STAFF SYMPOSIUM SERIES
INFORMATION TECHNOLOGY TRACK
FACILITATORS

Harold Garcia  System Manager - Atlanta, GA
              Chapter 13 Standing Trustee – Melissa Davey
Debbie Smith  System Manager - Robbinsville, NJ
              Chapter 13 Standing Trustee – Al Russo
Jim Smiley    System Manager – Philadelphia, PA
              Chapter 13 Standing Trustee – William Miller
Tom O’Hern    Program Manager, ICF, Baltimore, MD
              STACS - Standing Trustee Alliance for Computer Security
Staff Symposium IT Track

Material Download Site

https://www.stacs.net/symposium/2018
IT Track Outline

Day 1
- Session 1 (9:00 - 10:30) – NDC & PII Data Management Plans, Practices and Strategies
- Session 2 (10:45 - 12:15) – Cloud Migration

Lunch (12:15-1:30)
- Session 3 (1:30 – 3:00) – Security Standards and Audits
- Session 4 (3:15 – 4:45) – Solving the Tough Problem
- Happy Hour (5-7) – Dempsey’s in the Camden Yards Building (Walk up Eutaw)

DAY 2
- Session 5 (8:30 - 10:00) – System Management and Automation
- Session 6 (10:15 - 11:45) – Programming for the Trustee Office

IT Track
Session 3:
Security Standards & Audits

A guest speaker from ICF’s Computer Network Defense team will discuss current threats and attacks with a special focus on the cloud and the security challenges it presents.

Industry standards and practices used by STACS to help Trustees integrate business practices for IT Governance, Risk management and Compliance will be presented along with several new and existing program features. A grab bag of security topics and questions from the community will also be discussed.
Session Agenda

Security Threat Briefing
   Rianna Bedam – ICF Cyber

Security Standards & Audits

STACS Feedback
ICF Cyber Security Division

Rianna (Bedam) Davis
- 6+ Years Air Force
- Cyber Security, Crypto Key Management, Information Assurance
- NSA Network and Wireless Incident Response
- Instructor-Computer Incident Response at Defense Cyber Investigation Training Academy
- Current Sr. Cyber Project Manager & Network Defense Team Lead

- Lets Connect! https://www.linkedin.com/in/riannadavis
Highlighted Attacks 2017/2018

- Equifax
- Wannacry
- Spectre & Meltdown
- Drupal Exploitation (Current)
What's Changing in the Crimeware?

- Decline in the use of exploit kits and ransomware
- Cryptominer Malware on the rise
- Malspam being used to target systems
- Banking Malware still active
Analyzing the Data

• Encrypted data—grabbing it before it hits the cloud
  ◦ Break and Inspect methodology
  ◦ Dedicated analyst for analysis

• API Logs—understanding buckets, permissions, detecting changes

• Remember: Logs! Logs! Logs!
Security Tools

• AWS
  ◦ Amazon Guard Duty – threat detection
  ◦ Amazon Inspector – security assessment
  ◦ AWS Shield – DDoS Protection

• Azure Security Center
  ◦ Security Event Collection and Search
  ◦ Advance Threat Detection
  ◦ Threat Intelligence
  ◦ Built-in and custom alerts
Cloud Based Attacks

- AWS S3 Security Breaches

- Whose Responsible?
  Hint: not the cloud service provider....
Cloud Based Attacks & Threats

- Scalability
- Other VM’s potential to read host machine data
- Manipulating API calls to allow unauthorized access
- Configuration Vulnerabilities!
Challenges

• Contract Languages

• Cyber Security Service Provider required,
  ◦ sites migrating to cloud without one

• Communication Channels for reporting are defined,
  ◦ not yet properly established
Challenges

• Not all data readily available to monitoring analysts
• Different Cloud Service Provider’s
  ◦ different access/permissions to data
What can be done?
All basic prevention first
   Firewall
      filtering with SSL proxy capability to assess https encrypted connections
      Subscription based Intrusion Prevention Services (IPS) updated with based sites, IPs, and attack and compromised detection signatures
   No general users accounts with Administrator Rights
   Regular patch management of OS and 3rd party software, browsers and browser based plugins, addons and support apps (Adobe, etc.)
   Disabling unused scripting languages and utilities
      Remove Flash and Flash player from systems
      Can be a drastic measure with negative impact if you use centralized admin tool/services
         PowerShell -
            Already restricted to Administrator
         WMI -
   Signing executables
Latest Tech Threats and Trends

