

Tactical View for Cyber Security Framework

Collaboration with
SPAWAR SoS Engineer (Ret.) / Cyber Security Consultant
and
Cyber Clarity

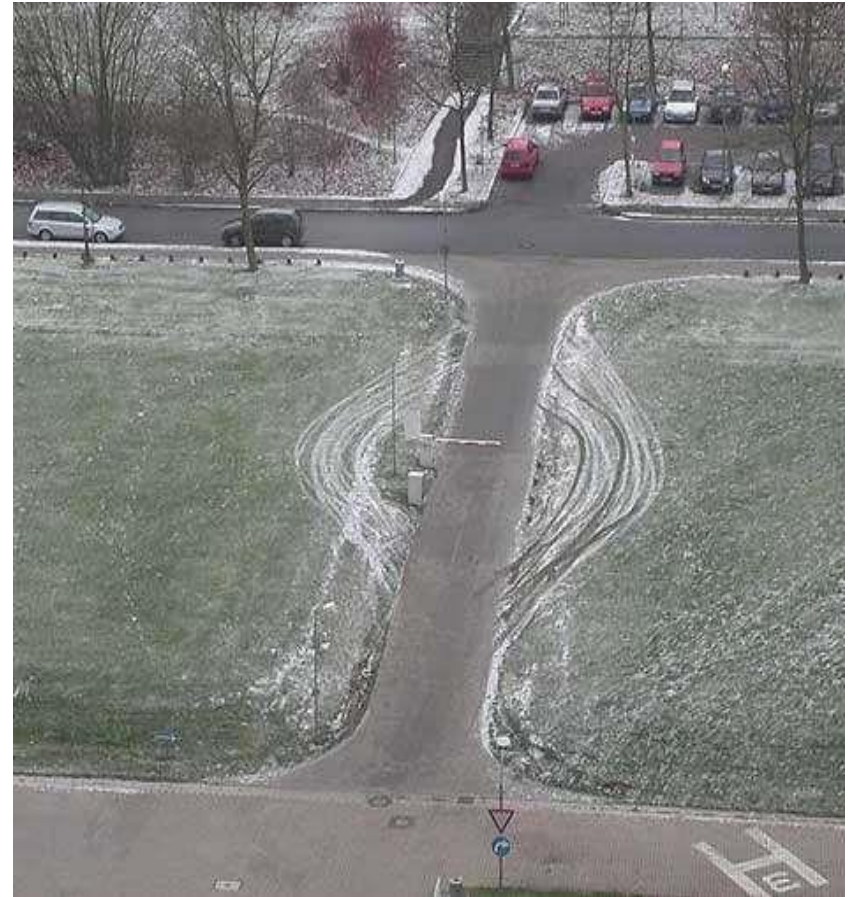
Mike.Davis.SD@gmail.com

And

rick@cyberclarity.com

What's Wrong With This Security?

What level of protection is really provided here?



When a capability is “invisible”, like IA, safety, reliability, etc, what you see is not the whole picture!

The gates were fully locked, properly configured and validated.

I could not get through *them*. But.... Thus Cyber can be an illusion...

Roadmap to Execution

“CSF” value points.

Threat overview / perspective

CSF background / pressure points

Tactical view















Summary

Be wary of a false sense of security
Monitor & measure using CSF



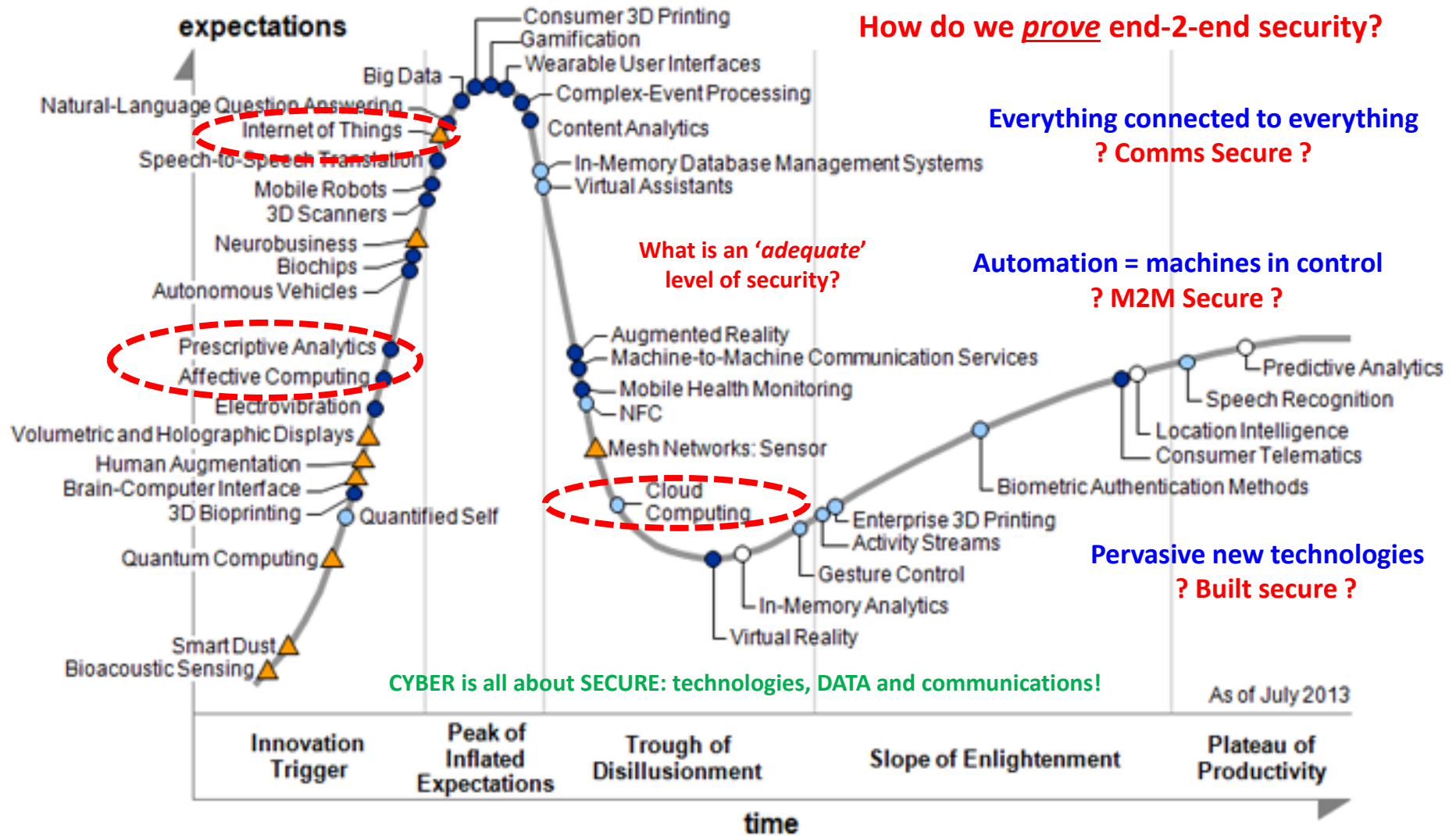
Cyber Security – Overall Status

(Senior IA VIP (Mike Jacobs) - *same issues as 40-50 years ago, but better in last 10*)

			<i>trending</i>	
Technology	---			We have what we NEED NOW
Business	---			Some LSIs resist change
Policy	---			Legislation poor Can't be voluntary
Procedures / standards	---			NIST done well Need uniform implementation
Education	---			NICE, 170+ CAEs (schools) 10,000+ / year
Leadership	---			Complexity vs CISO C-suite complacency and ability to absorb
Awareness	---			Education starting earlier, STEM, NICE

We all need to provide an integrated, cyber package that is affordable

Gartner's 2013 Hype Cycle for Emerging Technologies



Plateau will be reached in:

- less than 2 years
- 2 to 5 years
- 5 to 10 years
- ▲ more than 10 years
- ⊗ obsolete before plateau

“ALL” the technologies need built in security ... AND... support Privacy!

SO... what does matter in Cyber?

CYBER is fundamentally all about **TRUST** and **DATA**

(Identity / authentication / secure comms --- provenance, quality, pedigree, assured)

It's NOT about expensive new cyber capabilities / “toys”

but more about the interoperability “glue” (distributed trust, resiliency, automation, profiles)

90+% of security incidents are from lack of doing the basics!

HAVE effective **Security Continuous Monitoring (SCM / SIEM)** – a **MUST DO!**

USE enforced: cyber hygiene, enterprise access control, & reduce complexity (APLs)

Shift from only protecting the network, to the DATA security itself – information centric view

Embrace your Risk Management Plan (RMP) – **LIVE IT!**

Have an *enforceable security policy* – what is allowed / not – train to it

KNOW your baseline - Protect the business from the unknown risks as well

Employ a due diligence level of security – then **transfer residual risks!**

You can NOT buy cyber, so manage the cyber BASICS well!

An achievable 90-95% solution to MOST vulnerabilities – *stabilize the environment!*

Yes, It is ALL about the **DATA!**

2020 Vision

(Courtesy of Dan Green / SPAWAR):

Themes and Memes (*Technology* vs Technology Adoption)

Convergence = Genomics, Robotics, Informatics, Nanotech (each a \$B+ market)

“*CBAD*” = Cloud, Big Data, Analytics, Data Science (are you ‘all-in?’)

Telematics = Sensing robotics, Cyber Physical Systems (will kids need to learn to drive?)

Interactive 3D = Augmented Reality, HTML 5, Three.js (3D graphics for WebGL)

Embedded Computing = eHPC, Tessel (mCPU / Java), Programmable hardware

LBS = Location Based Services, IPS, Beacons, NFC

IoT = Internet of Things, M2M, Quantified Self

Mobilization = Preparation for Conflict/Competition, Autonomy, The Draft

STEM = Science Technology Engineering Math , Generation NOW, Old Dogs (*YOU*)

In a data-centric world, *we need Privacy by Design (PbD)*

Meme: an idea, behavior, or style that spreads from person to person within a culture

Verizon Data Breach Investigations Report - DBIR (2014)

A huge sample size! This includes YOUR business category too !!!

10 year series, 63,437 incidents, 1367 breaches, 95 countries

WHAT

- 92% incidents described by just nine patterns
- from geopolitical attacks to large-scale attacks on payment card system

Sectors

- Public (47, 479), Information (1132) and Finance (856)

Threats (%)

- POS intrusions - 31
- Web App Attacks - 21
- Cyber espionage - 15
- Card Skimmers - 14
- Insider misuse - 8
- Crimeware - 4

See also - **Ponemon Institute's cyber report**
Key threats – *from cost based activities*
Malware, malicious insiders and web-based attacks

