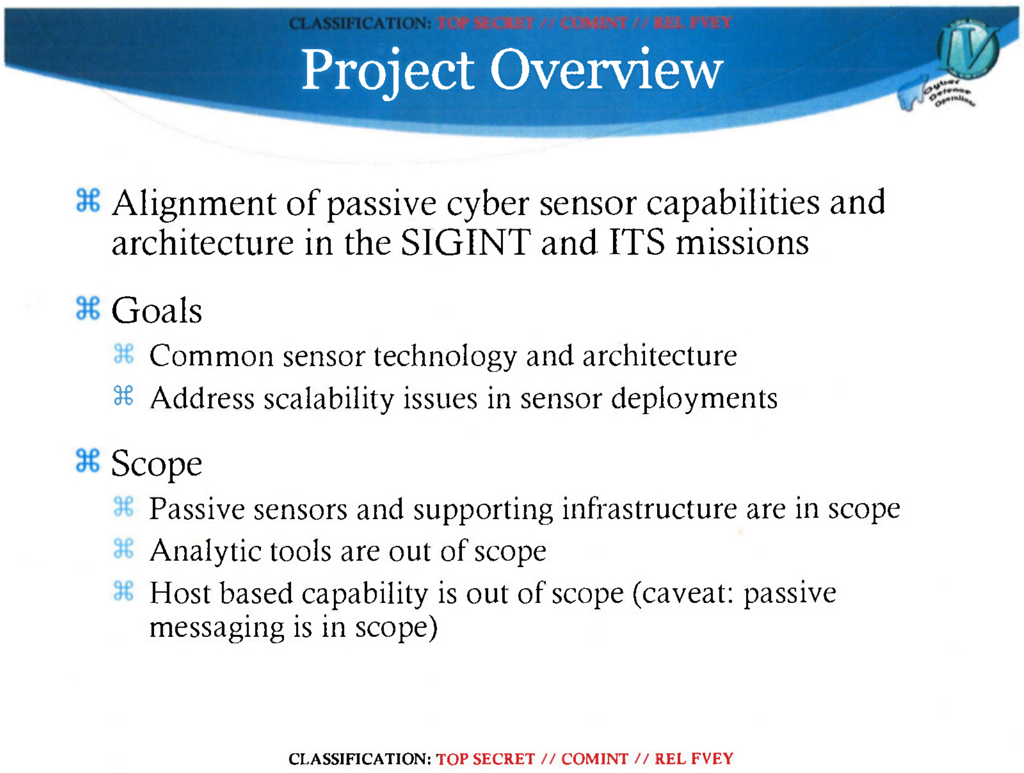
Joint Cyber Sensor Architecture

[redacted]

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Overview

- Project Overview
- Current Status
- Proposed Architecture
- Towards 2015



CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Project Overview

- Alignment of passive cyber sensor capabilities and architecture in the SIGINT and ITS missions
- Goals
  - Common sensor technology and architecture
  - Address scalability issues in sensor deployments
- Scope
  - Passive sensors and supporting infrastructure are in scope
  - Analytic tools are out of scope
  - Host based capability is out of scope (caveat: passive messaging is in scope)

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

What is the project about?
Define the goal of this project

Is it similar to projects in the past or is it a new effort?

Define the scope of this project

Is it an independent project or is it related to other projects?

* Note that this slide is not necessary for weekly status meetings

Our Sensors

SIGINT / ITS

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Photonic Prism

- Monitoring of GC Networks
- Includes:
  - Full-Take Packet Capture
  - Signature Based Detection
  - Anomaly Based Discovery
  - Analytic Environment
  - Oversight Compliance Tools

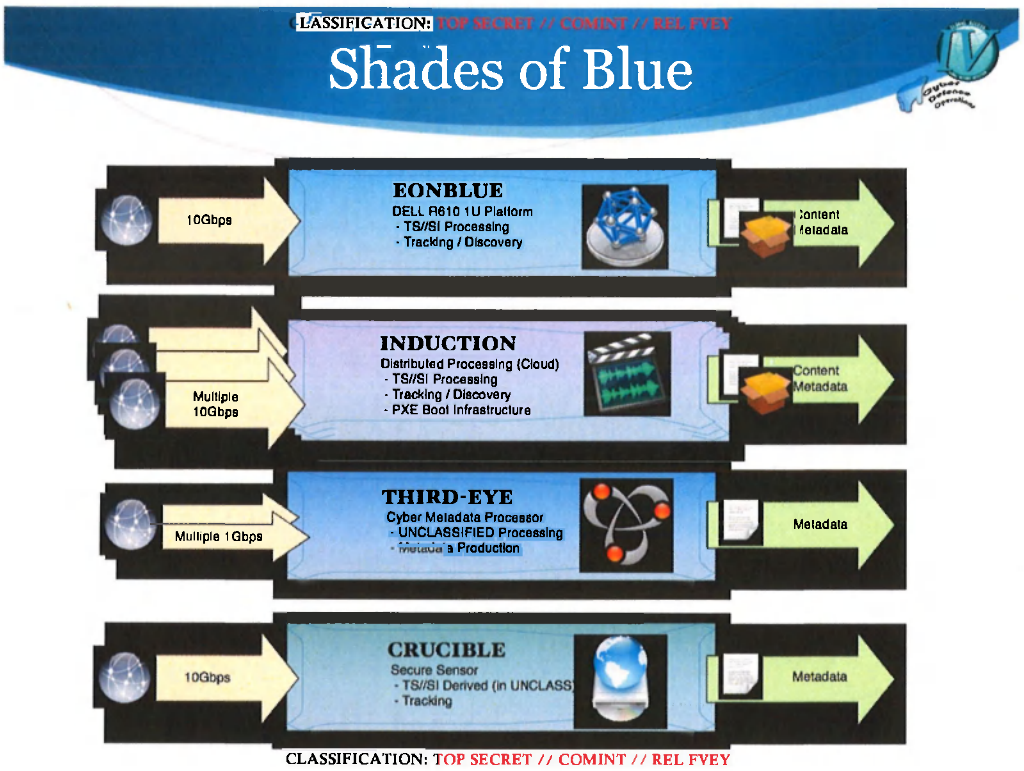
EONBLUE

- Monitoring in Passive SIGINT
- Includes:
  - Full-Take (on specific accesses)
  - Signature Based Detection
  - Anomaly Based Discovery
- Additional Functions are offloaded and exist further downstream:
  - Analytic Environment
  - Dataflow / Targeting
  - Oversight and Compliance Tools