- **Continued Loss of Privacy thru technology**
  - Voice to Digital conversions
  - Voice Activated Services (like embedded camera)
    - Cortana, Alexa and Siri – Shut up and stop listening

- **Other Big Vulnerabilities**
  - WPA2 - Wireless network encryption protocol bug
    - KRACK exploit can monitor all wireless communication
    - Vulnerability in the roaming among access point feature
  - All wireless devices and most WiFi routers are affected
    - Get WiFi devices off your LAN – Use a DMZ and Require VPN
    - Check your WiFi device manufacturer for KRACK vulnerability
    - Upgrade & Patch WiFi clients
In the wake of the Cambridge Analytica scandal, news articles and commentators have focused on what Facebook knows about us. A lot, it turns out. It collects data from our posts, our likes, our photos, things we type and delete without posting, and things we do while not on Facebook and even when we're offline. It buys data about us from others. And it can infer even more: our sexual orientation, political beliefs, relationship status, drug use, and other personality traits -- even if we didn't take the personality test that Cambridge Analytica developed.

But for every article about Facebook's creepy stalker behavior, thousands of other companies are breathing a collective sigh of relief that it's Facebook and not them in the spotlight. Because while Facebook is one of the biggest players in this space, there are thousands of other companies that spy on and manipulate us for profit.

Harvard Business School professor Shoshana Zuboff calls it "surveillance capitalism." And as creepy as Facebook is turning out to be, the entire industry is far creepier. It has existed in secret far too long, and it's up to lawmakers to force these companies into the public spotlight, where we can all decide if this is how we want society to operate and -- if not -- what to do about it.

There are 2,500 to 4,000 data brokers in the United States whose
business is buying and selling our personal data. Last year, Equifax was in the news when hackers stole personal information on 150 million people, including Social Security numbers, birth dates, addresses, and driver's license numbers.

You certainly didn't give it permission to collect any of that information. Equifax is one of those thousands of data brokers, most of them you've never heard of, selling your personal information without your knowledge or consent to pretty much anyone who will pay for it.

Surveillance capitalism takes this one step further. Companies like Facebook and Google offer you free services in exchange for your data. Google’s surveillance isn't in the news, but it's startlingly intimate. We never lie to our search engines. Our interests and curiosities, hopes and fears, desires and sexual proclivities, are all collected and saved. Add to that the websites we visit that Google tracks through its advertising network, our Gmail accounts, our movements via Google Maps, and what it can collect from our smartphones.

That phone is probably the most intimate surveillance device ever invented. It tracks our location continuously, so it knows where we live, where we work, and where we spend our time. It's the first and last thing we check in a day, so it knows when we wake up and when we go to sleep. We all have one, so it knows who we sleep with. Uber used just some of that information to detect one-night stands; your smartphone provider and any app you allow to collect location data knows a lot more.

Surveillance capitalism drives much of the internet. It's behind most of the "free" services, and many of the paid ones as well. Its goal is psychological manipulation, in the form of personalized advertising to persuade you to buy something or do something, like vote for a candidate. And while the individualized profile-driven manipulation exposed by Cambridge Analytica feels abhorrent, it's really no different from what every company wants in the end. This is why all your personal information is collected, and this is why it is so valuable. Companies that can understand it can use it against you.

None of this is new. The media has been reporting on surveillance capitalism for years. In 2015, I wrote a book about it. Back in 2010, the Wall Street Journal published an award-winning two-year series about how people are tracked both online and offline, titled "What They Know."

Surveillance capitalism is deeply embedded in our increasingly
computerized society, and if the extent of it came to light there would be broad demands for limits and regulation. But because this industry can largely operate in secret, only occasionally exposed after a data breach or investigative report, we remain mostly ignorant of its reach.

This might change soon. In 2016, the European Union passed the comprehensive General Data Protection Regulation, or GDPR. The details of the law are far too complex to explain here, but some of the things it mandates are that personal data of EU citizens can only be collected and saved for "specific, explicit, and legitimate purposes," and only with explicit consent of the user. Consent can't be buried in the terms and conditions, nor can it be assumed unless the user opts in. This law will take effect in May, and companies worldwide are bracing for its enforcement.