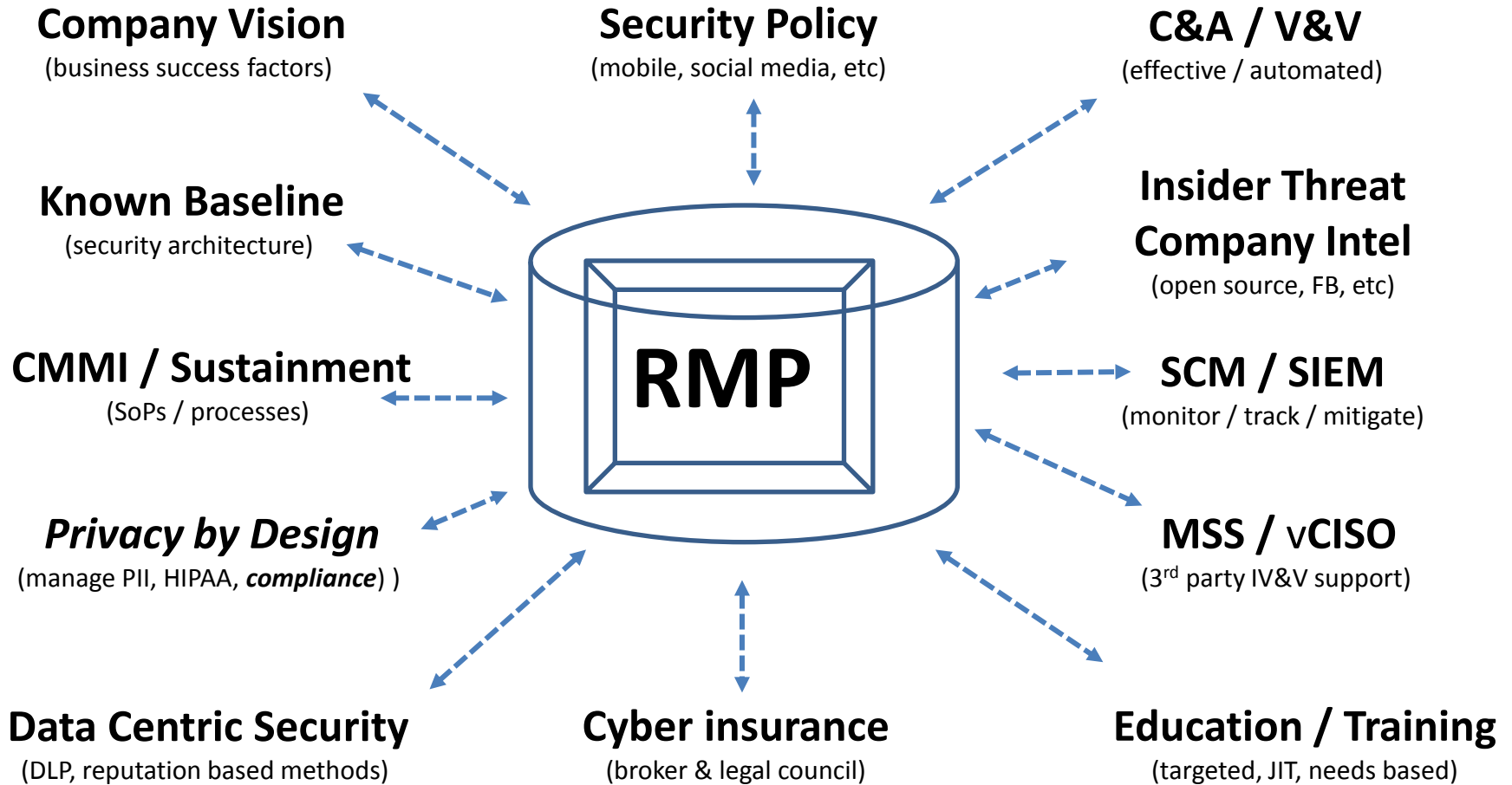
Mitigations

- restrict **remote access**
- enforce **password** policies
- Minimize “non” POS activity on those terminals
- Deploy **A/V** (everywhere, POS too)
- evaluate threats to prioritize treatments
- Look for suspicious network activity
- Use **two-factor authentication**

We have met the cyber enemy, and they are US

Integrated **Business RMP** Approach

+ Especially for *Small / Medium Business (SMB)* = [THE ANSWER](#) +



Common Risk Management Plan (RMP) model
AND IAW the NIST Cybersecurity Framework

DoD Cyber S&T Roadmap

What matters? Key Capability Gaps / Areas “4+1”

Assuring Effective Missions

Assess and control the cyber situation in mission context
Support essential business success functions

Agile Operations

Dynamically reshape cyber systems as conditions/goals change, to escape harm
Autonomous responses and C3 Tools



Resilient Infrastructure

Withstand cyber attacks, and sustain or recover critical functions
Environment is robust and self-healing

Trust

Establish known degree of assurance that devices, networks, and cyber-dependent functions perform as expected, despite attack or error
Mixed trust levels in heterogeneous space

Cyber M&S and Experimentation
(Cross Cutter)

Gaps are not “things / capabilities” but integration and interoperability!

Overview of Framework

- Framework Core
 - Core presents industry standards, guidelines, and practices
 - Focus on 5 functions (Identify, Protect, Detect, Respond, Recover)
- Framework Implementation Tiers
 - Provide a way to view cybersecurity risk and to manage the risk
 - Consideration from current risk management practices, threat environment, legal and regulatory environment, mission and organizational constraints
- Framework Profile
 - Organization selecting the Framework Category and Subcategory
 - Looking to improve “As Is” and “To Be”
 - Used to conduct self-assessment and communications within an organization

Framework Roadmap

what's still needed to enhance CSF

Automated Indicator sharing – more effective ways to detect and respond to events

Conformity Assessment – capability meets requirements within CSF

Cybersecurity workforce – adapt, design, develop maintain and improve security practices.

Data Analytics – tools with new computing methods = new processes to analyze all data

Agency alignment – Integrate CSF & RMF to enhance policy, reduce burden with common postures

International alignment – help effective operate globally and manage new risks.

Technical privacy standards – translate FIPPs into methods for effective privacy metrics / risks.

Tools to easily assess and organization's CSF posture,
Support analytics / trending, broad use – including privacy

Our Tactical View Focus On:

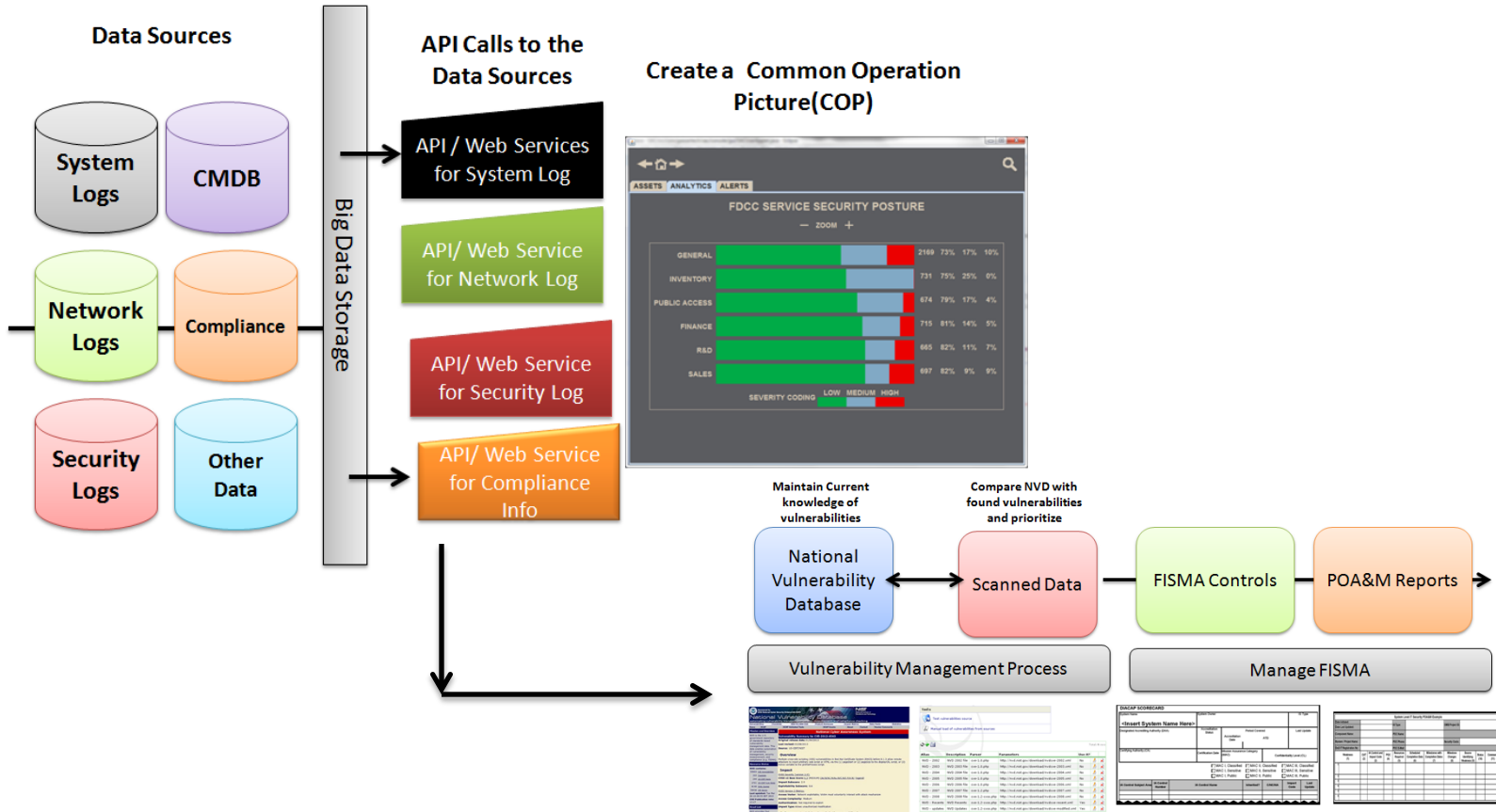
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Full Security Lifecycle Management

Understand, Validate, Execute, Sustain

- Building a Positive Security Posture for an organization requires **a focused approach**
- Building a Compliance Automation Reporting (**CAR**) process is your **first step**
- Once an organization is reached a **State of Positive Health**, Enhanced Situational Awareness (**ESA**) can be executed
- **Sustainability** of ESA is crucial to a Positive Security Posture
- **Integrates** easily in a **Compliance Risk Scoring Approach**
- Meets **CyberScope**

The BIG PICTURE



Prepare for a Positive State of Health

Executing ESA

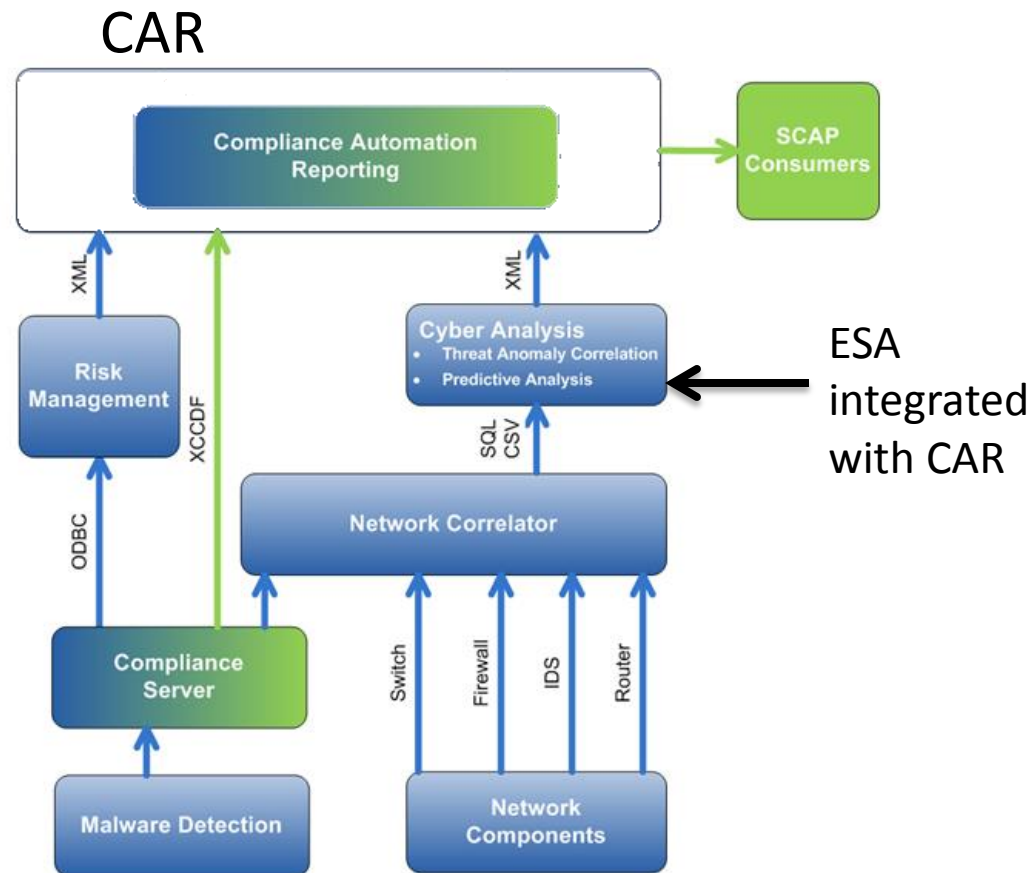
Sustaining State of Health with People, Process and Technology

Architectural View of ESA with CAR

Compliance Automation Report

Employs GOTS & open source software

- Reduced cost of ownership
- Vendor Agnostic
- Conforms to Federal standards
- Real-time, federated architecture
- Consumes and Produces SCAP (XCCDF)



