NORTH ATLANTIC TREATY
ORGANIZATION

SCIENCE AND TECHNOLOGY
ORGANIZATION

AC/323()

www.sto.nato.int

STO TECHNICAL REPORT

PUB REF STO-MP-SAS-114-PPL

ANNEX L
Information Systems Continuous Monitoring for Cyber-Security Risk Prioritization

Greg Weaver

ISCM Update for SAS 114

Greg Weaver
ARL/CISD/SBNAB
W: 301-394-1260

ISCM Widget Descriptions

Asset Mgmt. Widget

- Provides a unified view of asset information collected from all reporting tool feeds
- Represents each computing asset as an object comprised of information gathered from one or more cyber security tools.

Antivirus Compliance Widget

- Host based security requirements
- Determines overall anti-virus compliance
- Determines anti-virus engine compliance
- Determines anti-virus signature file compliance

Network Mgmt. Widget

- Discovers rogue or unmanaged hosts across the network
- Discovers active services and systems within a zone
- Discovers access patterns from external zones
- Determines inbound and outbound volumes of traffic

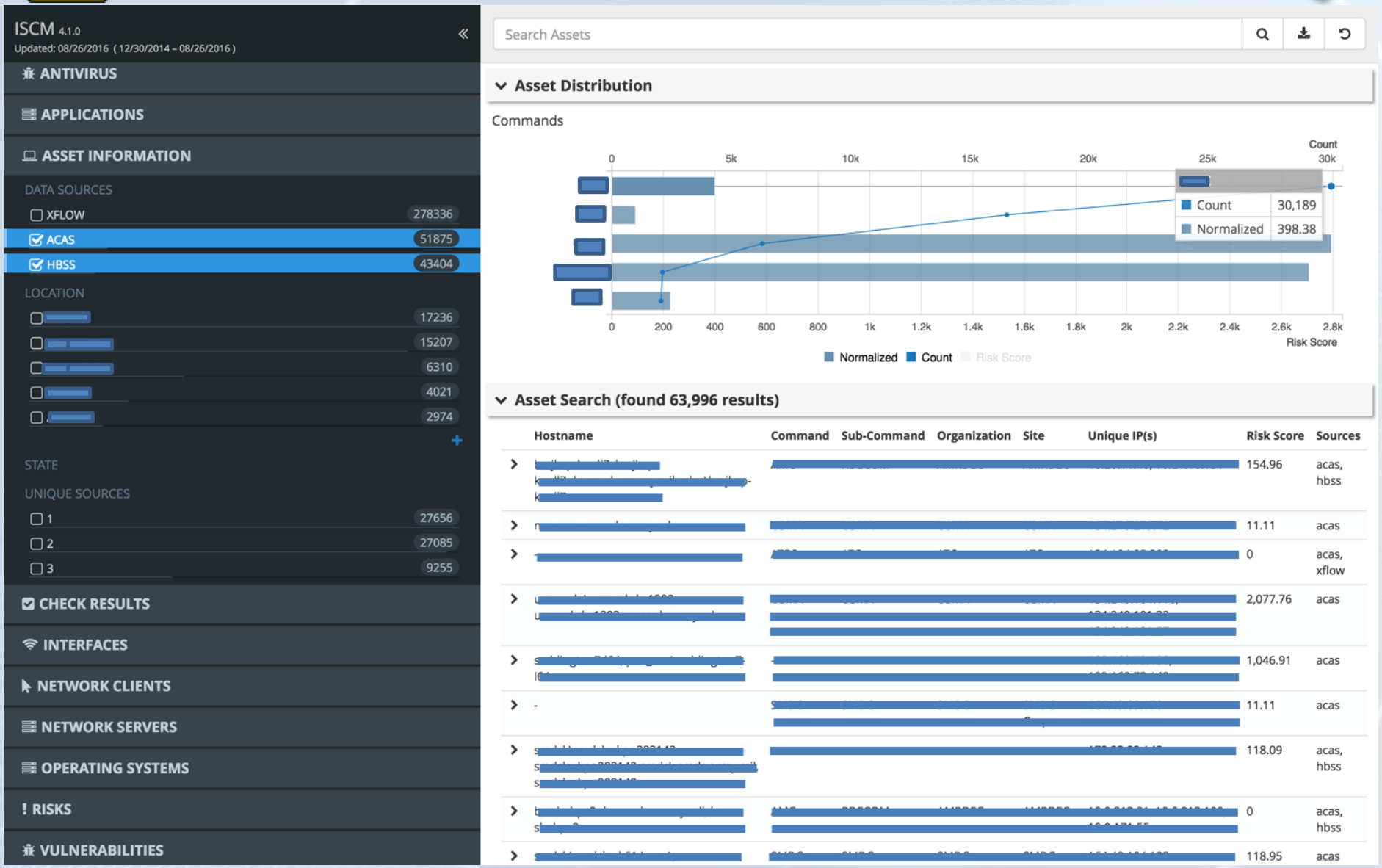
Vulnerability Widget

- Identifies vulnerable systems by CVE; includes confidence value for instances which lack definitive evidence
- Determines vulnerability distribution across enterprise for given software version/ platform
- Presents searchable catalog of security metadata (vulnerabilities, check definitions, platforms, software, ports)

