Excellence through Education

Intellectual POINT

CREATING THE NEXT GENERATION CYBER PROFESSIONALS

BEST PRACTICES & LESSONS LEARNED

Prem Jadhwani
President & CEO
Intellectual Point
Prem@IntellectualPoint.com

August 4, 2017

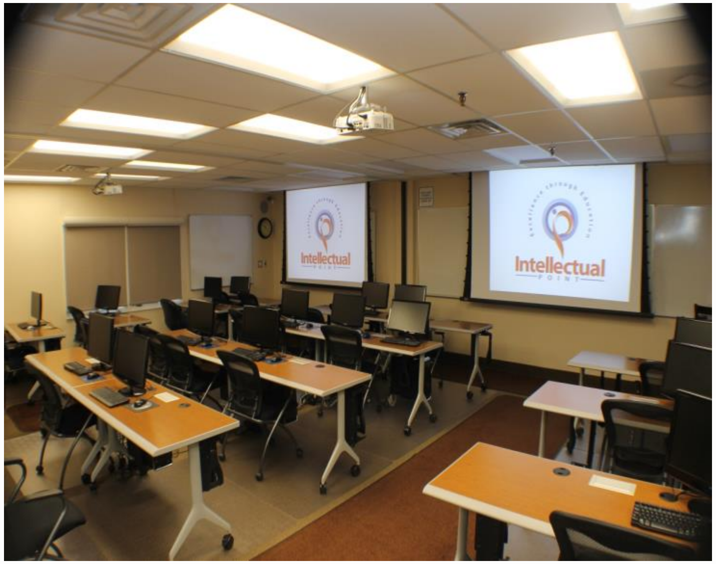
Agenda

- ❑ About Intellectual Point
- ❑ Today’s Cyber Threat Landscape
- ❑ Shortage of Cyber Security Skills
- ❑ Tools, Best Practices and Skills for building Next-Gen Cyber Security Workforce.
- ❑ Success Stories

Excellence through Education
Intellectual
POINT

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

Excellence through Education
Intellectual POINT

State Council of Higher Education for Virginia

Partnerships & Contracts

PMI Registered Education Provider

Project Management Institute

SKILLSOURCE GROUP

Northern Virginia Workforce System

CompTIA

AUTHORIZED PARTNER

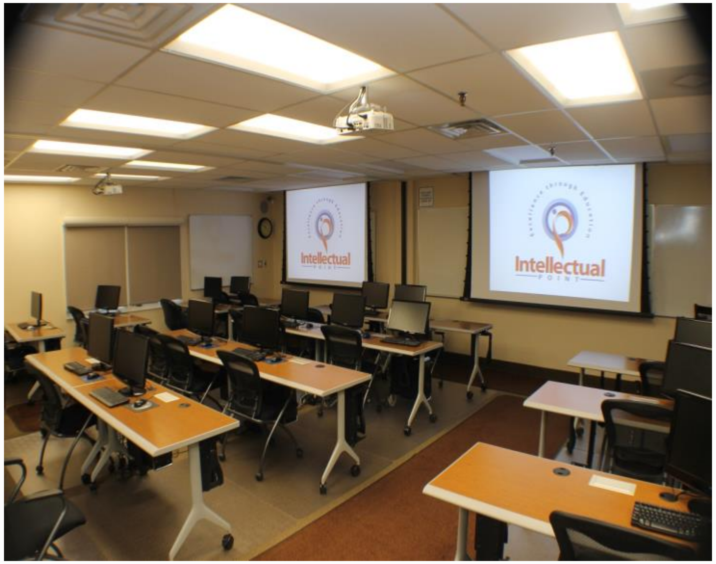
EC-Council

Accredited

Training Center

does

DEPARTMENT OF EMPLOYMENT SERVICES



PEARSON VUE

AUTHORIZED TEST CENTER

KRYTERION

SECURE TESTING SOLUTIONS

Authorized

PROMETRIC

TESTING CENTER

AUTHORIZED

Pan

Testing Center

dsst

ISO-QUALITY

TESTING, INC.

GLOBAL COMPUTERIZED EXAMINATION SOLUTIONS

GSA Contract Holder

Seaport-e

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

Excellence through Education

Intellectual

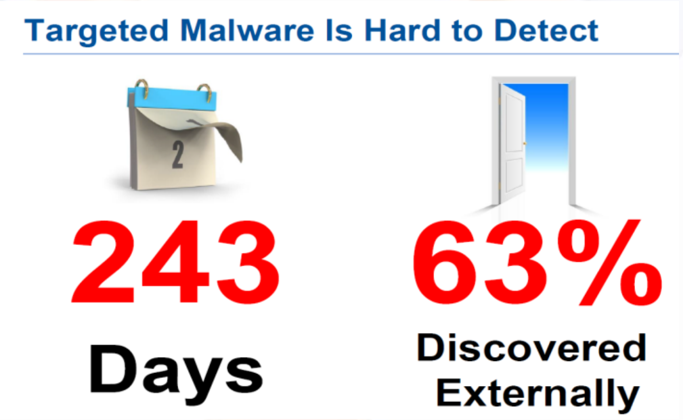
POINT

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



Targeted Malware Is Hard to Detect

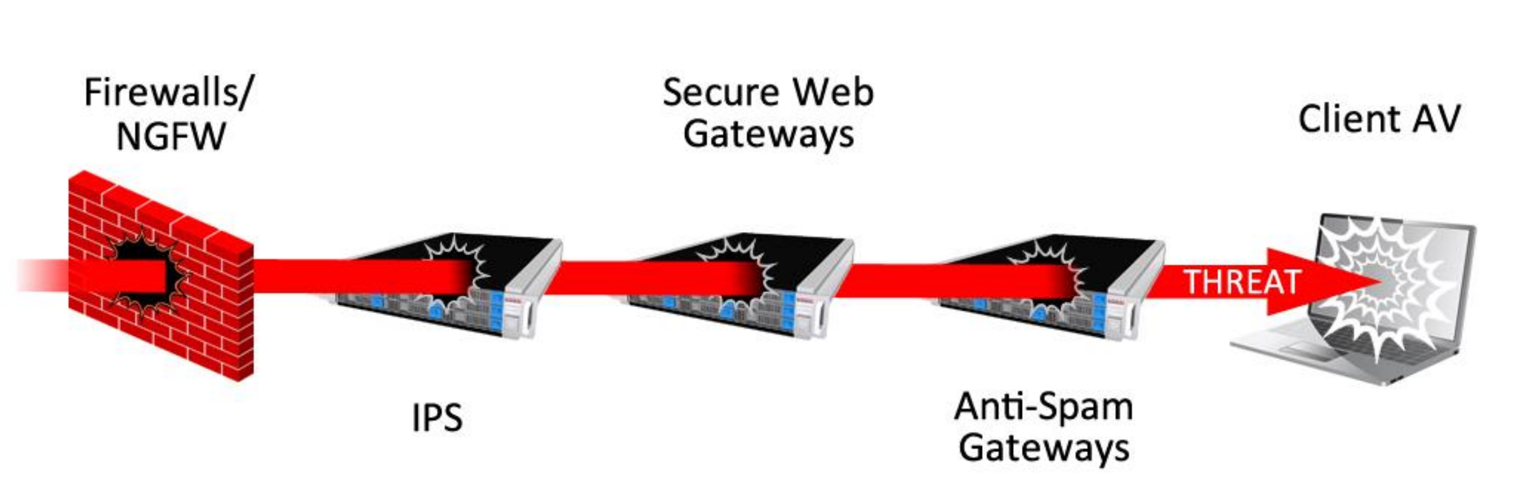
243 Days

63% Discovered Externally

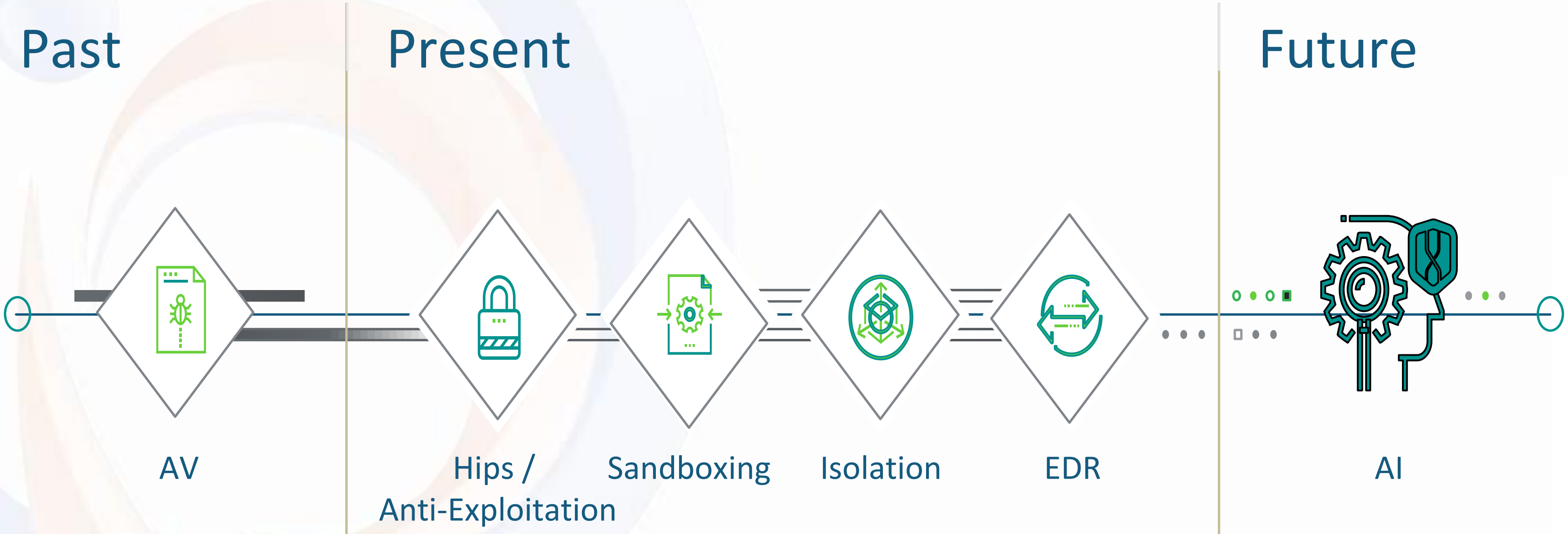
- Random Attack:
  - Viruses / Worms
  - Port Scans
  - Phishing
- Targeted Attack:
  - Denial of service
  - Theft of service
  - Information theft
  - IP theft
  - Ransomware

Traditional Defenses Don't Work

- The new breed of attacks evade signature-based defenses



The Future of Security



Humans Needed

Specialized Humans Needed

Post-Execution

Highly skilled

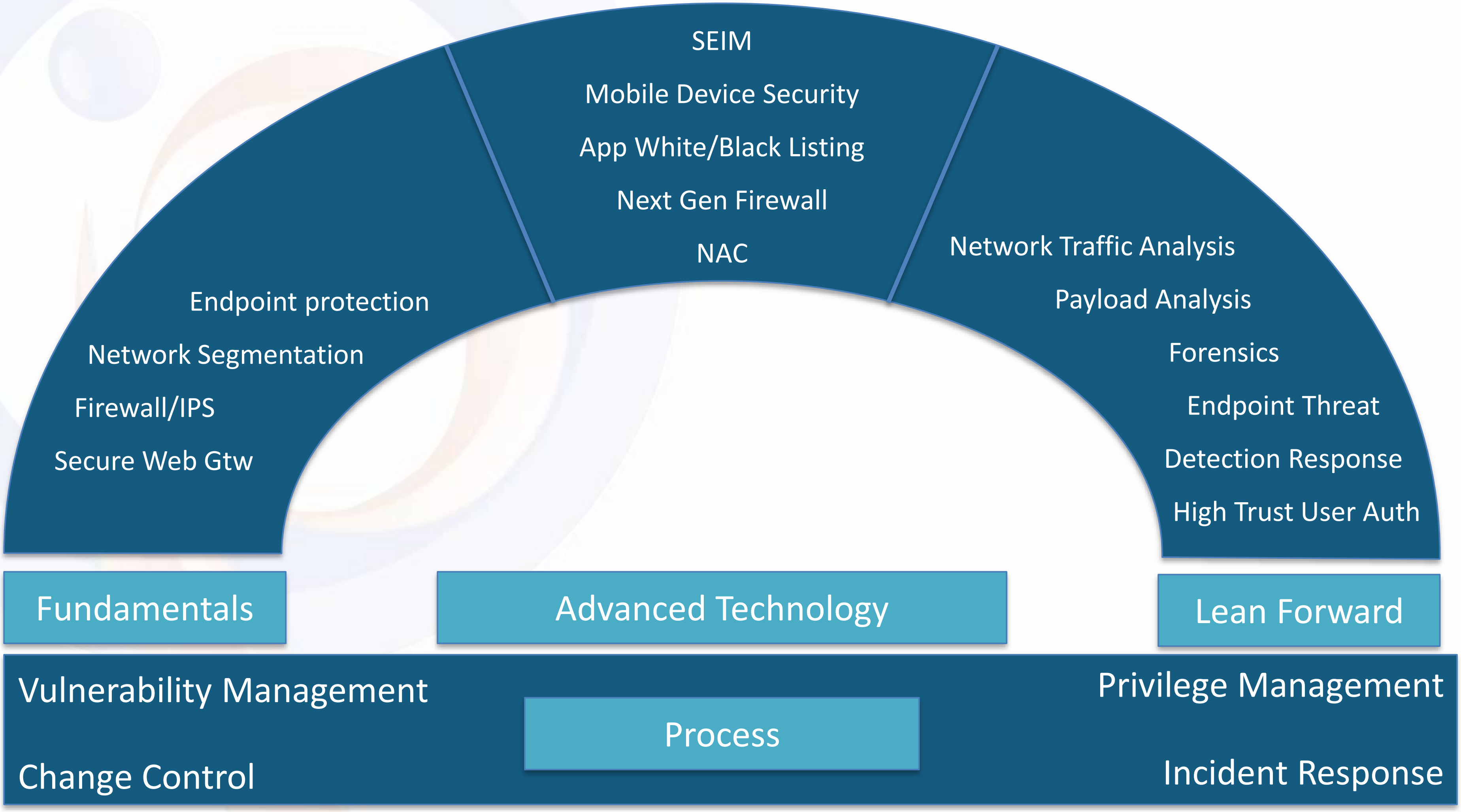
Humans + Machine Intelli

Pre-Execution

New Mindset for Information Security

Old Mindset		New Realities
Signatures	→	Algorithms
Point solutions	→	Platforms that correlate and share
Fixed perimeters	→	Adaptive perimeters
Ownership = trust	→	Repudiation services
Security “Boxes”	→	Security software, some in HW
Security solution silos	→	Security as an adaptive system
Manual policy config	→	Security automation
Block and prevent	→	Detect and Respond
Incident response	→	Continuous response
Protect devices / networks	→	Protect information

Security Technologies and Skills Spectrum



SEIM

Mobile Device Security

App White/Black Listing

Next Gen Firewall

NAC

Endpoint protection

Network Segmentation

Firewall/IPS

Secure Web Gtw

Network Traffic Analysis

Payload Analysis

Forensics

Endpoint Threat

Detection Response

High Trust User Auth

Fundamentals

Advanced Technology

Lean Forward

Vulnerability Management

Change Control

Process

Privilege Management

Incident Response

Excellence through Education

Intellectual POINT

SHORTAGE OF CYBER SECURITY SKILLS

MARKET SURVEY

1.5 Million

MORE cybersecurity professionals will be needed to accommodate the predicted global shortfall by 2020

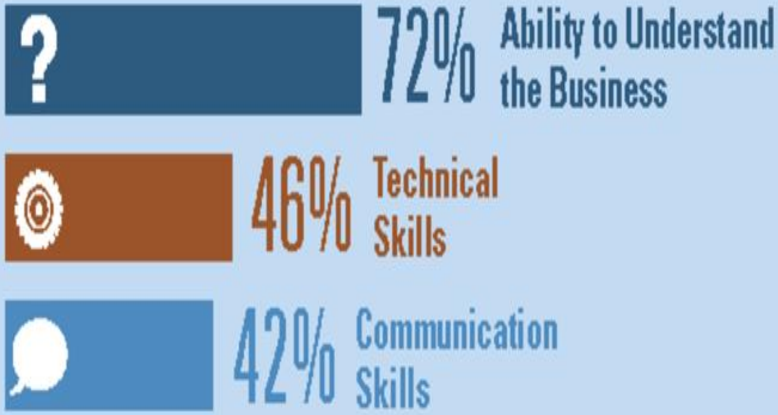
Source: (ISC)² 2015 Global Information Security Workforce Study

On average,

52% of IT professionals surveyed stated fewer than **25%** of all applicants were qualified

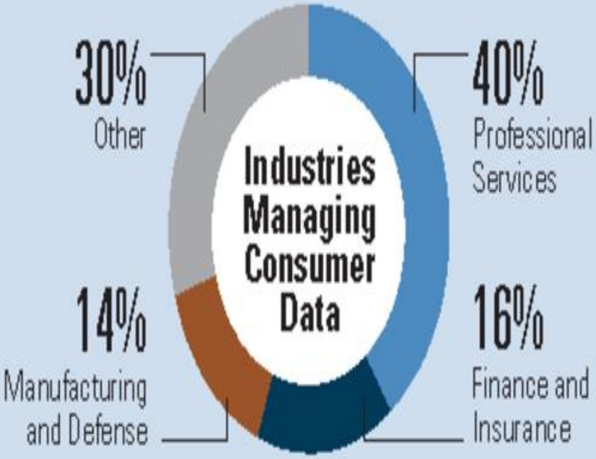
Source: State of Cybersecurity: Implications for 2015: An ISACA and RSA Conference Survey

The biggest skill gaps of today's cybersecurity professionals



Source: State of Cybersecurity: Implications for 2015 An ISACA and RSA Conference Survey

Fastest cybersecurity demand sectors are in industries managing consumer data



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

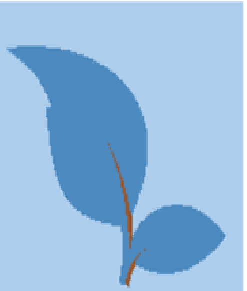
Source: Job Market Intelligence: Cybersecurity Jobs, 2015

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

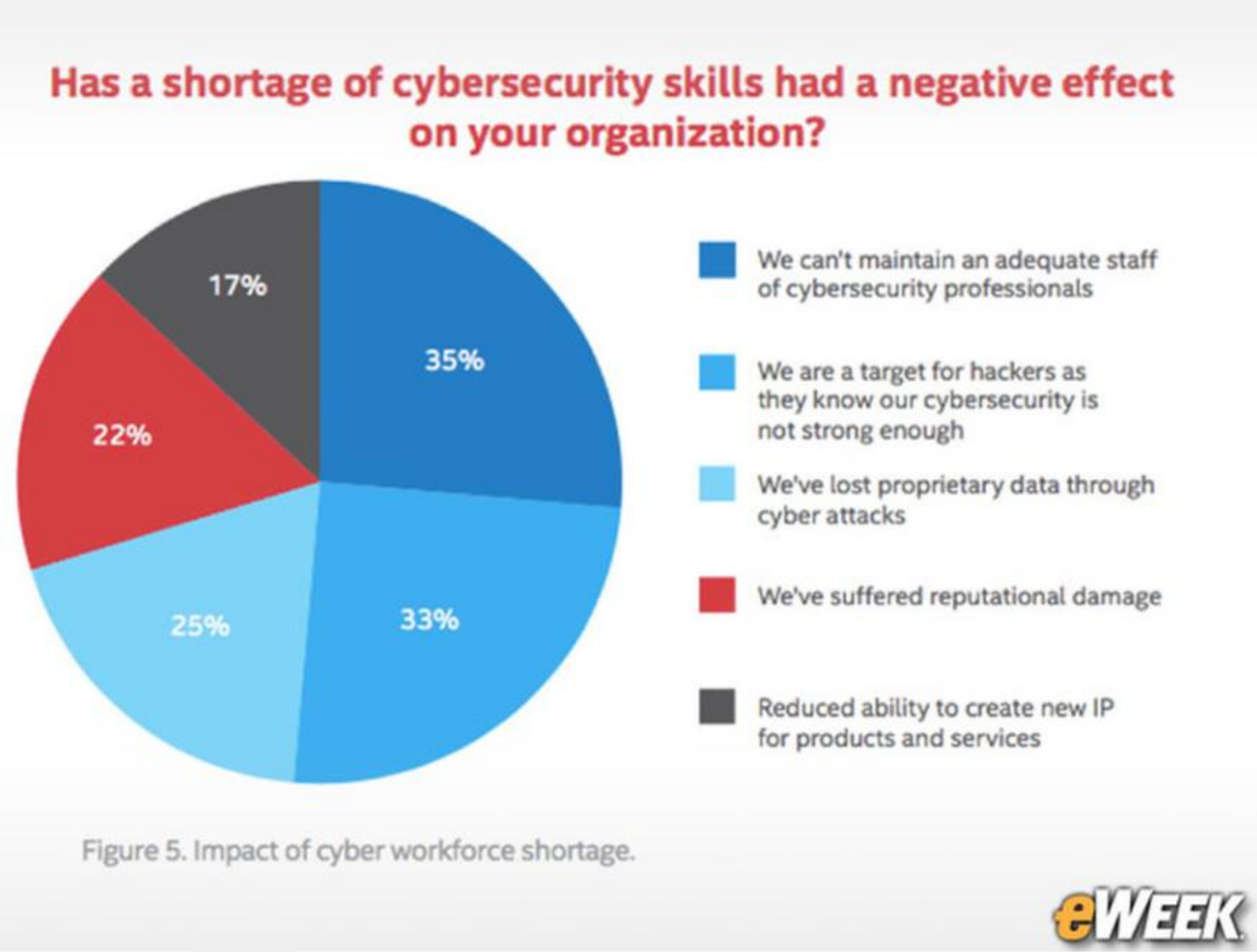
- Python
- HIPAA
- Risk Management
- Internal Auditing
- Audit Planning

Source: Partnership for Public Service

Hardest to fill skills in cybersecurity job postings

Source: Job Market Intelligence: Cybersecurity Jobs, 2015–2016 Burning Glass Technologies

- 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



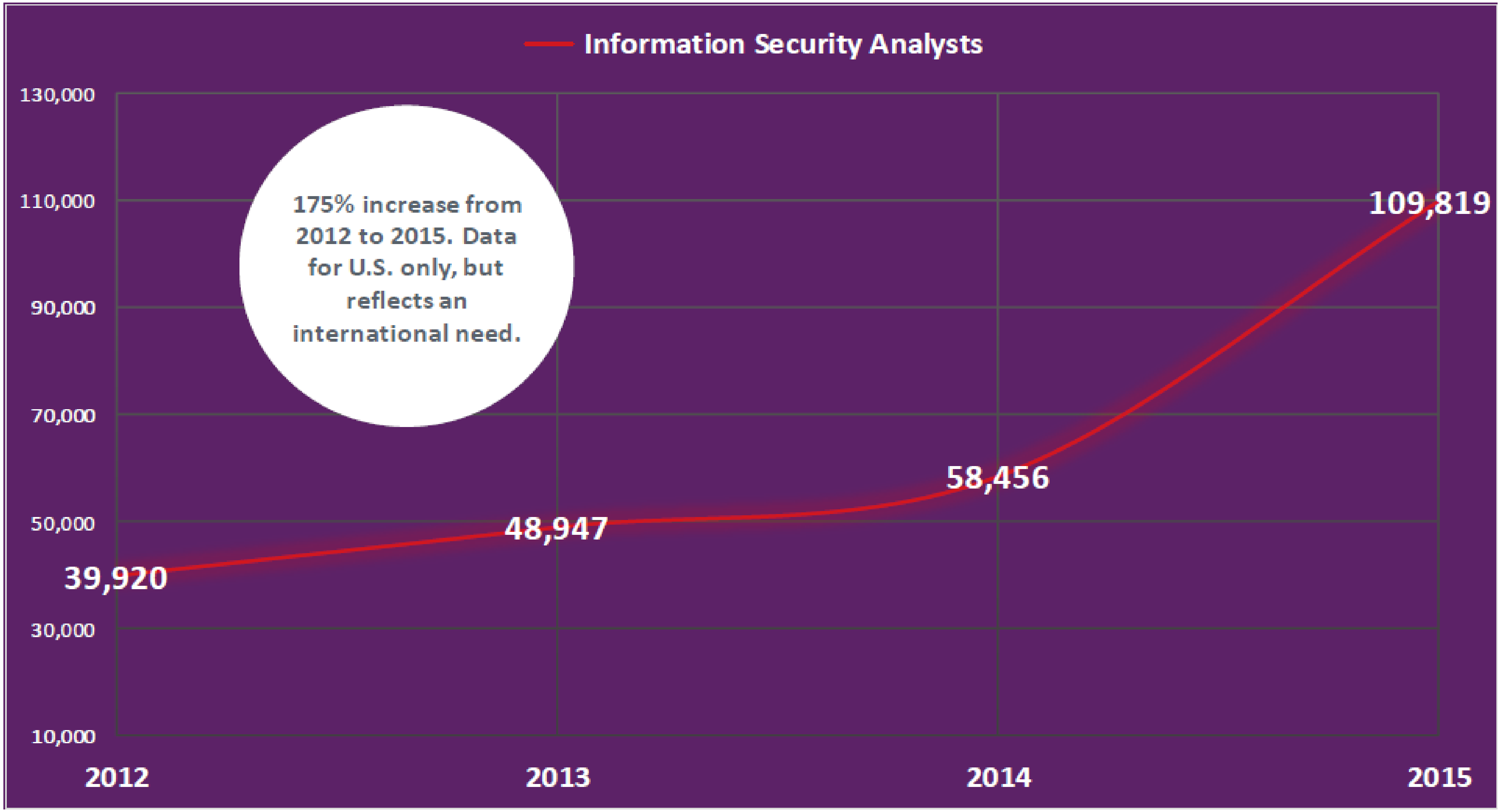
Has a shortage of cybersecurity skills had a negative effect on your organization?

