Agenda

- About Intellectual Point
- Today’s Cyber Threat Landscape
- Shortage of Cyber Security Skills
- Success Stories
About Intellectual Point

Intellectual Point is a Global Information Technology, Training, Consulting and Software Development Company. Intellectual Point provides professional hands-on computer and IT training and consulting to prepare you with the skills and knowledge needed for today’s competitive job market.

- Workforce Development
- IT Training & Certification
- Authorized Testing Center
- Job Placement & Staff Augmentation
- Cyber Security Consulting
- Risk Assessment & Compliance
Partnerships & Contracts
ABOUT ME

• CEO & Founder – Intellectual Point (IP) – IT Training and Workforce Development & Consulting
• CTO – Government Acquisitions Inc. (GAI) – IT Solutions Provider to the Federal Government
• 20+ years in IT Industry in various capacities
• BS & MS (Computer Science), IIT, Chicago
• MBA (Marketing and Strategy), IIT, Chicago
• Completed Coursework in Ph.D. (Information Assurance & Cyber Security), George Mason University (GMU)
• Hold 100+ certifications and advanced credentials including Security+, CISSP, CEH, CISM, CCNA, VCP, AWS, CCNP.
• Served as a Commissioner of the TechAmerica Commission for Big Data Analytics and Cloud Computing
• Speaker at reputable conferences and industry tradeshows and author of many publications.

PREM JADHWANI
CEO & PRESIDENT
PREM@INTELLECTUALPOINT.COM
PHONE: 703-554-3827
STATE OF THE CYBER SECURITY LANDSCAPE

MARKET SURVEY
New Threat Landscape and Advanced Targeted Attacks

- Malware has gone beyond most existing signature based security controls
- Organizations largely unaware of the problem
- They are actively and silently sending data out the door
- We MUST change our strategy to match the problem

Random Attack:
- Viruses / Worms
- Port Scans
- Phishing

Targeted Attack:
- Denial of service
- Theft of service
- Information theft
- IP theft
- Ransomware
Traditional Defenses Don’t Work

- The new breed of attacks evade signature-based defenses
The Future of Security

Past

AV

Hips / Anti-Exploitation

Sandboxing

Isolation

Present

Future

EDR

AI

Humans Needed

Specialized Humans Needed
Post-Execution

Highly skilled Humans + Machine Intelligence
Pre-Execution
New Mindset for Information Security

• Old Mindset
  • Signatures
  • Point solutions
  • Fixed perimeters
  • Ownership = trust
  • Security “Boxes”
  • Security solution silos
  • Manual policy config
  • Block and prevent
  • Incident response
  • Protect devices / networks

• New Realities
  • Algorithms
  • Platforms that correlate and share
  • Adaptive perimeters
  • Repudiation services
  • Security software, some in HW
  • Security as an adaptive system
  • Security automation
  • Detect and Respond
  • Continuous response
  • Protect information
Security Technologies and Skills Spectrum

Fundamentals
- Endpoint protection
- Network Segmentation
- Firewall/IPS
- Secure Web Gtw

Advanced Technology
- SEIM
- Mobile Device Security
- App White/Black Listing
- Next Gen Firewall
- NAC
- Network Traffic Analysis
- Payload Analysis
- Forensics
- Endpoint Threat
- Detection Response
- High Trust User Auth

Lean Forward
- Vulnerability Management
- Privilege Management

Process

Change Control
- Incident Response
SHORTAGE OF CYBER SECURITY SKILLS

MARKET SURVEY
1.5 Million
MORE cybersecurity professionals will be needed to accommodate the predicted global shortfall by 2020

Source: (ISC)² 2015 Global Information Security Workforce Study

On average, 52% of IT professionals surveyed stated fewer than 25% of all applicants were qualified


The biggest skill gaps of today’s cybersecurity professionals:

? 72% Ability to Understand the Business

跫 46% Technical Skills

 trò 42% Communication Skills


Fastest cybersecurity demand sectors are in industries managing consumer data:

 Industries Managing Consumer Data

- 40% Professional Services
- 16% Finance and Insurance
- 14% Manufacturing and Defense
- 30% Other

Source: Job Market Intelligence: Cybersecurity Jobs, 2015–2016 Burning Glass Technologies
Cybersecurity job postings took 8% longer to fill than IT job postings overall.

*Source: (ISC)² 2015 Global Information Security Workforce Study*

Expertise required for various cybersecurity roles in demand:
- Information Security
- Network Setup
- Auditing
- Network Protocols
- Core Database, Coding and Scripting
- Systems Administration

*Source: Job Market Intelligence: Cybersecurity Jobs, 2015*

Approximately 10% of the current cybersecurity workforce are comprised of women.

*Source: (ISC)² 2015 Women in Security: Wisely Positioned for the Future of InfoSec*

18% Growth
Computer and mathematical occupations will grow much faster than the average job during 2012–2024.

*Source: Bureau of Labor Statistics, U.S. Department of Labor*

Fastest growing skills in cybersecurity job postings:
- Python
- HIPAA
- Risk Management
- Internal Auditing
- Audit Planning

*Source: Partnership for Public Service*

Hardest to fill skills in cybersecurity job postings:
- Software Architecture
- Network Attached Storage (NAS)
- Software Issue Resolution
- Internet Security
- Legal Compliance
- Data Communications
- Platform as a Service (PaaS)
- Computer Forensics
- Internal Auditing
- Apache Hadoop
Has a shortage of cybersecurity skills had a negative effect on your organization?

