



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

September 2, 2015



ISOAG September 2, 2015 Agenda

- | | |
|--|---------------------------------------|
| I. Welcome & Opening Remarks | Michael Watson, VITA |
| II. Dealing with Overload | Eric Cowperthwaite, Core Security |
| III. National Cyber Security Awareness Month | Ed Miller, VITA |
| IV. Upcoming Events | Bob Baskette/Michael Watson, VIT |
| V. Partner/Operation Update | Bob Baskette, VITA, Michael Clark, NG |



Welcome and Opening Remarks

Michael Watson

September 2, 2015



Dealing with Overload

Eric Cowperthwaite, Core Security

September 2, 2015

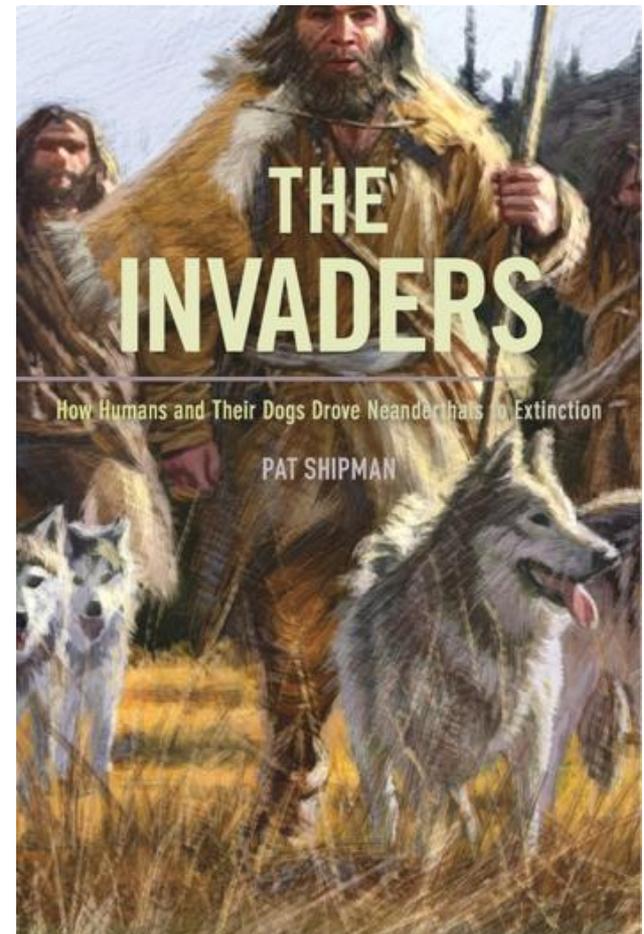
CISO Overload

Eric W. Cowperthwaite

Vice President Advanced Security and Strategy

Without Change, We Die

- Looks at why Homo Sapiens survived and Neanderthals did not
- A key issue was that Neanderthals didn't adapt to new threats
- Security today is behaving like Neanderthals



Another Military Analogy

- We are preparing for the last war
- Much like the French Maginot Line in WWII
- Our defenses are aimed at 2003
 - SQL Slammer
 - Email viruses
 - Lost and stolen devices
- We are fighting WWI and they are fighting WWII
- Who's going to win that fight?

And The Reality Is

Our current concept says:

- Build a strong outer defense
- Know who everybody on the network is
- Defend all systems with a standard set of security controls



In spite of this, the bad guys seem to be able to break in to whatever organization they want to.

Anatomy of a Breach

- Adobe breached by exploiting a ColdFusion vulnerability, according to Krebs on Security
- Attacker discovered vulnerabilities the defender didn't know about.



The Problem - Overload

- Security teams are overloaded –
 - Data – vulnerabilities, networks, viruses, SIEM, oh my
 - Regulations – Required security, reports, mandatory activity, oh my



Data Overload

- The advent of virtualization
- Data center sprawl
- End points, mobility, Internet of Things
- Vulnerability proliferation (Adobe)
- Event proliferation (Neiman Marcus)



Regulatory Overload

- HIPAA, GLBA, FISMA, PCI
- State breach notification laws
- State security regulations
- Commonwealth's Information Security Standard



Let's Start Here ...

- Predictive Security is a real term
- What it means is ...

Predictive security solutions enable you to understand the strengths and weaknesses of your infrastructure, network and human security and predict where an attacker is most likely to attack and exploit them successfully.

And ...

- Modern, innovative security solutions
- Are a force multiplier
- Deal with regulatory reality
- Improve security



How About Some Nuts & Bolts

- Need to understand your network, servers, & vulnerabilities
- And then be able to think like a hacker would
- Validate and prioritize vulnerabilities
- Demonstrate appropriate security
- Satisfy auditors and regulators



This Is A Big Data Problem

- My previous employer has over 100,000 nodes
- How many vulnerabilities? How many possible attack paths?
- Are the vulnerabilities exploitable
- Does the attack path lead to sensitive data
- 7 different regulations and security frameworks to satisfy

What's The Advantage?