Figure 5. Impact of cyber workforce shortage.

eWEEK

TOTAL NUMBER OF JOB POSTINGS:

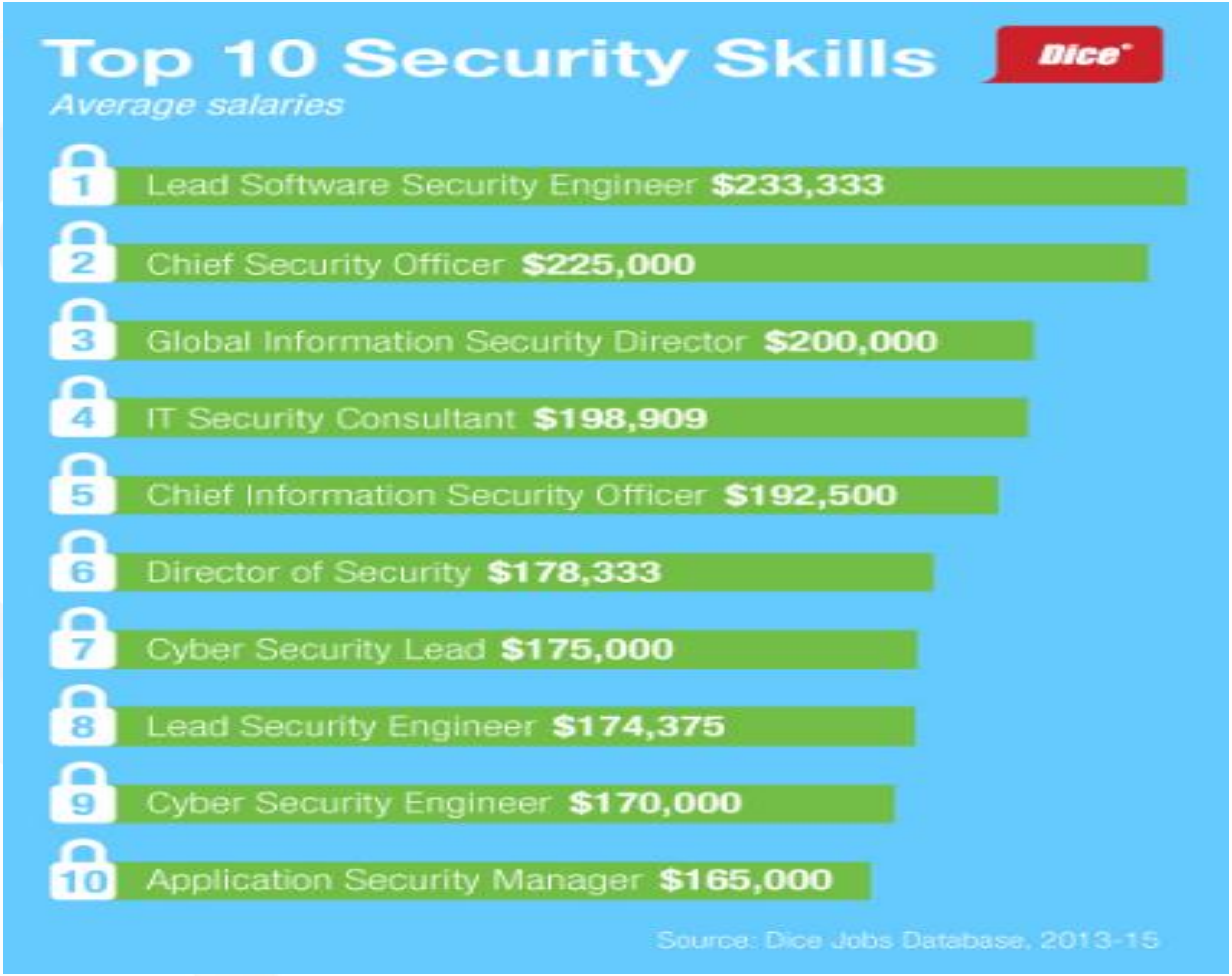
Security Analyst Job Role



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

CompTIA.

Source: Burning Glass Technologies Labor Insights, January 2016



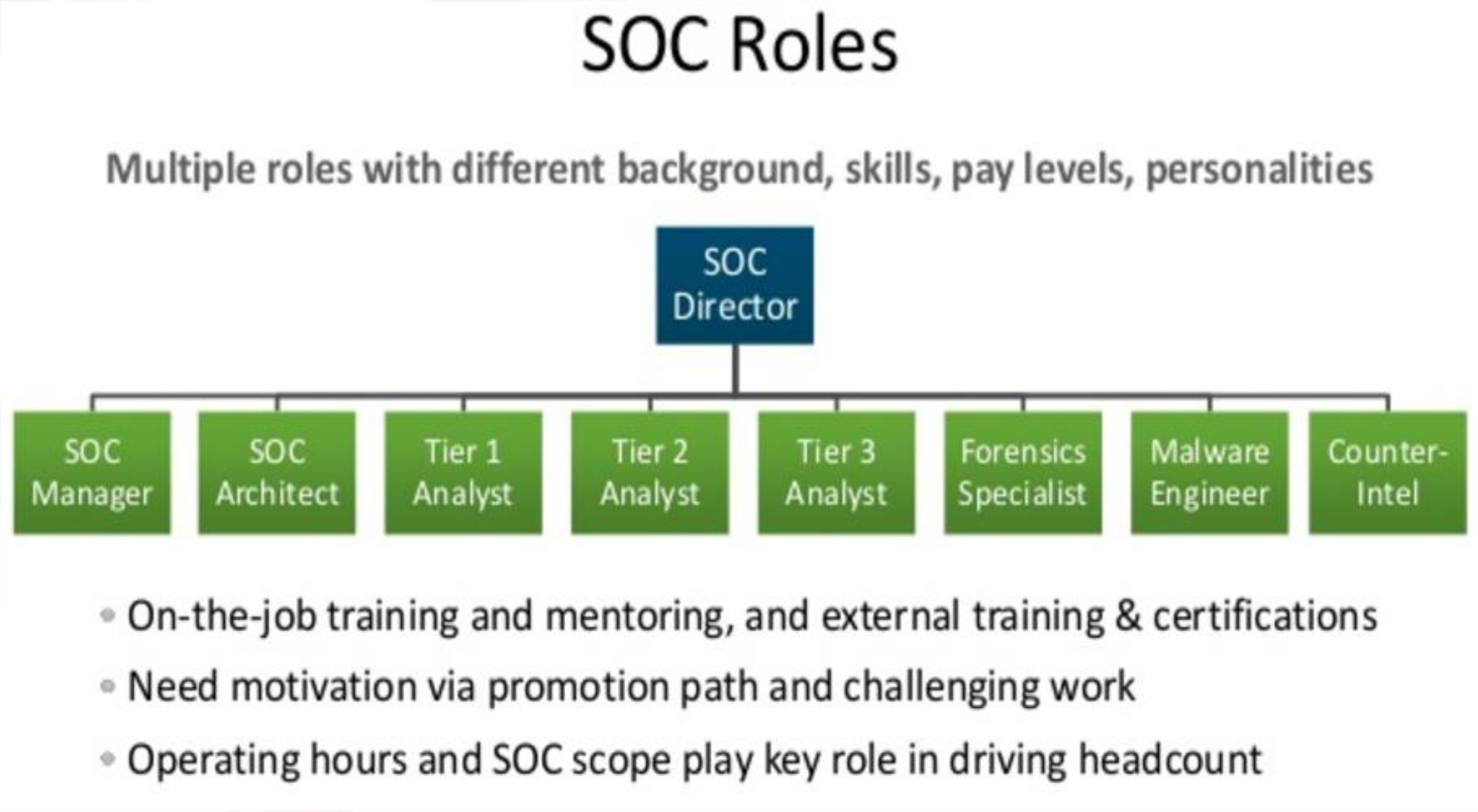
Top 10 Security Skills

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



SOC Roles

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

SOC Director

SOC Manager

SOC Architect

Tier 1 Analyst

Tier 2 Analyst

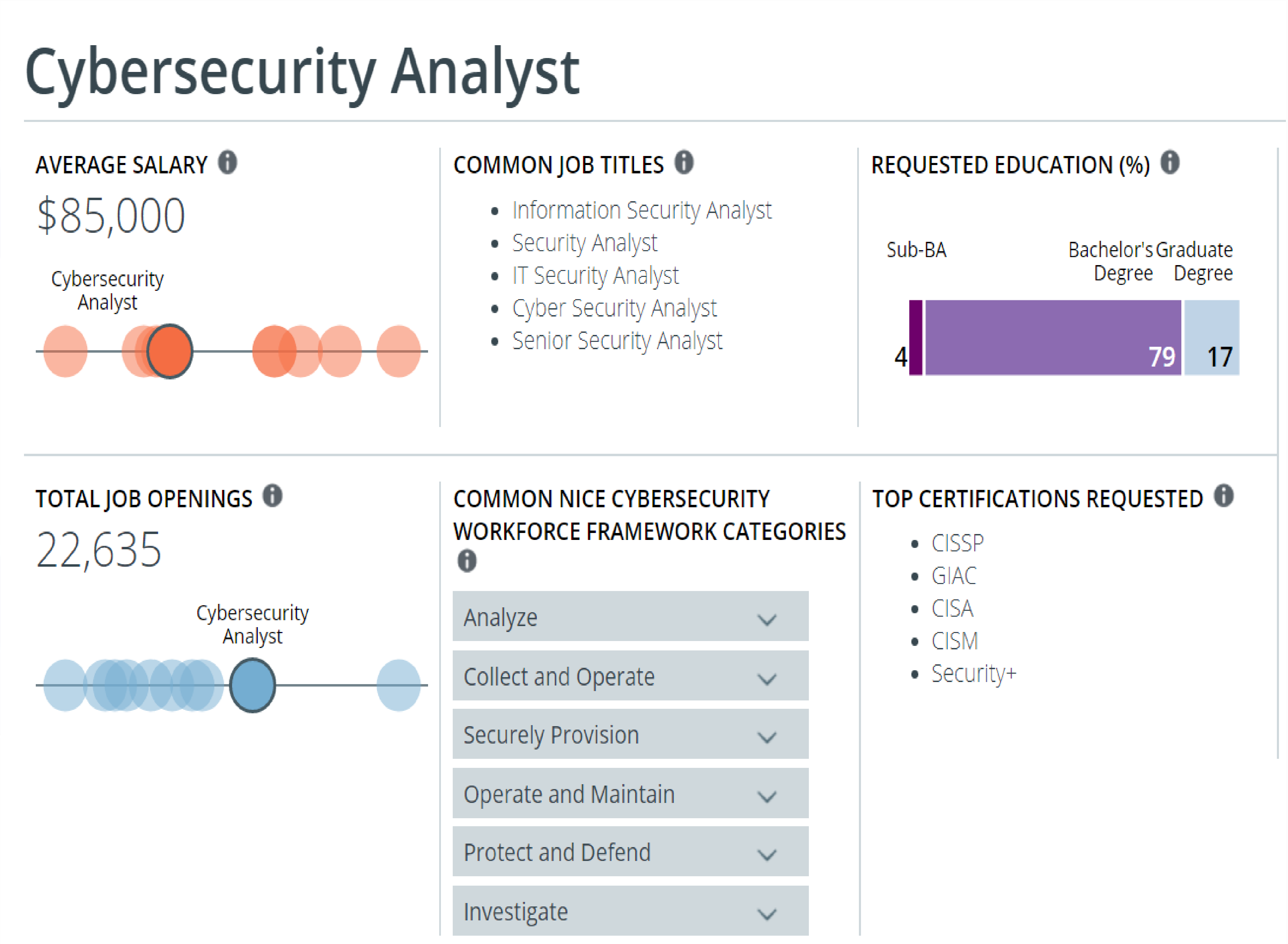
Tier 3 Analyst

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 (%)

TOTAL JOB OPENINGS

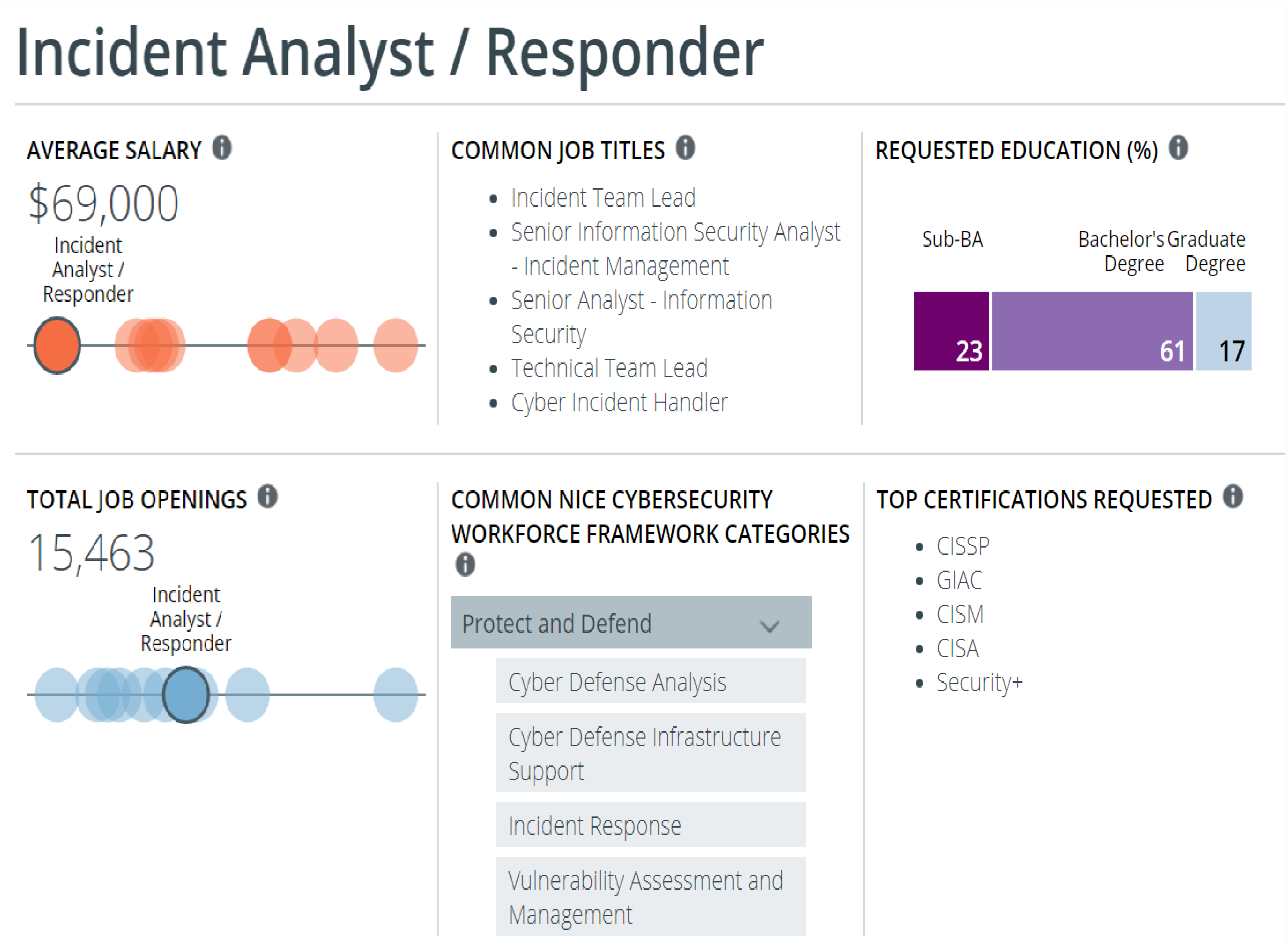
22,635

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

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	Bachelor's Degree	Graduate Degree
23	61	17

TOTAL JOB OPENINGS

15,463

COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES

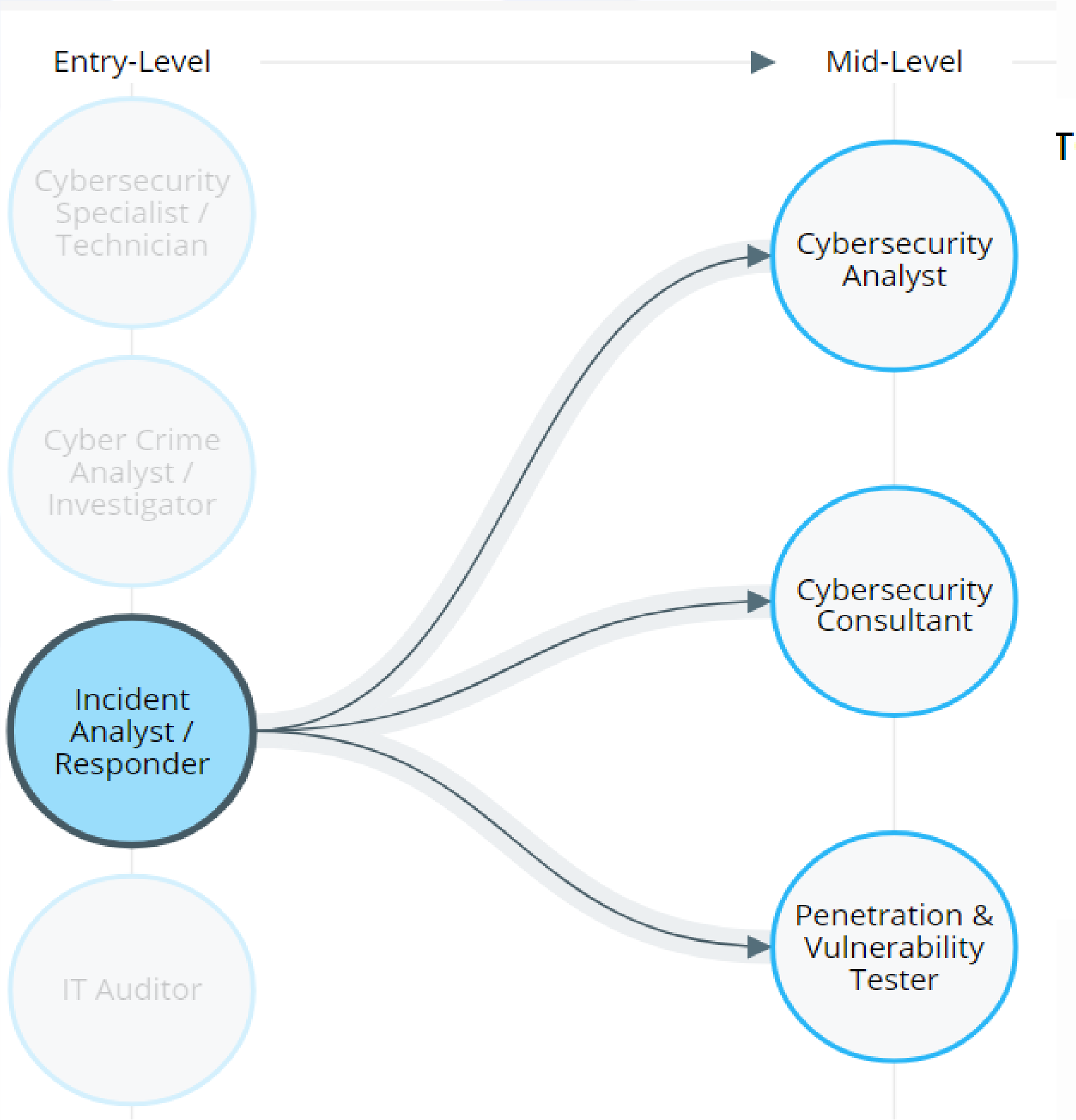
Protect and Defend

- 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)



Entry-Level

Mid-Level

Cybersecurity Specialist / Technician

Cyber Crime Analyst / Investigator

Incident Analyst / Responder

IT Auditor

Cybersecurity Analyst

Cybersecurity Consultant

Penetration & Vulnerability Tester

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)

Security Provision	Information Assurance Compliance	Software Engineering	Enterprise Architecture	Technology Demonstration	Systems Requirements Planning	Test and Evaluation	Systems Development
Operate & Maintain	Data Administration	Info System Security Mgt	Knowledge Mgt	Customer & Tech Support	Network Services	System Administration	Systems Security Analysis
Protect & Defend	Computer Network Defense (CND)	Incident Response	CND Infrastructure Support	Security Program Mgt	Vulnerability Assessment & Mgt		
Analyze	Cyber Threat Analysis	Exploitation Analysis	All-source Analysis	Targets			
Operate & Collect	Collection Operations	Cyber Operational Planning	Cyber Operations				
Oversight & Development	Legal Advice & Advocacy	Strategic Planning & Policy	Education & Training				
Investigate	Investigation	Digital Forensics					

Establishing National Standards

Job

Task/Workrole

Knowledge, Skills, and Abilities (KSA)