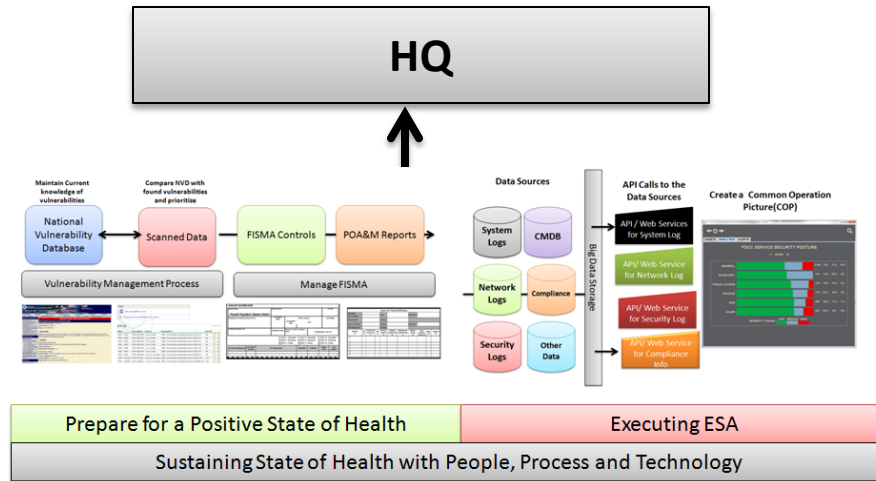
CAR Dashboard and Application

(Advantages of using CAR)

- CAR's Functions
 - Provides a unified dashboard to access and display multi-vendor security compliance and risk applications at the organizational level (lowest level)
 - Inputs FDCC scores in XCCDF format
 - Groups FDCC fail scores into 7 risk categories (0-6, risk category 0 = 100% compliance)
 - Provides a per desktop compliance score (0-100%) vs. risk score (0 – 7) of the organization on a two-dimensional graph that clearly identifies **outliers**
 - Transforms XCCDF to an industry standard lightweight data interchange format and compresses it to **two orders of magnitude less** than original format
 - Distributes the compressed risk and compliance data up the organizational hierarchy via the Federated Framework

Agencies can gain the ability to easily share and distribute compliance and risk information with CAR to provide a global defensive posture of your networks

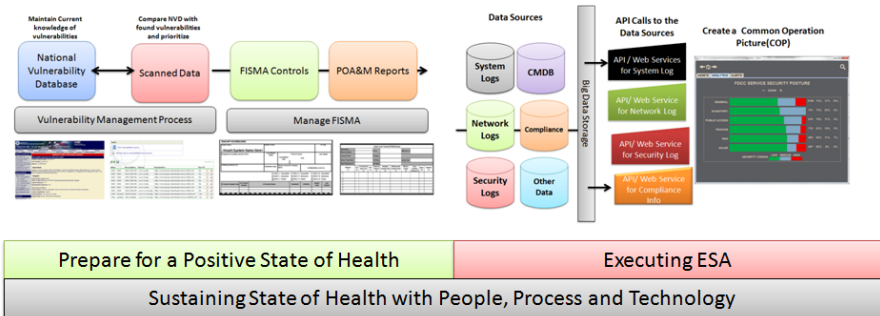
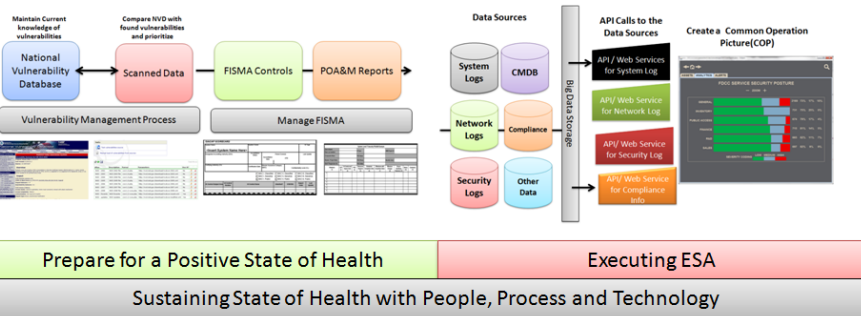
Integrating this into a large enterprise



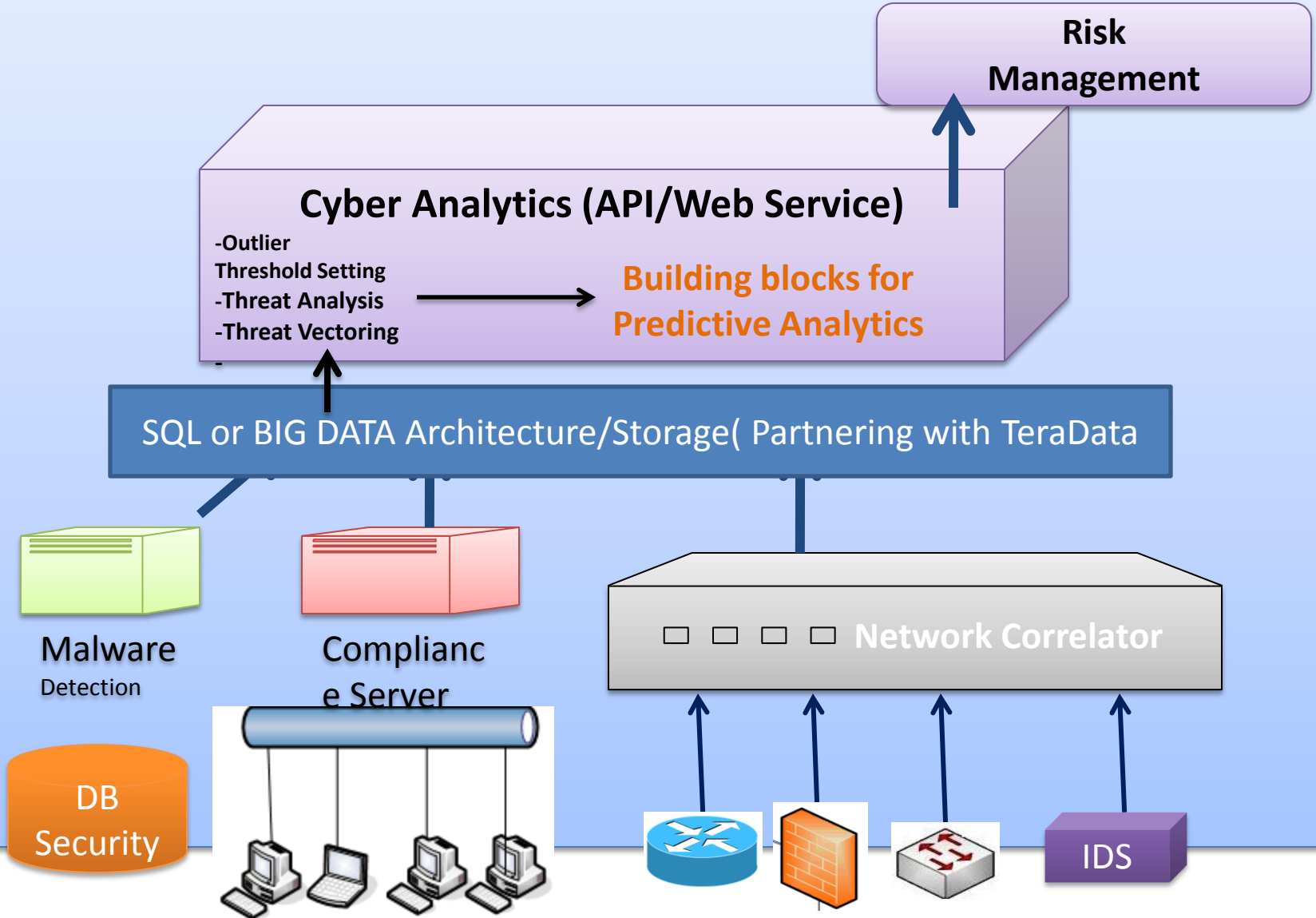
Data Sharing to HQ to provide Situational Awareness (SA)