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Shades of Blue



10Gbps

EONBLUE
DELL R610 1U Platform
- TS//SI Processing
- Tracking / Discovery

Content Metadata

Multiple 10Gbps

INDUCTION
Distributed Processing (Cloud)
- TS//SI Processing
- Tracking / Discovery
- PXE Boot Infrastructure

Content Metadata

Multiple 1Gbps

THIRD-EYE
Cyber Metadata Processor
- UNCLASSIFIED Processing
- Metadata Production

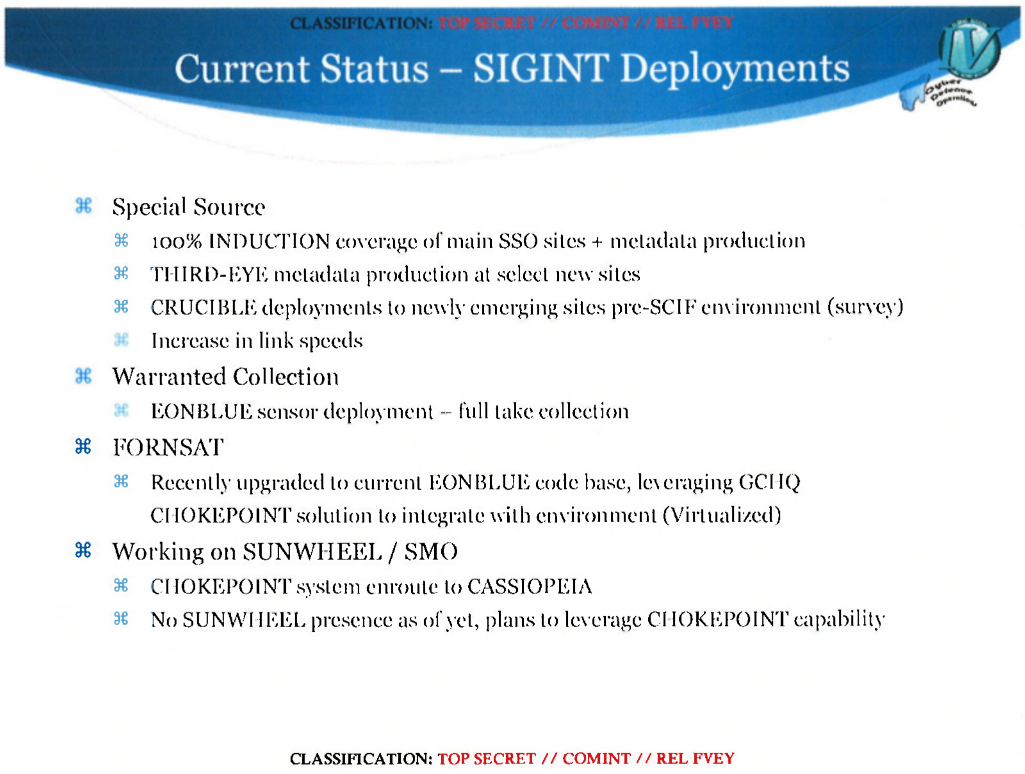
Metadata

10Gbps

CRUCIBLE
Secure Sensor
- TS//SI Derived (in UNCLASS)
- Tracking

Metadata

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY



CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Current Status – SIGINT Deployments

- Special Source
  - 100% INDUCTION coverage of main SSO sites + metadata production
  - THIRD-EYE metadata production at select new sites
  - CRUCIBLE deployments to newly emerging sites pre-SCIF environment (survey)
  - Increase in link speeds
- Warranted Collection
  - EONBLUE sensor deployment – full take collection
- FORNSAT
  - Recently upgraded to current EONBLUE code base, leveraging GCHQ CHOKEPOINT solution to integrate with environment (Virtualized)
- Working on SUNWHEEL / SMO
  - CHOKEPOINT system enroute to CASSIOPEIA
  - No SUNWHEEL presence as of yet, plans to leverage CHOKEPOINT capability

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

* If any of these issues caused a schedule delay or need to be discussed further, include details in next slide.

[redacted]

Current Status – IT Security Deployments

- Deployment at 3 edge gateway GC departments
  - Dynamic defence is enabled at two of these sites
- Deployment at the main government backbone
  - Dual 10Gbps links (~3Gbps loading)
  - Data volumes continue to increase due to Internet Access Point aggregation
- Currently performing full take and storage of all monitored traffic
  - System performance issues, overall analyst usability issues

Divergence – Sensor Deployments

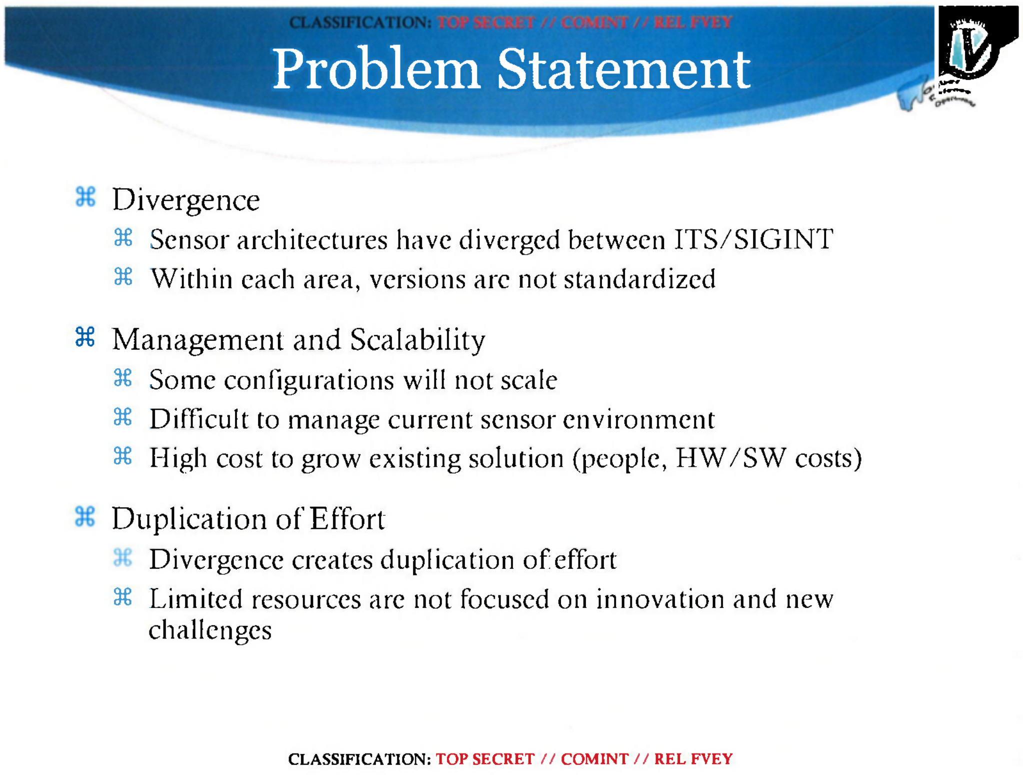
- While both ITS/SIGINT currently leverage EONBLUE software:
  - The architectures are not aligned
  - Configuration differs greatly
  - Software versions are not standard across programs
  - The full capability of EONBLUE is not being leveraged equally across programs