- 35%: We can't maintain an adequate staff of cybersecurity professionals
- 17%: We are a target for hackers as they know our cybersecurity is not strong enough
- 22%: We've lost proprietary data through cyber attacks
- 25%: We've suffered reputational damage
- 33%: Reduced ability to create new IP for products and services

Figure 5. Impact of cyber workforce shortage.
TOTAL NUMBER OF JOB POSTINGS:

Security Analyst Job Role

175% increase from 2012 to 2015. Data for U.S. only, but reflects an international need.

Source: Burning Glass Technologies Labor Insights, January 2016
## Top 10 Security Skills

### Average Salaries

1. **Lead Software Security Engineer** $233,333
2. **Chief Security Officer** $225,000
3. **Global Information Security Director** $200,000
4. **IT Security Consultant** $198,909
5. **Chief Information Security Officer** $192,500
6. **Director of Security** $178,333
7. **Cyber Security Lead** $175,000
8. **Lead Security Engineer** $174,375
9. **Cyber Security Engineer** $170,000
10. **Application Security Manager** $165,000

**Source:** Dice Jobs Database, 2013-15
Various Cyber Job Roles within the SOC

Multiple roles with different background, skills, pay levels, personalities

- SOC Director
- SOC Manager
- SOC Architect
- Tier 1 Analyst
- Tier 2 Analyst
- Tier 3 Analyst
- Forensics Specialist
- Malware Engineer
- Counter-Intel

- On-the-job training and mentoring, and external training & certifications
- Need motivation via promotion path and challenging work
- Operating hours and SOC scope play key role in driving headcount
Cybersecurity Analyst

**Average Salary**

$85,000

**Common Job Titles**

- Information Security Analyst
- Security Analyst
- IT Security Analyst
- Cyber Security Analyst
- Senior Security Analyst

**Requested Education (%)**

- Sub-BA: 4%
- Bachelor's: 79%
- Graduate Degree: 17%

**Total Job Openings**

22,635

**Common NICE Cybersecurity Workforce Framework Categories**

- Analyze
- Collect and Operate
- Securely Provision
- Operate and Maintain
- Protect and Defend
- Investigate

**Top Certifications Requested**

- CISSP
- GIAC
- CISA
- CISM
- Security+
**Incident Analyst / Responder**

**Average Salary**
- $69,000
- Incident Analyst / Responder

**Common Job Titles**
- Incident Team Lead
- Senior Information Security Analyst
- Incident Management
- Senior Analyst - Information Security
- Technical Team Lead
- Cyber Incident Handler

**Requested Education (%)**
- Sub-BA: 23%
- Bachelor's Degree: 61%
- Graduate Degree: 17%

**Total Job Openings**
- 15,463

**Common NICE Cybersecurity Workforce Framework Categories**
- Protect and Defend
  - Cyber Defense Analysis
  - Cyber Defense Infrastructure Support
  - Incident Response
  - Vulnerability Assessment and Management

**Top Certifications Requested**
- CISSP
- GIAC
- CISM
- CISA
- Security+
Roadmap from Entry Level to Mid Level Cyber Jobs (Cyberseek.org)

**TOP CYBERSECURITY JOB TITLES**
- Cyber Security Engineer
- Cyber Security Analyst
- Network Engineer / Architect
- Cyber Security Manager / Administrator
- Software Developer / Engineer
- Systems Engineer
- Systems Administrator
- IT Auditor
- Vulnerability Analyst / Penetration Tester
Mapping Job Roles to NIST NICE Cybersecurity Workforce Framework (SP 800-181) (7 Categories, 33 Specialty Areas, 52 Work Roles)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operate &amp; Maintain</td>
<td>Data Administration</td>
<td>Info System Security Mgt</td>
<td>Knowledge Mgt</td>
<td>Customer &amp; Tech Support</td>
<td>Network Services</td>
<td>System Administration</td>
<td>Systems Security Analysis</td>
</tr>
<tr>
<td>Protect &amp; Defend</td>
<td>Computer Network Defense (CND)</td>
<td>Incident Response</td>
<td>CND Infrastructure Support</td>
<td>Security Program Mgt</td>
<td>Vulnerability Assessment &amp; Mgt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyze</td>
<td>Cyber Threat Analysis</td>
<td>Exploitation Analysis</td>
<td>All-source Analysis</td>
<td>Targets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operate &amp; Collect</td>
<td>Collection Operations</td>
<td>Cyber Operational Planning</td>
<td>Cyber Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oversight &amp; Development</td>
<td>Legal Advice &amp; Advocacy</td>
<td>Strategic Planning &amp; Policy</td>
<td>Education &amp; Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investigate</td>
<td>Investigation</td>
<td>Digital Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Establishing National Standards

Knowledge, Skills, and Abilities (KSA)
TOOLS, SKILLS & BEST PRACTICES TO CREATE NEXT GEN CYBER SECURITY PROFESSIONALS

BASED ON INTELLECTUAL POINT EXPERIENCES
Essential Skills for Next Gen Cyber Security Professional (NEXT GEN CYBER WARRIORS)

- TCP/IP, NETWORKING, ROUTING & SWITCHING
- WINDOWS & LINUX OPERATING SYSTEMS
- N/W TRAFFIC MONITORING & PACKET ANALYSIS
- FIREWALL, IDS/IPS & PERIMETER DEFENSES
- VULNERABILITY SCANNING & PEN TESTING
- INCIDENT RESPONSE PROCEDURES
- SECURITY POLICIES & PROCEDURES
- SIEM TOOLS & CONTINUOUS THREAT MONITORING
- DLP, ENDPOINT PROTECTION FOR ZERO DAY & APT
- AUTOMATING COMPLIANCE & RISK (FISMA, RMF, FEDRAMP)
- CYBER THREAT & IOC & IOT LANDSCAPE AWARENESS
- USER BEHAVIOR ANALYTICS & INSIDER THREAT
- SECURITY CONTROLS USING MACHINE LEARNING & NLP
- HELP DESK / TECH SUPPORT EXPERIENCE
- UNDERSTANDING SOCIAL ENGINEERING
- OPEN SOURCE TOOLS & THREAT INTELLIGENCE
- COMMERCIAL SECURITY CONTROLS DEFENSE IN DEPTH
- SCRIPTING SKILLS WITH PYTHON
- BUSINESS SKILLS, COMMUNICATION SKILLS, REPORT WRITING SKILLS, ANALYTICAL SKILLS, INVESTIGATION & TROUBLESHOOTING SKILLS
- IT CERTIFICATIONS & EDUCATION
Security & Networking Concepts & Hands-On Cyber Analysis & Troubleshooting Skills Are Good Place to Start
Next Gen Cyber Professionals need a solid grasp on Open Source Cyber Security Tools
Hands-On Skills for Network Traffic Analysis with Wireshark Are Extremely Valuable