- Instead of defending everything/nothing
- You will know where the attacks will happen
- Defend the attack path
- Harden critical systems
- Increase the cost/difficulty for the bad guy

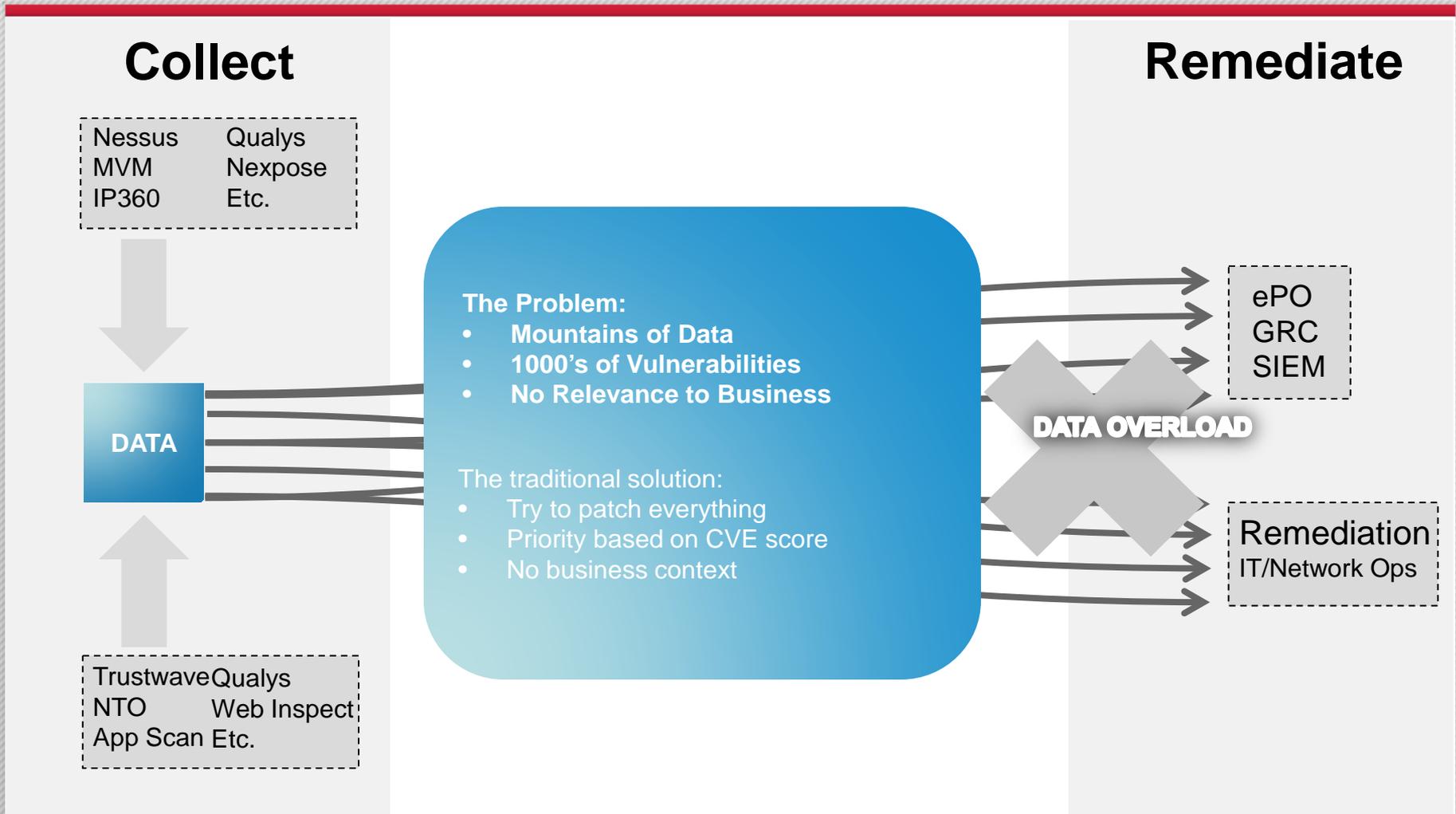


Bottom Line

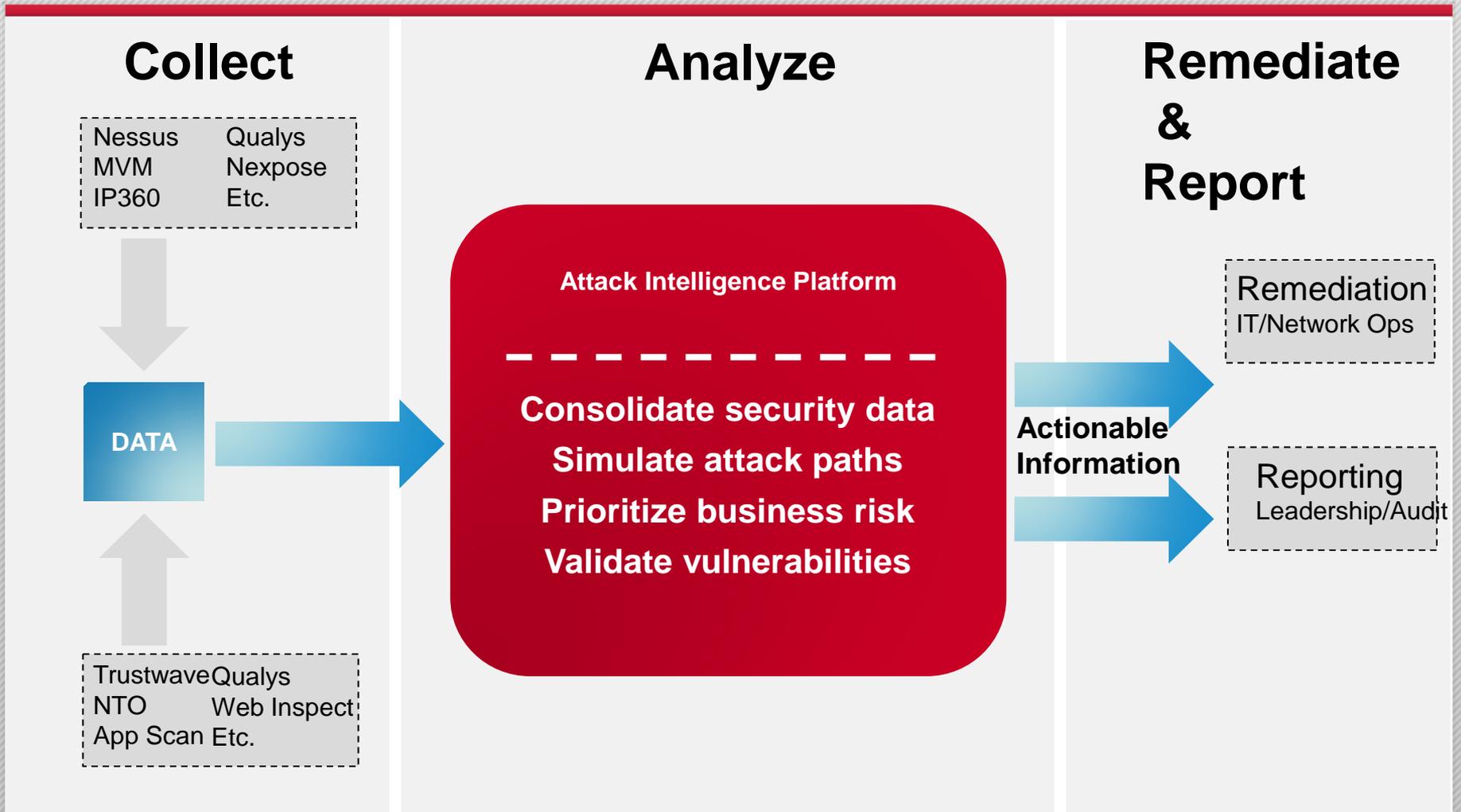
- This is the future of Information Security
- Success is going to require innovation