Subordinate Organization 1

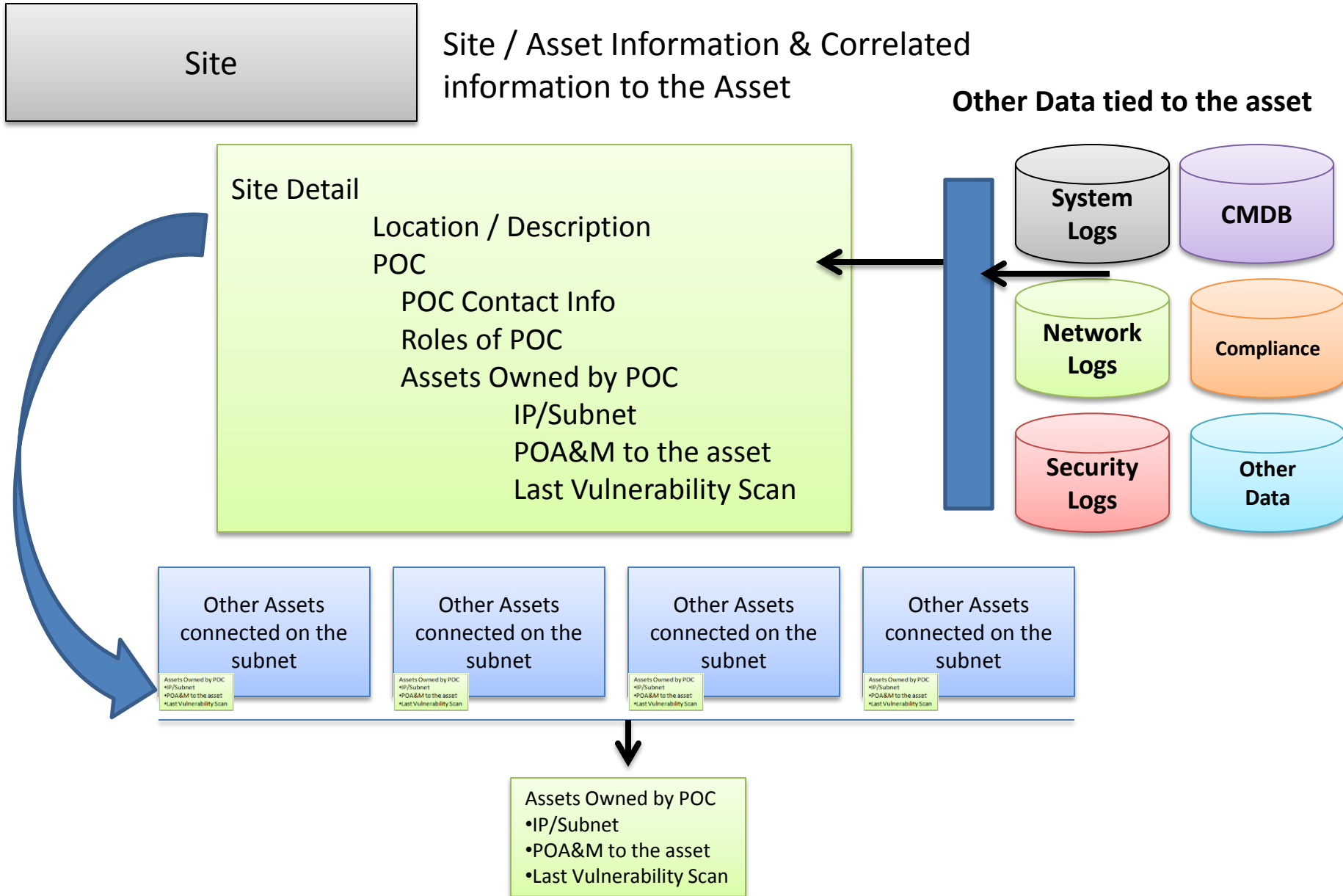
Subordinate Organization 2



Data Flow Chart for a Federated Framework at each Tier 3 level



Data Model of what you can view



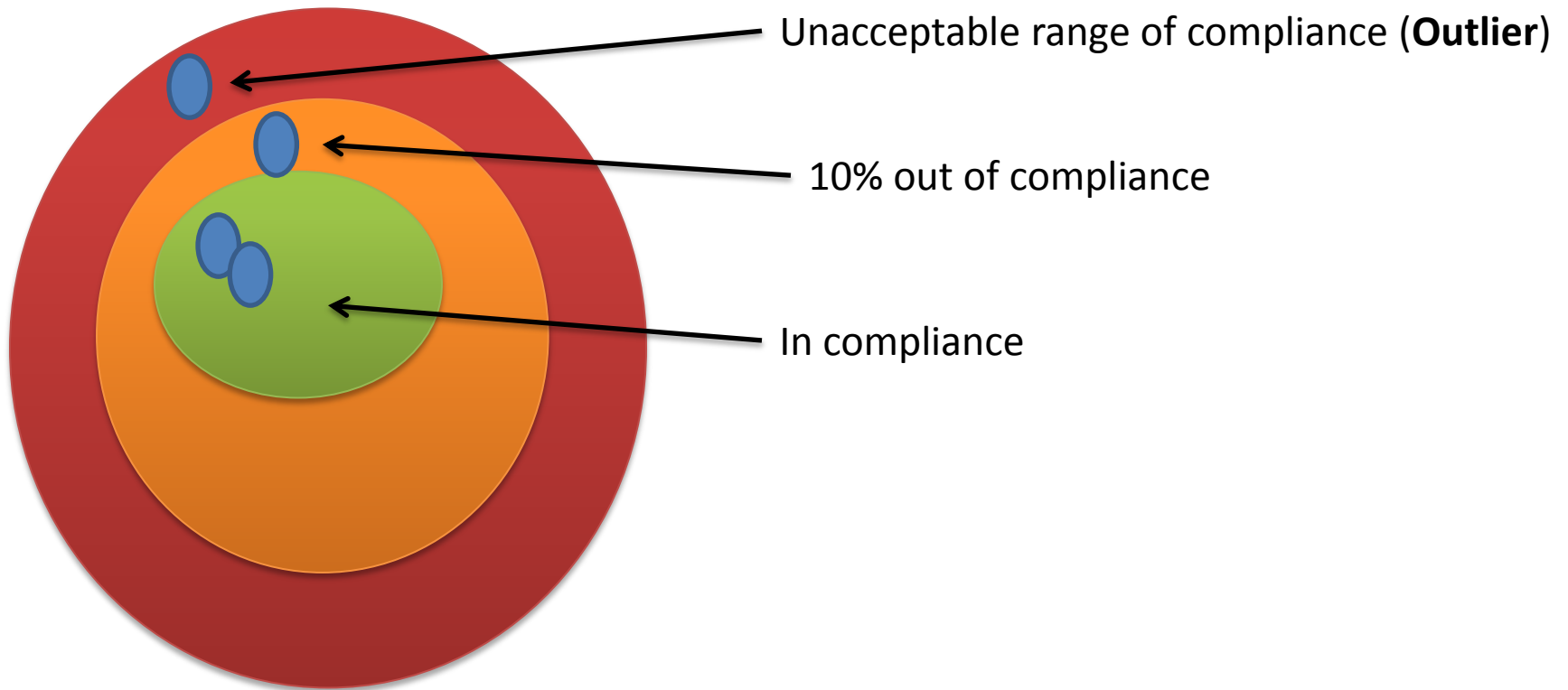
Building a common Taxonomy

- 1) Describe their current cybersecurity posture;
- 2) Describe their target state for cybersecurity;
- 3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- 4) Assess progress toward the target state;
- 5) Communicate among internal and external stakeholders about cybersecurity risk.

Describe their current cybersecurity posture;

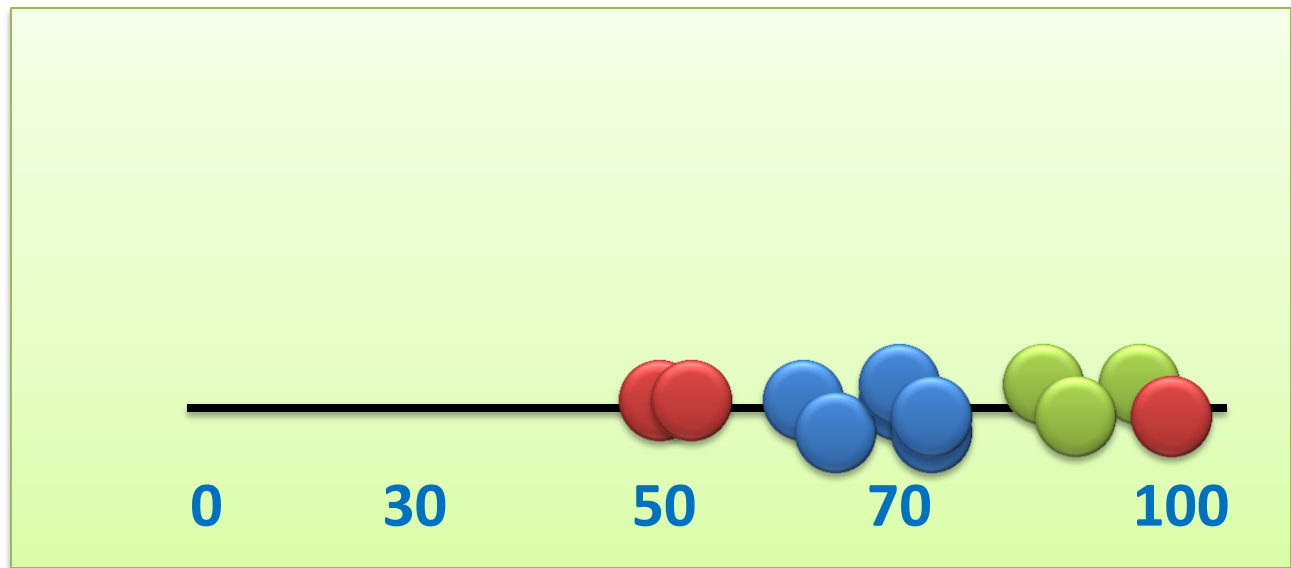
- Setting up agreed baseline metrics
- Example (**Outlier Reports**)

Outlier Explanation



Old way of viewing a FDDC report

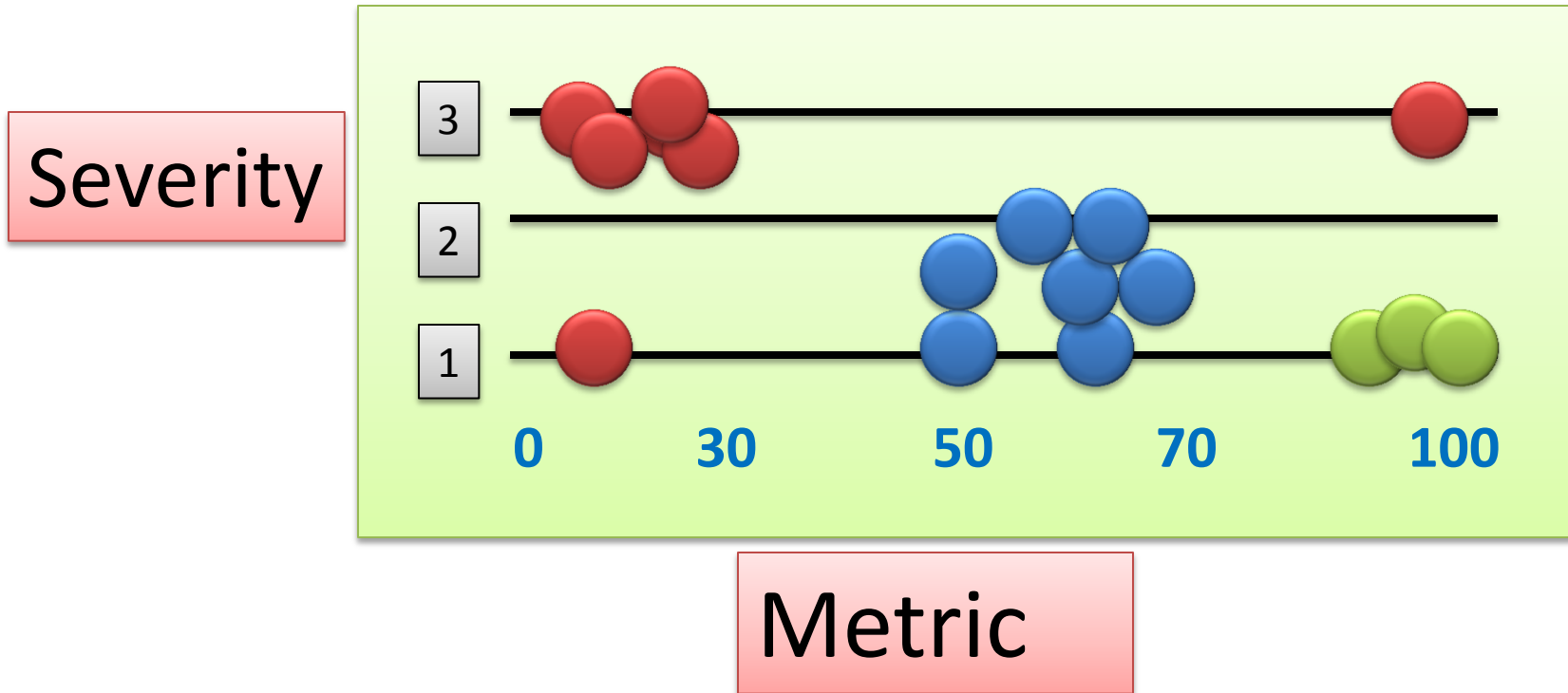
Old Approach



Metric

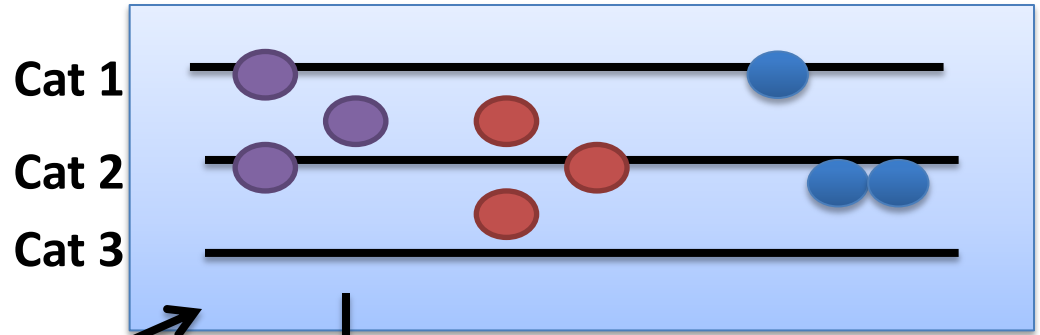
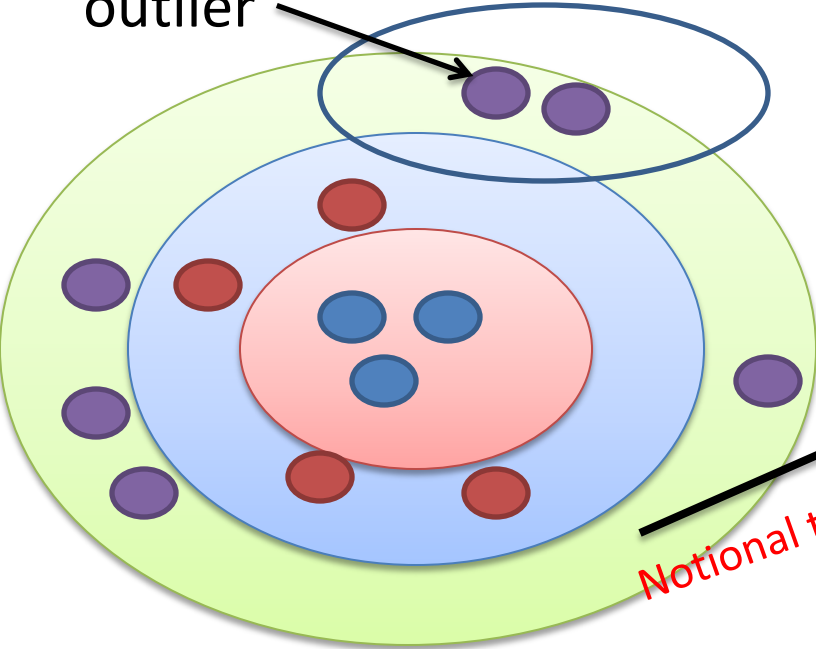
Applying Severity Rating to the FDCC Report