- Fundamentals of network traffic flow
- Structure of network traffic
- Common protocols
- How to use Wireshark for traffic analysis

Course Outline:
Section 1: Troubleshooting Methodology
Section 2: Master Key Wireshark Troubleshooting Tasks
Section 3: Learn Capture Methods and Use Capture Filters
Section 4: Troubleshoot with Time
Section 5: Master Basic and Advanced IO Graph Functions
Section 6: Focus on Traffic Using Display Filters
Section 7: TCP/IP Communications and Resolutions Overview
Section 8: Analyze Transmission Control Protocol (TCP) Protocol
Section 9: Identify Problems Using Wireshark’s Expert
Part 10: Command-Line and 3rd Party Tools
Ethical Hacking & Exploitation Skills using Kali Linux and Metasploit in a Virtual Environment
Cyber Analysts need to learn Open Source Intelligence Tools that can be leveraged on the job

Hidden Social Network Content
Cell Phone Subscriber Information
Deleted Websites & Posts
Missing Facebook Profile Data
Full Twitter Account Data
Alias Social Network Profiles
Free Investigative Software
Useful Browser Extensions
Alternative Search Engine Results
Website Owner Information
Photo GPS & Metadata
Live Streaming Social Content
Social Content by Location
IP Addresses of Users
Additional User Accounts
Sensitive Documents & Photos
Next Gen Cyber Security Professionals have hands-on knowledge of Commercial SOC Tools
Knowledge of FISMA/RMF Compliance is necessary for Public Sector Cyber Security Jobs

- 18 Security Control Families
- 256 Controls to Monitor
- Requires Continuous Monitoring of hundreds of metrics
- Across a range of Data Sources (Applications, Servers, Endpoints, VMs)
- Huge Volumes - Terabytes of data to be collected, indexed and searched daily
- Requires real-time visualization dashboards
- Requires ad-hoc search and forensic navigation across all IT data.
Cyber Professionals should know how to Analyze Vulnerability Scan Reports

<table>
<thead>
<tr>
<th>Severity</th>
<th>Plugin Id</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium (5.1)</td>
<td>18405</td>
<td>Microsoft Windows Remote Desktop Protocol Server Man-in-the-Medium (5.1)</td>
</tr>
<tr>
<td>Medium (5.0)</td>
<td>26920</td>
<td>Microsoft Windows SMB NULL Session Authentication Medium (5.0)</td>
</tr>
<tr>
<td>Medium (5.0)</td>
<td>57758</td>
<td>SMB Signing Disabled Medium (5.0)</td>
</tr>
<tr>
<td>Medium</td>
<td>57690</td>
<td>Terminal Services Encryption Level is Medium or Low Medium</td>
</tr>
<tr>
<td>Low (2.6)</td>
<td>30218</td>
<td>Terminal Services Encryption Level is not FIPS-140 Compliant Low (2.6)</td>
</tr>
<tr>
<td>Info</td>
<td>10150</td>
<td>Windows NetBIOS / SMB Remote Host Information Disclosure Info</td>
</tr>
<tr>
<td>Info</td>
<td>10287</td>
<td>Traceroute Information Info</td>
</tr>
<tr>
<td>Info</td>
<td>10394</td>
<td>Microsoft Windows SMB Log In Possible Info</td>
</tr>
<tr>
<td>Info</td>
<td>10785</td>
<td>Microsoft Windows SMB NativeLanManager Remote System Info</td>
</tr>
<tr>
<td>Info</td>
<td>10940</td>
<td>Windows Terminal Services Enabled Info</td>
</tr>
<tr>
<td>Info</td>
<td>11011</td>
<td>Microsoft Windows SMB Service Detection Info</td>
</tr>
<tr>
<td>Info</td>
<td>11219</td>
<td>Nessus SYN scanner Info</td>
</tr>
<tr>
<td>Info</td>
<td>11936</td>
<td>OS Identification Info</td>
</tr>
<tr>
<td>Info</td>
<td>12053</td>
<td>Host Fully Qualified Domain Name (FQDN) Resolution Info</td>
</tr>
<tr>
<td>Info</td>
<td>19606</td>
<td>Nessus Scan Information Info</td>
</tr>
<tr>
<td>Info</td>
<td>24786</td>
<td>Nessus Windows Scan Not Performed with Admin Privileges Info</td>
</tr>
<tr>
<td>Info</td>
<td>25220</td>
<td>TCP/IP Timestamps Supported Info</td>
</tr>
<tr>
<td>Info</td>
<td>26917</td>
<td>Microsoft Windows SMB Registry : Nessus Cannot Access the Ethernet Card Manufacturer Detection Info</td>
</tr>
<tr>
<td>Info</td>
<td>35716</td>
<td>Common Platform Enumeration (CPE)</td>
</tr>
<tr>
<td>Info</td>
<td>45609</td>
<td>Device Type</td>
</tr>
<tr>
<td>Info</td>
<td>54615</td>
<td></td>
</tr>
</tbody>
</table>
Cyber Professionals need to know how to Read and Write Plan of Action & Milestones (POAM) & SSP & SAR