Because pretty much all surveillance capitalism companies collect data on Europeans, this will expose the industry like nothing else. Here's just one example. In preparation for this law, PayPal quietly published a list of over 600 companies it might share your personal data with. What will it be like when every company has to publish this sort of information, and explicitly explain how it's using your personal data? We're about to find out.

In the wake of this scandal, even Mark Zuckerberg said that his industry probably should be regulated, although he's certainly not wishing for the sorts of comprehensive regulation the GDPR is bringing to Europe.

He's right. Surveillance capitalism has operated without constraints for far too long. And advances in both big data analysis and artificial intelligence will make tomorrow's applications far creepier than today's. Regulation is the only answer.

The first step to any regulation is transparency. Who has our data? Is it accurate? What are they doing with it? Who are they selling it to? How are they securing it? Can we delete it? I don't see any hope of Congress passing a GDPR-like data protection law anytime soon, but it's not too far-fetched to demand laws requiring these companies to be more transparent in what they're doing.

One of the responses to the Cambridge Analytica scandal is that people are deleting their Facebook accounts. It's hard to do right, and doesn't do anything about the data that Facebook collects about people who don't use Facebook. But it's a start. The market can put pressure on these companies to reduce their spying on us, but it can only do that if we
force the industry out of its secret shadows.
Latest Tech Threats and Trends

- Artificial Intelligence (AI) and Big Data Analytics
  - AI needs lots of data and the Internet provides it
  - Facebook – We weren’t focused on the malicious uses!
- Data Analytics for Malicious Purposes
  - Simplistic Smart Home example
    - Sensors detect movement patterns in house
    - Learn daily schedule and adjust temp for time of day
    - Learned schedule reveals when your home is unoccupied
  - Misguided AI intended for enhanced online experience
    - AI shaping access based on preferences
    - Reduces access to alternatives
    - Opinion Shaping for political outcome
Latest Tech Threats and Trends

Screen scrapping for data
- Exploiting authorized or unauthenticated access to data
- Aggregating data by 3rd parties
- Data analytics to produce Data Intelligence Products

Issues
- Free or cheap access to data
- Loss of data ownership and custody
- No extension of security protection requirements
- No ability to assure continues security of data
Latest Tech Threats and Trends

Screen scrapping defense
- Must monitor and report on access activity
- ** Assure authorized access is limited to min. required data
  - Attorney of record, party in interest
- Limit page results
- Use of Captcha to assure human access
  - Especially with Case# + Last4SSN authentication

- Good User Agreements provide firm legal position
System Management

Comingling Accounts
New technology is enabling, and in some case requiring, Trustee’s computing capabilities to creep into the cloud. Computing services traditionally run on servers in the office computer room are now wholly or partially operating in the cloud. We are finding Trustees and IT managers lack awareness and understanding of operational dependencies and security impacts of these cloud services.

Cloud based technologies often require the creation of numerous external accounts, one for each cloud service(s). Examples include your Apple ID, Microsoft.net, Office365 or Google gmail accounts. These accounts often create an intermingling of personal and work accounts. The unintended impact is a dependencies of the Trustee computing capability on staff and IT manager personal accounts. The departure of a critical staff member can have significant operational impact if you can’t get or reset the Apple ID or gmail account your service is dependent on.

Therefore, it is critical for Trustees to understand, document and establish ground rules for the use of external cloud based services. Some basic ground rules should include:

1. No personal accounts used for any Trustee computing services, cloud or internal.
2. When an account is needed
   a. List the Trustee as the account owner and in the service contact information
   b. Use an email list such as administrators@myCH13trustee.com for password resets, billing, license renewals, and expiration notices and reports. Add IT manger, support staff, Trustee, comptrollers, office managers as needed.
   c. Logging and alerting features that generate voluminous alerts or reports should go to
a secondary email list such as admin_alerts@myCH13trustee.com. Add IT manager and support staff as needed.

3. Configuration, administration and support account names and passwords for all cloud and vendor services should be stored in a master password list or password manager software with enough information to determine where and how to use the account credentials. Accounts can be accessed through a website or require the use of software installed on a specific computer in the office.