Two inputs – Severity and Metric



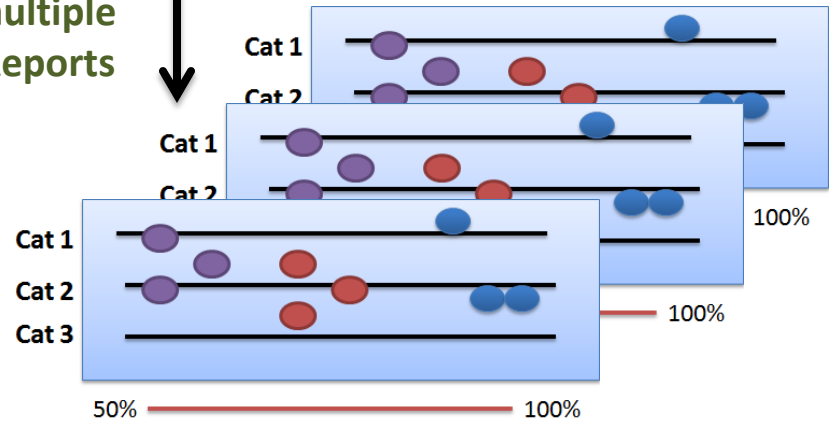
Outlier Reports 1 Of 3

outlier



Notional to Reality

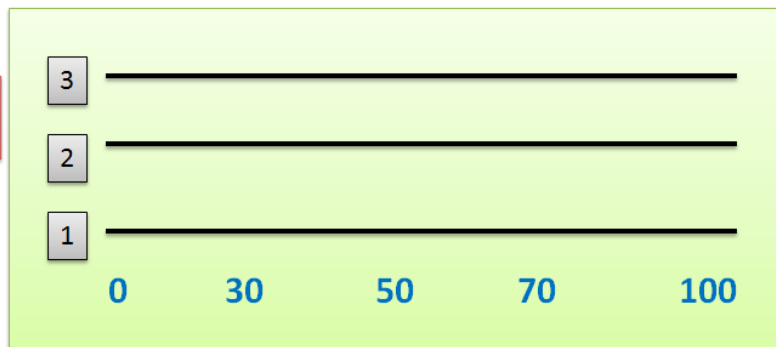
Create multiple
Outlier Reports



Outlier Reports 2 of 3

Create a Framework that inputs Severity & a Metric

- Idea is to create ways to measure impact universally
- Allows each client to set their OWN impact
- Still aligns with Strategic Data Strategy with some proprietary approach

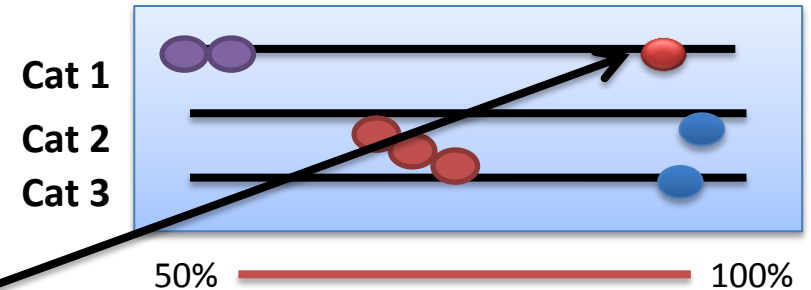
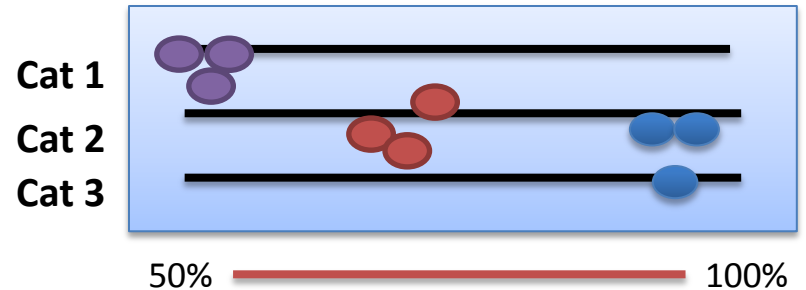


Severity

Metric

Create Multiple Outlier reports that help show Impact to the Mission

- Common Operational Picture
- Intuitive
- Can be re-purposed



Outlier

Outlier Reports 3 of 3

Defining Severity & Metric in other areas

Severity -Measuring against known vulnerabilities with a level of impact

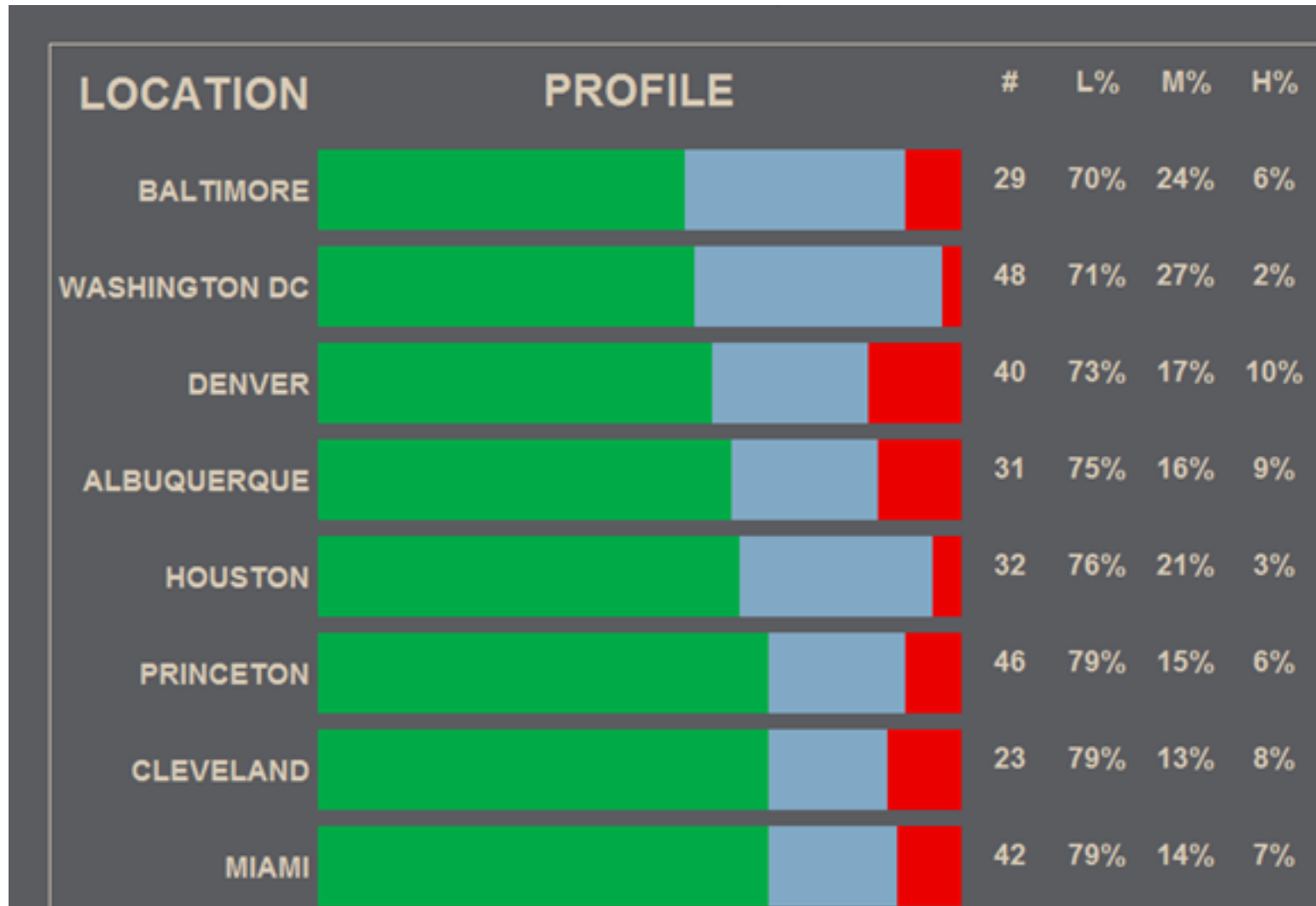
- Cat1, Cat2, Cat 3 Finding
- Patches
- Signatures
- Malwares

Metric – Component that shows average usage for sustainment

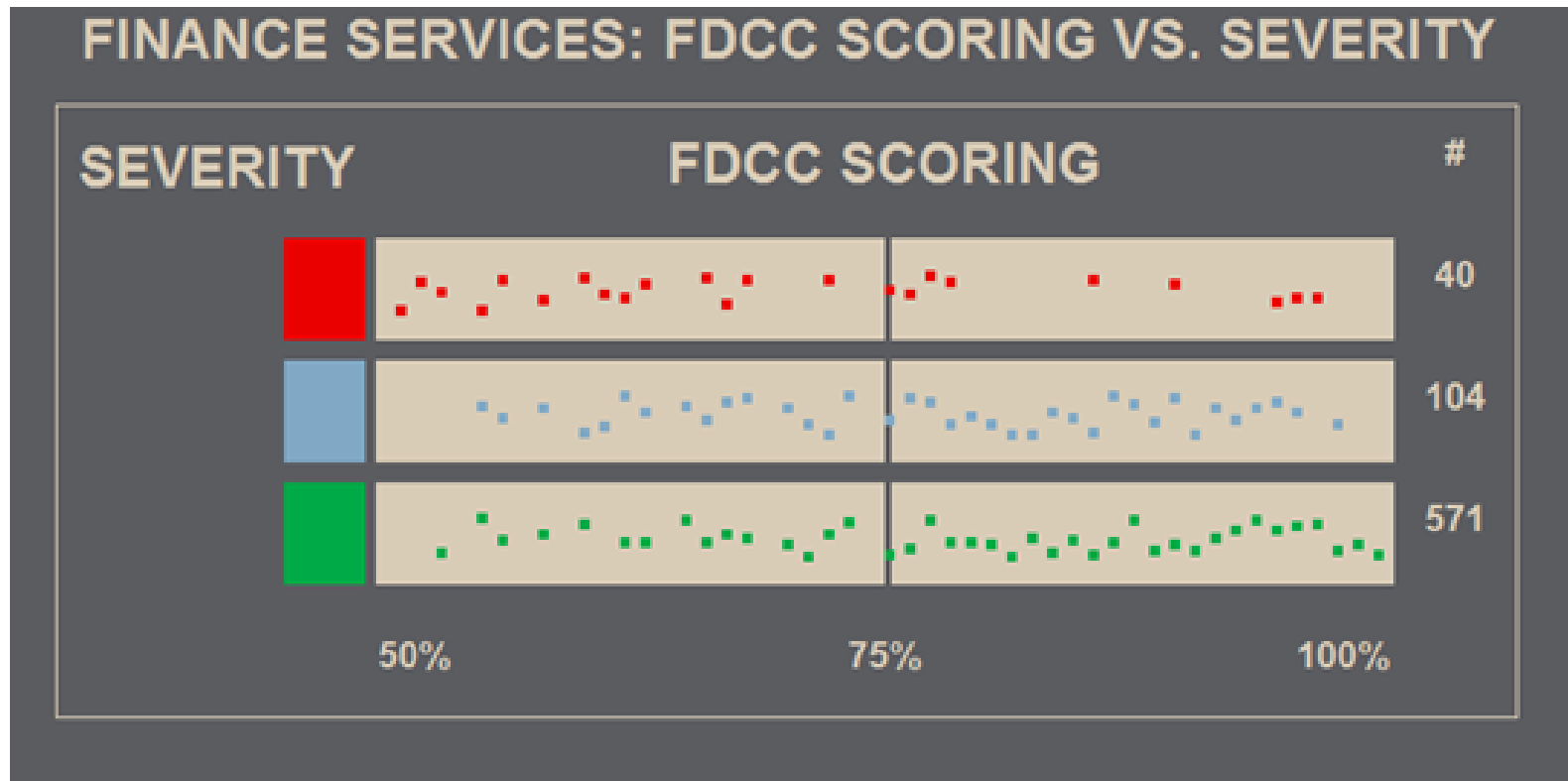
- Time
- Software Version
- Certain Percentage score

Item	Severity	Metric
FDCC	Registry items	FDCC Score (0 – 100)
Network Operations	Bandwidth Usage	Time of the day
Configuration Management	Software Vulnerability	Versions

Aggregate View of FDCC/USCGB Report in our pilot application



Outlier Report on one section in our pilot application



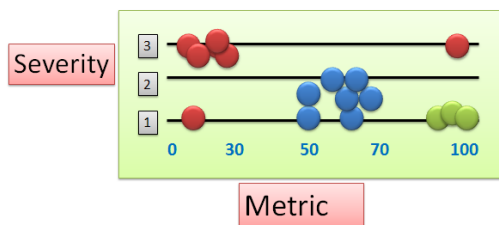
Describe their target state for cybersecurity;

- Understanding the targeted area and what level we need to set them is implemented through **Threshold Settings**.