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Proposal

CASCADE: A Way Forward

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY



CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Problem Statement

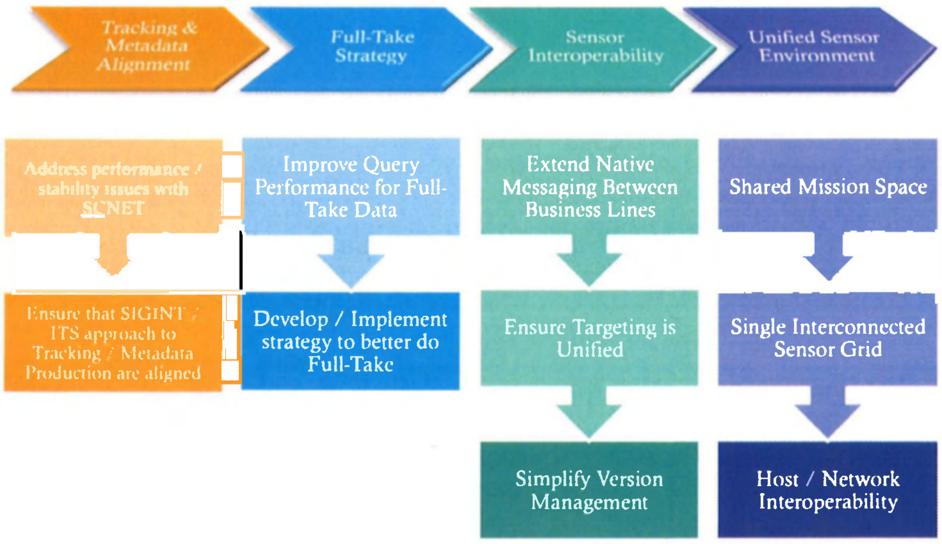
- Divergence
  - Sensor architectures have diverged between ITS/SIGINT
  - Within each area, versions are not standardized
- Management and Scalability
  - Some configurations will not scale
  - Difficult to manage current sensor environment
  - High cost to grow existing solution (people, HW/SW costs)
- Duplication of Effort
  - Divergence creates duplication of effort
  - Limited resources are not focused on innovation and new challenges

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Duplicate this slide as necessary if there is more than one issue.
This and related slides can be moved to the appendix or hidden if necessary.

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

A Phased Approach



Tracking & Metadata Alignment

Address performance / stability issues with SCNET

Ensure that SIGINT / ITS approach to Tracking / Metadata Production are aligned

Full-Take Strategy

Improve Query Performance for Full-Take Data

Develop / Implement strategy to better do Full-Take

Sensor Interoperability

Extend Native Messaging Between Business Lines

Ensure Targeting is Unified

Simplify Version Management

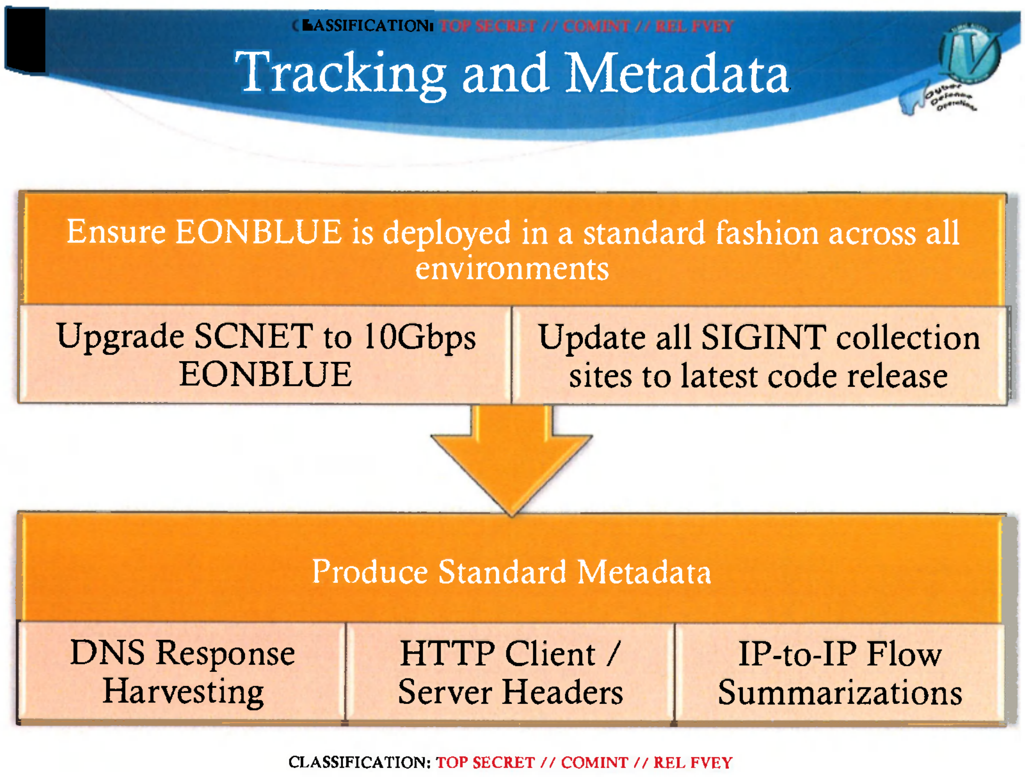
Unified Sensor Environment

Shared Mission Space

Single Interconnected Sensor Grid

Host / Network Interoperability

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY



[redacted]