Plan of Action and Milestones (POA&M)

Vendor Name
Information System Name
Version 1.0

System Name: DoD Network
Company/Organization Name: CDSE
Sponsoring Service/Agency: Defense Security Service

Date of this POA&M: 10/1/2016
Date of last update: 2/15/2016
Date of original POA&M: 10/1/2015

ISSM Name: John Doe
ISSM Phone: 410-xxxx-xxxx
ISSM Email Address: john.doe1000.cio@mail.mil

IS Type: Enclave
UID: 009-1111-2222

Item Identifier | Weakness or Deficiency | Security Control | POC | Resources Required | Scheduled Completion Date | Milestones with Completion Dates | Changes to Milestones | Weakness/Deficiency Identified by | Risk Level (Low/Med/High) | Estimated Cost | Status | Comments
--- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | ---
FY16_001 | Users are able to connect remotely | ACL-1/ | John Doe | Network Administrator | 1/15/2016 | Disable remote access 1/15/16 | N/A | Annual Audit | Medium | 500.00 | Completed |
Teaching Students Valuable Cyber Threat Hunting Skills

Security Information and Event Management

Event Data
- Network Device
- Application
- Server
- Database
- Directory
- Network Firewall
- Application Firewall
- Endpoint Protection
- Data Loss Prevention
- File Integrity Monitor

Context
- Threat Intelligence
- Vulnerability
- User
- Data
- Asset

SIM
- Data Collection
- Query

Repository
- Analysis

Reports

SIEM
- Normalization

SEM
- Incident Management
- Correlation

Real-Time Monitoring
Teaching Students how to Mine Machine Data

All Data is Security Relevant = Big Data

Traditional SIEM
- Firewall
- Authentication
- Vulnerability Scans
- Intrusion Detection
- Data Loss Prevention
- Anti-Malware

Databases, Email, Web, Desktops, Servers, DHCP/DNS, Network Flows, Hypervisor, Badges, Storage, Mobile, APP, Custom Apps, Service Desk, Industrial Control, Call Records
### Tracking RMF Reports Across Security Control Families

<table>
<thead>
<tr>
<th>Enterprise Capability Priorities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware Asset Management</strong></td>
</tr>
<tr>
<td><strong>Software Asset Management</strong></td>
</tr>
<tr>
<td><strong>Vulnerability Management</strong></td>
</tr>
<tr>
<td><strong>Configuration Management</strong></td>
</tr>
<tr>
<td><strong>Enterprise Audit</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Score</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>82.22</td>
</tr>
<tr>
<td>82.22</td>
</tr>
<tr>
<td>100.00</td>
</tr>
<tr>
<td>53.04</td>
</tr>
<tr>
<td>17.72</td>
</tr>
</tbody>
</table>

#### Hardware Asset Management

<table>
<thead>
<tr>
<th>NIST 800-53 Control</th>
<th>Control Name</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA-07</td>
<td>Continuous Monitoring</td>
<td>100.00</td>
</tr>
<tr>
<td>CM-02</td>
<td>Baseline Configuration</td>
<td>46.67</td>
</tr>
<tr>
<td>CM-04</td>
<td>Security Impact Analysis</td>
<td>100.00</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td></td>
<td>82.22</td>
</tr>
</tbody>
</table>

#### Software Asset Management

<table>
<thead>
<tr>
<th>NIST 800-53 Control</th>
<th>Control Name</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA-07</td>
<td>Continuous Monitoring</td>
<td>100.00</td>
</tr>
<tr>
<td>CM-02</td>
<td>Baseline Configuration</td>
<td>46.67</td>
</tr>
<tr>
<td>CM-04</td>
<td>Security Impact Analysis</td>
<td>100.00</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td></td>
<td>82.22</td>
</tr>
</tbody>
</table>

#### Vulnerability Management

<table>
<thead>
<tr>
<th>NIST 800-53 Control</th>
<th>Control Name</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA-02</td>
<td>Security Assessments</td>
<td>100.00</td>
</tr>
<tr>
<td>CA-07</td>
<td>Continuous Monitoring</td>
<td>100.00</td>
</tr>
<tr>
<td>IR-05</td>
<td>Incident Monitoring</td>
<td>100.00</td>
</tr>
<tr>
<td>RA-05</td>
<td>Vulnerability Scanning</td>
<td>100.00</td>
</tr>
<tr>
<td>SI-11</td>
<td>Error Handling</td>
<td>100.00</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td></td>
<td>100.00</td>
</tr>
</tbody>
</table>

#### Configuration Settings Management

<table>
<thead>
<tr>
<th>NIST 800-53 Control</th>
<th>Control Name</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-02</td>
<td>Account Management</td>
<td>49.00</td>
</tr>
<tr>
<td>AC-03</td>
<td>Access Enforcement</td>
<td>100.00</td>
</tr>
<tr>
<td>AC-05</td>
<td>Separation Of Duties</td>
<td>100.00</td>
</tr>
<tr>
<td>AC-07</td>
<td>Unsuccessful Logon Attempts</td>
<td>100.00</td>
</tr>
<tr>
<td>AC-10</td>
<td>Concurrent Session Control</td>
<td>100.00</td>
</tr>
<tr>
<td>AC-11</td>
<td>Session Lock</td>
<td>100.00</td>
</tr>
<tr>
<td>CA-02</td>
<td>Security Assessments</td>
<td>100.00</td>
</tr>
</tbody>
</table>
Cyber Forensic Analysis Skills for Incident Responders