Threshold Settings 1 of 3

FDCC Report

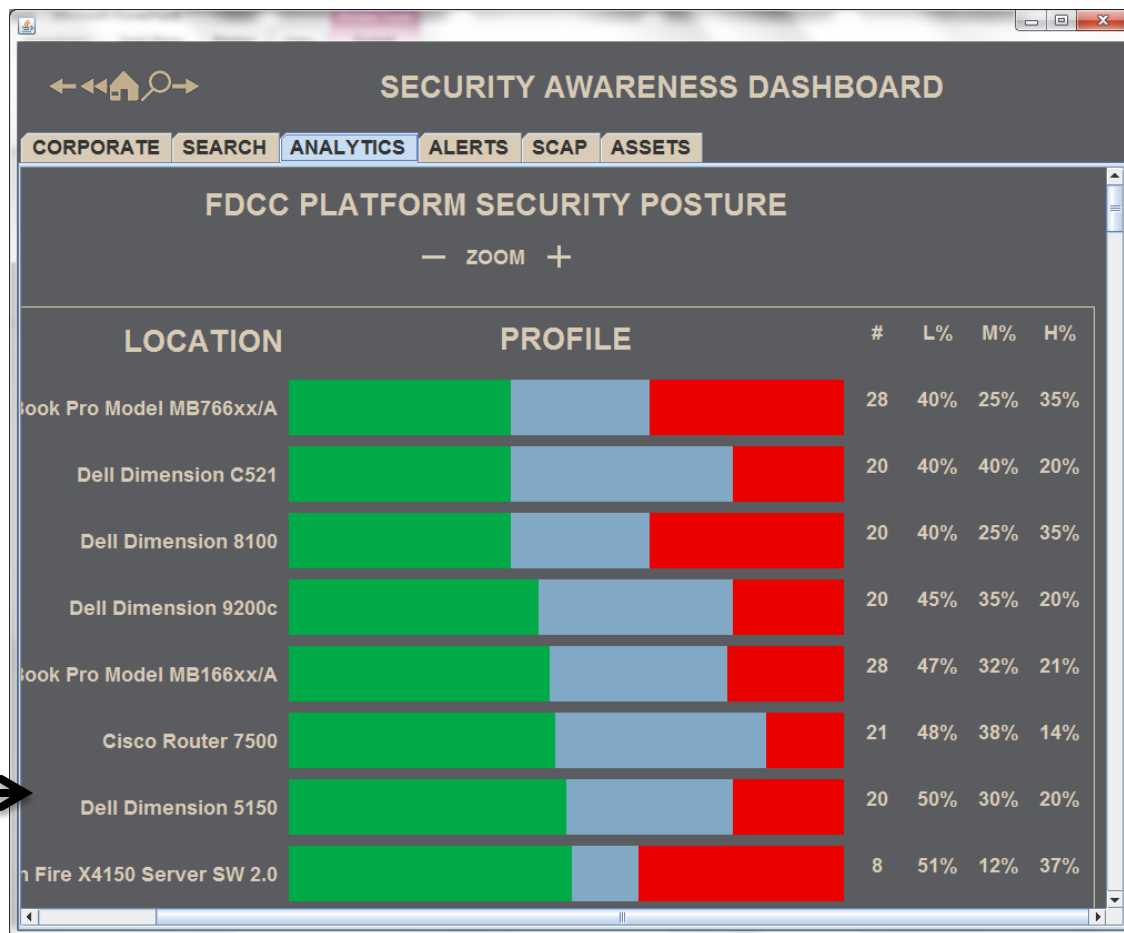
Two inputs – Severity and Metric



Outliers will help to set up the baseline status of Health and will be used to set up **thresholds**.

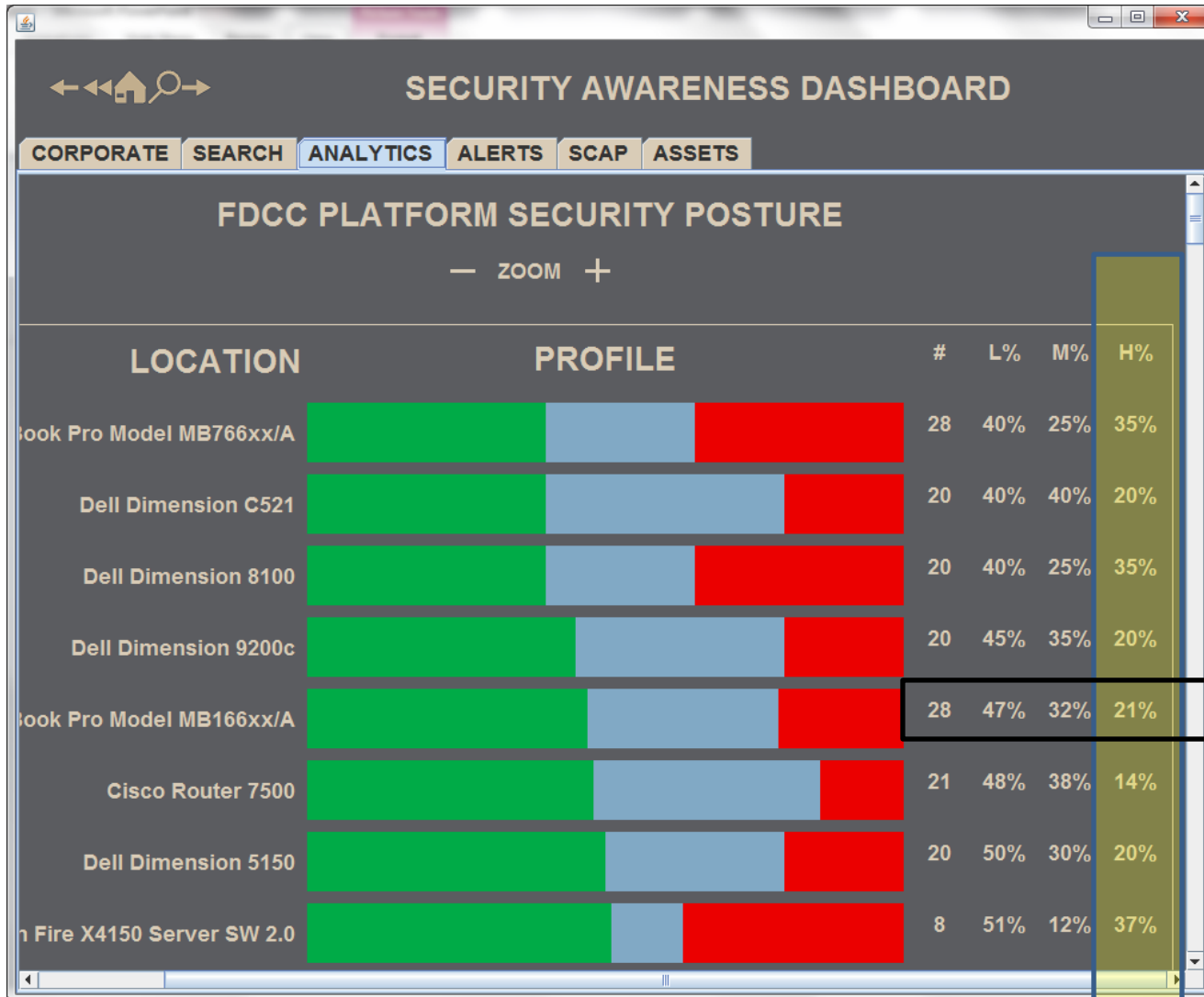
Algorithm

Risk Score = Total Assets/
number of severity



Threshold Settings 2 of 3

Setting up a threshold against the **Highs** will alert us when each location is exceeding the allowable threshold.



33
36
33
36
33
33
33

Threshold Settings 3 of 3

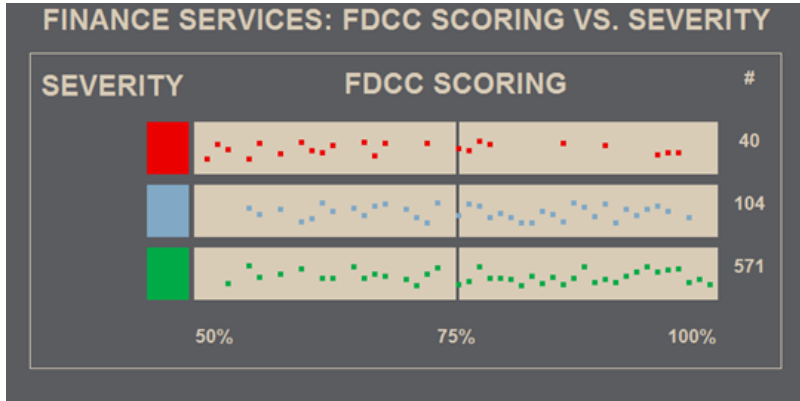
Location	Asset Over Threshold over 10%	Cat Findings causing the issues
Virginia	192.168.1.23	CVE 204-5098
	192.215.1.23	CVE 34-6098
Michigan	168.2.3.5	CVE 120-7864
	168.4.3.5	CVE 204-5098
New York	172.3.5.78	CVE 204-5098
	172.3.5.78	CVE 120-7864

Being able to identify assets that are outside of the thresholds are on the remediation list as soon as possible.

Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;

- Understanding the basic reporting and adding indicators to help prioritize the content
 - I.E (FDCC/USCGB graphs)

Continuous Monitoring to help Identify and prioritize



Outlier



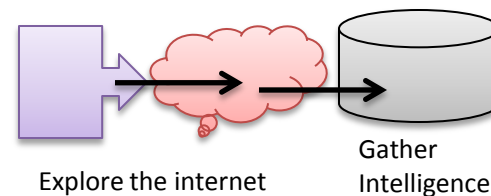
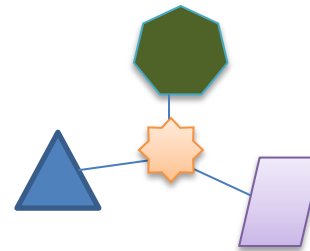
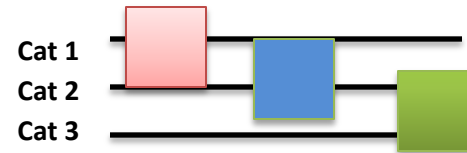
Threshold Settings

Assess progress toward the target state

- Defining baseline metrics through **Outlier Reports** and **Threshold Settings** can help your organization **Assess Progress**.
- Once you have set up the basic metrics, your organization can move into Threat Vectoring and Active Threat Management

Assess progress toward the target state (cont)

Data Sources	Algorithm
Known Alerts	Outlier
	Threshold Setting
Known Behavior Outside Data Source	Threat Vectoring
Not waiting for trouble, Seek trouble	Active Threat Management