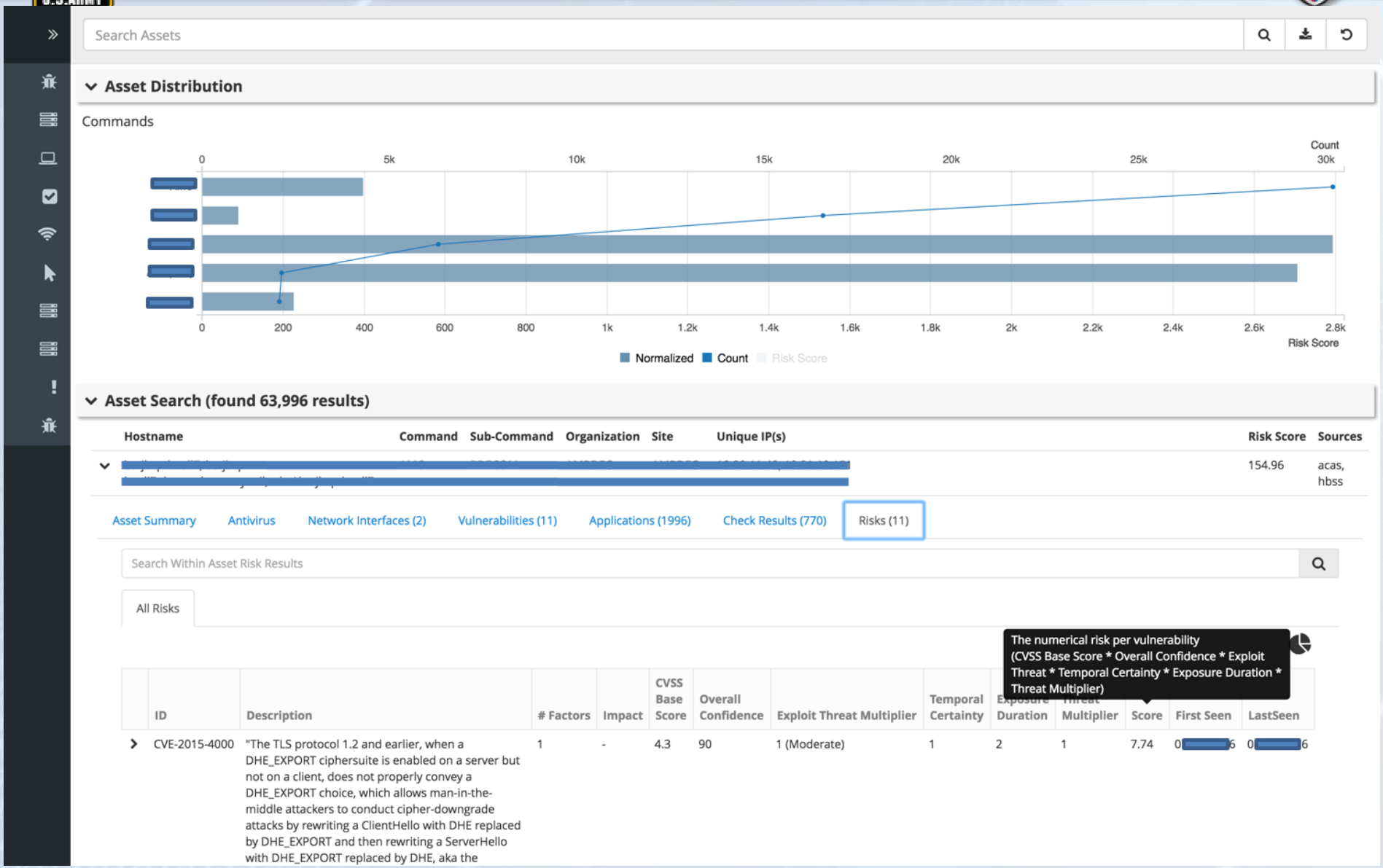
Risk Mgmt. Widget

- Use of vulnerability discovery results to estimate risk
- Risk = f(threat x vulnerabilities x impact)
- Risk scores are presented by zone, system, and vulnerability
- Identifies issues that need to be mitigated in order to eliminate a particular risk at the system or zone level
- Presents issues prioritized by their influence on risk

ISCM UI (v.4.1)