- Big Data solutions are crucial
- Must understand what the bad guy will do
- Must know where to expend limited resources
- Have to change the game from blind defense to intelligent defense



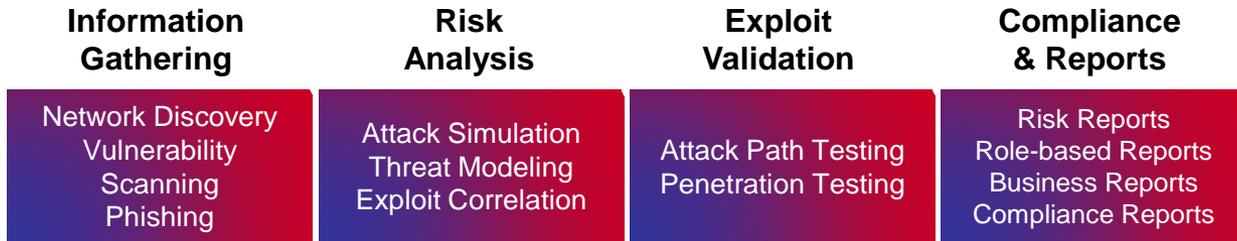
Visualizing the Problem



Visualizing the Solution

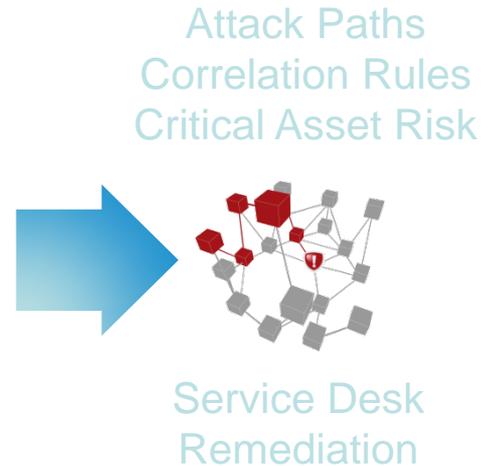
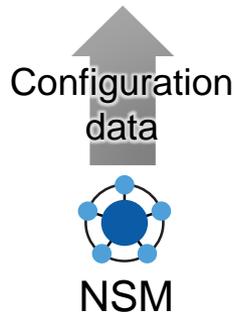