ENGAGING AMERICANS IN SECURING CYBERSPACE
NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION
Dod 8140

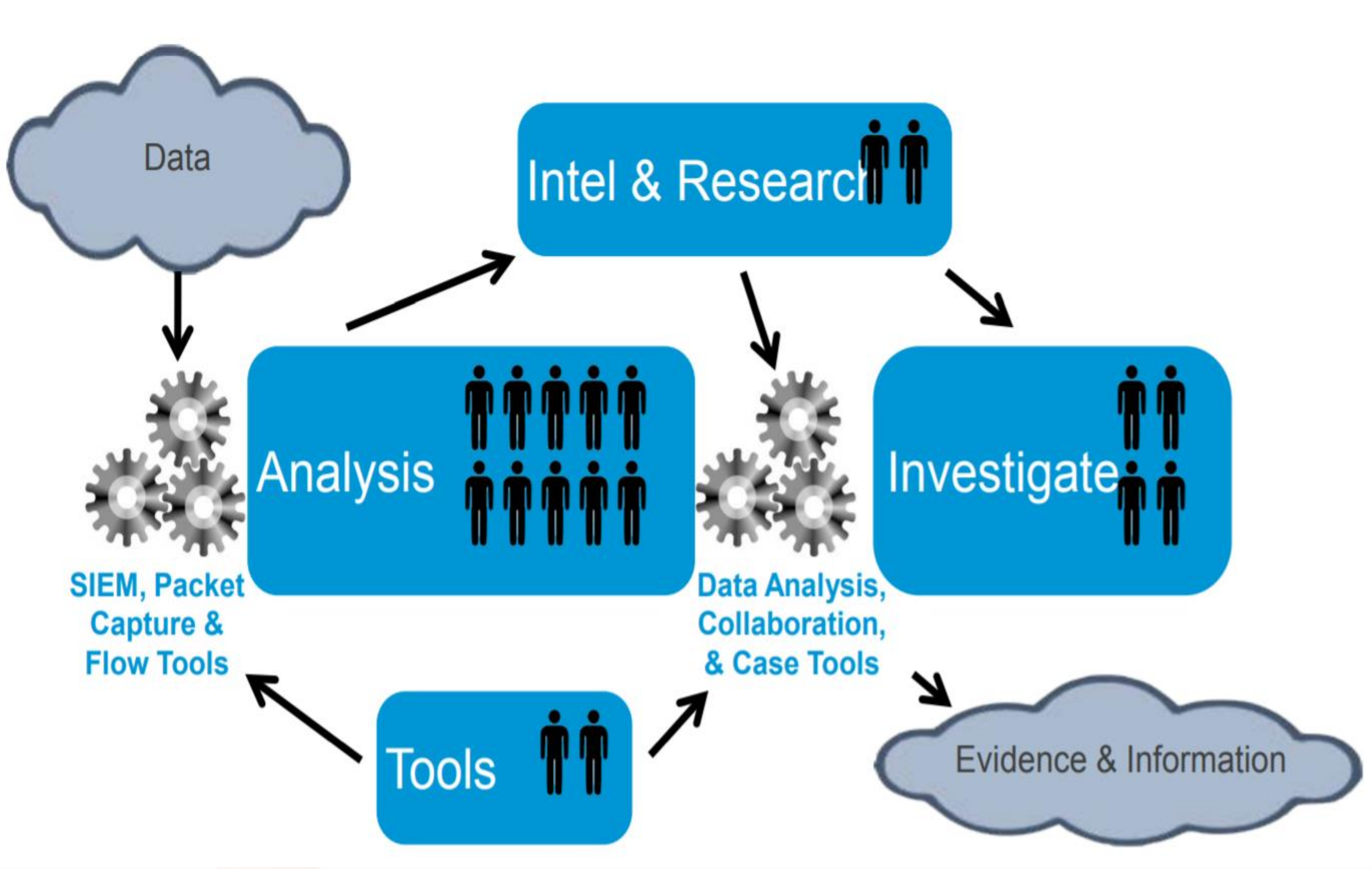
Excellence through Education

Intellectual
POINT

TOOLS, SKILLS & BEST PRACTICES TO CREATE NEXT GEN CYBER SECURITY PROFESSIONALS

BASED ON INTELLECTUAL POINT EXPERIENCES

Essential Skills for Next Gen SOC Analyst


Data
Intel & Research
Analysis
Investigate
SIEM, Packet Capture & Flow Tools
Data Analysis, Collaboration, & Case Tools
Tools
Evidence & Information

Excellence through Education
Intellectual
POINT

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

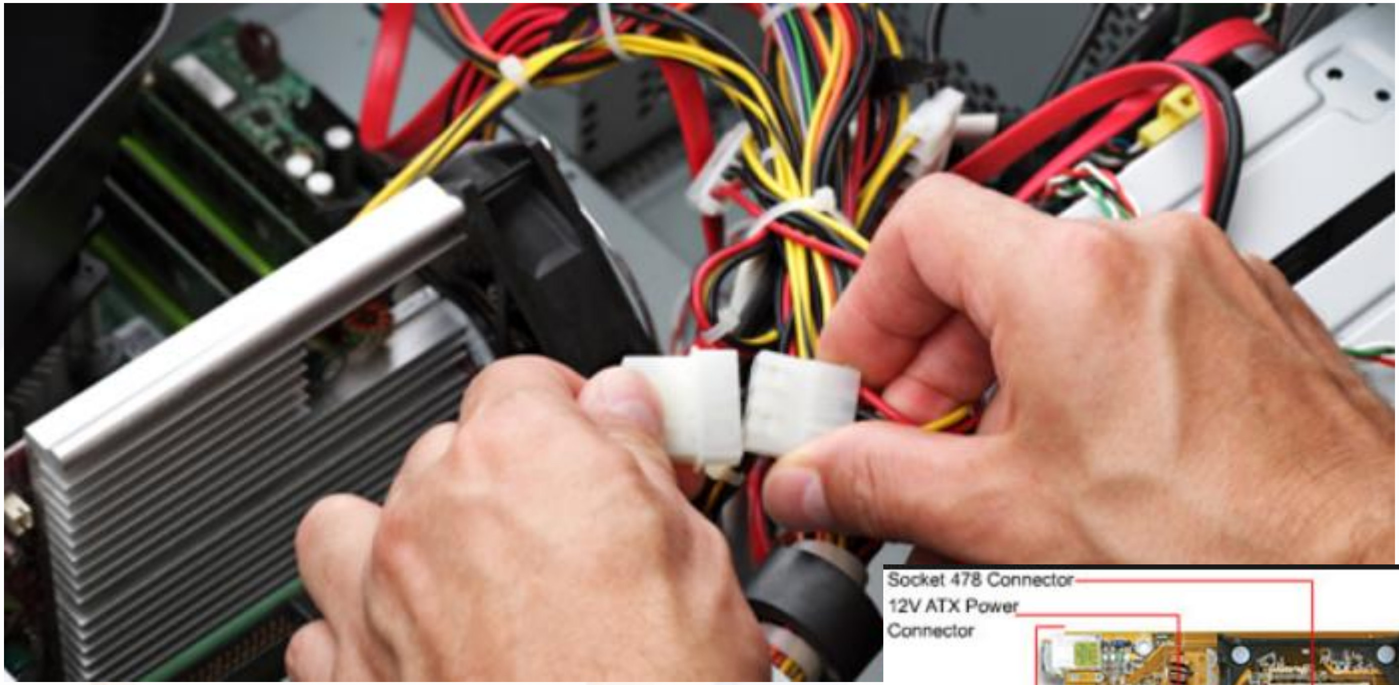
OPEN SOURCE TOOLS & THREAT INTELLIGENCE

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

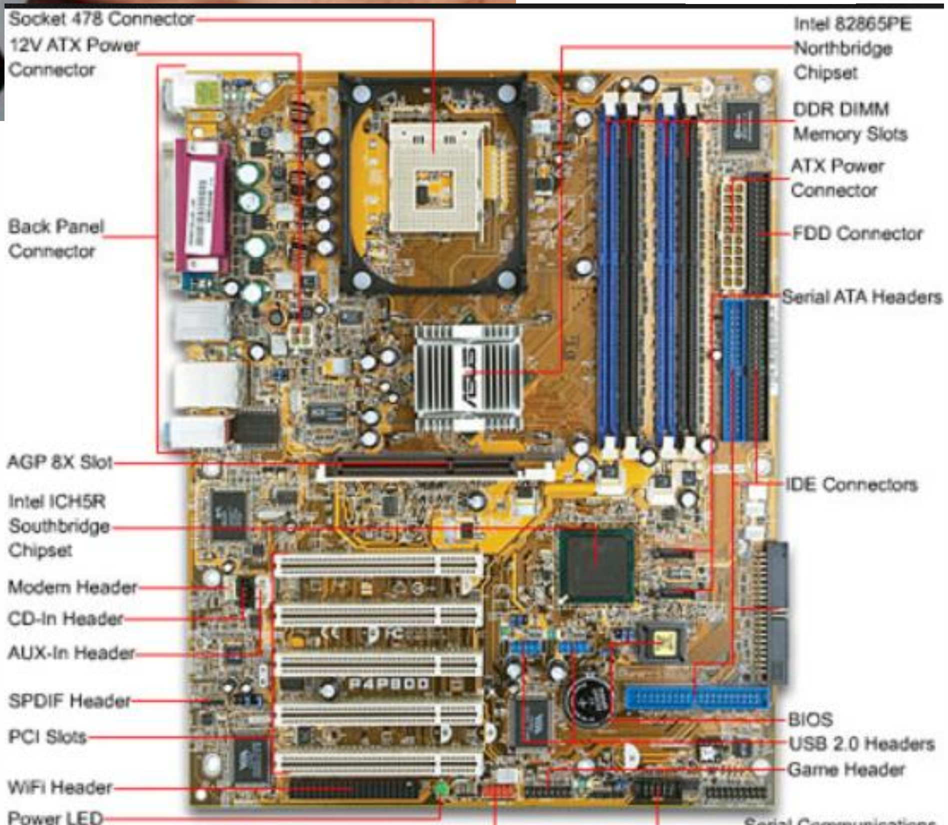


CompTIA A+ CERTIFIED

CompTIA CSA+

CompTIA Security+

CISCO CERTIFIED CCNA ROUTING & SWITCHING



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

OpenVAS
Open Vulnerability Assessment System

elastic + logstash
kibana

BeyondTrust
Retina CS

Microsoft
Baseline Security Analyzer

metasploit

NMAP

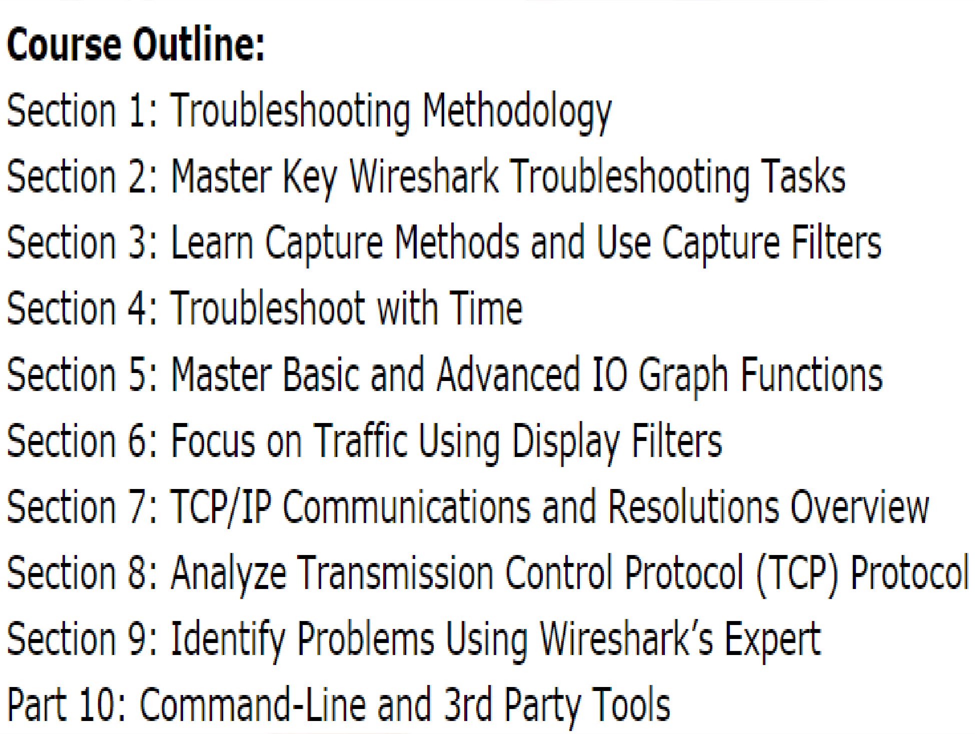
SNORT™

WIRESHARK

ALIEN VAULT OSSIM

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

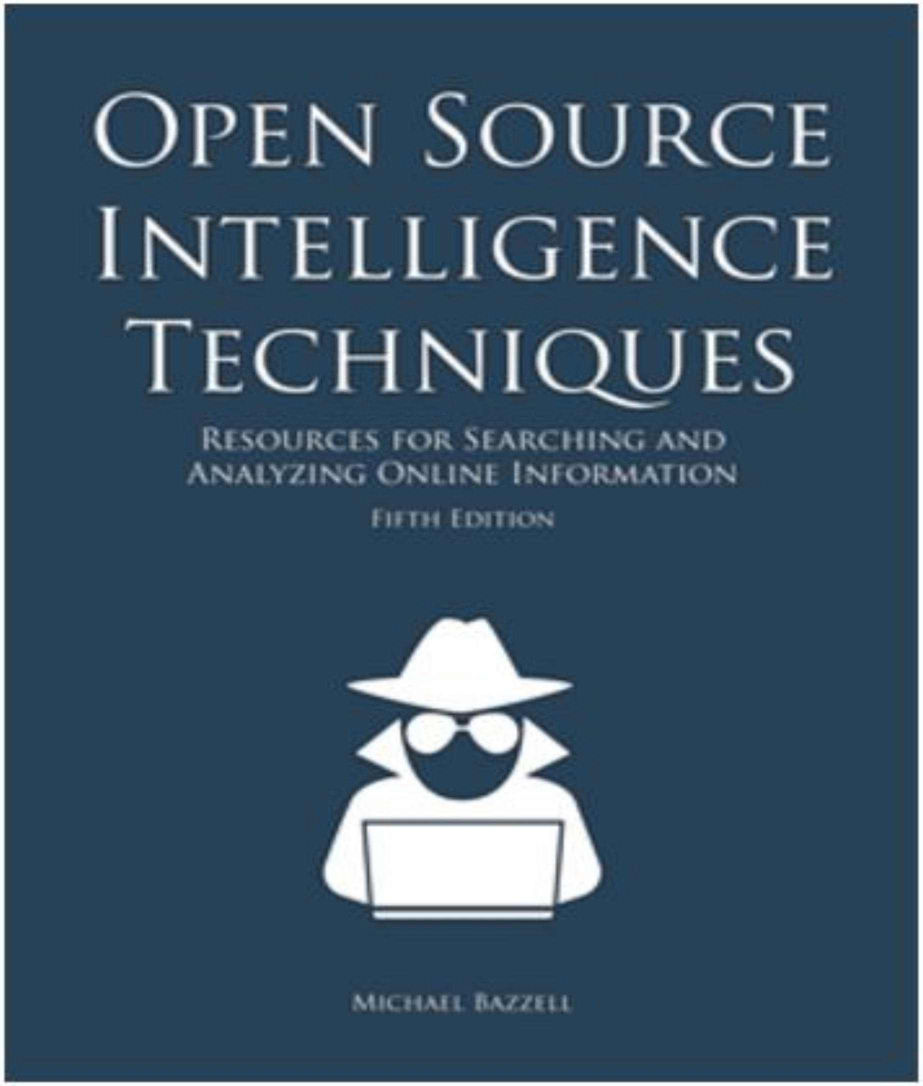
Section 9: Identify Problems Using Wireshark's Expert

Part 10: Command-Line and 3rd Party Tools

Ethical Hacking & Exploitation Skills using Kali Linux and Metasploit in a Virtual Environment

metasploit

Cyber Analysts need to learn Open Source Intelligence Tools that can be leveraged on the job


OPEN SOURCE INTELLIGENCE TECHNIQUES
RESOURCES FOR SEARCHING AND ANALYZING ONLINE INFORMATION
FIFTH EDITION
MICHAEL BAZZELL

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

tenable

Nessus

RSA® Archer GRC

splunk>®

BIGFIX

An IBM Company

McAfee

VARONIS

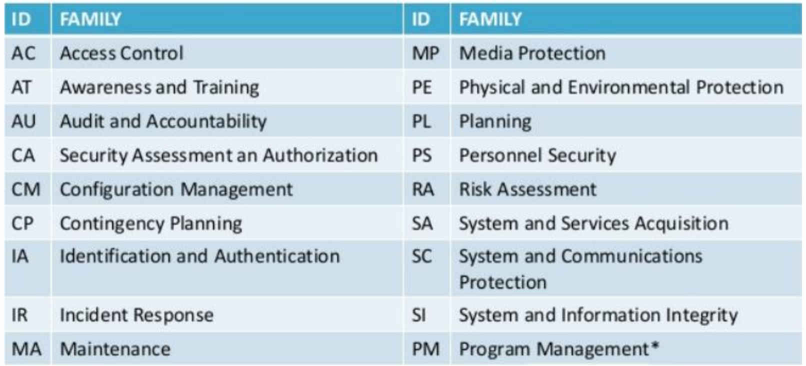
exabeam

TANIUM

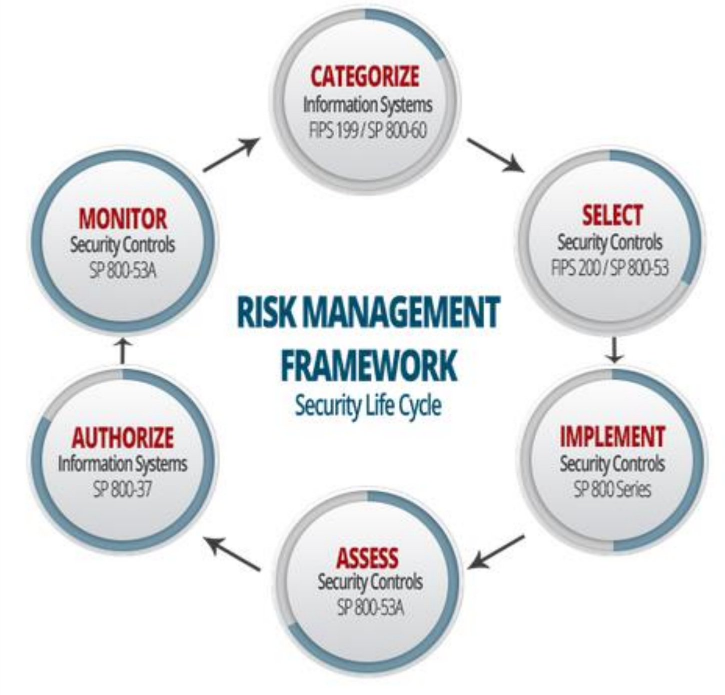
paloalto NETWORKS

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 of Data Sources (Applications, Servers, Endpoints, VMs)
- Huge Volumes - Terabytes of data to be collected, indexed and searched daily
- Create Authorization Package (System Security Plan, Security Assessment Report, Plan of Action & Milestones)
- Requires real-time visualization dashboards
- Requires ad-hoc search and forensic navigation across all IT data.

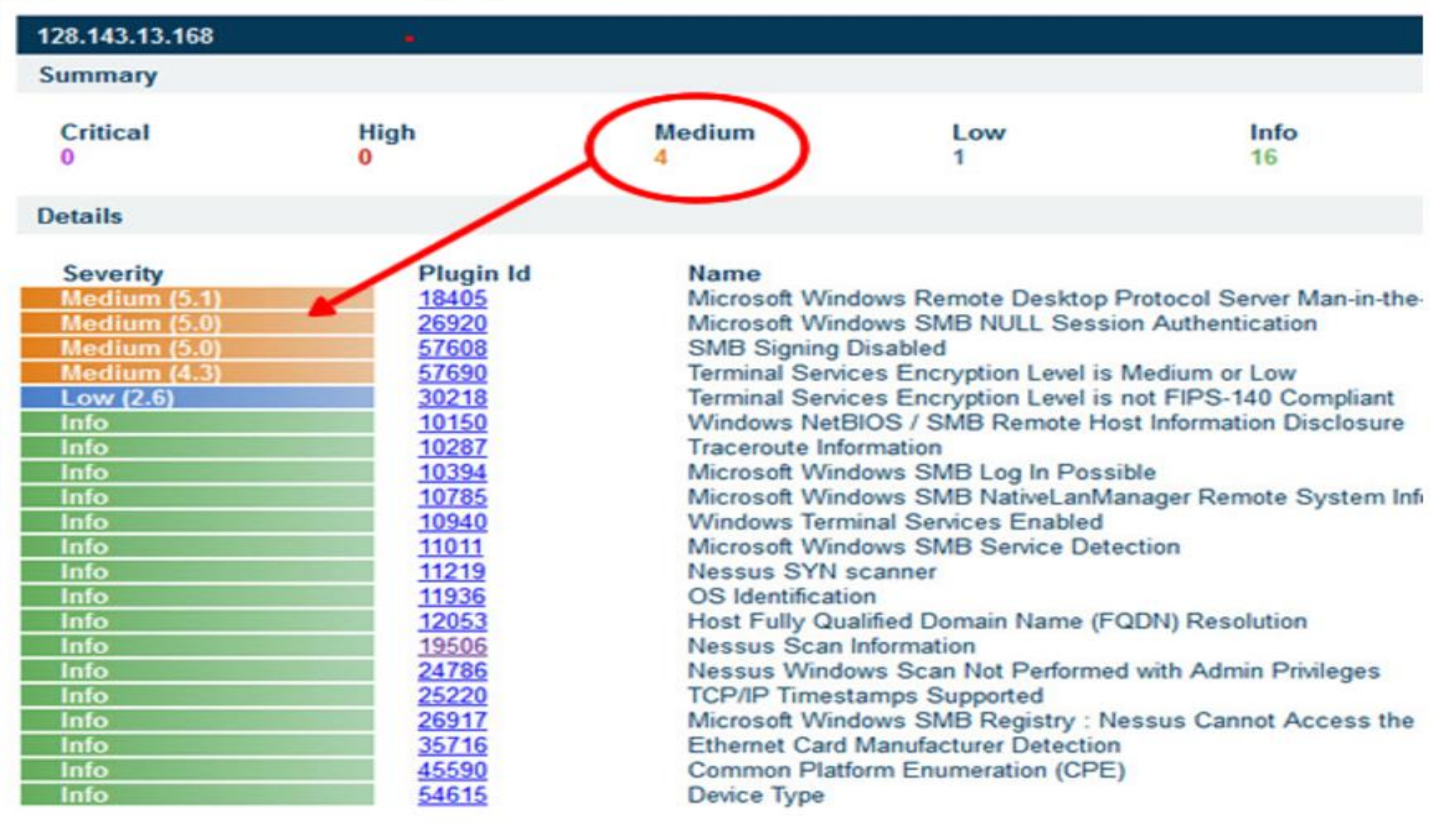


ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment an Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management*