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Tracking and Metadata

Ensure EONBLUE is deployed in a standard fashion across all environments

Upgrade SCNET to 10Gbps EONBLUE

Update all SIGINT collection sites to latest code release

Produce Standard Metadata

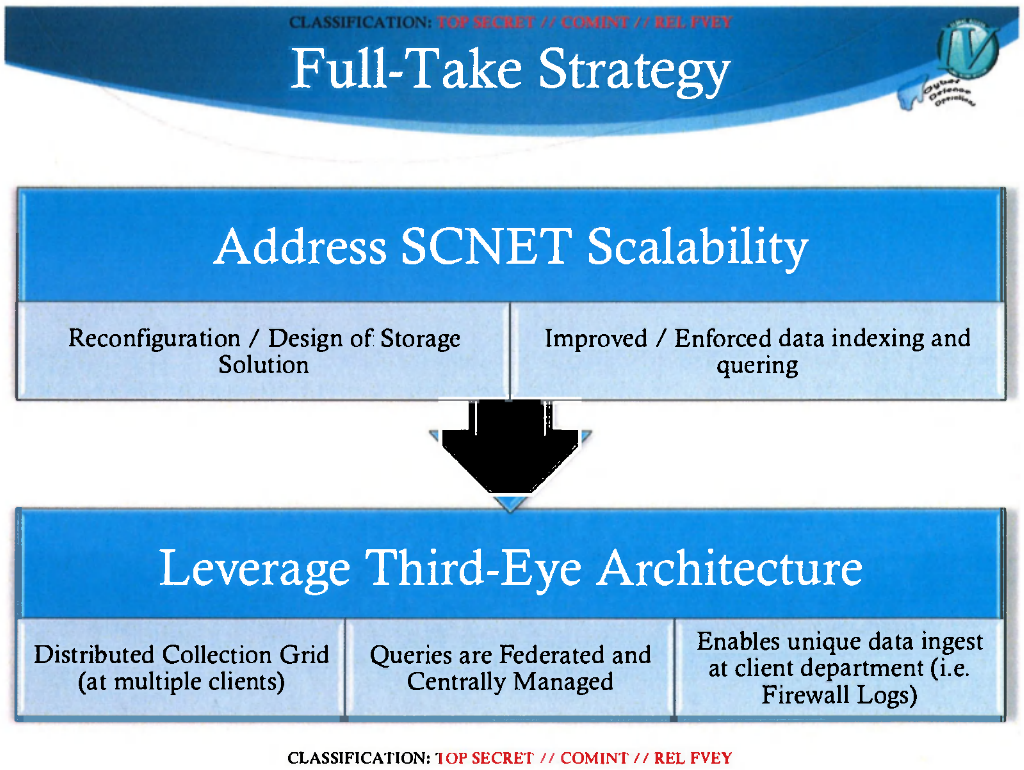
DNS Response Harvesting

HTTP Client / Server Headers

IP-to-IP Flow Summarizations

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Full-Take Strategy



Address SCNET Scalability

Reconfiguration / Design of Storage Solution	Improved / Enforced data indexing and quering

[redacted]

Leverage Third-Eye Architecture

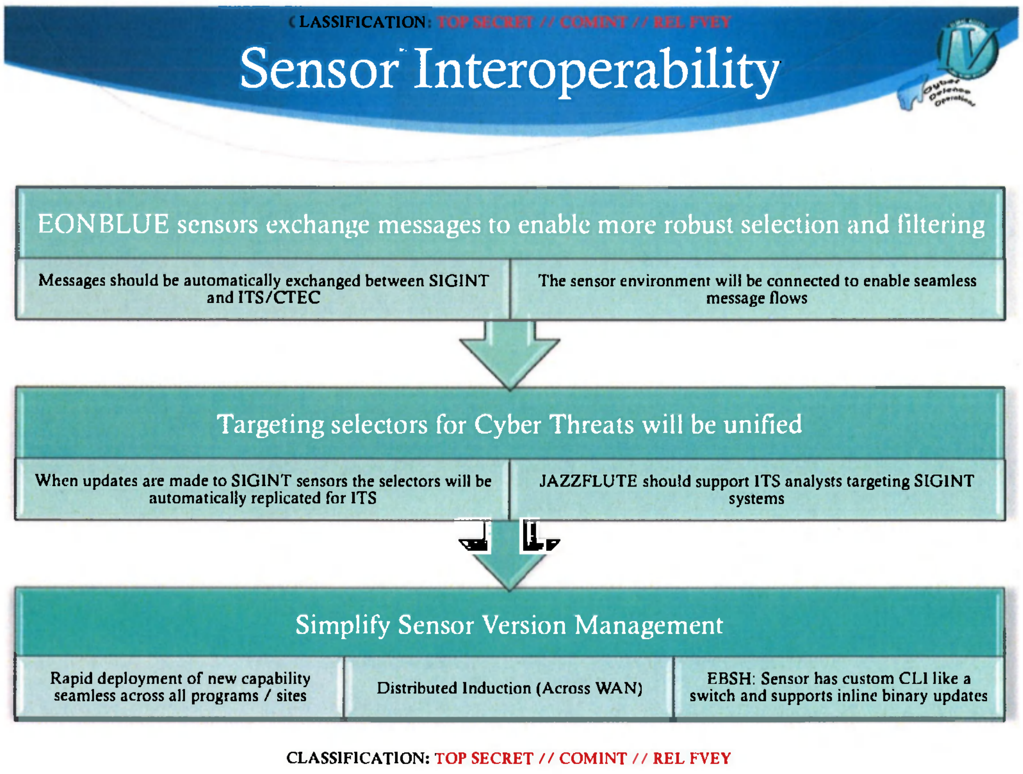
Distributed Collection Grid (at multiple clients)	Queries are Federated and Centrally Managed	Enables unique data ingest at client department (i.e. Firewall Logs)