Authentication Overview

- **10142** TOTAL AUTHS
- **6315** TOTAL SUCCESSFUL AUTHS
- **114** TOTAL USERS
- **59** TOTAL ENDPOINTS
- **28** TOTAL SERVICES
- **20** NAS USED

Incoming Auth Requests

- Count
  - 253
  - 500
  - 750

Time:
- 4:00 PM Thu Oct 30 2014
- 8:00 AM
- 12:00 AM Fri Oct 31

Auth Failures

- Count
  - 1

Time:
- 4:00 PM Thu Oct 30 2014
- 8:00 AM
- 12:00 AM Fri Oct 31

Service Categorization

- Other (25%)
- Guest MAC Authentication - Aruba
- Aruba Controller Access Auth
- 802.11 Controller Access Auth

Top 10 User Auths

<table>
<thead>
<tr>
<th>user_name</th>
<th>count</th>
<th>percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEEL Demo</td>
<td>5561</td>
<td>5.39121</td>
</tr>
<tr>
<td>d850e68fbd8f0</td>
<td>344</td>
<td>5.147348</td>
</tr>
<tr>
<td>7e-73-cf-da-05-478</td>
<td>46</td>
<td>0.728424</td>
</tr>
<tr>
<td>dconfort</td>
<td>27</td>
<td>0.427553</td>
</tr>
<tr>
<td>richte</td>
<td>17</td>
<td>0.296290</td>
</tr>
<tr>
<td>fmartos</td>
<td>14</td>
<td>0.221694</td>
</tr>
</tbody>
</table>

Top 10 Services Used

<table>
<thead>
<tr>
<th>service_name</th>
<th>count</th>
<th>percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppFf Controller Access Auth</td>
<td>5569</td>
<td>88.186877</td>
</tr>
<tr>
<td>Guest MAC Authentication - Aruba</td>
<td>359</td>
<td>5.649777</td>
</tr>
<tr>
<td>TACACS Service</td>
<td>52</td>
<td>0.323436</td>
</tr>
</tbody>
</table>

Top 10 Alerts Raised

<table>
<thead>
<tr>
<th>alert</th>
<th>count</th>
<th>percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed</td>
<td>3896</td>
<td>50.27</td>
</tr>
<tr>
<td>Applied 'Reject' profile</td>
<td>987</td>
<td>1.36</td>
</tr>
<tr>
<td>[Endpoints Repository]</td>
<td>148</td>
<td>1.961</td>
</tr>
<tr>
<td>MSCHAP: AD status Access denied (Oct000022)</td>
<td>84</td>
<td>1.04</td>
</tr>
</tbody>
</table>

Top 10 Incoming Client MAC

<table>
<thead>
<tr>
<th>mac_address</th>
<th>count</th>
<th>percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>d659e68fbd08f0</td>
<td>345</td>
<td>64.486981</td>
</tr>
<tr>
<td>7072cb5a0e70a7</td>
<td>46</td>
<td>8.592214</td>
</tr>
<tr>
<td>1c7b215302a7</td>
<td>9</td>
<td>1.582243</td>
</tr>
<tr>
<td>d4f446f740e2</td>
<td>8</td>
<td>1.495327</td>
</tr>
<tr>
<td>182332e683c6c</td>
<td>8</td>
<td>1.495327</td>
</tr>
<tr>
<td>00131a653c707c</td>
<td>7</td>
<td>1.368411</td>
</tr>
</tbody>
</table>

Top 10 IP Used

<table>
<thead>
<tr>
<th>ip_address</th>
<th>count</th>
<th>percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.75.219.233</td>
<td>142</td>
<td>6.666080</td>
</tr>
<tr>
<td>172.17.23.57</td>
<td>141</td>
<td>6.821480</td>
</tr>
<tr>
<td>172.17.219.52</td>
<td>141</td>
<td>6.664800</td>
</tr>
<tr>
<td>172.17.219.219</td>
<td>141</td>
<td>6.664800</td>
</tr>
<tr>
<td>172.17.212.25</td>
<td>140</td>
<td>6.773101</td>
</tr>
<tr>
<td>172.17.212.23</td>
<td>140</td>
<td>6.773101</td>
</tr>
</tbody>
</table>
Teaching Students how to track SOC KPIs & IOCs
Skills to Visualize Security Posture & Cyber IOCs
Skills to Create Dashboards for Tracking FISMA Compliance Trends
Use Case 1 - Incident Investigation/Forensics

- Often initiated by alert in another product
- May be a “cold case” investigation requiring machine data going back months
- Need all the original data in one place and a fast way to search it to answer:
  - What happened and was it a false positive?
  - How did the threat get in, where have they gone, and did they steal any data?
  - Has this occurred elsewhere in the past?
- Take results and turn them into a real-time search/alert if needed
Teaching Students how to create Real Time Dashboards for Compliance Reports

Case #2 – Security/Compliance Reporting

- Many types of visualizations
- Easy to create in Splunk
  - Ad-hoc auditor reports
  - New incident list
  - Historical reports
  - SOC/NOC dashboards
  - Executive/auditor dashboards
Skills for Monitoring Known Threats

Case #3 – Real-time Monitoring of Known Threats

Sources

Example Correlation – Data Loss

Windows Authentication

Endpoint Security

Intrusion Detection

Time Range


Aug 08 08:26:54 snort.acmetech.com (TCP) 10.11.36.20:5072 -> 10.11.36.26:443 itsec snort[18774]: [1:1000000:3] [Classification: Potential Corporate Network Compromise] [Correlation] [Priority: 2]:

Credit Card Number Detected in Clear Text

Data Loss

All three occurring within a 24-hour period
Customizing Dashboards for Monitoring Unknown Threats using Data Correlation

Case #4 – Real-time Monitoring of Unknown Threats

**Sources**

- Email Server
- Web Proxy
- Endpoint Logs

**Example Correlation - Spearphishing**

- 2013-08-09T12:40:25.475Z,,exch-hub-den-01,exch-mbx-cup-00,,STORE DRIVER,DELIVER,79426,,<20130809051115.18154.11234@acme.com,johndoe@acme.com,685191,1,hacker@neverseenbefore.com>. Please open this attachment with payroll information., 2013-08-09T12:40:25.475Z,,exch-hub-den-01,exch-mbx-cup-00,,STORE DRIVER,DELIVER,79426,,<20130809051115.18154.11234@acme.com,johndoe@acme.com,685191,1,hacker@neverseenbefore.com>. Please open this attachment with payroll information.