Attack & Threat Intelligence Platform



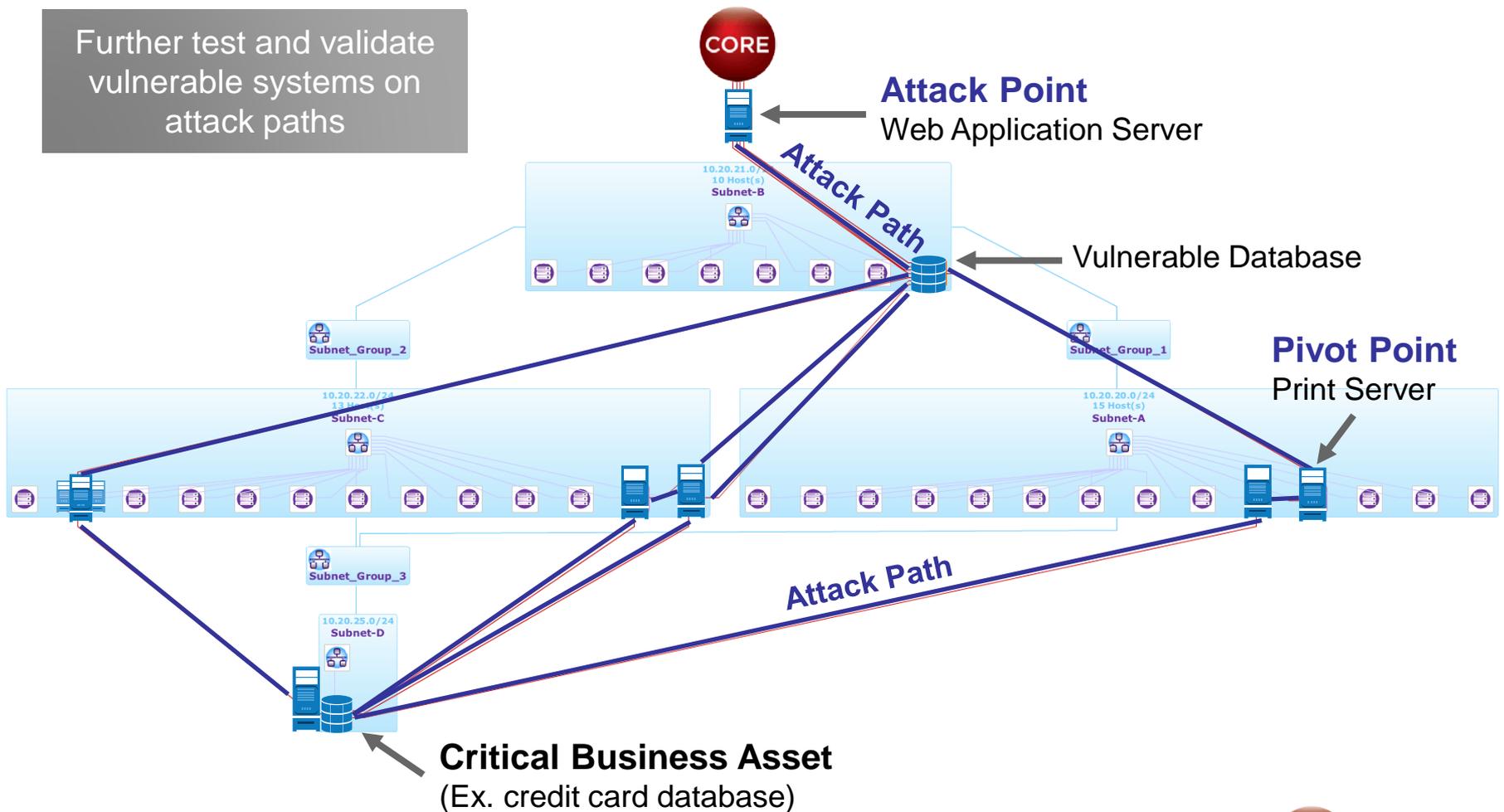
Attack Intelligence Platform

Integration Framework

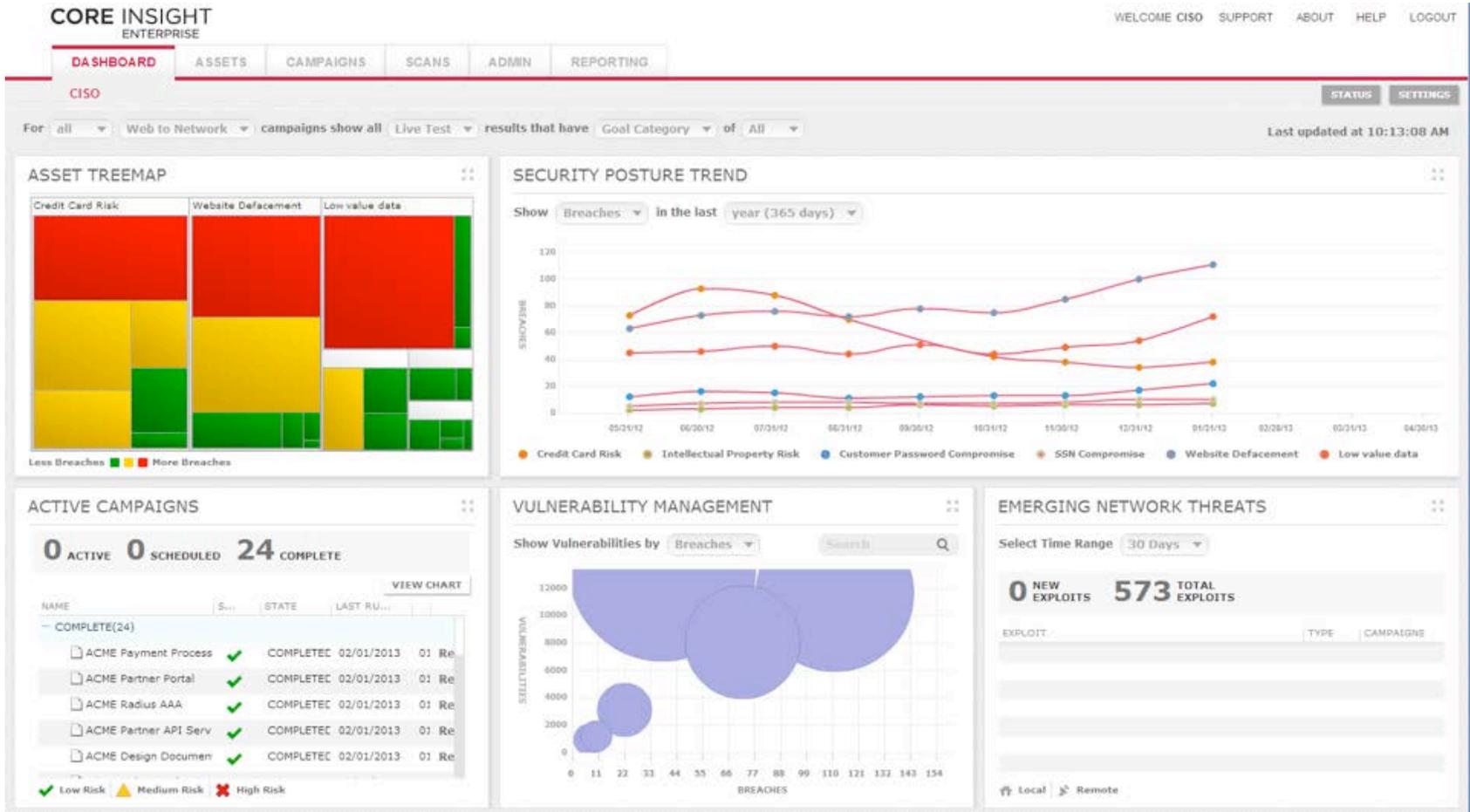


What Does It Look Like In Practice?

Further test and validate vulnerable systems on attack paths



CISO Dashboard Relieves Overload



Continue The Conversation





Virginia Information Technologies Agency

National Cyber Security Awareness Month





National Cyber Security Awareness Month is observed annually in October. This year marks the 12th anniversary of NCSAM and the 5th anniversary of Stop.Think.Connect Campaign



<http://www.stopthinkconnect.org/>

The Anti-Phishing Working Group (APWG) and National Cyber Security Alliance (NCSA) led the development of the STOP. THINK. CONNECT. campaign. The U.S. Department of Homeland Security provides the Federal Government's leadership for the STOP. THINK. CONNECT. campaign.



STOP | THINK | CONNECT™

Keeping the web a safer place for everyone.

Partner Resource Center Login:

email password

Forgot Password?

- HOME
- RESOURCES
- CAMPAIGNS
- GET INVOLVED
- TIPS & ADVICE
- RESEARCH & SURVEYS
- BLOGS

**BE A GOOD CYBER CITIZEN BY
OWNING YOUR ONLINE PRESENCE.**

STOP. THINK. CONNECT.