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Full-Take Strategy

- Benefits
  - Improve Performance
    - Better data indexing techniques
    - Federated queries across multiple systems
  - Reduced Cost (Storage local to client departments)
    - 10,000$ -> 25,000$ per client
    - Re-use of back-end Storage
  - Enable departmental security officers / operators
    - Capability of Third-Eye exceeds what is commercially available
- Cons
  - Requires network connections to each GC Department
  - Requires footprint within each departments datacenter
  - Complexity of distributed processing

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY



CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Sensor Interoperability

EONBLUE sensors exchange messages to enable more robust selection and filtering

Messages should be automatically exchanged between SIGINT and ITS/CTEC

The sensor environment will be connected to enable seamless message flows

Targeting selectors for Cyber Threats will be unified

When updates are made to SIGINT sensors the selectors will be automatically replicated for ITS

JAZZFLUTE should support ITS analysts targeting SIGINT systems

Simplify Sensor Version Management

Rapid deployment of new capability seamless across all programs / sites

Distributed Induction (Across WAN)

EBSH: Sensor has custom CLI like a switch and supports inline binary updates

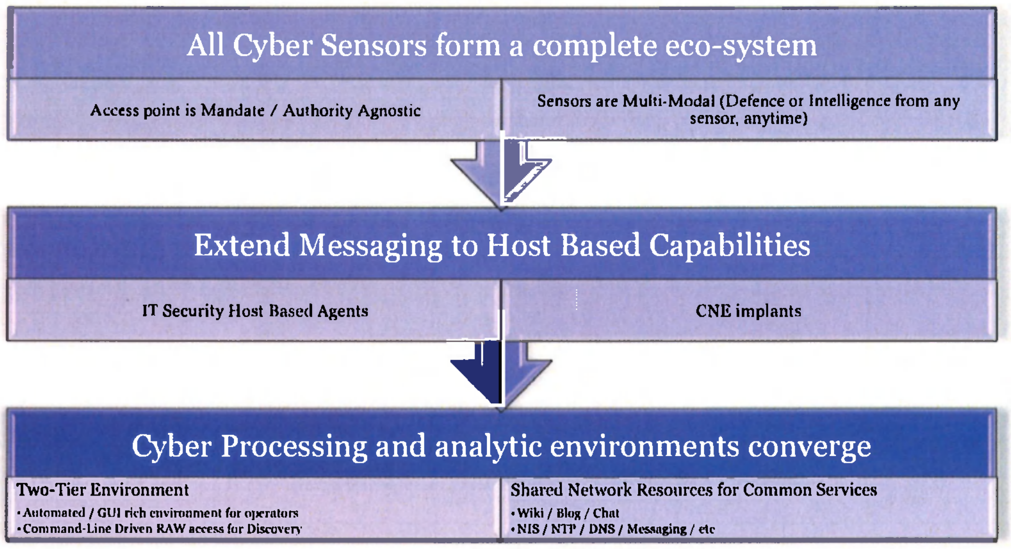
CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Interoperability enables Synchronization

- ITS access to data collected by SIGINT sensors
  - Outputs should be common to enable a common analyst platform
  - Sensor environment should be seamlessly integrated
- Capability remains at cutting-edge
  - Single release for all collection programs in SIGINT, all points of presence, and across both missions
  - Management is simplified for operators, focusing on sensor expansions
  - Standardized OS Versions and Optimizations

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Unified Sensor Environment



All Cyber Sensors form a complete eco-system

Access point is Mandate / Authority Agnostic

Sensors are Multi-Modal (Defence or Intelligence from any sensor, anytime)

Extend Messaging to Host Based Capabilities

IT Security Host Based Agents

CNE implants

Cyber Processing and analytic environments converge

Two-Tier Environment

- Automated / GUI rich environment for operators
- Command-Line Driven RAW access for Discovery

Shared Network Resources for Common Services

- Wiki / Blog / Chat
- NIS / NTP / DNS / Messaging / etc

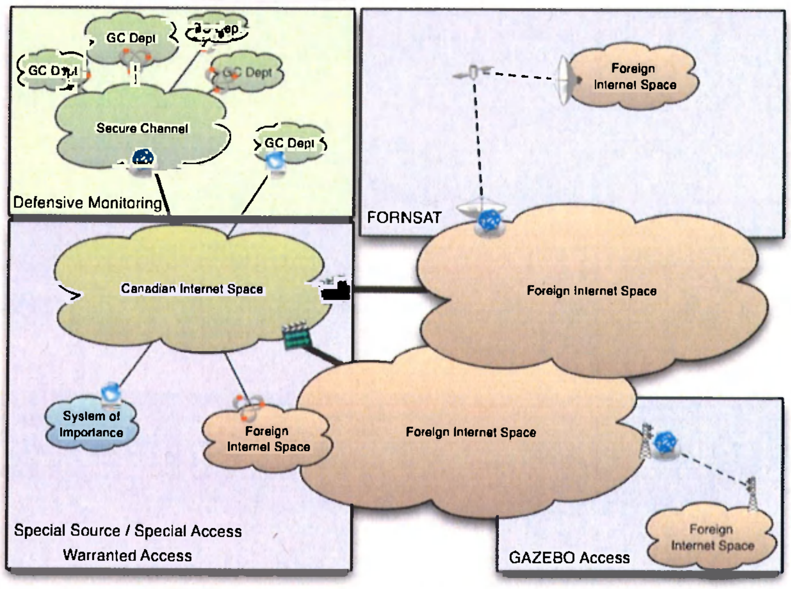
CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Synchronized Deployment Strategy

- Where do you deploy sensors to maximize detection capabilities for Foreign Intelligence collection and Network Defence
- Coverage-based deployment considerations – what are the gaps?
  - [redacted]
  - [redacted]
  - [redacted]
- Threat-based deployment considerations – what are the gaps?
  - Based on EPRs
  - Threat trends and forecasting reports
  - Adversary TTPs