ISCM 4.1.0
Updated: 08/26/2016 (12/30/2014 – 08/26/2016)
ANTIVIRUS
APPLICATIONS
ASSET INFORMATION
DATA SOURCES
XFLOW 278336
ACAS 51875
HBSS 43404
LOCATION
17236
15207
6310
4021
2974
STATE
UNIQUE SOURCES
1 27656
2 27085
3 9255
CHECK RESULTS
INTERFACES
NETWORK CLIENTS
NETWORK SERVERS
OPERATING SYSTEMS
! RISKS
VULNERABILITIES
Search Assets
Asset Distribution
Commands
Count
0 5k 10k 15k 20k 25k 30k
Count 30,189
Normalized 398.38
0 200 400 600 800 1k 1.2k 1.4k 1.6k 1.8k 2k 2.2k 2.4k 2.6k 2.8k
Risk Score
Normalized Count Risk Score
Asset Search (found 63,996 results)
Hostname Command Sub-Command Organization Site Unique IP(s) Risk Score Sources
154.96 acas, hbss
11.11 acas
0 acas, xflow
2,077.76 acas
1,046.91 acas
11.11 acas
118.09 acas, hbss
0 acas, hbss
118.95 acas

ISCM UI (v.4.1) cont...



ISCM Data Types

ARL data types:

ACAS Assured Compliance Assessment Solution

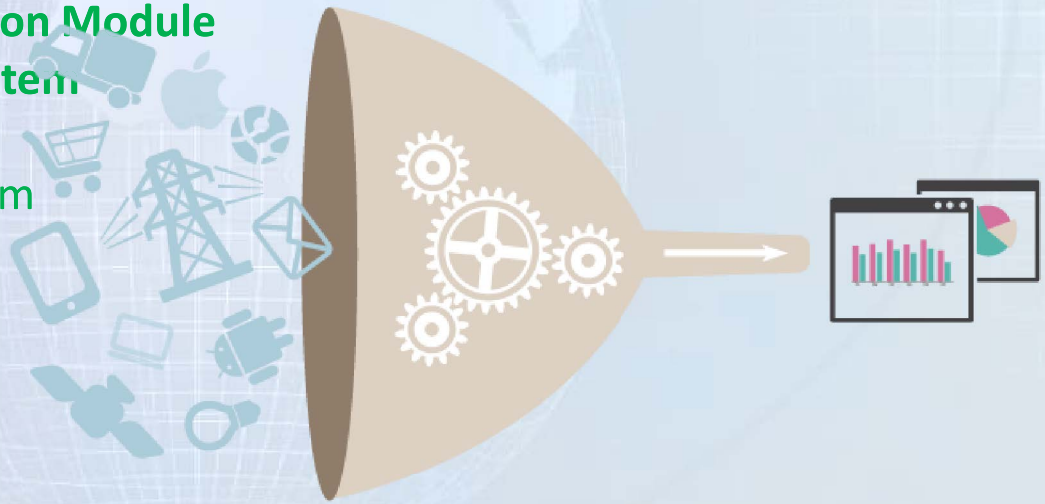
- **Vulnerability Scan Results**

HBSS Host Based Security System Modules (PA, ACCM, HIPS, VSE)

- **Policy Auditor**
- **Asset Compliance Configuration Module**
- **Host Intrusion Prevention System**
- **Virus Scan Enterprise**

Interrogator Intrusion Detection System

- **XFLOW**
- **ISTR/Internet strings**
- **DSTR/DNS strings**
- **IDS Detects/Alerts**
- **IDS Incident reports**
- **IDS libpcap (packet capture)**



Green = Current
Yellow = Planned
Red = Future

Image attribution: http://www.virdata.com/wp-content/uploads/2014/02/datapump_3.png

One Page Summary

Our Information Systems Continuous Monitoring (ISCM) is an integrated big-data capability that provides situational awareness down to the asset level as well as cyber security risk prioritization and categorization for multiple enclaves, as each asset object is a fusion of data gathered from reports generated via the endpoint security, vulnerability assessments and intrusion detection system data flows. These data sources were chosen because they are ubiquitous across the department, but they could be easily swapped with other data sources if the attributes of interest were available for extraction.

Our ISCM big-data capability supports our overarching goal in efforts to conduct research and development to deploy an operational framework that will:

- Enhance cyber situational awareness – The ability to ingest, aggregate, correlate and enrich cyber data from a variety of sources and provide an interface or dashboard view that enables commanders and missions owners to make higher confidence decisions and prioritize cyber security risks and responses.
- Support continuous monitoring – The ability to transform the historically static security control assessment and authorization process into an integral part of a dynamic enterprise-wide risk management process. Providing the Army with an ongoing, near real-time, cyber defense awareness and asset assessment capability.
- Enable technical transfer – The ability to be packaged and transitioned to other organizations with a similar cyber security mission and data sets. In particular, it is important that ISCM be transferable with minimal software refactoring and systems reengineering.
- Provide a scalable architecture – The ability to scale quickly be augmented with minimal impact to uptime and support the storage and processing of large data sets at the TB/PB scale.
- Enable low latency queries – The ability to provide rapid responses to simple and compound queries from both end users and statistic/analytic processes (query focused)