Take security precautions, understand the consequences of your actions and behaviors and enjoy the benefits of the Internet.

STOP: Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

THINK: Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's.

CONNECT: Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

Protect yourself and help keep the web a safer place for everyone.

The Anti-Phishing Working Group (APWG) and National Cyber Security Alliance (NCSA) led the development of the STOP. THINK. CONNECT campaign. The U.S. Department of Homeland Security provides the

DID YOU KNOW?

54% of Americans are extremely concerned about loss of personal or financial information.

[MORE FACTS](#)

TWO STEPS AHEAD
PROTECT YOUR DIGITAL LIFE

Protect your digital life by adding layers of security to your online accounts.



[LEARN HOW](#)

Get Involved!



It's easy to get involved with STOP. THINK. CONNECT. We're creating free resources for anyone to use.

[GET STARTED](#)

TIP OF THE WEEK



Stop. Think.
Connect.

National Cyber
Security
Awareness Month
Partner Packet



STOP.THINK.CONNECT.™
NATIONAL CYBER SECURITY
AWARENESS MONTH PARTNER PACKET

| | |
|--|----|
| CONTENTS | 2 |
| Planning for NCSAM | 3 |
| Getting Started: Make a Plan | 3 |
| Planning Checklist: Countdown to NCSAM | 4 |
| Daily Ideas to for NCSAM | 5 |
| Sample Language | 6 |
| Talking Points | 6 |
| Intranet or Website Language | 8 |
| Sample Auto Signature Text | 8 |
| Sample Announcement Email | 9 |
| Sample Social Media Posts | 10 |
| Sample Articles | 14 |
| Cybersecurity: A Shared Responsibility | 14 |
| Five Years of Stop.Think.Connect.™ | 15 |
| The Three Major Ways You Put Your Data at Risk | 17 |
| Fostering a Culture of Cybersecurity at [ORGANIZATION NAME] | 19 |
| Cybersecurity 101: Common Cyber Threats and Risks | 20 |
| Protect Your Evolving Digital Life | 22 |
| Stay Safe on Your Mobile Devices | 23 |
| In Our "Smart World" the Internet Touches All Aspects of Our Daily Lives | 25 |
| Building a Strong Cyber Workforce | 26 |
| Interactive Ideas for NCSAM Events | 27 |
| Just For Fun: Spread Awareness at the Office | 28 |



Start Planning Now

1. Determine weekly themes relevant to your agency
2. Solicit ideas from departments within your agency for NCSAM
3. Identify what communications channels you will use to distribute your tips or resources i.e. webpage, social media, tweets, instagram
4. Determine how you will distribute your information i.e. posters, tip cards, informational materials.
5. Most importantly, make it your own brand – You know the unique needs of your agency.



Planning Checklist: Countdown Time

September

1. Continue planning your event
2. Brief your leadership on your plans and solicit their support
3. Work with your communications teams to develop a strategy to promote NCSAM
4. Publicize your event

October

1. Post a message on your website or newsletter to announce NCSAM
2. Add a NCSAM auto signature to your emails
3. Post cybersecurity and safety messages on social media throughout the month
4. Post cyber security blogs
5. Hold agency events for employees to attend



Activity List Examples

Week 1 – General Cyber Security Awareness Information

1. Upload the NCSAM banner to your website
2. Post a cyber security message on your website or on social media announcing NCSAM

Week 2 – Creating a Culture of Cybersecurity at Work

1. Share tips on protecting your workplace
2. Encourage employees to use a NCSAM auto signature. i.e. “Cybersecurity is a shared responsibility”, etc.

Week 3 – Staying Protected While Connected

1. Post a mobile safety tip on social media
2. Share a link to a cybersecurity video on your website
3. Hold a cybersecurity event



Activity List Examples

Week 4 – Your Evolving Digital Life

1. Post a cybersecurity story in an online newsletter
2. Email a cybersecurity tip to employees

Week 5 – Building the Next Generation of Cyber Professionals

1. Share a news story about the importance of cybersecurity
2. Post a cybersecurity fact or figure on social media



Virginia Information Technologies Agency

Additional Resources

www.stopthinkconnect.org

ftc.gov/bulkorder

Order free resource materials from the Federal Trade Commission

www.staysafeonline.org/stay-safe-online/

www.microsoft.com/security/default.aspx

www.us-cert.gov/ncas/tips

www.dhs.gov/national-cyber-security-awareness-month



Virginia Information Technologies Agency

VITA Activity List

Week 1 – Cyber Security: It's Our Shared Responsibility

1. Open Message from VITA's CIO to employees about the importance of National Cyber Security Awareness Month
2. Cyber security games, videos and informational links will be emailed to all employees
3. We will kick off the MS ISAC's annual "Kids Safe Online" Poster Contest for school age kids K through 12
4. Oct 1 – **Brown bag lunch and learn** session featuring a Security Family Feud Game to test employees knowledge of cyber security etiquette
5. Setup a Cyber Security Information table in the hallway
6. Publish the Governor's Cyber Security Month Proclamation
7. Post Security Awareness Toolkit on our website
8. Post weekly Cyber Security Awareness Blog by David Ihrie, Center for Information Technology
9. Twitter Thursday – Invite employees to tweet security awareness tips based on the theme of the week



