Joint Regional Security Stack (JRSS)

Col Scott Jackson, USAF
Chief, JIE Solutions Division
21 April 2016
“The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government. This brief may also contain references to United States Government future plans and projected system capabilities. Mention of these plans or capabilities in no way guarantees that the U.S. Government will follow these plans or that any of the associated system capabilities will be available or releasable to foreign governments.”
Joint Regional Security Stack – Analogy

JRSS - 25 regional “Stacks” or “Vaults”

- Firewall
  Access Block (Basic Access)
- Prevention systems (IPS)
- Detection Systems (IDS)
- Logs/ Analytics (ArcSight)
- Isolated internal protections (VRF/ Multi-tenant)

24/7 Management and Control
Joint Regional Security Stack - Actual

Unclassified NIPRNET “N-JRSS”

“A” side of JRSS used for active traffic

“B” Side of JRSS for Hot Fail Over

Classified SIPRNET “S-JRSS”

Joint Management System

Intrusion Prevention Systems (IPS)

Intrusion Detection Systems (IDS)

Firewalls

Routers

Transport Cu/Fiber/SW

Management, Logging & Forensic systems
**JRSS/JMS Deployment Plan**

**JRSS 1.0**
- Dual Core Switch Fabric
  - MPLS Cloud
  - Load Balanced Firewalls
  - Traffic Tap for Passive sensing
- Firewalls (FW)
- Multi-Tenant Management
- Alerts / Logs
- Intrusion Prevention Systems (IPS)
- Intrusion Detection Systems (IDS)
  - Access Control to provide trusted/authenticated access to the JRSS Stack
  - Active Directory (authentication)
  - Element Management for Stack equipment
  - Ticketing System (ITSM)
  - Logging / Alerting and storing data for analytics

**JRSS 1.5**
- Full Packet Capture for Deep packet analysis
  - Upgraded Identity Management (IDAM)
  - VDI and Secure View (Secure Access Gateway)
  - Backup and Recovery
  - Performance management
  - Additional Event Management

**JRSS 2.0 (Projected)**
- Forward Proxy for Web Content Filtering
- SSL Decrypt
- Enterprise Inline IPS
- Detonation Chamber
- WANX
- Log Aggregation
  - Upgrade Element Management for all JRSS 2.0 capabilities

**Note:** JRSS 2.0 Functional Requirements Document expected approval April ’16

---

**LEGEND**
- Stack Capability
- Management Capability

---

**UNCLASSIFIED**

**UNITED IN SERVICE TO OUR NATION**

5
Joint Regional Security Stack (JRSS)

- Addresses immediate needs:
  - Defend the cyber warfighting domain
  - Shrinks attack surface
  - Standardize security architecture
  - Streamline Command and Control
  - Synchronize Global Network Operations

JRSS Value Proposition = Security + Network Modernization + Cyber SA
Many Partnerships ...

<table>
<thead>
<tr>
<th>JRSS components:</th>
<th>Contract Support:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Palo Alto</td>
<td>• GSMO/LMCO</td>
</tr>
<tr>
<td>• Hewlett Packard</td>
<td>• Cambridge</td>
</tr>
<tr>
<td>• Fidelis</td>
<td>• NES</td>
</tr>
<tr>
<td>• Hadoop</td>
<td>• VAE</td>
</tr>
<tr>
<td>• InQuest</td>
<td>• EMC2</td>
</tr>
<tr>
<td>• Gigamon</td>
<td></td>
</tr>
<tr>
<td>• Stealth Watch</td>
<td>... and growing!</td>
</tr>
<tr>
<td>• Trend Micro</td>
<td></td>
</tr>
<tr>
<td>• Source Fire</td>
<td></td>
</tr>
<tr>
<td>• OpsWat</td>
<td></td>
</tr>
<tr>
<td>• F5</td>
<td></td>
</tr>
<tr>
<td>• Bivio</td>
<td></td>
</tr>
<tr>
<td>• Niksun</td>
<td></td>
</tr>
<tr>
<td>• RedSeal</td>
<td></td>
</tr>
<tr>
<td>• Blue Coat</td>
<td></td>
</tr>
<tr>
<td>• vmWare</td>
<td></td>
</tr>
<tr>
<td>• Juniper</td>
<td></td>
</tr>
<tr>
<td>• Splunk</td>
<td></td>
</tr>
<tr>
<td>• Microsoft</td>
<td></td>
</tr>
<tr>
<td>• BMC</td>
<td></td>
</tr>
<tr>
<td>• CISCO</td>
<td></td>
</tr>
<tr>
<td>• ArcSight</td>
<td></td>
</tr>
<tr>
<td>• Ciena</td>
<td></td>
</tr>
<tr>
<td>• Ciena</td>
<td></td>
</tr>
</tbody>
</table>

... and growing!