4. A common list of cloud and external account dependencies often overlooked include:
   a. Hosted email services like Office 365, hosted Exchange or gmail,
   b. Phone, voice mail, and conferencing systems and services
   c. Remove Video surveillance services
   d. Hosted backup solutions
   e. Hosted Trustee Website
   f. Remote Monitoring and Management support services by external IT support vendors
   g. Cloud based password manager services
   h. Internet service (IP addresses) and Trustee domain name registration (myCH13Trustee.com) providers
   i. Antivirus, Firewall, and VPN vendor support site
   j. Hardware, Software, and Equipment procurement vendors with licenses, renewal, warranty and maintenance services
Cloud based technologies often require the creation of numerous external accounts, one for each cloud service(s). Examples include your Apple ID, Microsoft.net, Office365 or Google gmail accounts. These accounts often create an intermingling of personal and work accounts. The unintended impact is a dependencies of the Trustee computing capability on staff and IT manager personal accounts. The departure of a critical staff member can have significant operational impact if you can’t get or reset the Apple ID or gmail account your service is dependent on.

Therefore, it is critical for Trustees to understand, document and establish ground rules for the use of external cloud based services. Some basic ground rules should include:

1. No personal accounts used for any Trustee computing services, cloud or internal.
2. When an account is needed
   a. List the Trustee as the account owner and in the service contact information
   b. Use an email list such as administrators@myCH13trustee.com for password resets, billing, license renewals, and expiration notices and reports. Add IT manager, support staff, Trustee, comptrollers, office managers as needed.
   c. Logging and alerting features that generate voluminous alerts or reports should go to a secondary email list such as admin_alerts@myCH13trustee.com. Add IT manager and support staff as needed.
3. Configuration, administration and support account names and passwords for all cloud and vendor services should be stored in a master password list or password manager software with enough information to determine where and how to use the account.
credentials. Accounts can be accessed through a website or require the use of software installed on a specific computer in the office.

4. A common list of cloud and external account dependencies often overlooked include:
   a. Hosted email services like Office 365, hosted Exchange or gmail,
   b. Phone, voice mail, and conferencing systems and services
   c. Remove Video surveillance services
   d. Hosted backup solutions
   e. Hosted Trustee Website
   f. Remote Monitoring and Management support services by external IT support vendors
   g. Cloud based password manager services
   h. Internet service (IP addresses) and Trustee domain name registration (myCH13Trustee.com) providers
   i. Antivirus, Firewall, and VPN vendor support site
   j. Hardware, Software, and Equipment procurement vendors with licenses, renewal, warranty and maintenance services
4. A common list of cloud and external account dependencies often overlooked include:
   a. Hosted email services like Office 365, hosted Exchange or gmail,
   b. Phone, voice mail, and conferencing systems and services
   c. Remove Video surveillance services
   d. Hosted backup solutions
   e. Hosted Trustee Website
   f. Remote Monitoring and Management support services by external IT support vendors
   g. Cloud based password manager services
   h. Internet service (IP addresses) and Trustee domain name registration (myCH13Trustee.com) providers
   i. Antivirus, Firewall, and VPN vendor support site
   j. Hardware, Software, and Equipment procurement vendors with licenses, renewal, warranty and maintenance services
4. A common list of cloud and external account dependencies often overlooked include:
   a. Hosted email services like Office 365, hosted Exchange or gmail,
   b. Phone, voice mail, and conferencing systems and services
   c. Remove Video surveillance services
   d. Hosted backup solutions
   e. Hosted Trustee Website
   f. Remote Monitoring and Management support services by external IT support vendors
   g. Cloud based password manager services
   h. Internet service (IP addresses) and Trustee domain name registration (myCH13Trustee.com) providers
   i. Antivirus, Firewall, and VPN vendor support site
   j. Hardware, Software, and Equipment procurement vendors with licenses, renewal, warranty and maintenance services
4. A common list of cloud and external account dependencies often overlooked include:
   a. Hosted email services like Office 365, hosted Exchange or gmail,
   b. Phone, voice mail, and conferencing systems and services
   c. Remove Video surveillance services
   d. Hosted backup solutions
   e. Hosted Trustee Website
   f. Remote Monitoring and Management support services by external IT support vendors
   g. Cloud based password manager services
   h. Internet service (IP addresses) and Trustee domain name registration (myCH13Trustee.com) providers
   i. Antivirus, Firewall, and VPN vendor support site
   j. Hardware, Software, and Equipment procurement vendors with licenses, renewal, warranty and maintenance services
Therefore, it is critical for Trustees to understand, document and establish ground rules for the use of external cloud based services. Some basic ground rules should include:

1. No personal accounts used for any Trustee computing services, cloud or internal.

2. When an account is needed
   a. List the Trustee as the account owner and in the service contact information
   b. Use an email list such as administrators@myCH13trustee.com for password resets, billing, license renewals, and expiration notices and reports. Add IT manger, support staff, Trustee, comptrollers, office managers as needed.
   c. Logging and alerting features that generate voluminous alerts or reports should go to a secondary email list such as admin_alerts@myCH13trustee.com. Add IT manger and support staff as needed.