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Canadian Cyber Sensor Grid



CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

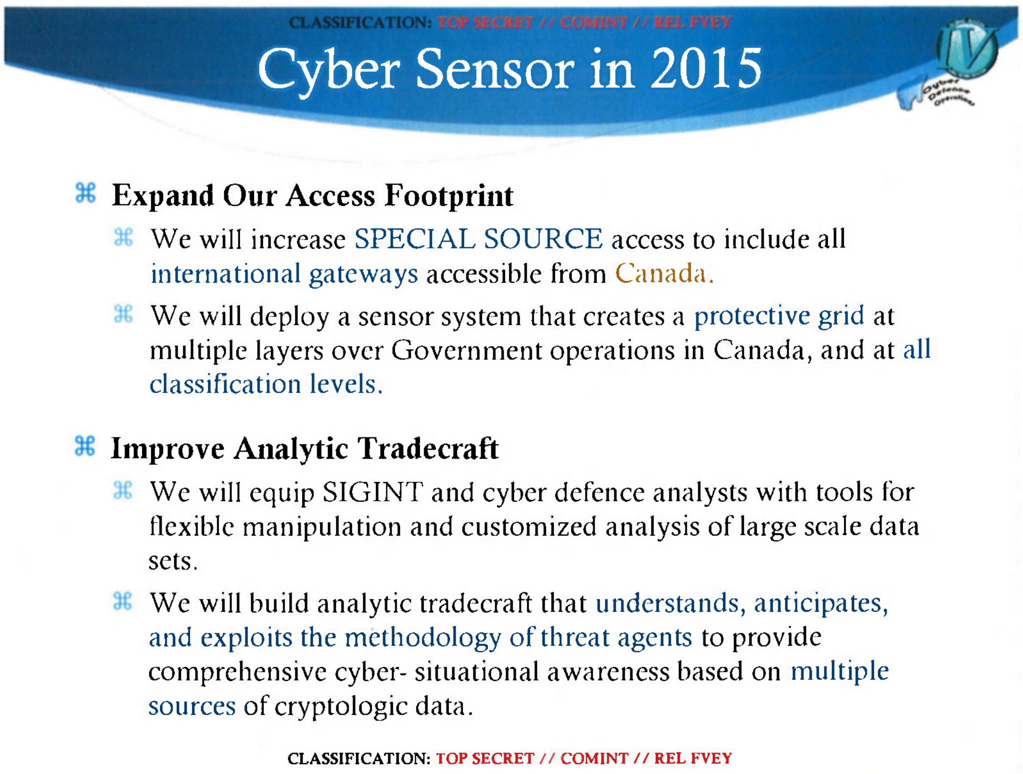
Towards 2015

Beyond sensor unification

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

CSEC 2015

- Strategic Priorities for CSEC
  - Strengthen "Team CSEC" and Prepare for Our New Facility
  - Adopt Innovative and Agile Business Solutions
  - **Expand Our Access Footprint**
  - **Improve Analytic Tradecraft**
  - Automate Manual Processes
  - **Synchronize the Cryptologic Enterprise for Cyber Security Mission**
  - **Enable "Effects" for Threat Mitigation**



CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Cyber Sensor in 2015

- **Expand Our Access Footprint**
  - We will increase SPECIAL SOURCE access to include all international gateways accessible from Canada.
  - We will deploy a sensor system that creates a protective grid at multiple layers over Government operations in Canada, and at all classification levels.
- **Improve Analytic Tradecraft**
  - We will equip SIGINT and cyber defence analysts with tools for flexible manipulation and customized analysis of large scale data sets.
  - We will build analytic tradecraft that understands, anticipates, and exploits the methodology of threat agents to provide comprehensive cyber- situational awareness based on multiple sources of cryptologic data.

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

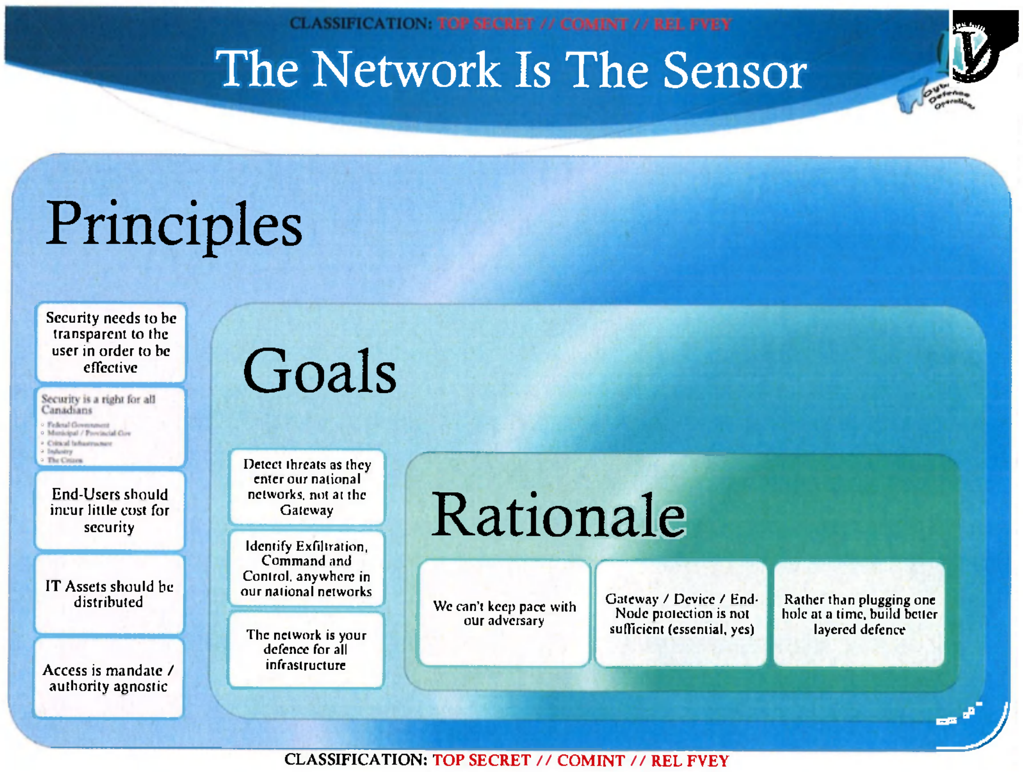
CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Cyber Sensor in 2015

- **Synchronize the Cryptologic Enterprise for the Cyber Security Mission**
  - We will improve how we anticipate, identify, track and mitigate cyber threats on government systems through new concepts of joint operations.
  - We will design and develop joint SIGINT-ITS systems, including common data repositories, joint tasking and analytic systems.
  - We will increase operational capacity by ensuring SIGINT, ITS, and cryptologic partner sensors interoperate seamlessly.
  - We will synchronize and use ITS and SIGINT capabilities and complementary analyses to thwart cyber threats.