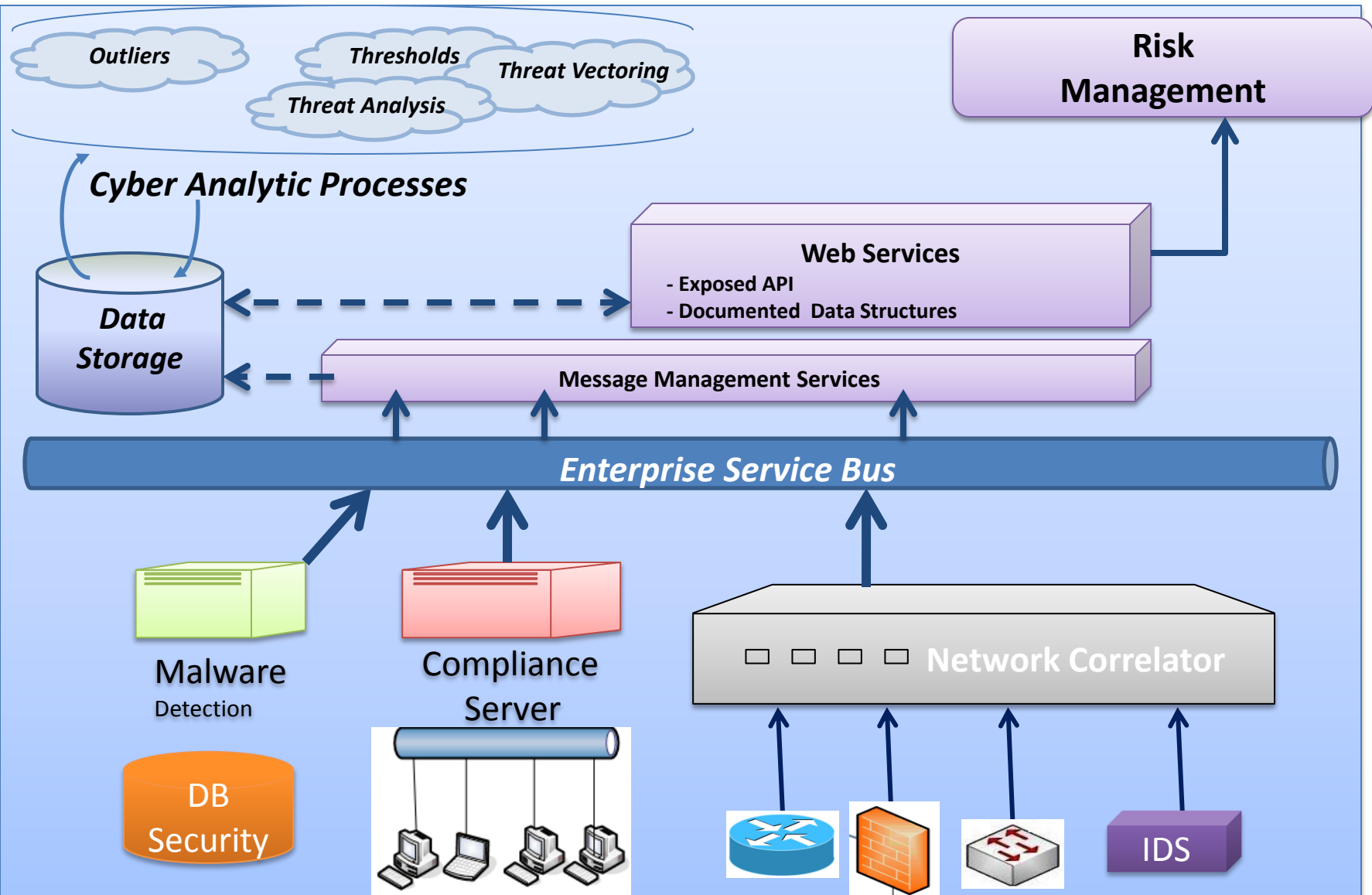


Communicate among internal and external stakeholders about cybersecurity risk.

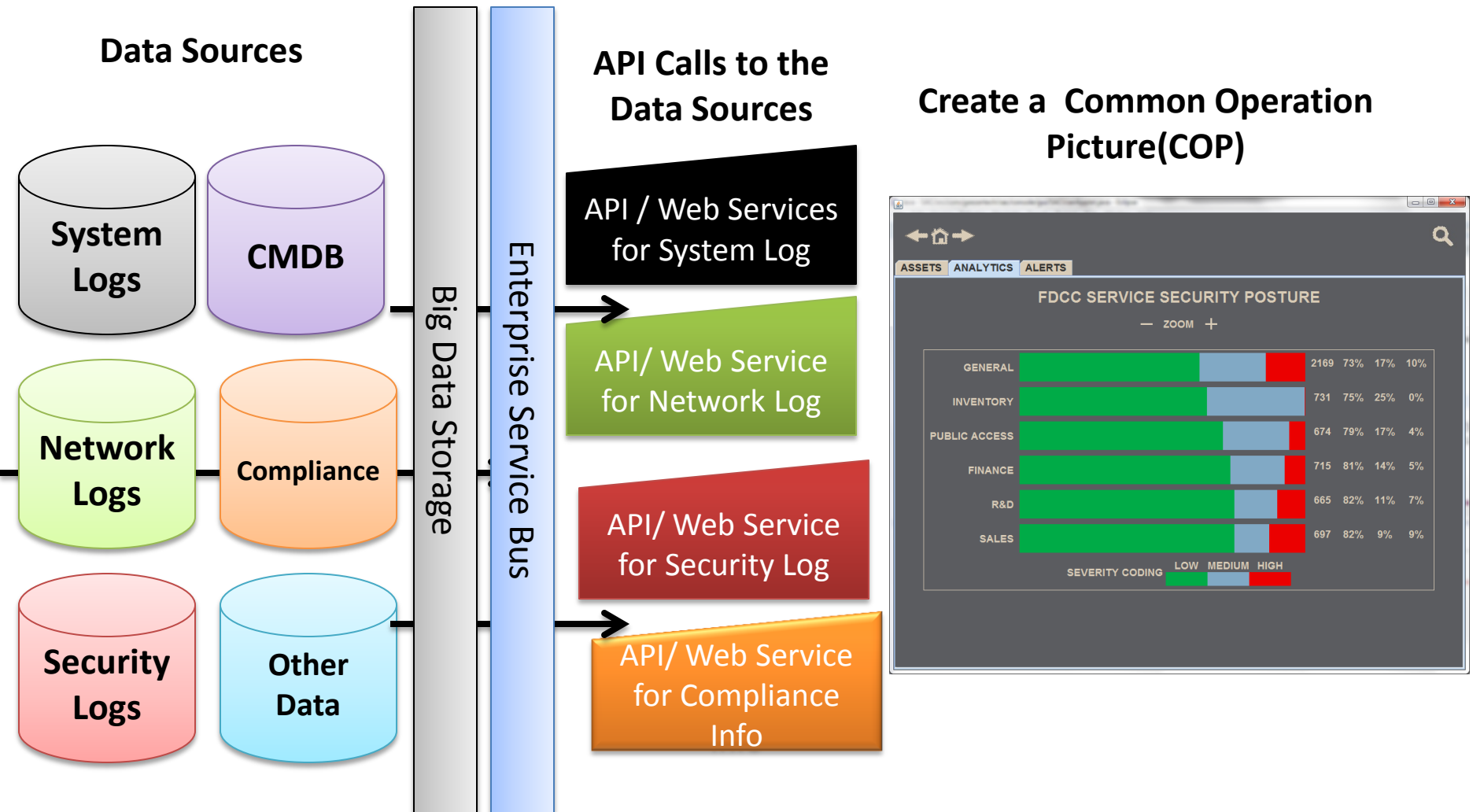
- Building Common Operation Picture (COP) and sharing definitions can help improve communications with stakeholders
- Having an open architecture to help communicate with other disparate data sources
- Implementing SCAP to provide automated reporting to other stakeholders

Open Architecture

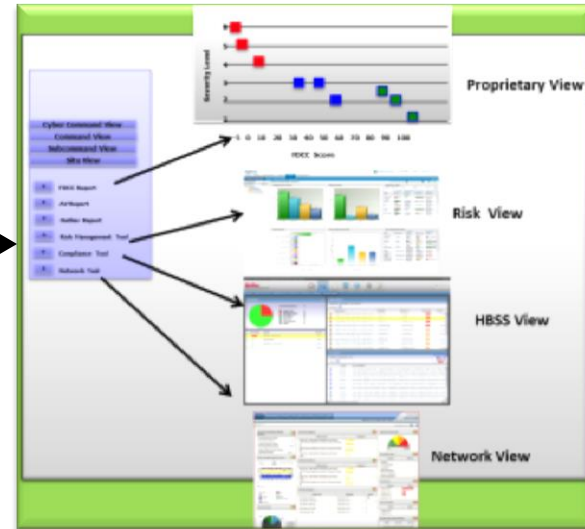
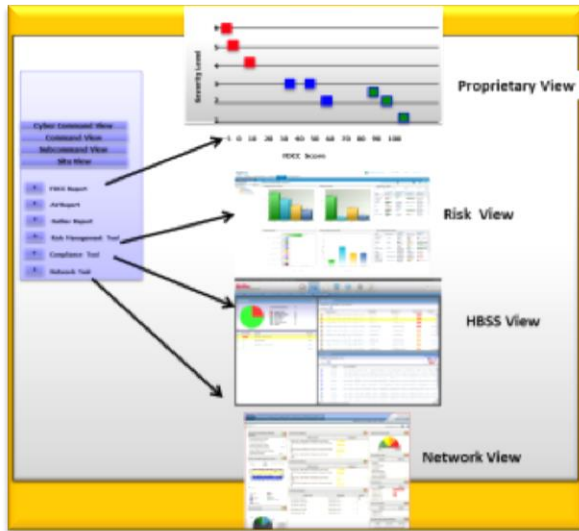
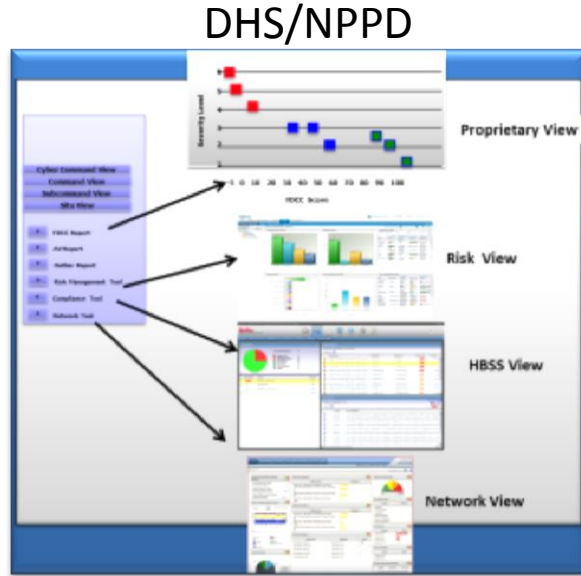
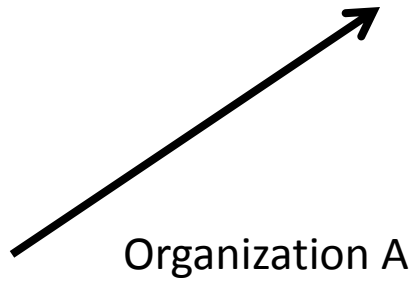
Data Flow Chart for a Federated Framework at each Tier 3 level