VITA Activity List

Week 2 – Social Media – Be Careful What you Post

1. Social Media related security games, videos and informational links will be emailed to all employees
2. Cyber Security Information table in the hallway
3. Oct 7 – Information Security Officers Advisory Group (ISOAG) monthly meeting. Security Awareness posters and pamphlets will be distributed to all attendees.
4. Post weekly Cyber Security Awareness Blog by David Ihrie, Center for Information Technology
5. Twitter Thursday – Invite employees to tweet security awareness tips based on the theme of the week



Virginia Information Technologies Agency

VITA Activity List

Week 3 – Securing Our Work Environment (If you see something, say something)

1. Securing Our Work Environment games, videos and informational links will be emailed to all employees
2. Cyber Security Information table in the hallway
3. Oct 13 – Employee Popcorn Social to celebrate “National Cyber Security Awareness Day”
4. Oct 14 - **Brown bag lunch-and-learn** session on “Protecting Our Infrastructure” presented by the Department of Homeland Security
5. Link to weekly Cyber Security Awareness Blog by David Ihrie, Center for Information Technology
6. Cyber Security Information table in the hallway
7. Post weekly Cyber Security Awareness Blog by David Ihrie, Center for Information Technology
8. Twitter Thursdays – Invite employees to tweet security awareness tips based on the theme of the week



VITA Activity List

Week 4 – Protecting Your Privacy Online – Know the Risks

1. Privacy related games, videos and informational links will be emailed to all employees
2. Cyber Security Information table in the hallway
3. Oct 21 - **A brown bag lunch-and-learn** session presentation by Special Agent James LaMattina, United States Secret Service in conjunction with Capital One on “ATM Skimming”
4. Post weekly Cyber Security Awareness Blog by David Ihire, Center for Information Technology
5. Twitter Thursday – Invite employees to tweet security awareness tips based on the theme of the week



Virginia Information Technologies Agency

VITA Activity List

Week 5 – Keeping Children Safe Online

1. Keep Children Safe online security related games, videos and informational links will be emailed to all employees
2. Oct 28: **Brown bag lunch-and learn** session presentation by Captain Robert P. Chappell, Virginia State Police. Captain Chappell is the author of the book *“Child Identity Theft : What Every Parent Needs to Know”*.
3. Oct 29: Cyber Security bake and cyber games for donations to benefit the Commonwealth of Virginia Charities
4. Post weekly Cyber Security Awareness Blog by David Ihrie, Center for Information Technology
5. Twitter Thursday – Invite employees to tweet security awareness tips based on the theme of the week



2016 “Kids Safe Online Poster Contest”

VITA will be kicking off the 2016 MS ISAC Kids Safe Online Poster Contest this month. The contest is open to students in grades kindergarten through 12.

The contest is sponsored by the Virginia Information Technologies Agency (VITA) in conjunction with the Multi-State Information Sharing and Analysis Center (MS-ISAC). This is a national contest which encourages our youth to use the Internet safely and securely.



2016 “Kids Safe Online Poster Contest

The top three winning posters from Virginia for each grade group (K-5, 6-8 and 9-12) will be submitted to the national Multi-State Cyber Security Awareness poster contest.

The national winning posters in each age group will have their artwork displayed in the 2017 National Stay Safe Online Calendar. The calendar will be distributed throughout the country and may also be used in campaigns to raise awareness among children of all ages about internet and computer safety.

Virginia has three national winners in last two years.



2016 “Kids Safe Online Poster Contest”