- Rarely seen email domain
- Rarely visited web site

- 08/09/2013 11:29:48.329 148 TCP_HIT 200 200 0 622 - - OBSERVED GET www.neverbeenseenbefore.com HTTP/1.1 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1); .NET CLR 2.0.50727; InfoPath.1; MS-RTC LM 8; .NET CLR 1.1.4322; .NET CLR 3.0.4506.2152; " User:John Doe

- Rarely seen service

All three occurring within a 24-hour period
## Valuable skills on Indicators of Compromise

### Case #4 – More Examples

<table>
<thead>
<tr>
<th>Attack Phase</th>
<th>What Threat is Doing</th>
<th>What to Look For</th>
<th>Data Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lateral movement</td>
<td>Creating new admin accounts</td>
<td>Account creation without corresponding IT service desk ticket</td>
<td>AD/Service Desk logs</td>
</tr>
<tr>
<td>Data gathering</td>
<td>Stealing credentials</td>
<td>For single employee: Badges in at one location, then logs in countries away</td>
<td>Badge/VPN/Auth</td>
</tr>
<tr>
<td>Data gathering</td>
<td>Gathering confidential data for theft</td>
<td>Employee makes standard deviations more data requests from file server with confidential data than normal</td>
<td>OS</td>
</tr>
<tr>
<td>Exfiltration</td>
<td>Exfiltration of info</td>
<td>Standard deviations larger traffic flows (incl DNS) from a host to a given IP</td>
<td>NetFlow</td>
</tr>
</tbody>
</table>
Valuable Skills to understand IOCs & Ability to perform Correlations with Context

### Examples: Correlations / Detections / Context

<table>
<thead>
<tr>
<th>Detection</th>
<th>Indicator</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printer usage</td>
<td>Number of print jobs over a given period of time</td>
<td>Outlier</td>
</tr>
<tr>
<td></td>
<td>Increase in size of print jobs</td>
<td>Outlier</td>
</tr>
<tr>
<td></td>
<td>Unusual times of day</td>
<td>Outlier</td>
</tr>
<tr>
<td></td>
<td>Rare network printer use (the one not closest employee)</td>
<td>Outlier</td>
</tr>
<tr>
<td>Logins to AD or use of SSO</td>
<td>Local vs. remote</td>
<td>Outlier</td>
</tr>
<tr>
<td></td>
<td>Time of day</td>
<td>Outlier</td>
</tr>
<tr>
<td></td>
<td>During vacation times</td>
<td>Outlier</td>
</tr>
<tr>
<td>Abrupt change in the ratio of website categories visited</td>
<td>Monitor’s employee behavior and attitude changes (proxy data)</td>
<td>Outlier/Context</td>
</tr>
</tbody>
</table>
# Learning Valuable Skills on Next Generation Firewalls (NGFW) Security Platform

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>The solution includes a stateful inspection.</td>
</tr>
<tr>
<td>VPN</td>
<td>Offers IPSEC (for site-to-site tunnels) and SSL VPN (for remote access) options.</td>
</tr>
<tr>
<td>Anti-Malware</td>
<td>Built-in perimeter anti-virus and anti-spyware protection.</td>
</tr>
<tr>
<td>Intrusion Prevention</td>
<td>Ability to recognize and restrict inappropriate and unauthorized access.</td>
</tr>
<tr>
<td>Identity-Based Control</td>
<td>Mapping of specific security policies to defined user groups and individuals.</td>
</tr>
<tr>
<td>Data Leakage Protection</td>
<td>Restriction on the egress of sensitive privileged or confidential data.</td>
</tr>
<tr>
<td>Network Access Control</td>
<td>Endpoint integration to ensure each connecting device has appropriate security.</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>Restrictive filtering of web surfing to limit exposure to harmful and inappropriate sites.</td>
</tr>
<tr>
<td>Application Control</td>
<td>Ability to restrict, on a granular level, which web apps are allowed to run.</td>
</tr>
<tr>
<td>Wi-Fi Network Control</td>
<td>Ensuring Wi-Fi networks have the same security stance and abilities as the perimeter.</td>
</tr>
<tr>
<td>WAN Routing &amp; Optimization</td>
<td>Dynamic routing of WAN traffic backed by QoS and prioritization capabilities.</td>
</tr>
<tr>
<td>Encrypted Data Control</td>
<td>Native decryption and re-encryption of SSL and SFTP traffic for thorough inspection.</td>
</tr>
<tr>
<td>Web App Firewalling</td>
<td>Ability to protect web servers against attacks like SQL injections.</td>
</tr>
</tbody>
</table>
User Behavior Analytics Skills for Insider Threat Detection
Risk Management on Unstructured Human Generated Data

Identify Risk – Over-exposed Sensitive Data
DoD ACAS Solution Skills Are Very Valuable for the Public Sector Cyber Jobs

• In 2012, the Defense Information Systems Agency (DISA) awarded the Assured Compliance Assessment Solution (ACAS) to HP Enterprise Services and Tenable Network Security. The ACAS mission is simple: Assess DoD enterprise networks and connected IT systems against DoD standards, as well as identify any known system vulnerabilities.