- **Enable "Effects" for Threat Mitigation**
  - We will seek the authority to conduct a wide spectrum of Effects operations in support of our mandates.
  - We will build the technical infrastructure, policy architecture and tradecraft necessary to conduct Effects operations.
  - We will further integrate ITS and SIGINT authorities and operations to leverage common sensors, systems and capabilities necessary for active and expanded dynamic cyber defence measures.

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY



CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

The Network Is The Sensor

[redacted]

Cyber Defence Operations

Principles

- Security needs to be transparent to the user in order to be effective
- Security is a right for all Canadians
  - Federal Government
  - Municipal / Provincial Gov
  - Critical Infrastructure
  - Industry
  - The Citizen
- End-Users should incur little cost for security
- IT Assets should be distributed
- Access is mandate / authority agnostic

Goals

- Detect threats as they enter our national networks, not at the Gateway
- Identify Exfiltration, Command and Control, anywhere in our national networks
- The network is your defence for all infrastructure

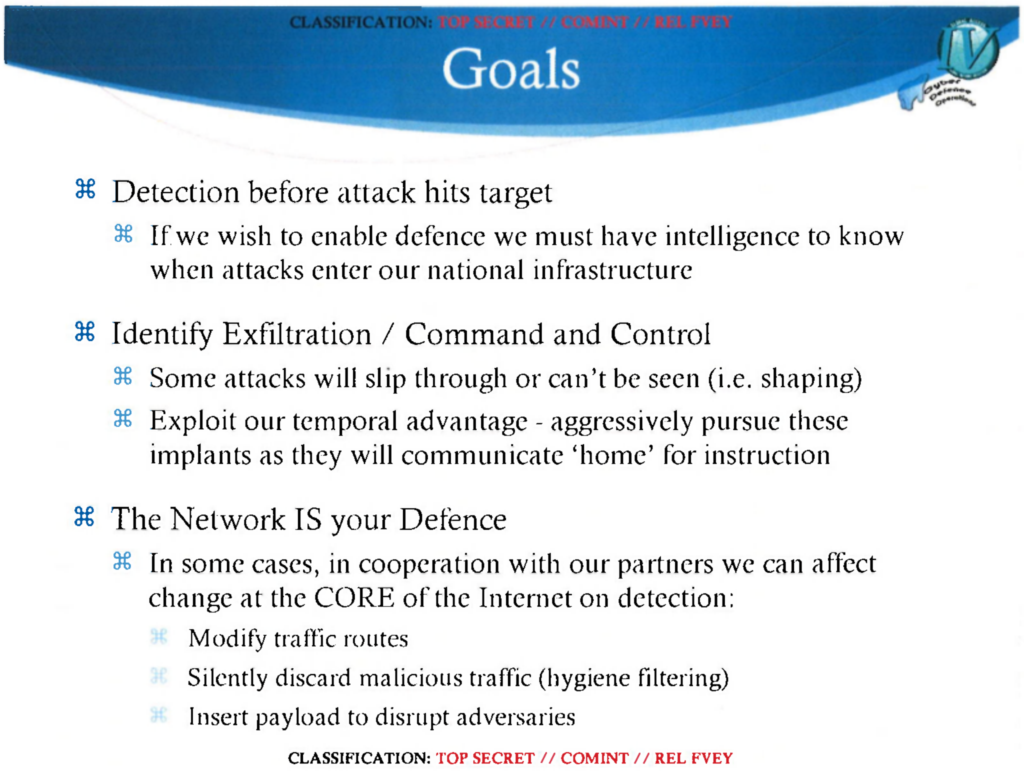
Rationale

- We can't keep pace with our adversary
- Gateway / Device / End-Node protection is not sufficient (essential, yes)
- Rather than plugging one hole at a time, build better layered defence

CLASSIFICATION: TOP SECRET // COMINT // REL FVEY

Principles Explained

- Security is Transparent
  - If security inhibits functionality, or interferes with user experience it will be bypassed
- Security is a right
  - Attempting to protect everybody with end-node / gateway defenses is not feasible.
- IT Assets should be distributed
  - We run an open market, network providers will compete to provide access
  - Consolidated gateways creates single points of failure
  - Cost / Redundancy considerations