FISMA

Cyber Professionals should know how to Analyze Vulnerability Scan Reports



128.143.13.168

Summary

Critical	High	Medium	Low	Info
0	0	4	1	16

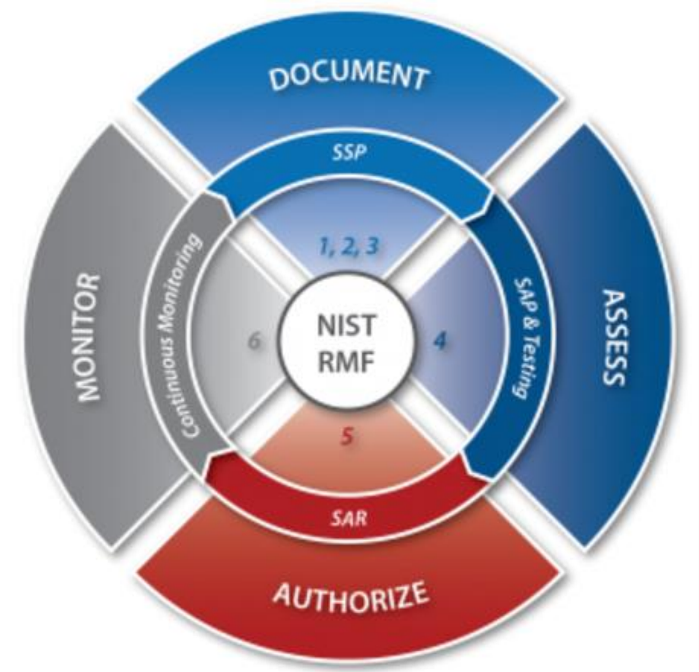
Details

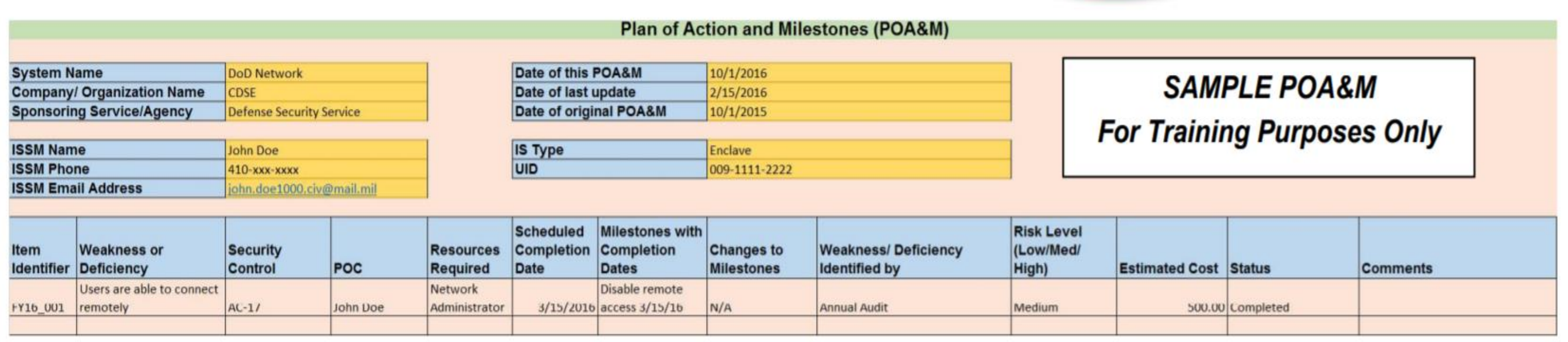
Severity	Plugin Id	Name
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-
Medium (5.0)	26920	Microsoft Windows SMB NULL Session Authentication
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Inf
Info	10940	Windows Terminal Services Enabled
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

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





Plan of Action and Milestones (POA&M)

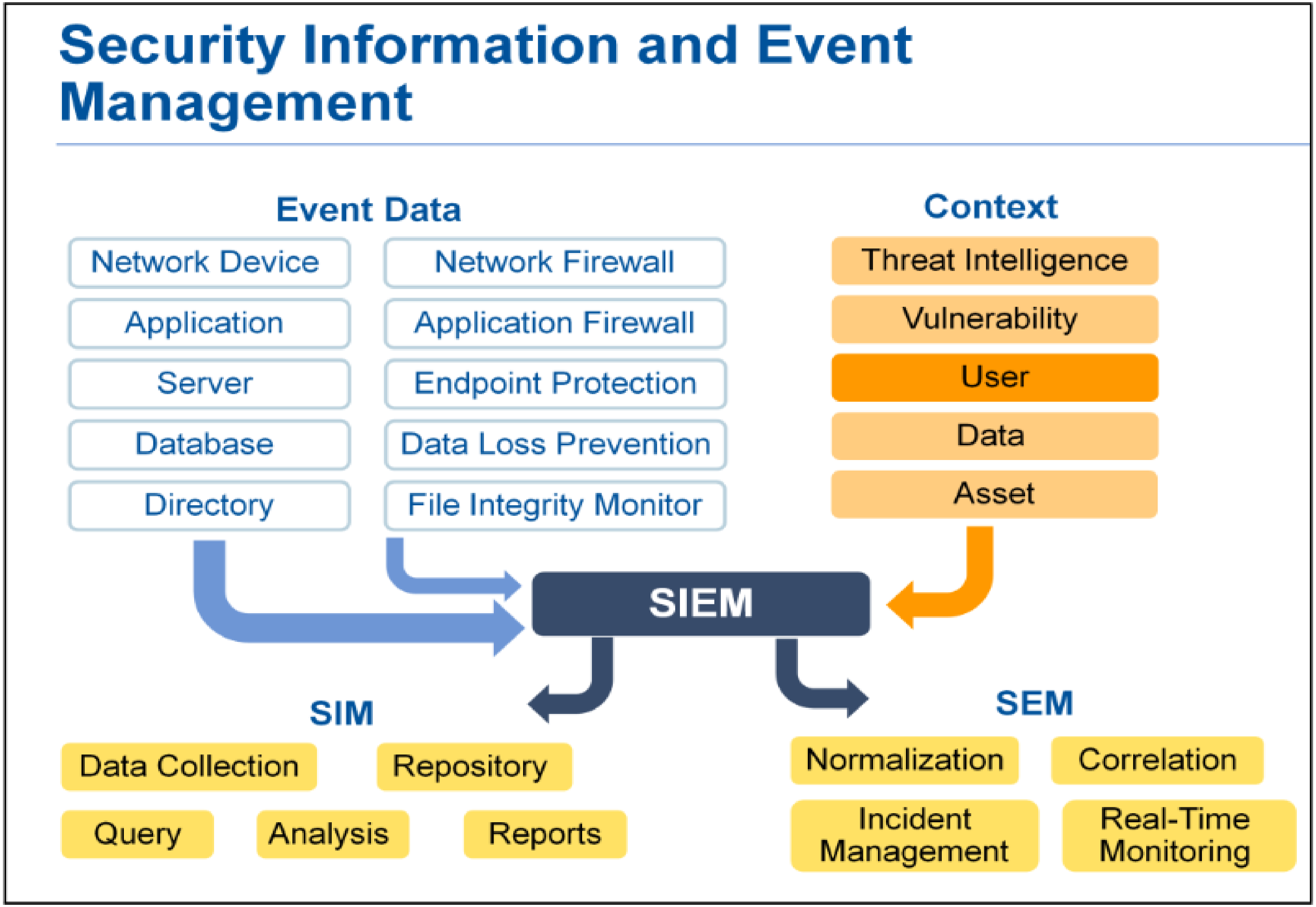
System Name	DoD Network	Date of this POA&M	10/1/2016
Company/ Organization Name	CDSE	Date of last update	2/15/2016
Sponsoring Service/Agency	Defense Security Service	Date of original POA&M	10/1/2015
ISSM Name	John Doe	IS Type	Enclave
ISSM Phone	410-xxx-xxxx	UID	009-1111-2222
ISSM Email Address	john.doe1000.civ@mail.mil		

SAMPLE POA&M

For Training Purposes Only

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	AC-17	John Doe	Network Administrator	3/15/2016	Disable remote access 3/15/16	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

SIEM

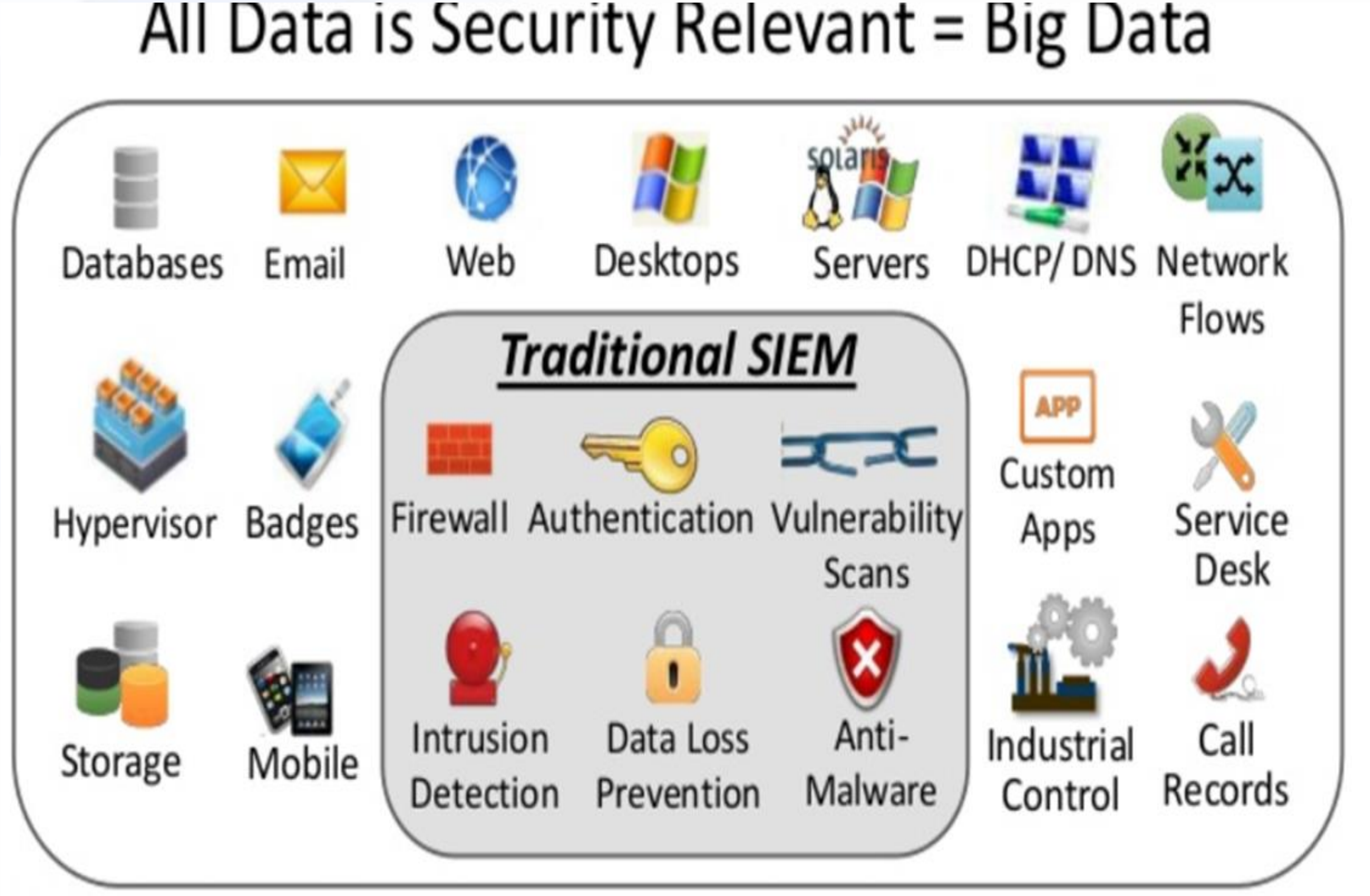
SIM

- Data Collection
- Repository
- Query
- Analysis
- Reports

SEM

- Normalization
- Correlation
- Incident Management
- Real-Time Monitoring

Teaching Students how to Mine Machine Data



All Data is Security Relevant = Big Data

Databases

Email

Web

Desktops

Servers

DHCP/ DNS

Network Flows

Hypervisor

Badges

Traditional SIEM

Firewall

Authentication

Vulnerability Scans

Intrusion Detection

Data Loss Prevention

Anti-Malware

Custom Apps

Service Desk

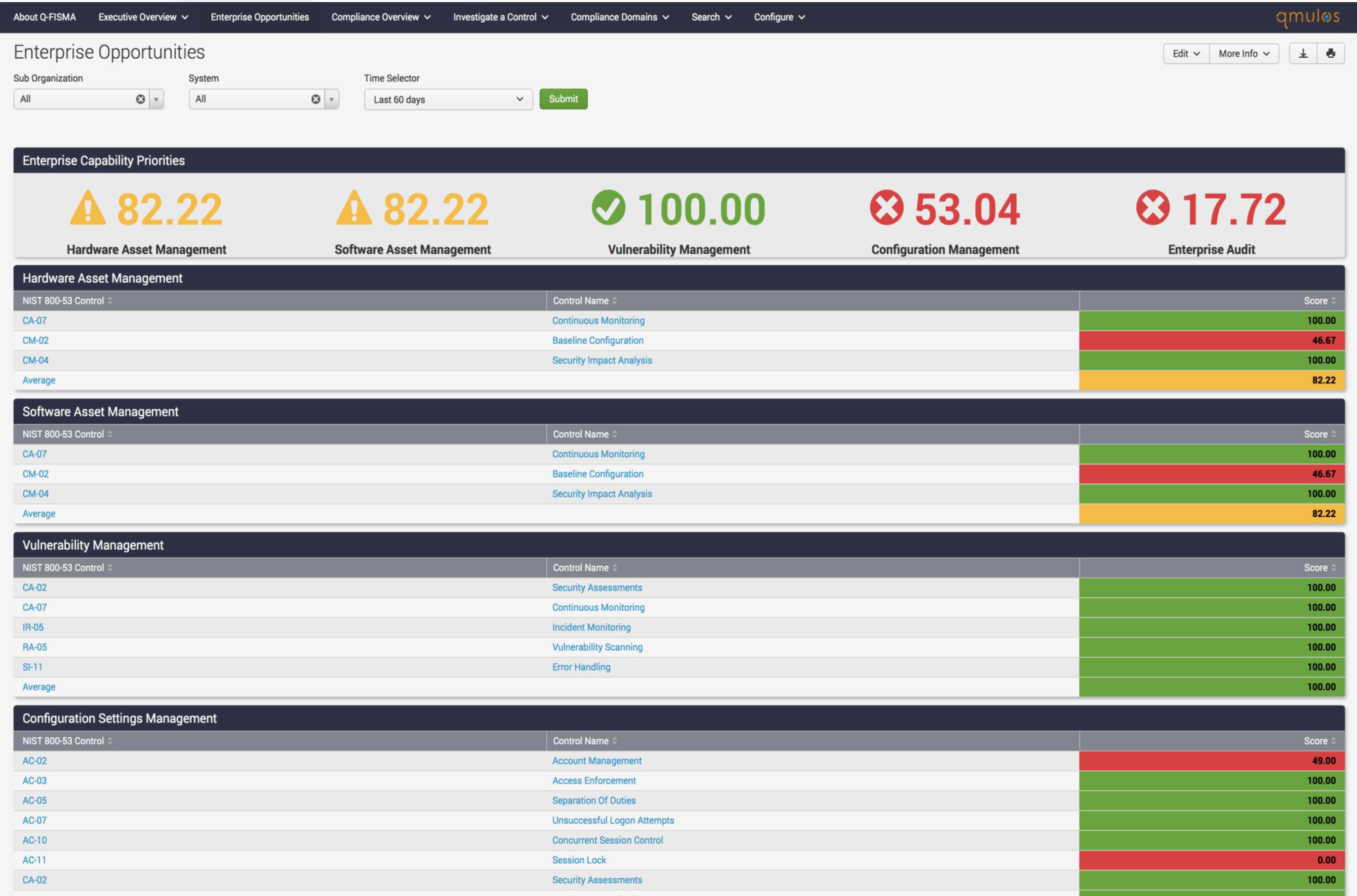
Storage

Mobile

Industrial Control

Call Records

Tracking RMF Reports Across Security Control Families



Enterprise Opportunities

Sub Organization
All

System
All

Time Selector
Last 60 days

Enterprise Capability Priorities

82.22	82.22	100.00	53.04	17.72
Hardware Asset Management	Software Asset Management	Vulnerability Management	Configuration Management	Enterprise Audit

Hardware Asset Management

NIST 800-53 Control	Control Name	Score
CA-07	Continuous Monitoring	100.00
CM-02	Baseline Configuration	46.67
CM-04	Security Impact Analysis	100.00
Average		82.22

Software Asset Management

NIST 800-53 Control	Control Name	Score
CA-07	Continuous Monitoring	100.00
CM-02	Baseline Configuration	46.67
CM-04	Security Impact Analysis	100.00
Average		82.22

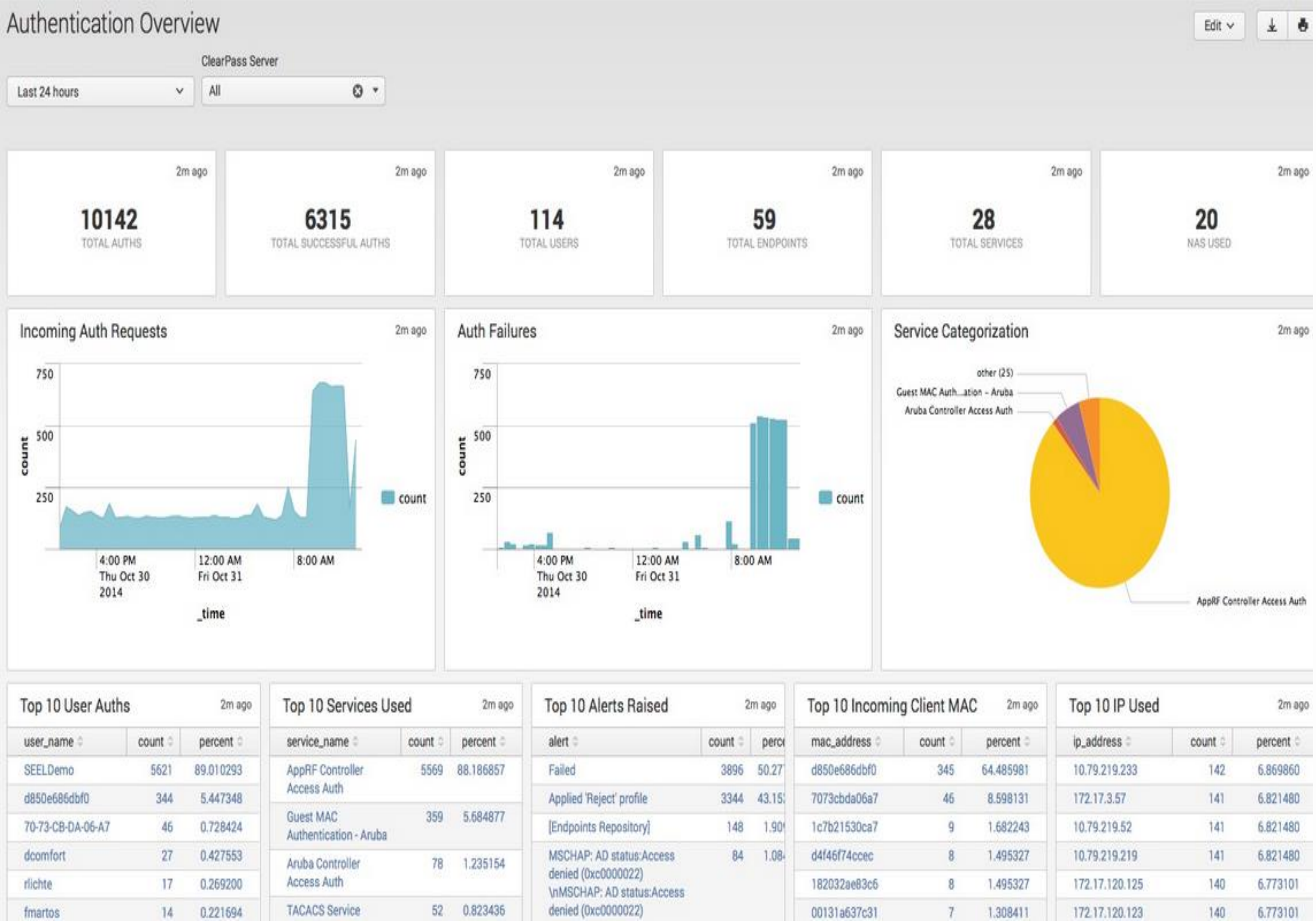
Vulnerability Management

NIST 800-53 Control	Control Name	Score
CA-02	Security Assessments	100.00
CA-07	Continuous Monitoring	100.00
IR-05	Incident Monitoring	100.00
RA-05	Vulnerability Scanning	100.00
SI-11	Error Handling	100.00
Average		100.00

Configuration Settings Management

NIST 800-53 Control	Control Name	Score
AC-02	Account Management	49.00
AC-03	Access Enforcement	100.00
AC-05	Separation Of Duties	100.00
AC-07	Unsuccessful Logon Attempts	100.00
AC-10	Concurrent Session Control	100.00
AC-11	Session Lock	0.00
CA-02	Security Assessments	100.00

Cyber Forensic Analysis Skills for Incident Responders



Authentication Overview

Last 24 hours ⌄

ClearPass Server: All

2m ago	2m ago	2m ago	2m ago	2m ago	2m ago
10142 TOTAL AUTHS	6315 TOTAL SUCCESSFUL AUTHS	114 TOTAL USERS	59 TOTAL ENDPOINTS	28 TOTAL SERVICES	20 NAS USED

Incoming Auth Requests

2m ago

Auth Failures

2m ago

Service Categorization

2m ago

other (25)
Guest MAC Auth...ation - Aruba
Aruba Controller Access Auth
AppRF Controller Access Auth

Top 10 User Auths

2m ago

user_name	count	percent
SEELDemo	5621	89.010293
d850e686dbf0	344	5.447348
70-73-CB-DA-06-A7	46	0.728424
dcomfort	27	0.427553
rlichte	17	0.269200
fmartos	14	0.221694

Top 10 Services Used

2m ago

service_name	count	percent
AppRF Controller Access Auth	5569	88.186857
Guest MAC Authentication - Aruba	359	5.684877
Aruba Controller Access Auth	78	1.235154
TACACS Service	52	0.823436

Top 10 Alerts Raised

2m ago

alert	count	perc
Failed	3896	50.27
Applied 'Reject' profile	3344	43.15
[Endpoints Repository]	148	1.90
MSCHAP: AD status:Access denied (0xc0000022) \nMSCHAP: AD status:Access denied (0xc0000022)	84	1.08