• ACAS provides complete visibility and prioritized, actionable data through customized reporting. It’s also Security Content Automation Protocol (SCAP) 1.2 compliant and is a follow-on capability to the Secure Configuration Compliance Validation Initiative (SCCVI) tool commonly referred to as “Retina.”
DoD HBSS / ESS Skills are very valuable for the Public Sector Cyber Jobs

- The DOD Endpoint Security Solutions (ESS) is an integrated set of capabilities that work together to detect, deter, protect, and report on cyber threats across all DOD networks. Endpoint security is a DOD-wide effort that leverages the collaborative capabilities of the NSA, Services, DOD CYBER Range, Red Team support, and continuous market research through components and the MITRE corporation.
- The Endpoint ecosystem includes integrated solutions such as Comply to Connect (C2C), Containment, Visibility, and Assessment tools.
- Evolve DOD HBSS to Endpoint Security and integrate endpoint data to situational awareness tools such as SECDEF CYBER SCORE CARD.
eMASS Skills for RMF Automation are very valuable for the Public Sector Cyber Jobs

- eMASS (Enterprise Mission Assurance Support Service) is a government-owned web-based application which supports cybersecurity program management.
- The students learn the features of eMASS specific to their roles. It describes the role of eMASS in the Risk Management Framework for Information Technology; defines eMASS’s implementation of the Authorization Process; and covers how to operate through eMass in order to support the creation, assessment, and authorization of a completed RMF A&A package.
Hands-on Python Skills are highly valued for Cyber Jobs

• It's easy to learn and it is a great language to know when working in InfoSec and Cybersecurity
• Programming knowledge is crucial for analyzing software for vulnerabilities, identifying malicious software and other tasks required for cyber security analysts
• It is a very popular language used to create many security tools
• Python on your resume helps you stand out from other candidates and industry professionals
• Employers are looking for fully stacked programmers. you can automate daily tasks with scripts written in Python

- Introduction to Python Concepts
- Advanced use of Python
- Web Recon
- Port Scanning
- TCP Packet Sniffing
- Perform Forensic Analysis
- Evasion of Antivirus Software
Intellectual Point hosts free Meetups to educate the workforce and spread Cyber Awareness

NoVA IT & Cyber Security Group

This group is for all IT professionals, past, present, and future. We are a dedicated group of professionals who love to learn about anything in the broad IT field, and our group is for all skill levels. We host at least one meetup a month where we get together to learn about new technologies, fields, and opportunities. Our guest speakers are full time professionals who work with cutting edge technologies and want to share their passions.

Recruiters are always welcome at our events. Networking is a key to success when you are job hunting, so please reach out to any of the organizers with your resume if you would like us to give it to our recruiting partners.

Intellectual Point has been kind enough to host our meetup since its inception and as such is our only group sponsor at this point. If you would like to connect with someone at Intellectual Point please use info@intellectualpoint.com.
Our attendees are from various backgrounds

Business, Arts, Science, Math
We welcome all!
We love keeping them updated with emerging technologies

And we’re dedicated to spreading the knowledge
Career Counseling is important step to success and launch of Cyber Professionals

• Pre & Post Career Counseling
• Discuss career options, job roles, pay-scales, growth opportunities
• Helping candidates pick the right courses and make informed decisions aligned with their skills & career aspirations
• Mentoring students throughout the course and after the course completion.
• Part of Intellectual Point Culture
Overcoming Skills Gap via Career Counseling is very critical
Utilizing Cybersecurity Career Pathway at Cyberseek.org to mentor students

Cybersecurity Career Pathway

There are many opportunities for workers to start and advance their careers within cybersecurity. This interactive career pathway shows key jobs within cybersecurity, common transition opportunities between them, and detailed information about the salaries, credentials, and skillsets associated with each role.

Source: CyberSeek
Assisting Clients with writing a cyber oriented resume leveraging past skills like Help Desk, QA, Breakfix etc.
On-The-Job (OJT) Training is Extremely Valuable for workers entering Cyber Workforce.

- On-the-job training, also known as OJT, is teaching the skills, knowledge, and competencies that are needed for employees to perform a specific job within the workplace and work environment.
- Employees learn in an environment in which they will need to practice the knowledge and skills taught in the on-the-job training.
Providing Job Placement Assistance & OJT for potential Clients

Presented by Fairfax County DFS Employment and Training Program
In partnership with Intellectual Point

CAREER Fair

NEUSOLIS

APEX Systems
corporate brokers
Beyond Resumes

eIntern.
hirestrategy
AN ADDISON GROUP COMPANY

veredus
<table>
<thead>
<tr>
<th>IAT LEVEL I</th>
<th>IAT LEVEL II</th>
<th>IAT LEVEL III</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>CCNA-Security</td>
<td>CASP</td>
</tr>
<tr>
<td>CCNA-Security</td>
<td>Security+</td>
<td>CISSP</td>
</tr>
<tr>
<td>Network+</td>
<td></td>
<td>CISM</td>
</tr>
<tr>
<td>IAM LEVEL I</td>
<td>IAM LEVEL II</td>
<td>IAM LEVEL III</td>
</tr>
<tr>
<td>Security+</td>
<td>CASP</td>
<td>CISSP</td>
</tr>
<tr>
<td></td>
<td>CISSP</td>
<td>CISM</td>
</tr>
<tr>
<td>IASAE I</td>
<td>IASAE II</td>
<td>IASAE III</td>
</tr>
<tr>
<td>CASP</td>
<td>CASP</td>
<td>NA – at this time</td>
</tr>
<tr>
<td>CISSP</td>
<td>CISSP</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CNDSP Analyst</th>
<th>CNDSP Infrastructure Support</th>
<th>CNDSP Incident Responder</th>
<th>CNDSP Auditor</th>
<th>CNDSP Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEH</td>
<td>CEH</td>
<td>CEH</td>
<td>CEH</td>
<td>CISM</td>
</tr>
</tbody>
</table>
CAREER TRANSFORMATION
SUCCESS STORIES
Putting People into Cyber Security Careers

**Career Transformation**

- We get many students that come from a non-IT background.
- We ascertain that they have analytical skills, writing skills, communication skills, teamwork skills, quick learning ability.
- We put them through the cyber programs, short courses, workshops and certifications and get them into successful cyber security careers.