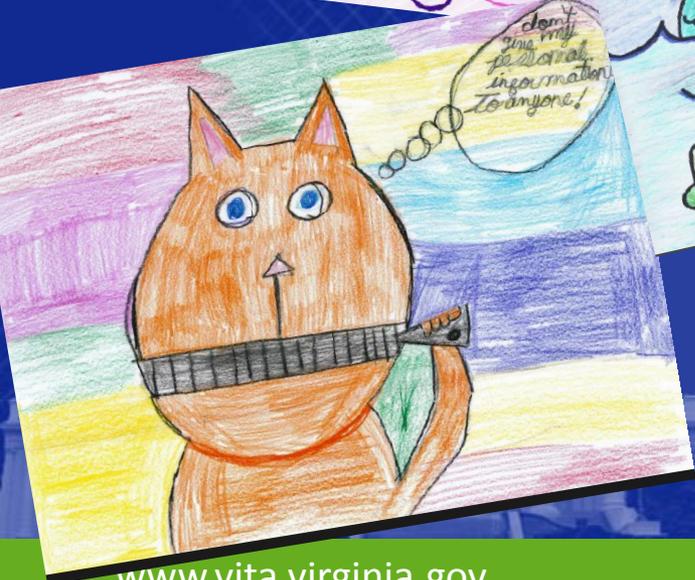
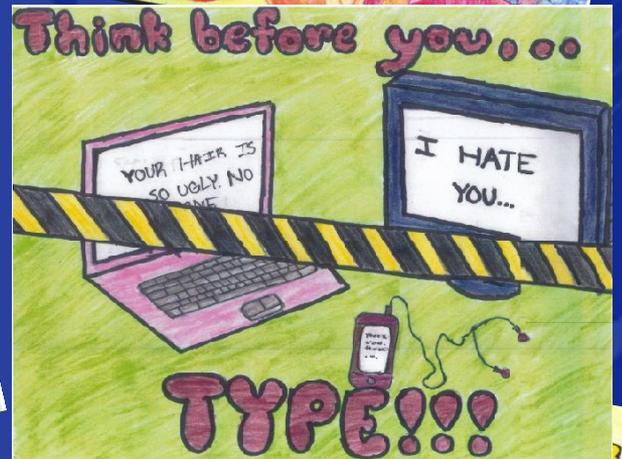
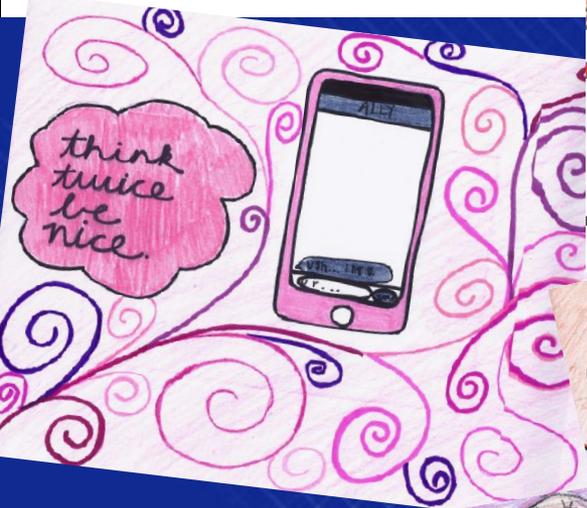
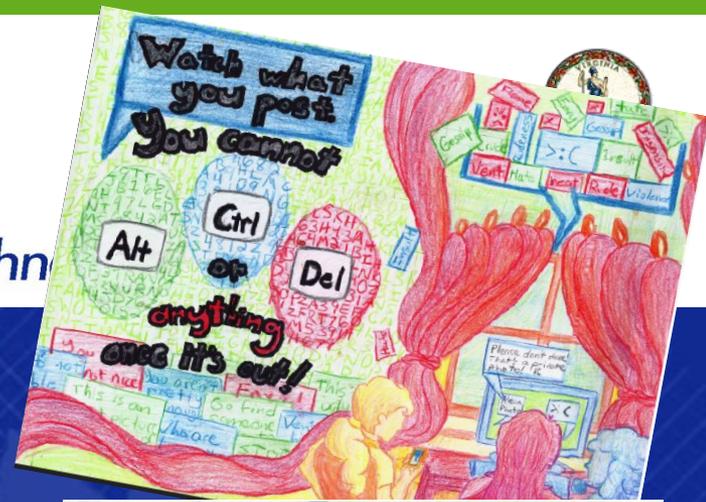
The 2015 Virginia national winners posters can be found on our website
www.vita.virginia.gov/security/default.aspx?id=11232

**more details will be forthcoming.....



VITA

DON'T BULLY ONLINE BE KIND ONLINE





Questions or Assistance with NCSAM

Contact:

CommonwealthSecurity@vita.virginia.gov

Tina.Harris-Cunningham@vita.virginia.gov



Virginia Information Technologies Agency

Upcoming Events





IS Orientation

When: Thursday, September 24, 2015

Time: 1:00 pm to 3:00 pm

Where: CESC , Room 1211

Register here:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>



Announcement: VASCAN Conference 2015



They Will Get In. What Are We Doing About It?

Date: October 1-2, 2015

Location: UVA, Newcomb Hall Ballroom

Topics:

- information security
- advanced defense techniques
- IT risk management
- IT regulatory compliance

Bonus Content:

SANS: *Incident Response Management*
MGT535

Meals

- Breakfast and lunch both days
Conference reception Thursday evening,
October 1

To Register: <http://www.virginia.edu/vascan2015/>



Future ISOAG

October 7, 1:00 - 4:00 pm @ CESC
Speaker: Mike Watson, VITA

ISOAG meets the 1st Wednesday of each month in 2015



ADJOURN

THANK YOU FOR ATTENDING