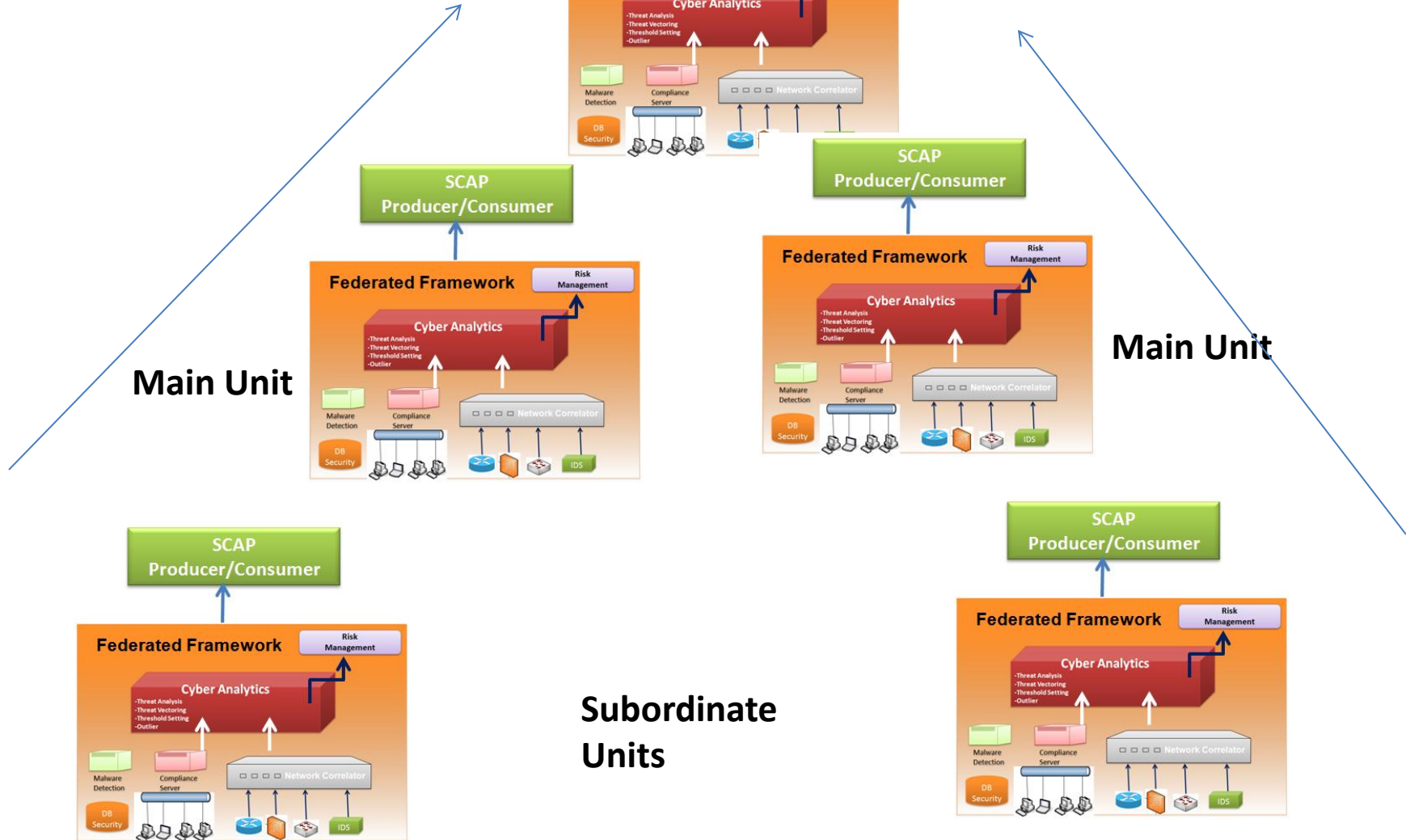
Data flow through the open architecture



Share Views Common Operational Picture



Applying SCAP to help automate communications



Common Operation Picture for CAR

- A vendor neutral network security capability
- Aggregates and distributes the networks' defensive posture across the organizational hierarchy
- SCAP compliant

The screenshot displays the 'Accenture Cyber Security Reporting Dashboard' in a Mozilla Firefox browser. The dashboard is titled 'Compliance Automation Reporting - Accenture Cyber Range'. It features a left-hand navigation pane with a tree view of reports categorized by 'Views', 'Cyber Command Reports', 'Divisional Reports', and 'Site Reports'. The 'Site Reports' section is expanded to show 'West', which includes sub-sections for 'Compliance Summary', 'FDCC Outliers Summary', 'Unix Outliers Summary', 'Windows Patch Outliers Summary', 'Virus Outliers Summary', and 'Top Talkers Summary'. A central chart titled 'West A FDCC Report' shows a scatter plot of 'Number of Outliers' versus 'FDCC Score'. To the right, there are three distinct views: 1) 'LITS, Proprietary View' showing a McAfee console with a 'Total Machines' pie chart and a table of system details. 2) 'System / Network View' showing a dashboard with multiple bar and line charts. 3) 'SEIM View' showing a Security Information and Event Management interface with various data feeds and charts. Arrows point from the dashboard's navigation pane to each of these three views.

LITS, Proprietary View

System / Network View

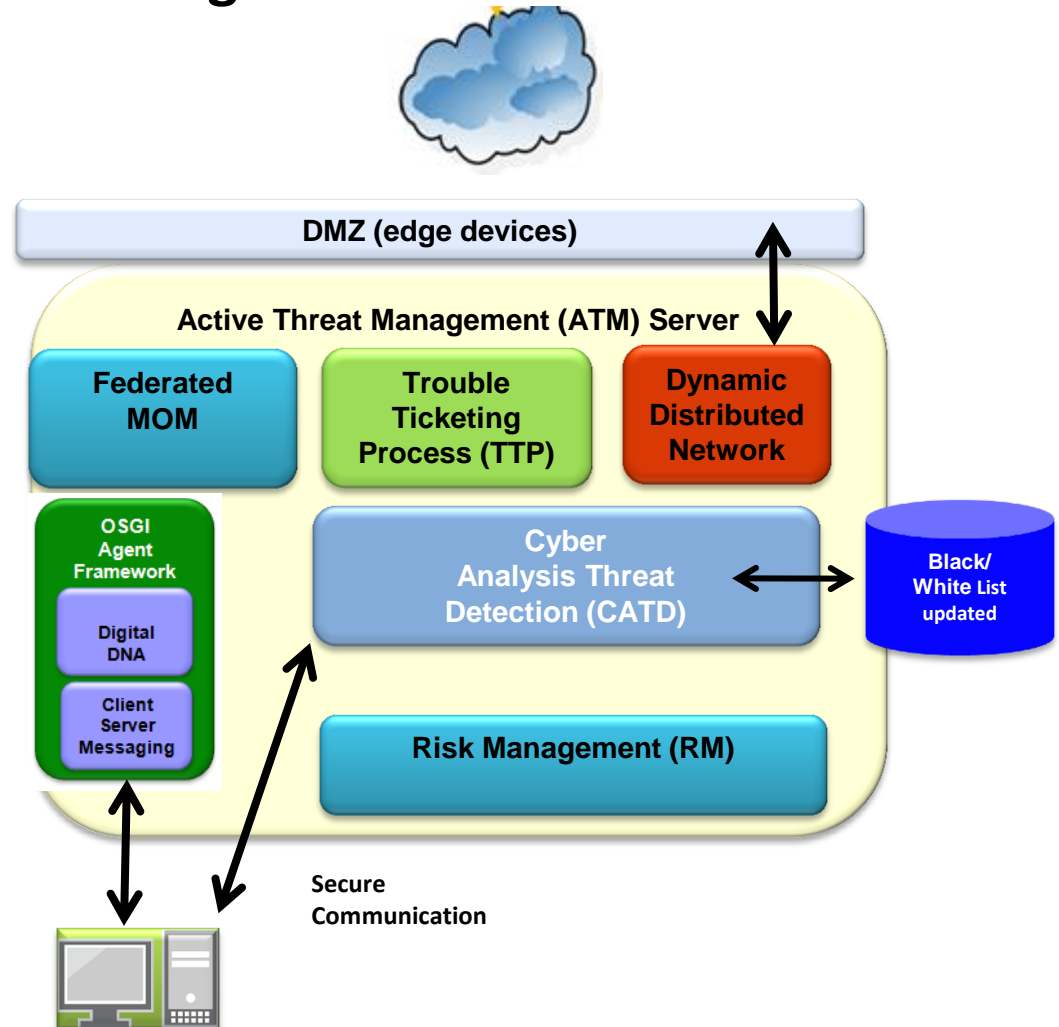
FISMA View

SEIM View

After sustaining an organization,
move into
Active Threat Management (ATM)

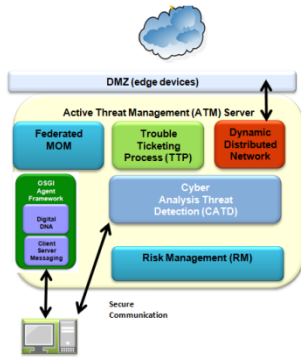
1. Digital DNA detects zero-day malware on a host
2. Agent framework distributes malware signature to CATD
3. CATD monitors network for new malware signature, correlates signature, and runs business logic against data
4. CATD sends required network changes to block the spread of the malware from infected host to ATM
5. The ATM sends TTP the appropriate information to open ticket and alert security/network personnel
6. Human then accepts or denies suggested remediation
7. TTP communicates back to ATM server with response
8. ATM signals DDN to configure network devices to protect network from new malware if applicable
9. ATM distributes malware signature to all sites in federation and sends confirmation of applied network change to CATD if applicable
10. CATD sends confirmation of change back to ATM server if applicable and updates Black/White list
11. ATM sends confirmation of change back to TTP for ticket closure if applicable or apply open issues to RM

Use Case for Active Threat Management

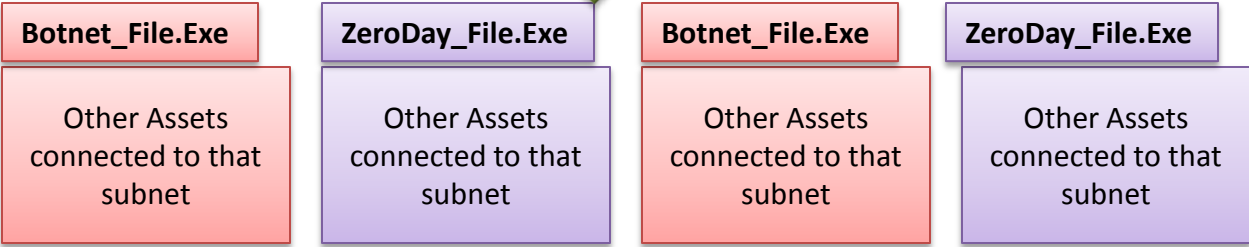


Correlate ATM Findings across the Enterprise

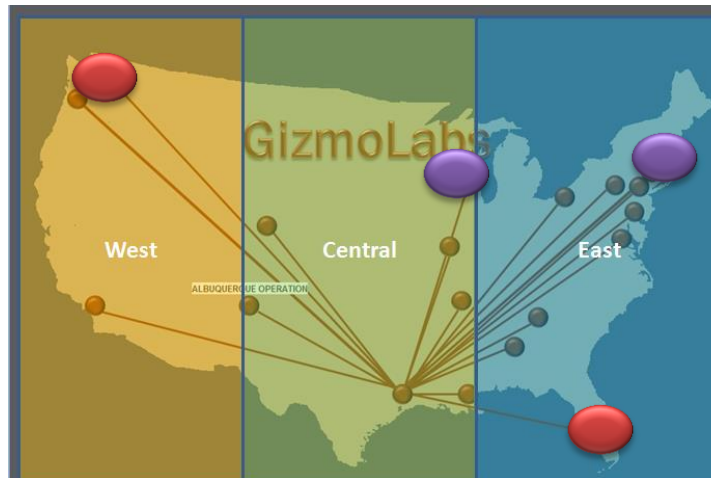
Apply ATM to all Assets



Correlate Vulnerability Scans and other Intel across the environment



Same Vulnerability Files found across GEO Locations



Business & Cyber Security opportunities

(& related System Engineering / Integration efforts)

IT / Cyber Global factors – user pull

World-wide B2B

Trust / cloud / sharing

IoT / M2M

Automation / Sensors

Consumerization of IT

*Phones / wireless / **apps***

Privacy / Data

IP / PII / compliance

GAPS / Needs

(from the Federal cyber priority council S&T gaps)

TRUST

Distributed / MLS

Resiliency

*SW / apps / **APIs** / services*

Agile operations

BE the vanguard / integration

Effective missions

Business success factors

Vulnerabilities / Threats

(Verizon BDR, Forbes, etc threat reports - what ails us most)

CM / Hygiene

patching / settings

Access control

Authentication is key

TOP security mitigations

Whitelist, patch, limit access

Risk Mgmt

Adhoc / not global

Future Opportunities

Effective Business risk management (BRM) = cybersecurity framework (CMMI / RMF / COBIT)

Reducing business risk / liabilities... *Managed security services (MSS) & cyber insurance ...*

SIEM / SCM

QA hygiene / sensors

“ESA” / simple tools!

Mobile Security

Poor apps / IOS weak

billions users = volume

Mitigate Obsolescence

Minimize patching, legacy vulnerabilities

OA / modularity / APIs & SCRUM

Data Security

Predictive analytics

Privacy by design

Summary

- Applying algorithms to help define metrics
- Aggregate the metrics to define Threshold Settings
- Once your baseline metrics have been defined, Threat Vectoring can be achieved
- Moving to proactive posture through Active Threat Management

Mike.Davis.SD@gmail.com

And

rick@cyberclarity.com