Top 10 Incoming Client MAC

2m ago

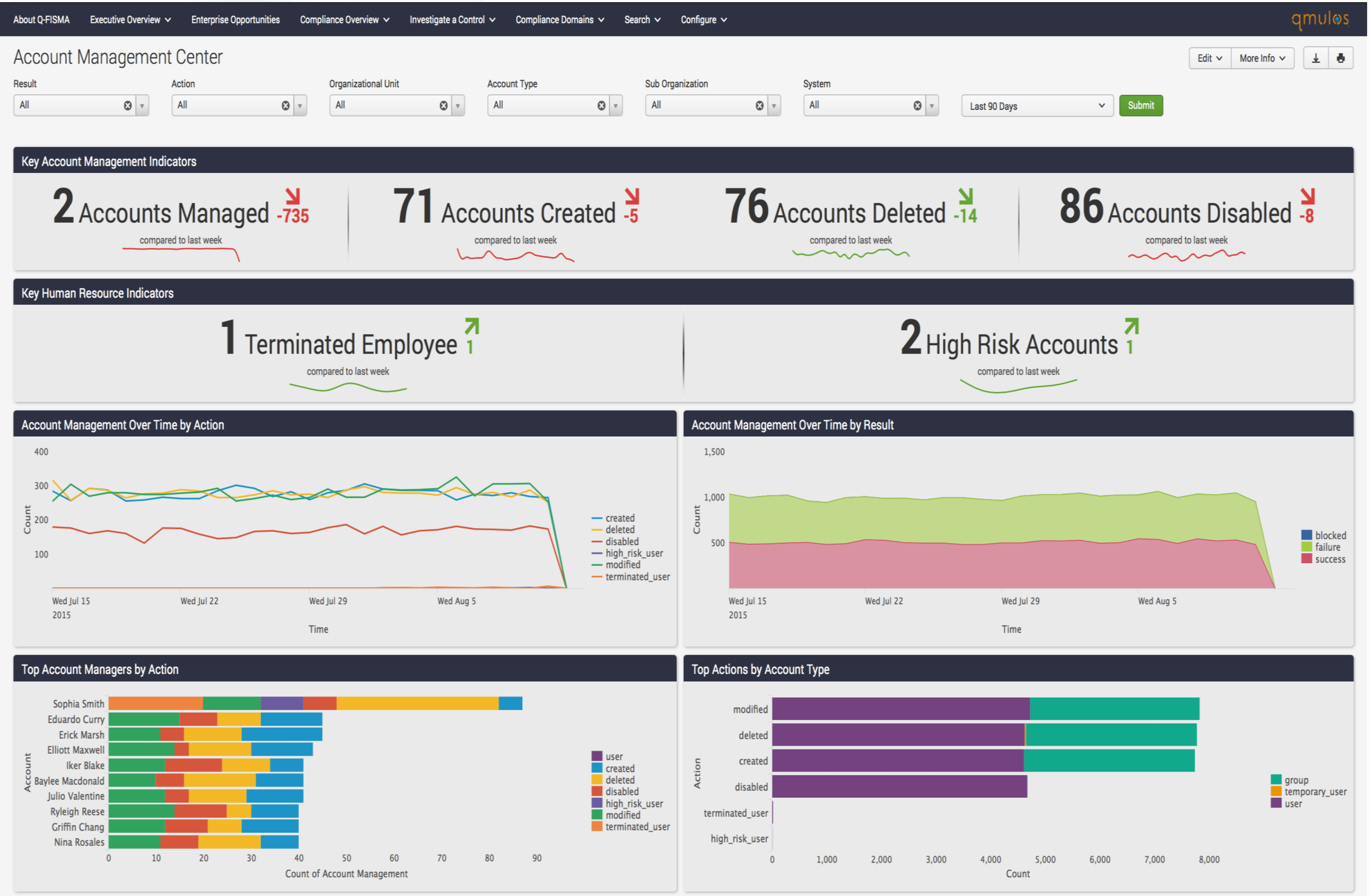
mac_address	count	percent
d850e686dbf0	345	64.485981
7073cbda06a7	46	8.598131
1c7b21530ca7	9	1.682243
d4f46f74ccec	8	1.495327
182032ae83c6	8	1.495327
00131a637c31	7	1.308411

Top 10 IP Used

2m ago

ip_address	count	percent
10.79.219.233	142	6.869860
172.17.3.57	141	6.821480
10.79.219.52	141	6.821480
10.79.219.219	141	6.821480
172.17.120.125	140	6.773101
172.17.120.123	140	6.773101

Teaching Students how to track SOC KPIs & IOCs



Account Management Center

Result: All

Action: All

Organizational Unit: All

Account Type: All

Sub Organization: All

System: All

Last 90 Days

Key Account Management Indicators

2 Accounts Managed -735 compared to last week

71 Accounts Created -5 compared to last week

76 Accounts Deleted -14 compared to last week

86 Accounts Disabled -8 compared to last week

Key Human Resource Indicators

1 Terminated Employee 1 compared to last week

2 High Risk Accounts 1 compared to last week

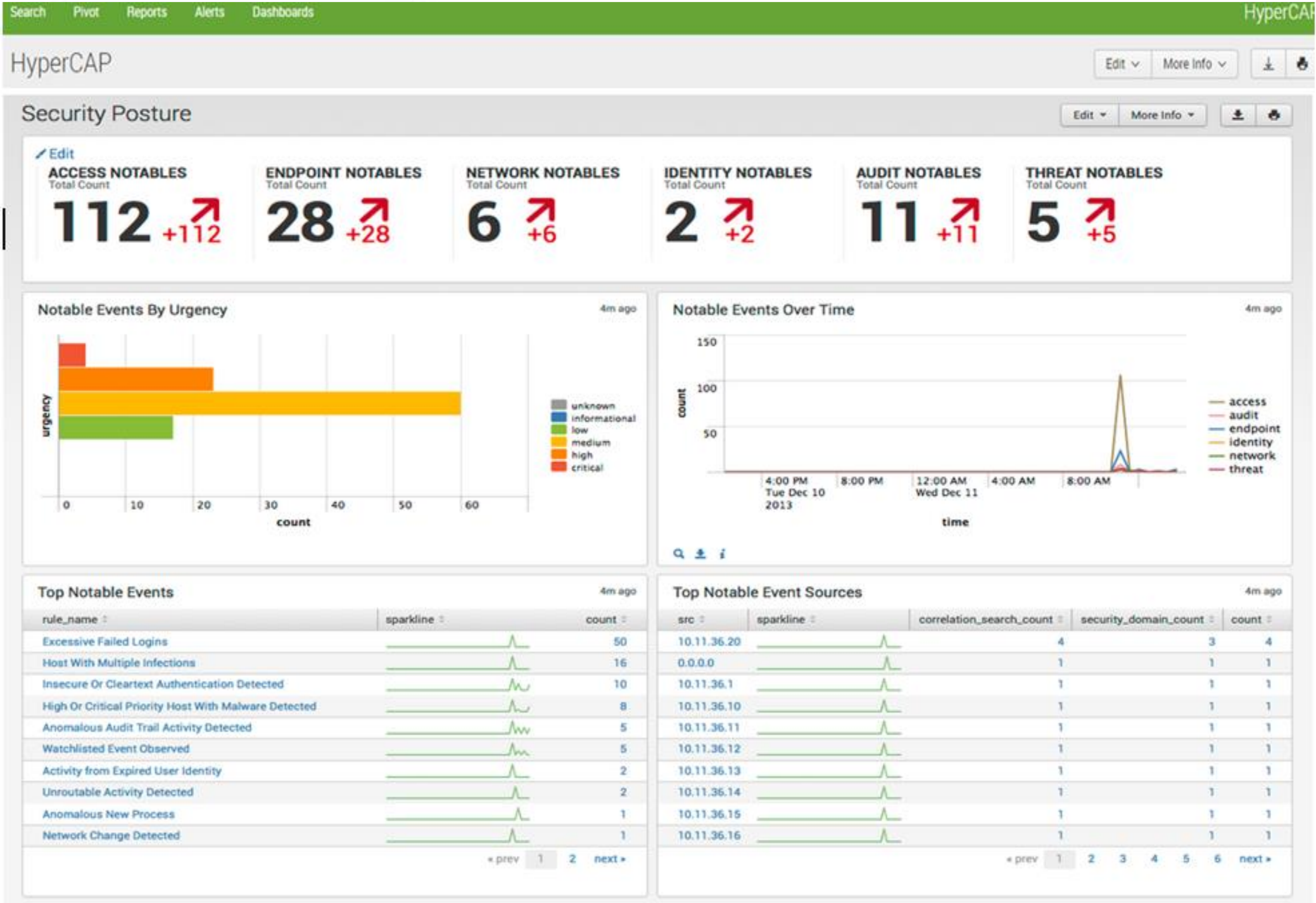
Account Management Over Time by Action

Account Management Over Time by Result

Top Account Managers by Action

Top Actions by Account Type

Skills to Visualize Security Posture & Cyber IOCs



Security Posture

ACCESS NOTABLES Total Count	ENDPOINT NOTABLES Total Count	NETWORK NOTABLES Total Count	IDENTITY NOTABLES Total Count	AUDIT NOTABLES Total Count	THREAT NOTABLES Total Count
112 ↗ +112	28 ↗ +28	6 ↗ +6	2 ↗ +2	11 ↗ +11	5 ↗ +5

Notable Events By Urgency

Notable Events Over Time

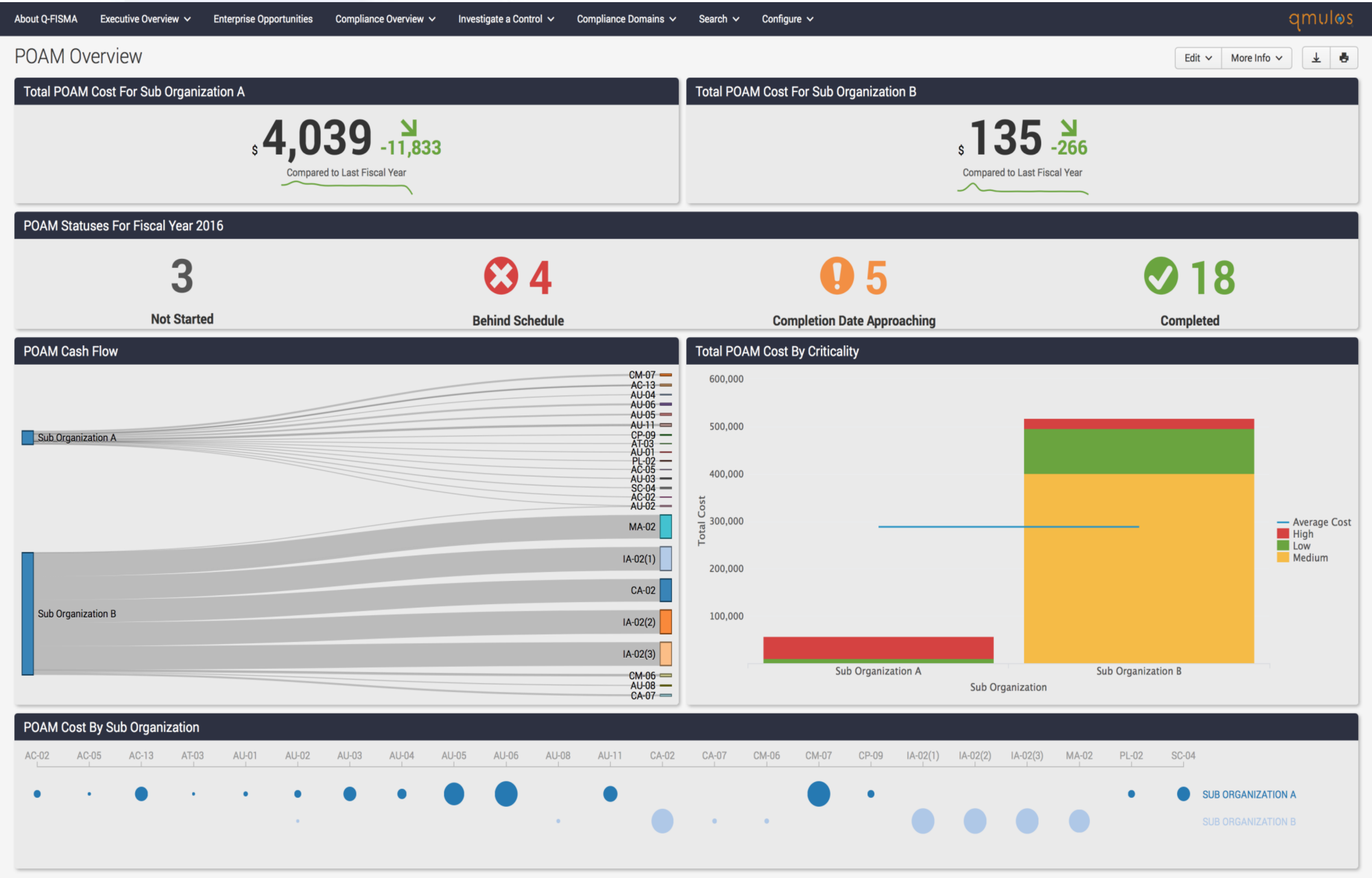
Top Notable Events

rule_name	sparkline	count
Excessive Failed Logins		50
Host With Multiple Infections		16
Insecure Or Cleartext Authentication Detected		10
High Or Critical Priority Host With Malware Detected		8
Anomalous Audit Trail Activity Detected		5
Watchlisted Event Observed		5
Activity from Expired User Identity		2
Unroutable Activity Detected		2
Anomalous New Process		1
Network Change Detected		1

Top Notable Event Sources

src	sparkline	correlation_search_count	security_domain_count	count
10.11.36.20		4	3	4
0.0.0.0		1	1	1
10.11.36.1		1	1	1
10.11.36.10		1	1	1
10.11.36.11		1	1	1
10.11.36.12		1	1	1
10.11.36.13		1	1	1
10.11.36.14		1	1	1
10.11.36.15		1	1	1
10.11.36.16		1	1	1

Skills to Create Dashboards for Tracking FISMA Compliance Trends



POAM Overview

Total POAM Cost For Sub Organization A

$ 4,039 -11,833

Compared to Last Fiscal Year

Total POAM Cost For Sub Organization B

$ 135 -266

Compared to Last Fiscal Year

POAM Statuses For Fiscal Year 2016

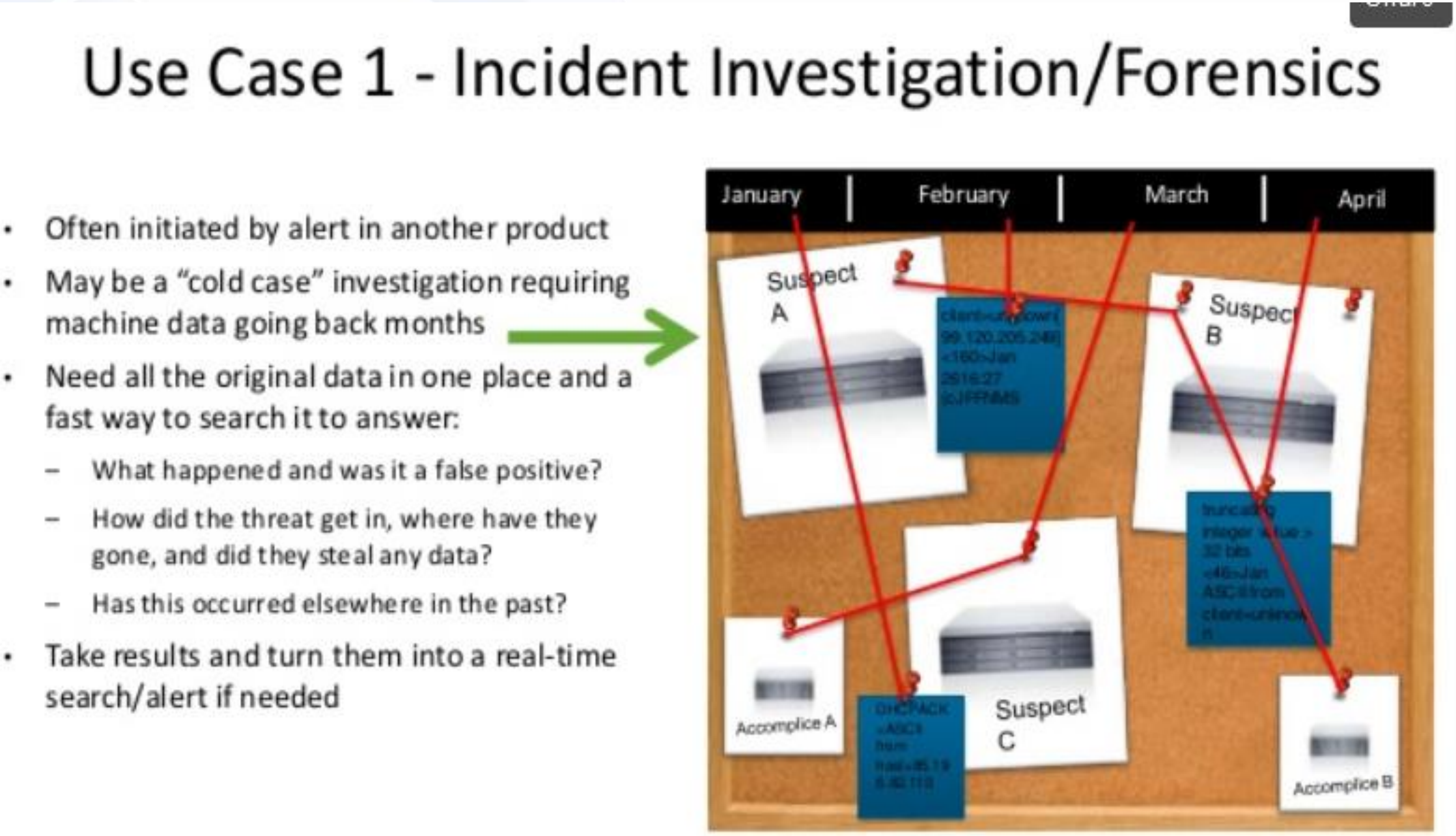
3	4	5	18
Not Started	Behind Schedule	Completion Date Approaching	Completed

POAM Cash Flow

Total POAM Cost By Criticality

POAM Cost By Sub Organization

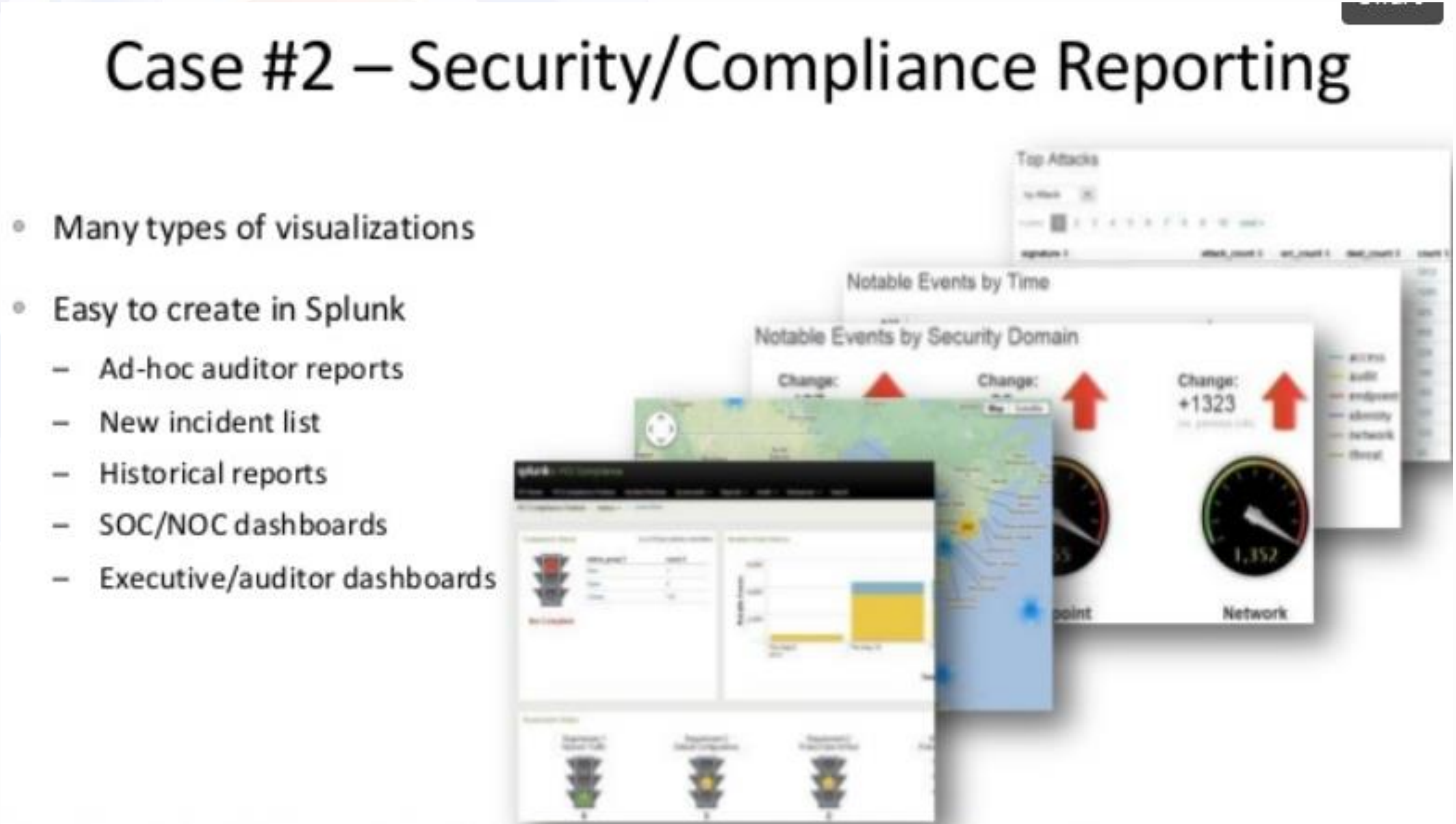
Teaching Students Incident Investigation Techniques



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

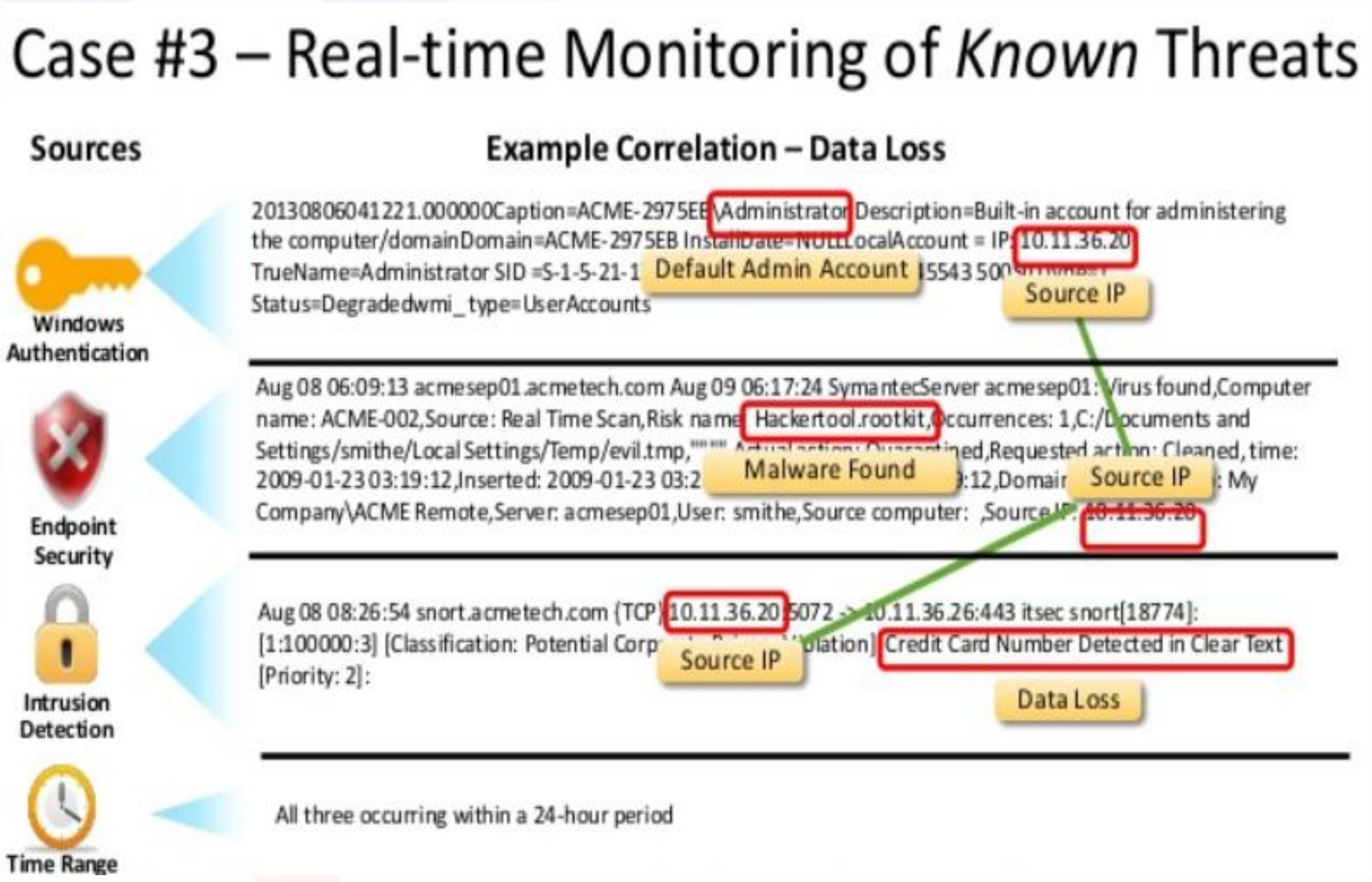
Teaching Students how to create Real Time Dashboards for Compliance Reports