3. Configuration, administration and support account names and passwords for all cloud and vendor services should be stored in a master password list or password manager software with enough information to determine where and how to use the account credentials. Accounts can be accessed through a website or require the use of software installed on a specific computer in the office.
Therefore, it is critical for Trustees to understand, document and establish ground rules for the use of external cloud based services. Some basic ground rules should include:

1. No personal accounts used for any Trustee computing services, cloud or internal.
2. When an account is needed
   a. List the Trustee as the account owner and in the service contact information
   b. Use an email list such as administrators@myCH13trustee.com for password resets, billing, license renewals, and expiration notices and reports. Add IT manger, support staff, Trustee, comptrollers, office managers as needed.
   c. Logging and alerting features that generate voluminous alerts or reports should go to a secondary email list such as admin_alerts@myCH13trustee.com. Add IT manger and support staff as needed.
3. Configuration, administration and support account names and passwords for all cloud and vendor services should be stored in a master password list or password manager software with enough information to determine where and how to use the account credentials. Accounts can be accessed through a website or require the use of software installed on a specific computer in the office.
Therefore, it is critical for Trustees to understand, document and establish ground rules for the use of external cloud based services. Some basic ground rules should include:

1. No personal accounts used for any Trustee computing services, cloud or internal.
2. When an account is needed
   a. List the Trustee as the account owner and in the service contact information
   b. Use an email list such as administrators@myCH13trustee.com for password resets, billing, license renewals, and expiration notices and reports. Add IT manger, support staff, Trustee, comptrollers, office managers as needed.
   c. Logging and alerting features that generate voluminous alerts or reports should go to a secondary email list such as admin_alerts@myCH13trustee.com. Add IT manger and support staff as needed.
3. Configuration, administration and support account names and passwords for all cloud and vendor services should be stored in a master password list or password manager software with enough information to determine where and how to use the account credentials. Accounts can be accessed through a website or require the use of software installed on a specific computer in the office.
Setup Accountability to Protect Yourself

- Maintain Separation of Duties
  - Sole responsibility = Sole accountability

- Assign backup staff to perform and back check critical tasks

Can you go on vacation for a week and all your regular operational tasks get done?
Incidents and Data Breaches
Response, Recovery, and Prevention Pitfalls
The Incident Response processes focus on clarifying incident details, containing the activity, reestablishing control over the computing environment and recovering normal business operations. These processes can progress in parallel, but have interdependencies and pitfalls if certain tasks are not performed or performed out of sequence. Therefore Clients and their IT staff are encouraged to immediately engage ICF-Cyber to leverage our experience, guidance and support.
DETECT: Incident response begins with the detection of activity that raises suspicion or concern. Incident activity is often assumed to be detected by security systems or software, but experience shows incident activities are more frequently detected when people see and report unusual events or problems. It is important to have annual security awareness training for your staff so they are aware of new and current trends signs and indicators of computer incident activity.

TRIAGE: Containment, isolation and preservation of critical data and information are the priority. Critical tasks include preserving backups to prevent overwriting with compromised data and outlining response and recovery game plans. The triage investigation attempts determine if the detected activity is an actual security incident and results in one of three outcomes:
• OK - no security incident but some corrective action may be needed to prevent further issues.
• Limited - incident such as a virus or automated malware infection contained quickly, had manageable (although inconvenient) impact on operations, and low probability of access or theft of sensitive data
• Compromise – confirmed or apparent; requiring additional forensics to determine the extent of access, damage and impact.
Additional information can be revealed during the response or recovery phases to escalate the initial outcome to an incident or compromise.