**Current Profession**
- Accountants
- Technical Writers
- Banking
- ATM Tellers
- QA / Testing
- Uber Drivers
- Help Desk / Tech Support
- Network Engineers
- Project Managers
- Business Analyst

**New Profession**
- Cyber Security Analysts
- SOC Analysts
- Firewall Engineers
- Incident Responders
- Tech Support
- Jr. Network Engineers
- Help Desk Support
- Security Engineer
- Technical Project Managers
Eric Jennings’ Success Story

**Lucrative Employment Follows Certification Training**

Eric Jennings, an Army Veteran with a Service-Connected Disability, was referred to the Northern Virginia Jobs for Veterans (J4Vets) program in June 2014, after being laid off from a Cyber Security Analyst position with AT&T. One month later he enrolled and received J4Vets-funded assistance to develop a Federal Government style resumes tailor his resume for two Federal Government positions.

In parallel, Jennings pursued Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH) training. In August, he successfully completed both programs. One month later, Jennings gained employment as a Security Analyst with Apex Systems and is now collecting a six-figure salary. Jennings stated his J4Vets funded CEH and CISSP trainings were essential to the interview process, since he was asked to recall many of the topics that he learned in class.

- Name: Eric Jennings
- Previous Profession: Business Analyst
- New Profession: Cyber Security Analyst
- Program: WIOA J4VETS
- Certifications Completed: Security+, CEH, CISSP
Mary Clark’s Success Story

• Lost her job at BT as Config Specialist
• Came as a referral from Fairfax Skillsource Center under WIOA program.
• Completed the following certifications at Intellectual Point
  – CompTIA Security+ & Cloud+
  – ITIL Foundation
  – Cisco CCNA
  – Certified Ethical Hacker (CEH)
• Got placed at ASM Research (Accenture Federal Services Company in Fairfax) in June 2015 as a Cyber Security Analyst in record time.
John Leach’s Success Story

DOL Working for You
Training Program Gets Veteran Off the Sidelines and Into a Job

Even with 22 years of accounting and sales experience and five years in the U.S. Air Force, John Leach could not find a job. His last contracting job had ended in July 2012, and he spent the next year applying for countless positions without even landing an interview. Feeling hopeless, Leach believed that making a transition to a more in-demand career field would open up doors. In September 2013, he dropped by a Leesburg, Va., event and, by what he calls "an act of God," met a representative from the Jobs 4 Veterans program. Funded by the department’s Veterans Workforce Investment Program, J4Vets provides employment and training services for Virginia veterans and creates a pipeline of qualified veterans to high-demand industries. J4Vets connected Leach to an information technology training and education company based in Reston, Va., that provided career guidance and assisted him in obtaining certifications in project management and IT. He then participated in the Northern Virginia Technology Council’s Vetworking pilot program, where he learned about a six-week IT training program offered by Accenture. Leach completed the program and, on Oct. 22, began working at Accenture as a software engineering associate. "I would have continued to be overlooked and on the sidelines indefinitely, and would have lost my house and been homeless if it was not for these programs that help veterans," he said. Leach plans to give back by helping other veterans seeking employment.

• Name: John Leach
• Profession: Accountant
• Program: WIOA J4VETS
• Certifications Completed: CAPM, ITIL, Security+, Cloud+
• Went from unemployed accountant through a full career change and now gainfully employed at Accenture as a Software Engineering Associate
Doug Pedersen’s Success Story

• **Name:** Doug Pedersen
• **Degree:** Liberal Arts
• **Previous Profession:** Help Desk Lead
• **New Career:** Cyber Security
• **Certifications Earned:** Sec+, Cloud+, ITIL, CISSP, CEH, CCNA, Splunk Power User, CISM, AWS Cloud Architect
• **Current Title:** Global Managing Consultant at IBM (Cyber Intelligence & Operations).
• Went from Help Desk Lead to cyber security intelligence and operations managing consultant at IBM/Trustwave in 6 months. Almost doubled his salary in 6 months.
Cyber Security Pathways to Success Program Success

- Special Honor Trophies for students successfully completing multiple certifications in the cyber program and getting placed in cyber analyst roles from help desk positions.
• Cyber Threat Landscape around us has changed dramatically.
• Traditional point products and security tools are no longer effective and there is an acute shortage of trained and skilled cyber professionals.
• IT Certifications are extremely valuable in today’s market.
• Hands-on experience and On the Job Training are extremely valuable.
• Providing a continuous learning environment to workforce with access to open source and commercial cyber security tools is critical in building the next gen cyber workforce.
• Non-technical skills such as communication, writing, analytical & investigative skills are equally important as technical skills for a successful cyber career.
• Automation, Machine Learning, Co-relating events with Big Data Tools & AI is changing the way we all deal with massive amounts of cyber events.
• Mentoring and career counseling is a critical element to guide the workforce transitioning from non-IT and non-cyber jobs into highly lucrative next generation cyber security careers.
Prem Jadhwani
President and CEO
Intellectual Point
Prem@IntellectualPoint.com
703-554-3827
http://www.intellectualpoint.com