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

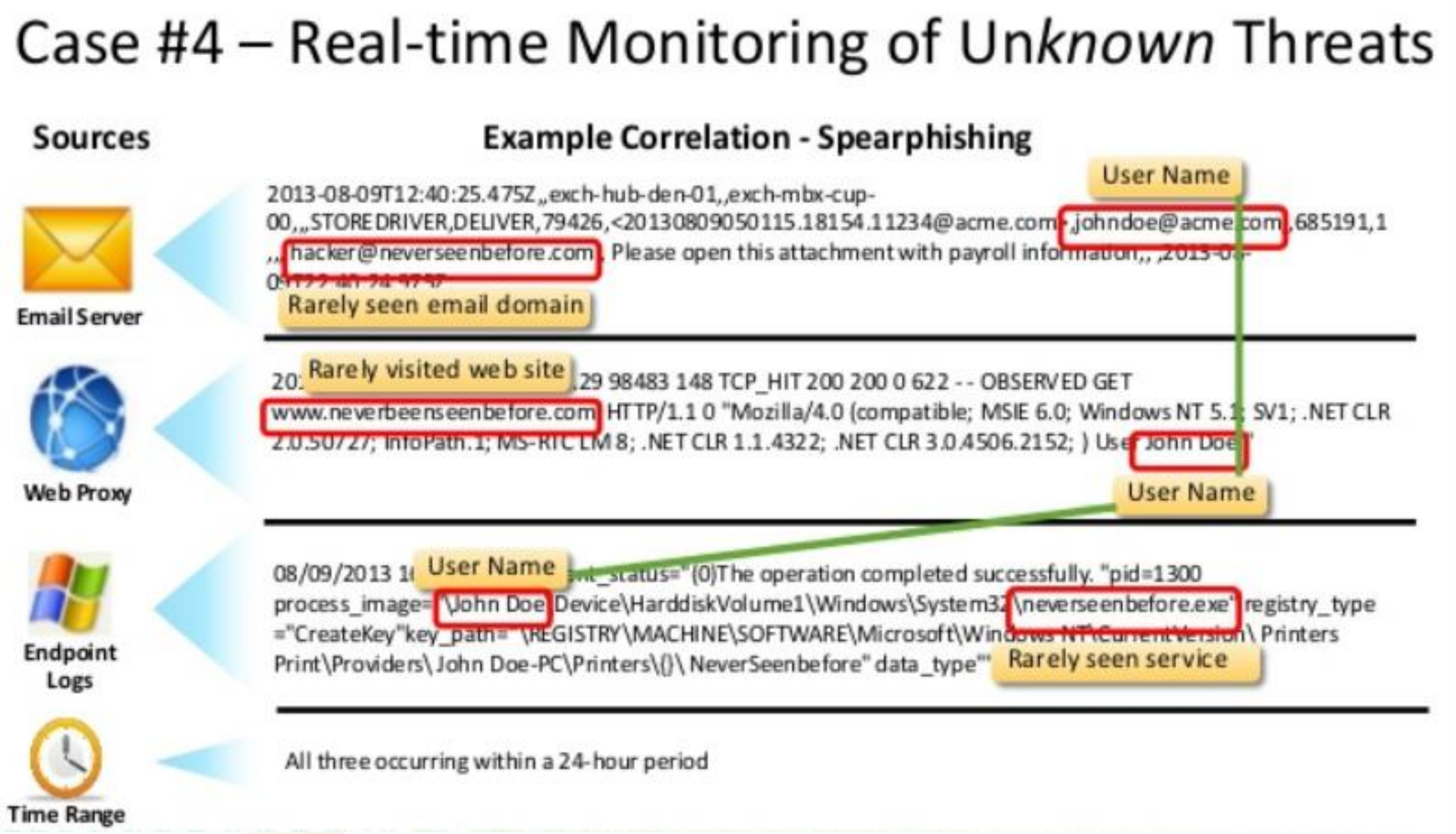
```
20130806041221.000000Caption=ACME-2975EB\Administrator Description=Built-in account for administering
the computer/domainDomain=ACME-2975EB InstallDate=NULLLocalAccount = IP:10.11.36.20
TrueName=Administrator SID =S-1-5-21-1                         15543 500
Status=Degradedwmi_type=UserAccounts
```

```
Aug 08 06:09:13 acmesep01.acmetech.com Aug 09 06:17:24 SymantecServer acmesep01: Virus found,Computer
name: ACME-002,Source: Real Time Scan,Risk name: Hackertool.rootkit,Occurrences: 1,C:/Documents and
Settings/smithe/Local Settings/Temp/evil.tmp,"""" Actual action: Quarantined,Requested action: Cleaned, time:
2009-01-23 03:19:12,Inserted: 2009-01-23 03:2                 9:12,Domain                : My
Company\ACME Remote,Server: acmesep01,User: smithe,Source computer: ,Source IP: 10.11.36.20
```

```
Aug 08 08:26:54 snort.acmetech.com {TCP} 10.11.36.20:5072 -> 10.11.36.26:443 itsec snort[18774]:
[1:100000:3] [Classification: Potential Corp               Violation] Credit Card Number Detected in Clear Text
[Priority: 2]:
```

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

Example Correlation - Spearphishing

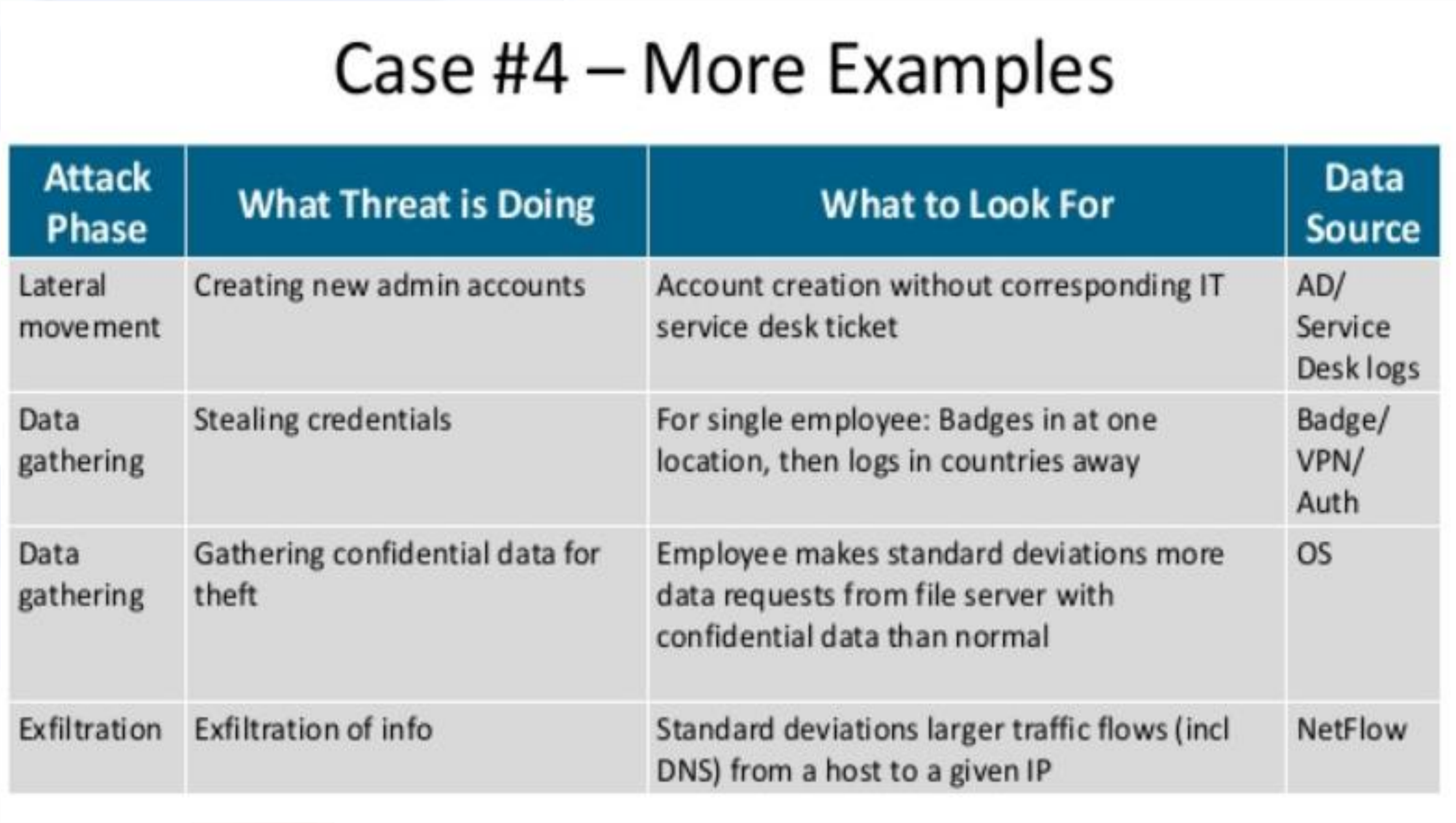
```
2013-08-09T12:40:25.475Z,,exch-hub-den-01,,exch-mbx-cup-
00,,,STOREDRIVER,DELIVER,79426,<20130809050115.18154.11234@acme.com>,johndoe@acme.com,685191,1
,,,hacker@neverseenbefore.com, Please open this attachment with payroll information,, ,2013-08-
09T22:40:24.975Z
```

```
20: .29 98483 148 TCP_HIT 200 200 0 622 - - OBSERVED GET
www.neverbeenseenbefore.com HTTP/1.1 0 "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"
```

```
08/09/2013 1 nt_status="(0)The operation completed successfully. "pid=1300
process_image="\John Doe Device\HarddiskVolume1\Windows\System32\neverseenbefore.exe" registry_type
="CreateKey"key_path="\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Printers
Print\Providers\ John Doe-PC\Printers\{}\ NeverSeenbefore" data_type""
```

All three occurring within a 24-hour period

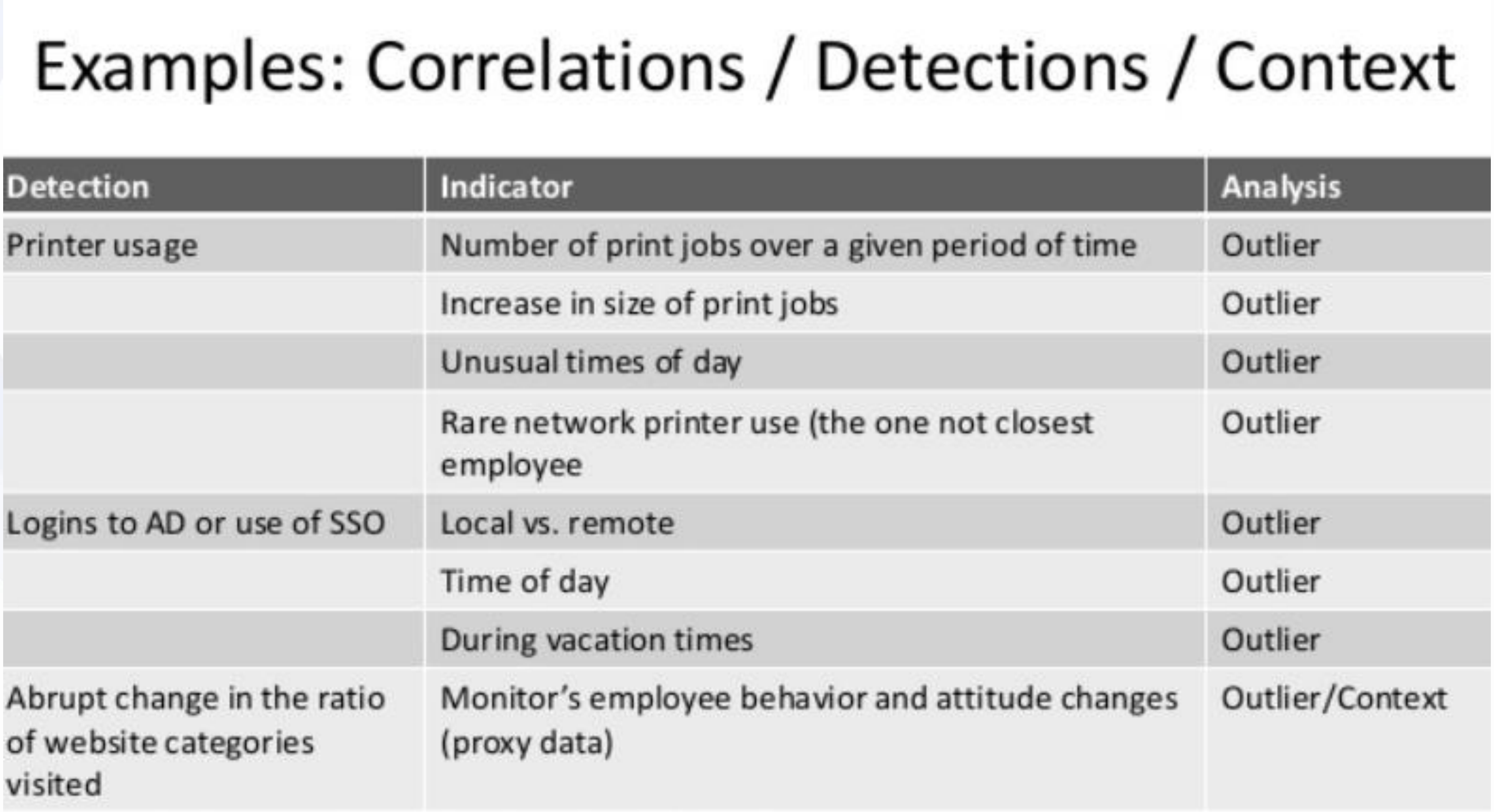
Valuable skills on Indicators of Compromise



Case #4 – More Examples

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

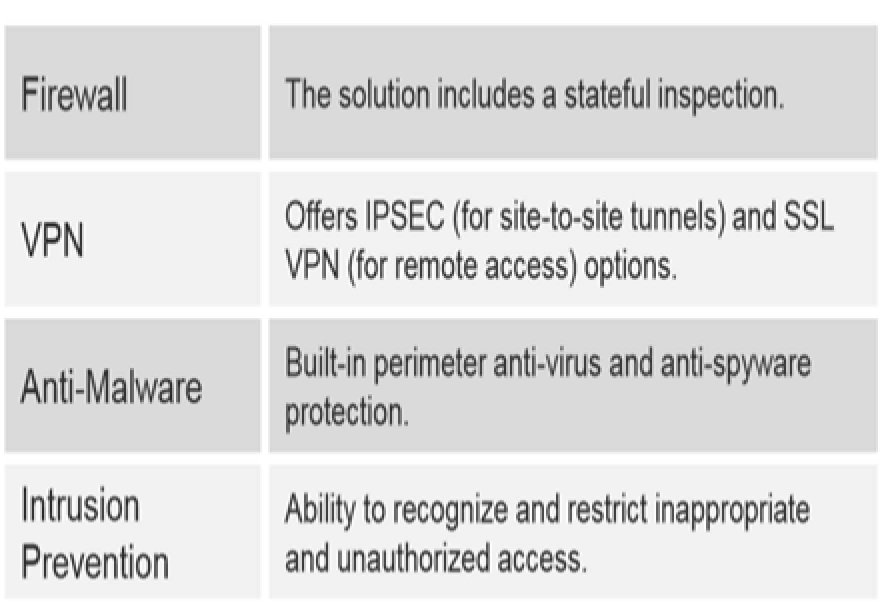
Valuable Skills to understand IOCs & Ability to perform Correlations with Context



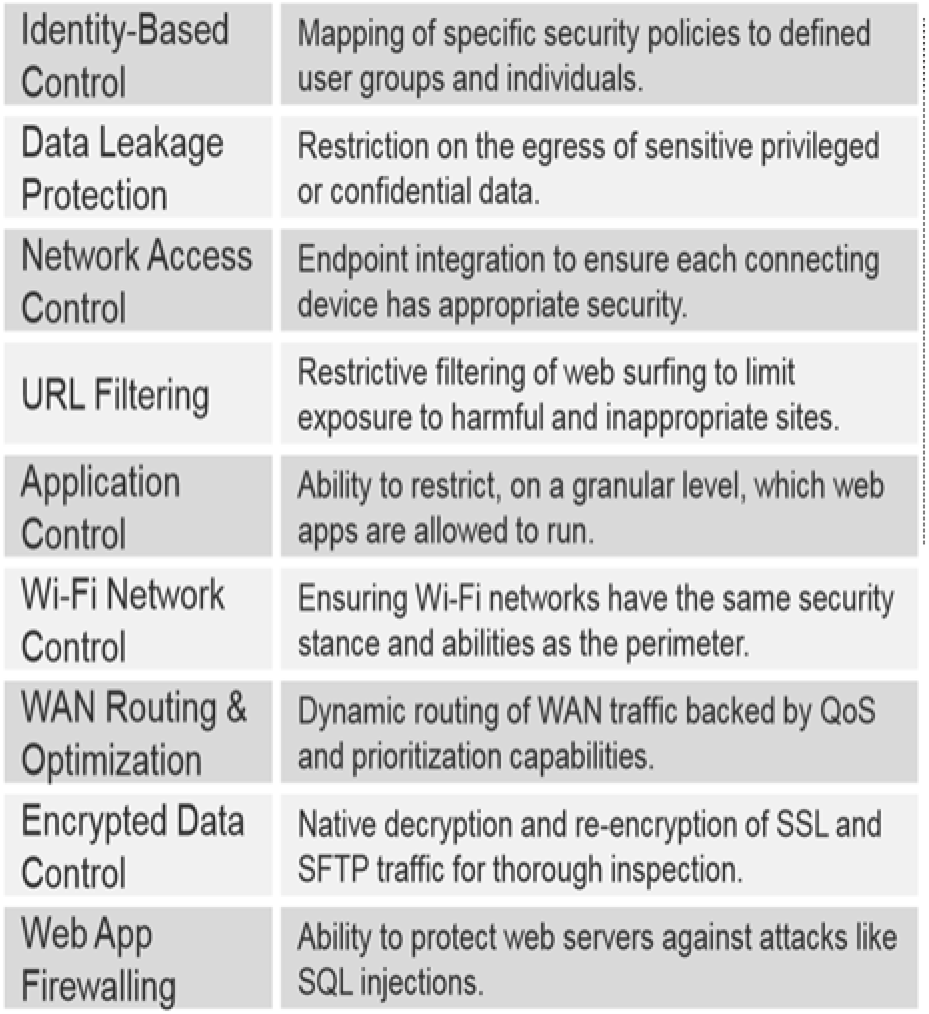
Examples: Correlations / Detections / Context

Detection	Indicator	Analysis
Printer usage	Number of print jobs over a given period of time	Outlier
	Increase in size of print jobs	Outlier
	Unusual times of day	Outlier
	Rare network printer use (the one not closest employee	Outlier
Logins to AD or use of SSO	Local vs. remote	Outlier
	Time of day	Outlier
	During vacation times	Outlier
Abrupt change in the ratio of website categories visited	Monitor's employee behavior and attitude changes (proxy data)	Outlier/Context

Learning Valuable Skills on Next Generation Firewalls (NGFW) Security Platform

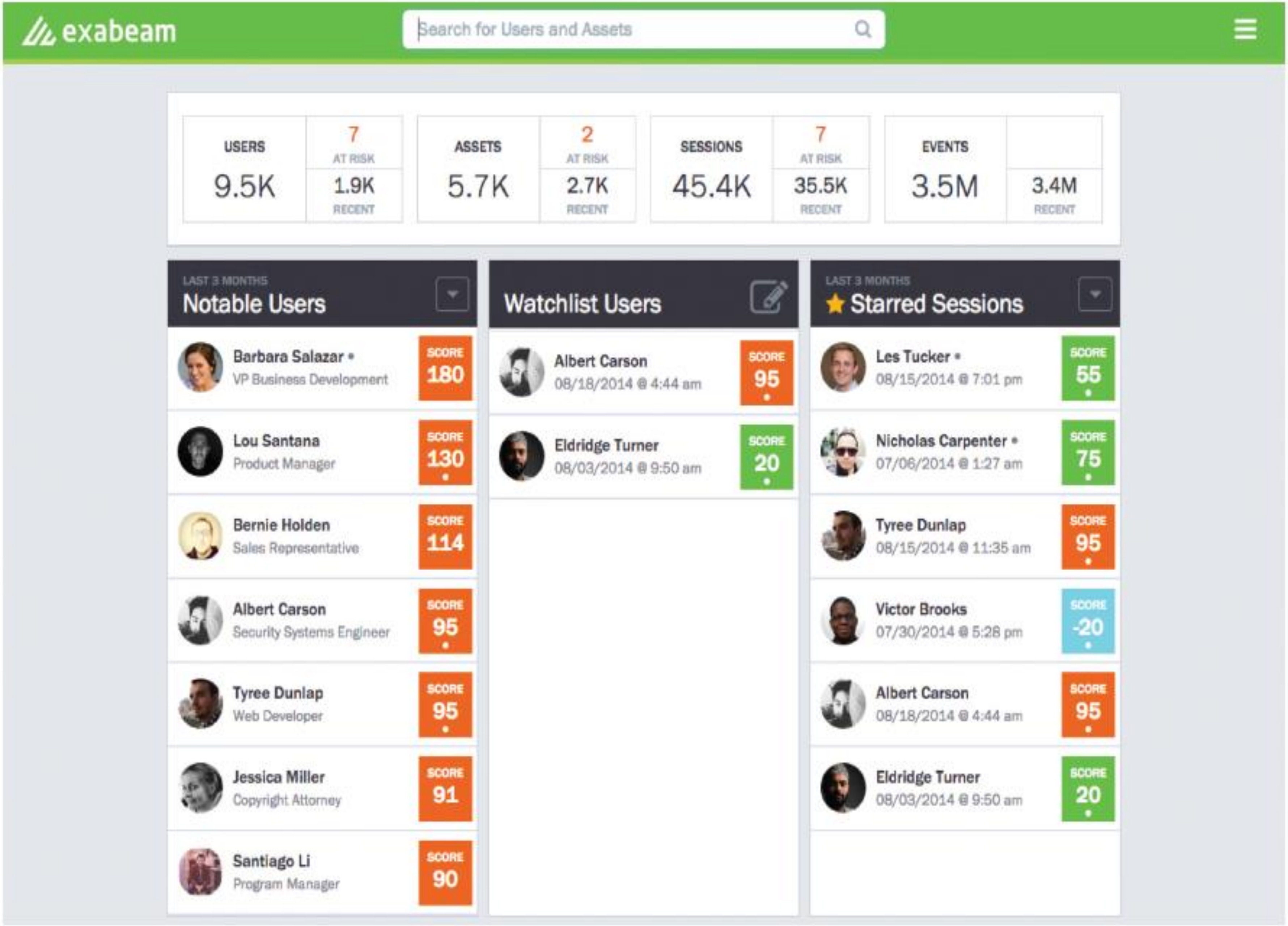


Firewall	The solution includes a stateful inspection.
VPN	Offers IPSEC (for site-to-site tunnels) and SSL VPN (for remote access) options.
Anti-Malware	Built-in perimeter anti-virus and anti-spyware protection.
Intrusion Prevention	Ability to recognize and restrict inappropriate and unauthorized access.