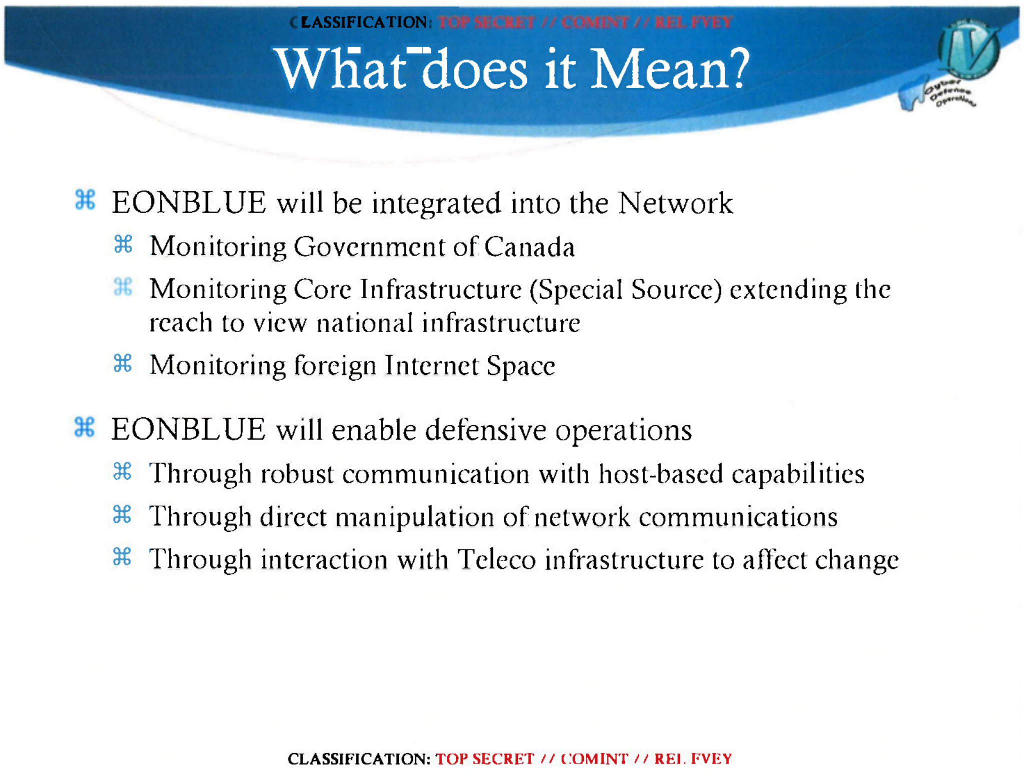


Goals

- Detection before attack hits target
  - If we wish to enable defence we must have intelligence to know when attacks enter our national infrastructure
- Identify Exfiltration / Command and Control
  - Some attacks will slip through or can't be seen (i.e. shaping)
  - Exploit our temporal advantage - aggressively pursue these implants as they will communicate 'home' for instruction
- The Network IS your Defence
  - In some cases, in cooperation with our partners we can affect change at the CORE of the Internet on detection:
    - Modify traffic routes
    - Silently discard malicious traffic (hygiene filtering)
    - Insert payload to disrupt adversaries

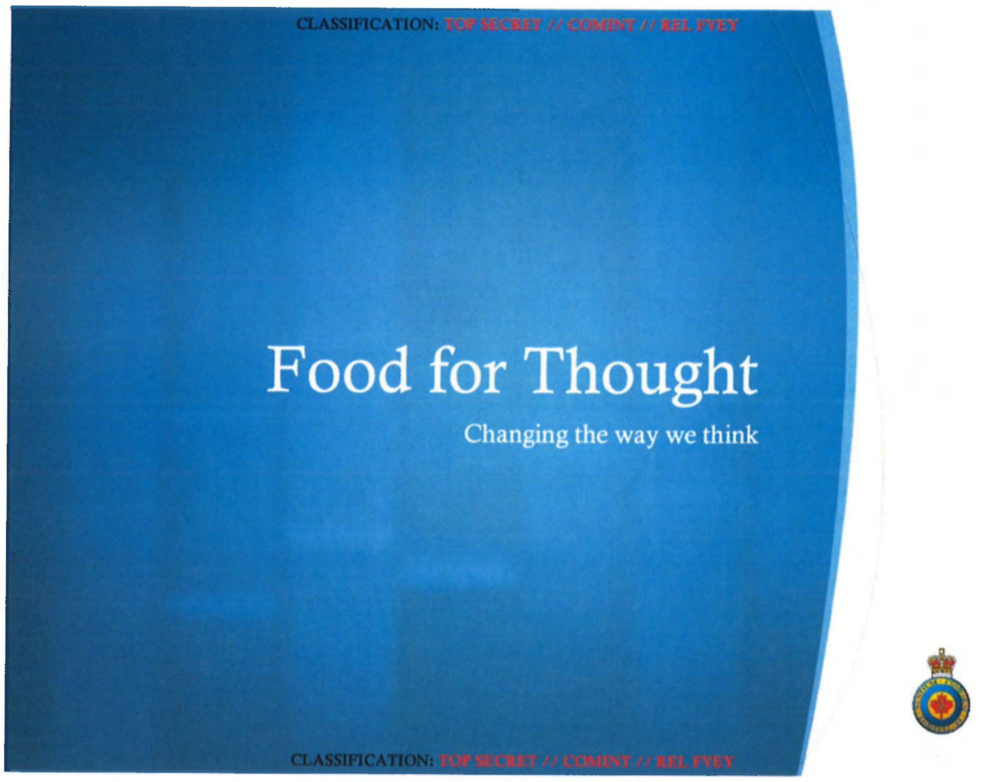
Rationale

- Keeping pace with the Adversary
  - From the time a malicious PDF is opened, till SEEDSPHERE has interactive control of a workstation is <3 minutes
  - There are countless malicious actors (state, crime, generic malware)
- Gateway / End-Node Defence by itself is insufficient
  - It is only one part of the problem
  - Over 600,000 Apps in the iTunes Appstore (How do you secure that?)
  - Defence in Depth includes network monitoring, and network interaction
- Build better Defence
  - Our current MO is to resolve one incident at a time
  - Automate the defence through a robust network capable of not only detection, but manipulation of malicious traffic



What does it Mean?

- EONBLUE will be integrated into the Network
  - Monitoring Government of Canada
  - Monitoring Core Infrastructure (Special Source) extending the reach to view national infrastructure
  - Monitoring foreign Internet Space
- EONBLUE will enable defensive operations
  - Through robust communication with host-based capabilities
  - Through direct manipulation of network communications
  - Through interaction with Teleco infrastructure to affect change



Food for Thought

Changing the way we think

Changing the way we think

- Tipping and Cueing
  - If the purpose is to enable defence of national infrastructure it becomes unnecessary in a 5-eyes context
    - We have full visibility of our national infrastructure
    - The chance of 'beating' the internet for latency of an attack is minimal
    - The network will perform the filtering
  - What if instead T&C enables intelligence collection (Cyber Session Collection)?
- Targeting and Tasking
  - We all share common targets and we will all target using our national capability the cyber threats we know about
  - No need for 2nd party tasking / targeting requests. Instead expose cyber information across the community
  - What if instead we focus on analytic collaboration and knowledge transfer
    - TEXPRO information, federated repositories (malware/traffic), etc

Changing the way we think

- Foreign SIGINT Intercept
  - Becomes the 'hunting ground' for discovery of new threats
  - Enables attribution and counter-intelligence reporting
  - Defence is taken care of by 'The Network'
  - Mobile Platforms are the next frontier, what is their implication on Cyber?
- Domestic Defence
  - We will exhaust the treasury deploying network appliances to perform dynamic defence
  - The same capabilities will be integrated into the CORE of the Internet
  - Defence in Depth through complimentary capabilities on end-nodes, at the gateway, and in the core of the Internet.

Conclusion

- CASCADE
  - The harmonization of ITS/SIGINT Sensor capabilities
  - Lays the foundation for long-term integration of Cyber within the Cryptologic Enterprise
- Towards 2015
  - The Network is the Sensor
    - Defence, Mitigation, Intelligence all formed from a single comprehensive network creating a perimeter around Canada
    - Extending our reach through 5-eyes partnerships to ensure mutual defence of national assets.