REPORT: We advise Clients to report limited and compromise incidents to their Governance
Body. Best practice is to initially report an incident then follow up to avoid any delay especially if a limited incident turns into a compromise. Similarly, cyber liability polices require timely reporting of covered incidents to assure adequate incident response. Failure to timely report can result in a denied claim.
Pit Falls – Incident Response & Recovery

- Not reporting potential incident right away or at all
- Not being prepared to respond immediately
- Leaving an infected computer attached to the network
- Assuming the antivirus caught it all and removed it
- Not having expertise to determine extent of an incident
- Trusting your IT staff/provider who said its OK
- Moving to recovery before incident is fully understood
- Trying to clean an infected computer
- Not changing passwords used from infected systems
- Not testing your backups for a catastrophic recovery
- Not having cyber liability insurance
The notification process starts with confirmation of a data breach. Unfortunately, it is rare to find a digital smoking gun to definitively prove and quantify what specific data was accessed or taken. Before making a notification decision, an assessment of supporting facts and circumstantial evidence must be considered to determine the likelihood and impact of a breach.

**CYBER LIABILITY INSURER**

The second notification option is to engage the data breach services provided under your cyber liability insurance coverage.

With any potential data breach incident, it is a good practice to engage your insurer to meet your coverage’s incident notification requirement, even if you decide not to make a claim.
Without Cyber Liability Insurance, Client will need to complete and perform the Breach Tasks
The Major Pitfalls – Breach Notification

- Not having cyber liability coverage
- Trying to go it alone – Forensics, Recovery, Scope and Impact analysis
- Not reporting timely to governance body, Insurer, State AG
- Not having a perpetual data reduction process
- Not knowing it’s the state of residency of the data owner that matters
Governance, Risk Management & Compliance (GRC)
GRC – In lay terms

- Governance
  - The external laws, rules, and regulations my business and I are required to comply with and the internal policies and procedures I established to support these requirements.

- Risk Management
  - A life cycle process by which I identify my risks, plan and implement controls to cost effectively minimize risk to a reasonable level.

- Compliance
  - How I measure or audit my adherence to Governance
CH13 Governance

• International Standards & Regulations
  ◦ EU GDPR — General Data Protection Regulation
  ◦ ISO — International Standards Organization

• National/Federal/Defense
  ◦ US Code and Legal Decisions
  ◦ Critical Infrastructure
  ◦ NIST — National Institute of Standards and Technology
  ◦ Risk Management Framework (RMF)

• State Laws — privacy and data

• Industry Regulation
  ◦ GLB, HIPAA, PCI

• Trustee Specific
  ◦ DOJ Standing Trustee Handbook
  ◦ Trustee’s policy
CH13 Risk Management

01 Categorize System
02 Collect Security Controls
03 Implement Security Controls
04 Assess Security Controls
05 Authorize System
06 Monitor Security Controls

RMF Compliance Life Cycle

STACS program built around helping Trustees implement this process
CH13 Compliance

- Auditing to assure compliance to a standard
GRC - What it all boils down to...

Having a defensible position if something happens!

- Use a reasonable level of standards and practices
- Show continuously improvement over time (CMM)
- Show a reasonable level of due diligence
STACS

As a Governance, Risk Management and Compliance Support Program
STACS: Services and Features

How to leverage STACS for specific issues?

- Proactive auditing
  - Perimeter protection (Remote scanning)
  - War dialing (Phones)
- Onsite Assessments
  - Behind the firewall scanning
  - Operational observation of practice and procedure (no technology)
  - Physical Security
- Remediation guidance
- Incident Response
- General Security guidance
- Training
  - Online – Video library and Courseware User and Admin tracks
  - Onsite – Conferences, IT Manager Track Symposium
STACS: Feedback for the Future

- Help us help you better?
  - Do you have feedback, thoughts or ideas for us?
  - Krispen Carrol, STACS Committee or Tom

- Summer is our planning and prep time for next year
- Renegotiating agreements with our support partners

- Changing tech horizon = Changing Risk Management Strategies
  - Cloud migration and services

- Remediation Concerns
  - Timeliness or no remediation of issues
  - Speed from vulnerability to exploit
STACS: Planning for the Future

New STACS Website
  ◦ Added Phishing Tool
  ◦ Revamping our onsite assessment this summer
  ◦ Content Management System to better organize our online content

Continuous monitoring Concept
  • Why? Time to exploit from vulnerability < 30 days
    ◦ (Example: last years incident from Qualys)
  • More regular assessment behind the firewall
  • Scanning appliances, agent/cloud based

* STACS Remediation Support
  • Traditionally Auditor and Operator rolls are separated