Identity-Based Control	Mapping of specific security policies to defined user groups and individuals.
Data Leakage Protection	Restriction on the egress of sensitive privileged or confidential data.
Network Access Control	Endpoint integration to ensure each connecting device has appropriate security.
URL Filtering	Restrictive filtering of web surfing to limit exposure to harmful and inappropriate sites.
Application Control	Ability to restrict, on a granular level, which web apps are allowed to run.
Wi-Fi Network Control	Ensuring Wi-Fi networks have the same security stance and abilities as the perimeter.
WAN Routing & Optimization	Dynamic routing of WAN traffic backed by QoS and prioritization capabilities.
Encrypted Data Control	Native decryption and re-encryption of SSL and SFTP traffic for thorough inspection.
Web App Firewalling	Ability to protect web servers against attacks like SQL injections.

User Behavior Analytics Skills for Insider Threat Detection



USERS	7 AT RISK	ASSETS	2 AT RISK	SESSIONS	7 AT RISK	EVENTS	
9.5K	1.9K RECENT	5.7K	2.7K RECENT	45.4K	35.5K RECENT	3.5M	3.4M RECENT

LAST 3 MONTHS

Notable Users

Barbara Salazar •	VP Business Development	SCORE 180
Lou Santana	Product Manager	SCORE 130 •
Bernie Holden	Sales Representative	SCORE 114
Albert Carson	Security Systems Engineer	SCORE 95 •
Tyree Dunlap	Web Developer	SCORE 95 •
Jessica Miller	Copyright Attorney	SCORE 91
Santiago Li	Program Manager	SCORE 90

Watchlist Users

Albert Carson	08/18/2014 @ 4:44 am	SCORE 95 •
Eldridge Turner	08/03/2014 @ 9:50 am	SCORE 20 •

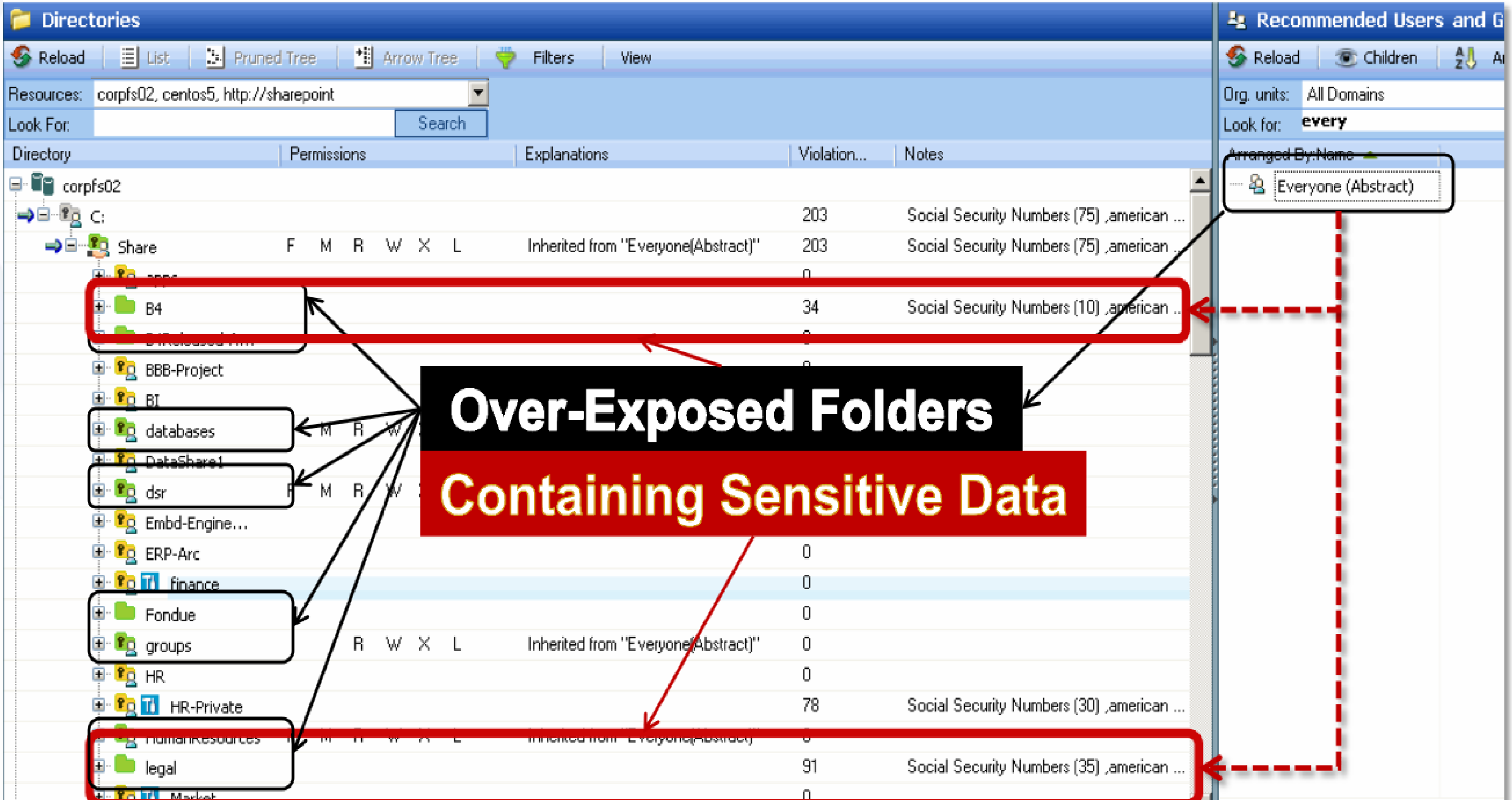
LAST 3 MONTHS

★ Starred Sessions

Les Tucker •	08/15/2014 @ 7:01 pm	SCORE 55 •
Nicholas Carpenter •	07/06/2014 @ 1:27 am	SCORE 75 •
Tyree Dunlap	08/15/2014 @ 11:35 am	SCORE 95 •
Victor Brooks	07/30/2014 @ 5:28 pm	SCORE -20 •
Albert Carson	08/18/2014 @ 4:44 am	SCORE 95 •
Eldridge Turner	08/03/2014 @ 9:50 am	SCORE 20 •

Risk Management on Unstructured Human Generated Data

Identify Risk – Over-exposed Sensitive Data



Resources: corpfs02, centos5, http://sharepoint

Look For:

Org. units: All Domains

Look for: every

Everyone (Abstract)

Directory	Permissions	Explanations	Violation...	Notes
corpfs02				
C:			203	Social Security Numbers (75) ,american ...
Share	F M R W X L	Inherited from "Everyone(Abstract)"	203	Social Security Numbers (75) ,american ...
apps			0	
B4			34	Social Security Numbers (10) ,american ...
B4Released-frm			0	
BBB-Project			0	
BI				
databases	M R W			
DataShare1				
dsr	F M R W			
Embd-Engine...				
ERP-Arc			0	
finance			0	
Fondue			0	
groups	R W X L	Inherited from "Everyone(Abstract)"	0	
HR			0	
HR-Private			78	Social Security Numbers (30) ,american ...
HumanResources	M R W X L	Inherited from "Everyone(Abstract)"	0	
legal			91	Social Security Numbers (35) ,american ...
Market			0	

Over-Exposed Folders

Containing 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.”

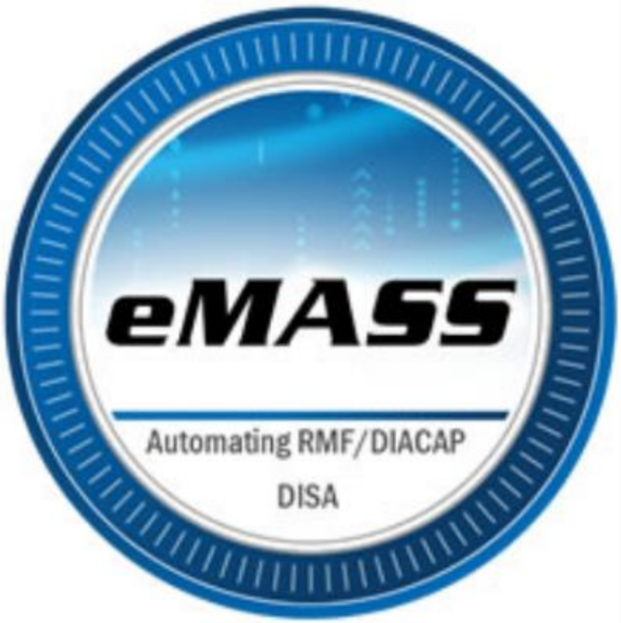
DoD HBSS / ESS Skills are very valuable for the Public Sector Cyber Jobs

- 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.

McAfee

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.



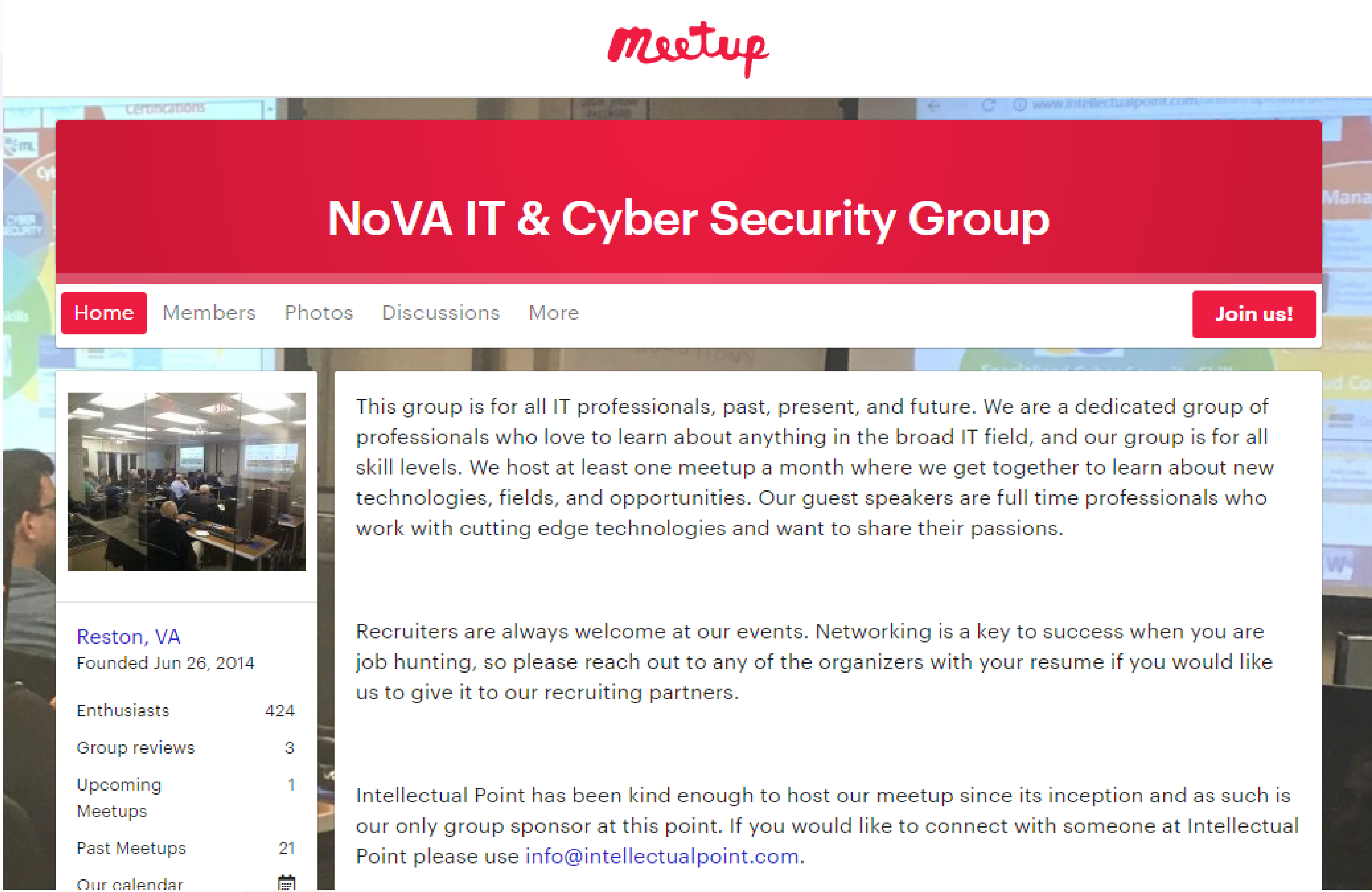
Hands-on Python Skills are highly valued for Cyber Jobs

- 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

Excellence through Education
Intellectual POINT

Intellectual Point hosts free Meetups to educate the workforce and spread Cyber Awareness



NoVA IT & Cyber Security Group

Reston, VA
Founded Jun 26, 2014

Enthusiasts	424
Group reviews	3
Upcoming Meetups	1
Past Meetups	21
Our calendar	

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.

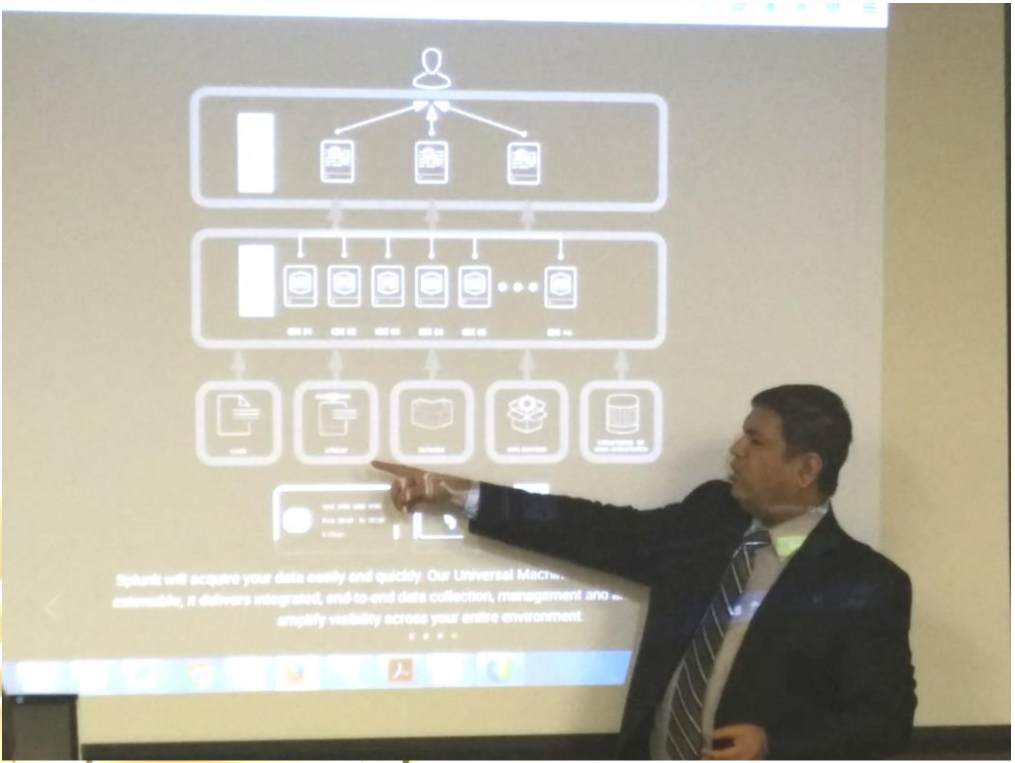
Recruiters are always welcome at our events. Networking is a key to success when you are job hunting, so please reach out to any of the organizers with your resume if you would like us to give it to our recruiting partners.

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

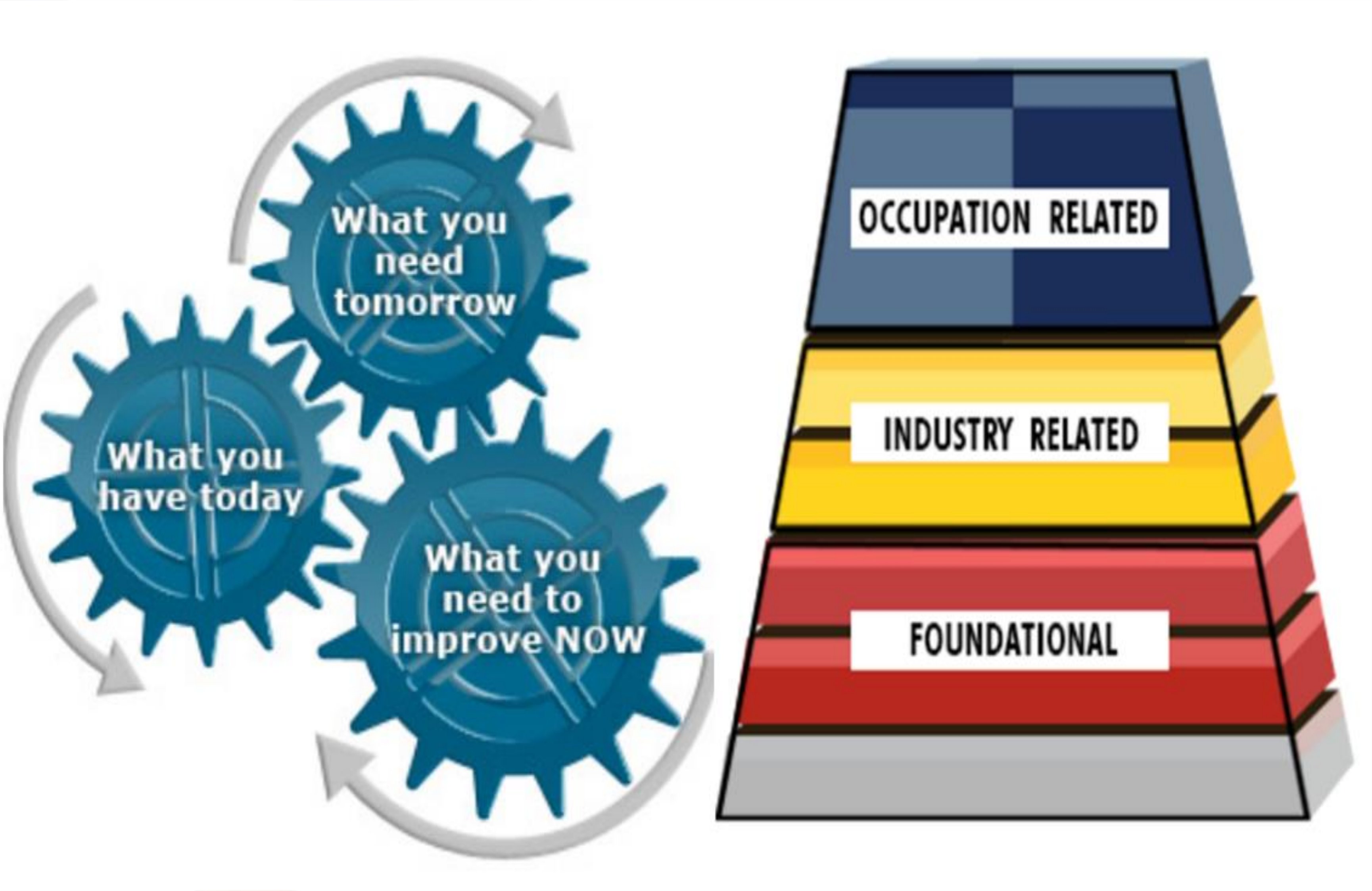

Splunk will acquire your data easily and quickly. Our Universal Machi...
extensible, it delivers integrated, end-to-end data collection, management and ...
amplify visibility across your entire environment.

And we’re dedicated to spreading the knowledge

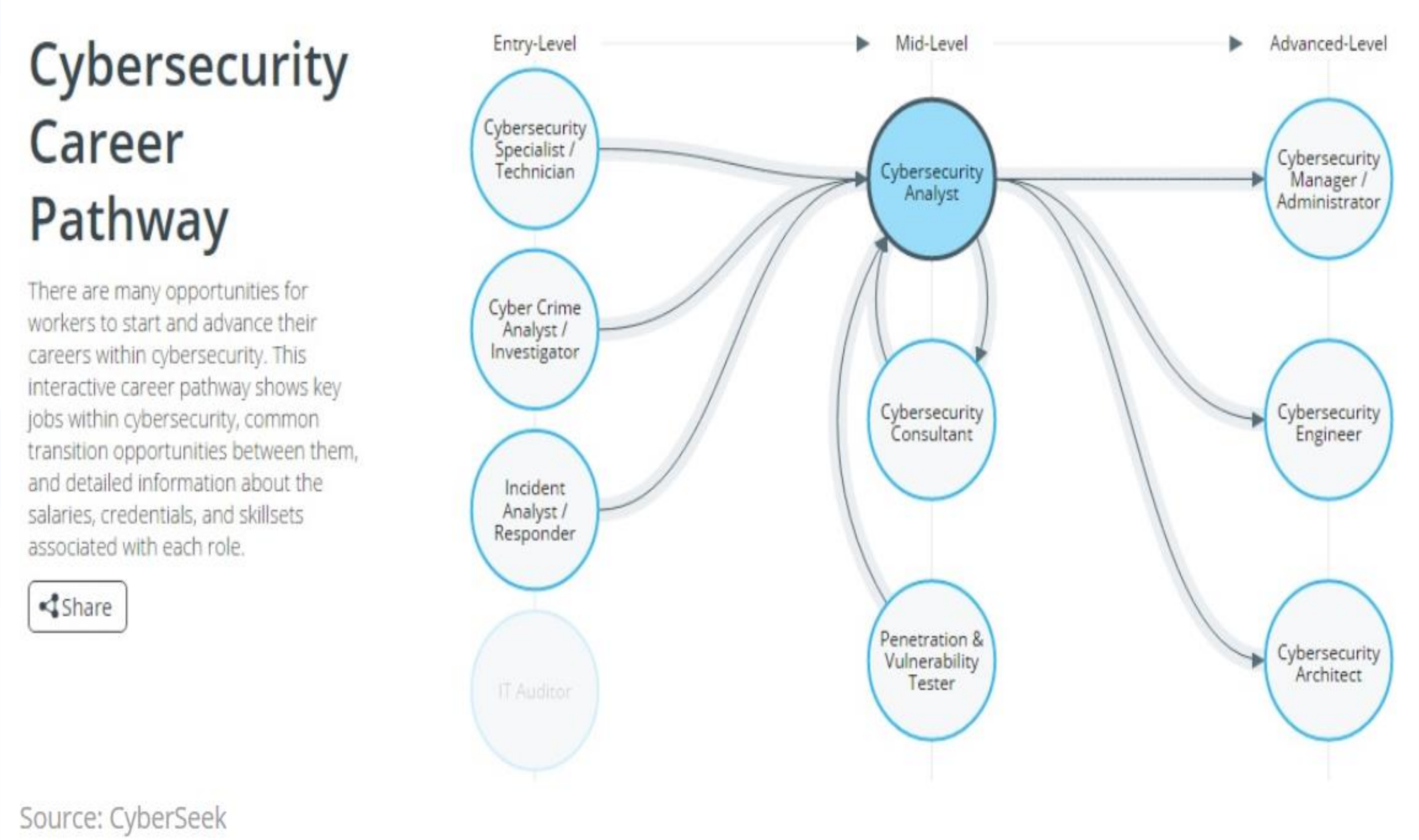
Career Counseling is important step to success and launch of Cyber Professionals

- 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



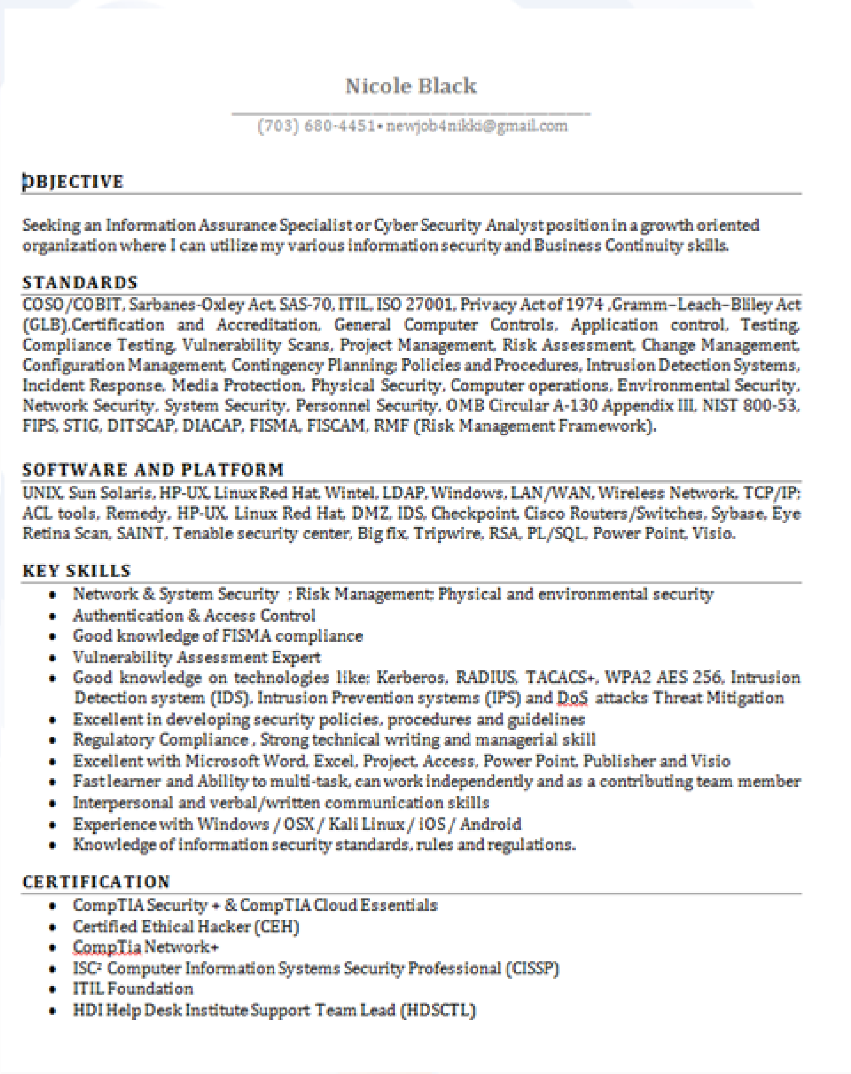
Cybersecurity Career Pathway

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.

Share
Entry-Level
Mid-Level
Advanced-Level
Cybersecurity Specialist / Technician
Cyber Crime Analyst / Investigator
Incident Analyst / Responder
IT Auditor
Cybersecurity Analyst
Cybersecurity Consultant
Penetration & Vulnerability Tester
Cybersecurity Manager / Administrator
Cybersecurity Engineer
Cybersecurity Architect

Source: CyberSeek

Assisting Clients with writing a cyber oriented resume leveraging past skills like Help Desk, QA, Breakfix etc.



Nicole Black

(703) 680-4451 • newjob4nikki@gmail.com

OBJECTIVE

Seeking an Information Assurance Specialist or Cyber Security Analyst position in a growth oriented organization where I can utilize my various information security and Business Continuity skills.

STANDARDS

COSO /COBIT, Sarbanes-Oxley Act, SAS-70, ITIL, ISO 27001, Privacy Act of 1974 ,Gramm–Leach–Bliley Act (GLB).Certification and Accreditation, General Computer Controls, Application control, Testing, Compliance Testing, Vulnerability Scans, Project Management, Risk Assessment, Change Management, Configuration Management, Contingency Planning; Policies and Procedures, Intrusion Detection Systems, Incident Response, Media Protection, Physical Security, Computer operations, Environmental Security, Network Security, System Security, Personnel Security, OMB Circular A-130 Appendix III, NIST 800-53, FIPS, STIG, DITSCAP, DIACAP, FISMA, FISCAM, RMF (Risk Management Framework).

SOFTWARE AND PLATFORM

UNIX, Sun Solaris, HP-UX, Linux Red Hat, Wintel, LDAP, Windows, LAN/WAN, Wireless Network, TCP/IP; ACL tools, Remedy, HP-UX, Linux Red Hat, DMZ, IDS, Checkpoint, Cisco Routers/Switches, Sybase, Eye Retina Scan, SAINT, Tenable security center, Big fix, Tripwire, RSA, PL/SQL, Power Point, Visio.

KEY SKILLS

- Network & System Security ; Risk Management; Physical and environmental security
- Authentication & Access Control
- Good knowledge of FISMA compliance
- Vulnerability Assessment Expert
- Good knowledge on technologies like; Kerberos, RADIUS, TACACS+, WPA2 AES 256, Intrusion Detection system (IDS), Intrusion Prevention systems (IPS) and DoS attacks Threat Mitigation
- Excellent in developing security policies, procedures and guidelines
- Regulatory Compliance , Strong technical writing and managerial skill
- Excellent with Microsoft Word, Excel, Project, Access, Power Point, Publisher and Visio
- Fast learner and Ability to multi-task, can work independently and as a contributing team member
- Interpersonal and verbal/written communication skills
- Experience with Windows / OSX / Kali Linux / iOS / Android
- Knowledge of information security standards, rules and regulations.

CERTIFICATION

- CompTIA Security + & CompTIA Cloud Essentials
- Certified Ethical Hacker (CEH)
- CompTia Network+
- ISC² Computer Information Systems Security Professional (CISSP)
- ITIL Foundation
- HDI Help Desk Institute Support Team Lead (HDSCTL)

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

COUNTY OF FAIRFAX 1742 VIRGINIA

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

Excellence through Education
Intellectual
POINT

NEUSOLIS

APEX Systems

corporate brokers
Beyond Resumes

eIntern.

hirestrategy
AN ADDISON GROUP COMPANY

veredus

DOD 8570.1M

DOD DIRECTIVE 8570.01M CHANGE 2 PROVIDES THE BASIS FOR AN ENTERPRISE-WIDE SOLUTION TO TRAIN, CERTIFY, AND MANAGE THE DOD INFORMATION ASSURANCE (IA) WORKFORCE

Intellectual Point Course Offerings

IAT LEVEL I
A+
CCNA-Security
Network+

IAM LEVEL I
Security+

IASAE I
CASP
CISSP

IAT LEVEL II
CCNA-Security
Security+

IAM LEVEL II
CASP
CISSP
CISM

IASAE II
CASP
CISSP

IAT LEVEL III
CASP
CISSP

IAM LEVEL III
CISSP
CISM

IASAE III
NA – at this time

CNDSP Analyst	CNDSP Infrastructure Support	CNDSP Incident Responder	CNDSP Auditor	CNDSP Manager
CEH	CEH	CEH	CEH	CISM

Intellectual

INTELLECTUAL POINT
11321 SUNSET HILLS RD
RESTON, VA 20190

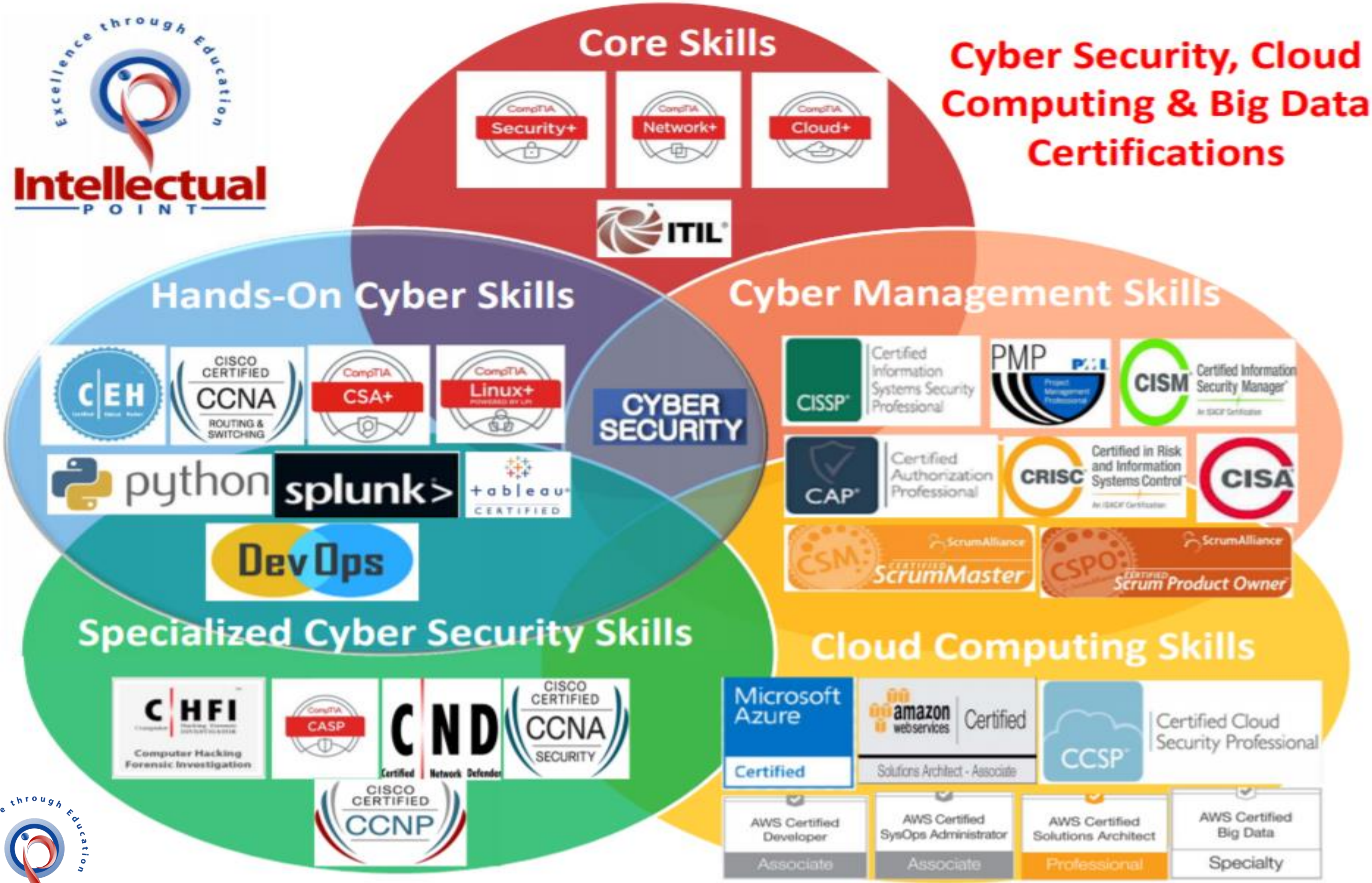
Email | info@intellectualpoint.com
Phone | 703.554.3827
Phone | 571.577.7890

www.intellectualpoint.com

CYBER SECURITY CAREER PATHWAY

Excellence through Education
Intellectual
POINT

Cyber Security, Cloud Computing & Big Data Certifications



Core Skills

Hands-On Cyber Skills

Cyber Management Skills

CYBER SECURITY

Specialized Cyber Security Skills

Cloud Computing Skills

CompTIA Security+
CompTIA Network+
CompTIA Cloud+
ITIL
CEH
CISCO CERTIFIED CCNA ROUTING & SWITCHING
CompTIA CSA+
CompTIA Linux+
python
splunk>
tableau CERTIFIED
DevOps
CISSP Certified Information Systems Security Professional
PMP PMI
CISM Certified Information Security Manager
CAP Certified Authorization Professional
CRISC Certified in Risk and Information Systems Control
CISA
CSM ScrumAlliance Certified ScrumMaster
CSPO ScrumAlliance Certified Scrum Product Owner
CHFI Computer Hacking Forensic Investigation
CompTIA CASP
CND Certified Network Defender
CISCO CERTIFIED CCNA SECURITY
CISCO CERTIFIED CCNP
Microsoft Azure Certified
amazon webservices Certified Solutions Architect - Associate
CCSP Certified Cloud Security Professional
AWS Certified Developer Associate
AWS Certified SysOps Administrator Associate
AWS Certified Solutions Architect Professional
AWS Certified Big Data Specialty

Excellence through Education

Intellectual
POINT

CAREER TRANSFORMATION SUCCESS STORIES

How 2015 CEHRT Automates Permitted Uses and Patient Access

Putting People into Cyber Security Careers

Career Transformation

- We get many students that come from a non-IT backgroud.
- 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.

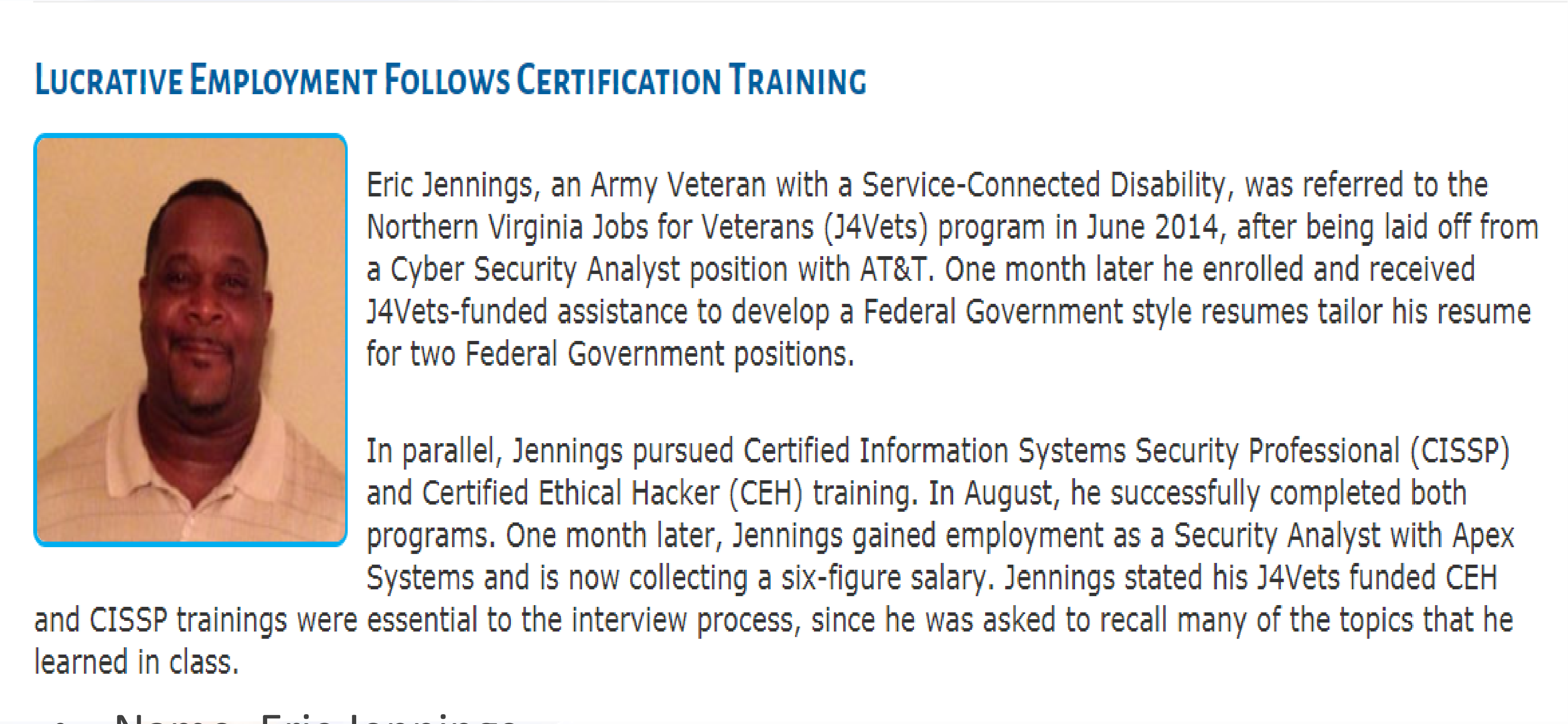
Current Profession

- 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

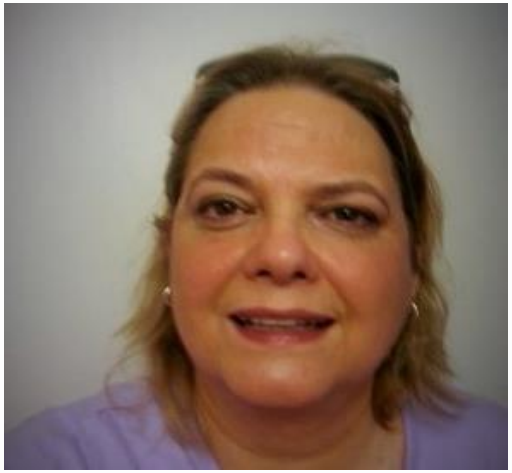
Eric Jennings, an Army Veteran with a Service-Connected Disability, was referred to the Northern Virginia Jobs for Veterans (J4Vets) program in June 2014, after being laid off from a Cyber Security Analyst position with AT&T. One month later he enrolled and received J4Vets-funded assistance to develop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

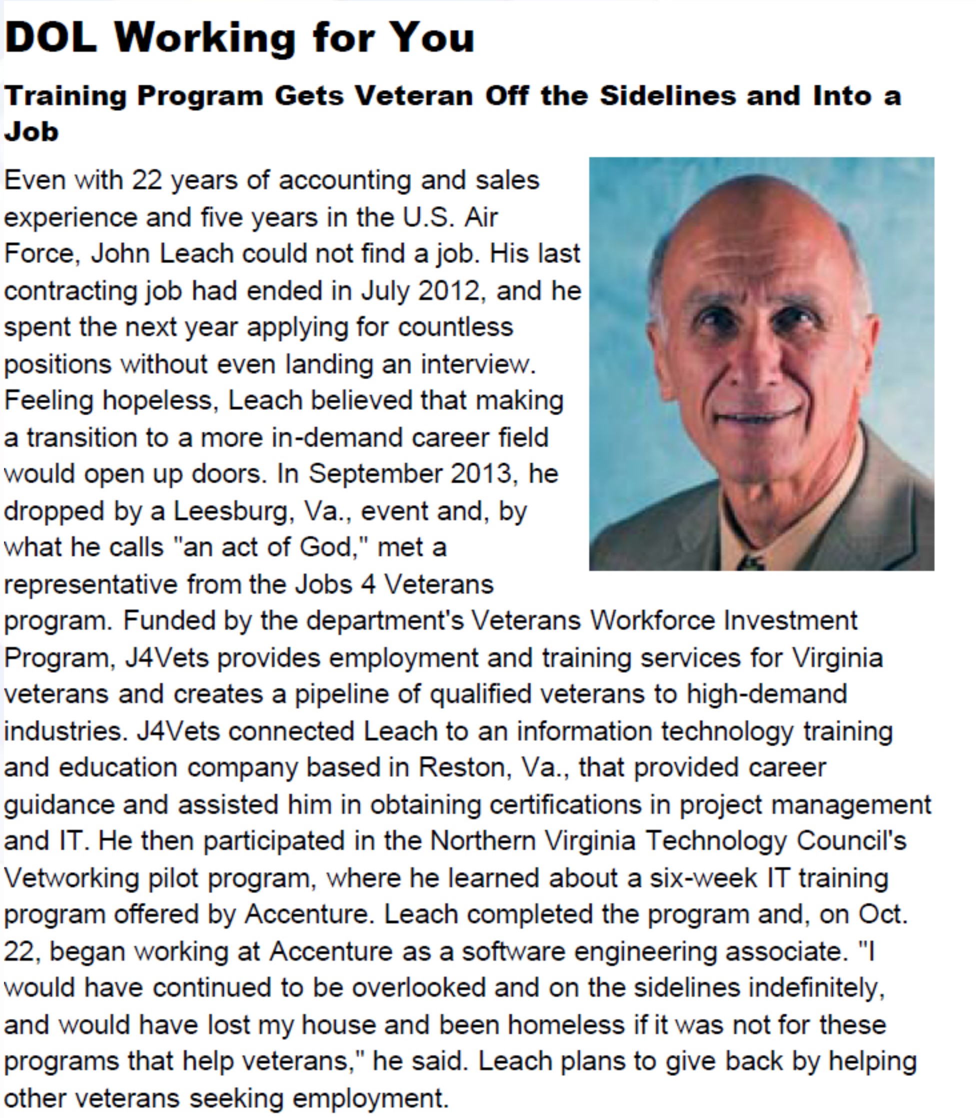
- Lost her job at BT as Config Specialist
- Came as a referral from Fairfax Skillsource Center under WIOA program.
- Completed the following certifications at Intellectual Point
  - CompTIA Security+ & Cloud+
  - ITIL Foundation
  - Cisco CCNA
  - Certified Ethical Hacker (CEH)
- Got placed at ASM Research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



ASM Research
An Accenture Federal Services Company

Excellence through Education
Intellectual
POINT

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.

Intellectual POINT
Excellence through Education

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.

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

Summary & Key Take-Aways

- 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.

How to Contact Us

Contact Us

Should you wish to contact us via email, please click the following link, or call us at the number provided below.

Intellectual Point LLC
Sunset Hills Professional Center
11321 Sunset Hills Road,
Reston, VA 20190.

Phone : 703-554-3827
Email: contact@intellectualpoint.com

Prem Jadhwani
President and CEO
Intellectual Point
Prem@IntellectualPoint.com
703-554-3827
http://www.intellectualpoint.com