SEC530

Presentation based on SEC530: Defensible Security Architecture and Engineering

SANS

Defensible Security Architecture and Engineering – **Part 1**: How to become an All-Round Defender - the Secret Sauce

About Us

Justin Henderson

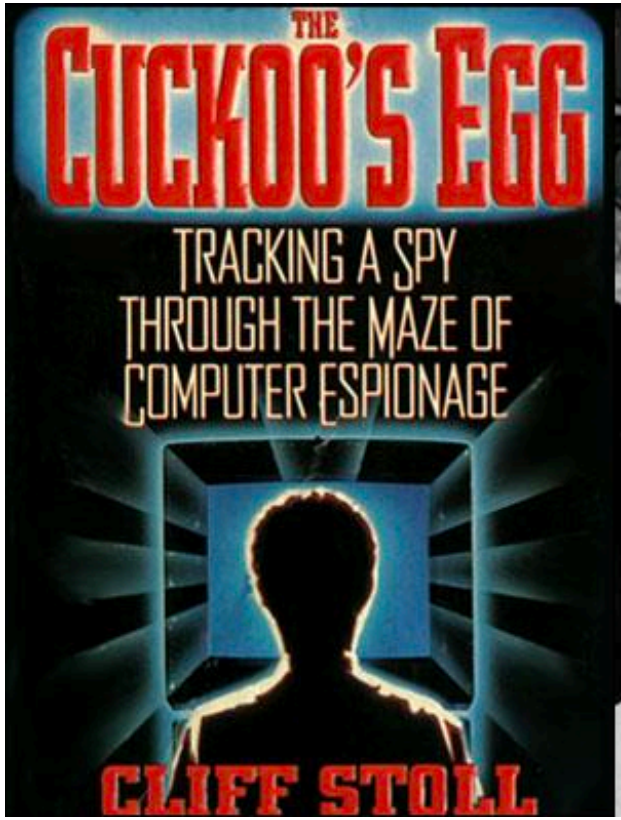
- SEC555 Author / SEC455 and SEC530 Co-Author
- GSE #108 / Cyber Guardian Blue + Red / 60 certs
- Owner of H & A Security Solutions
- **Twitter**: @SecurityMapper

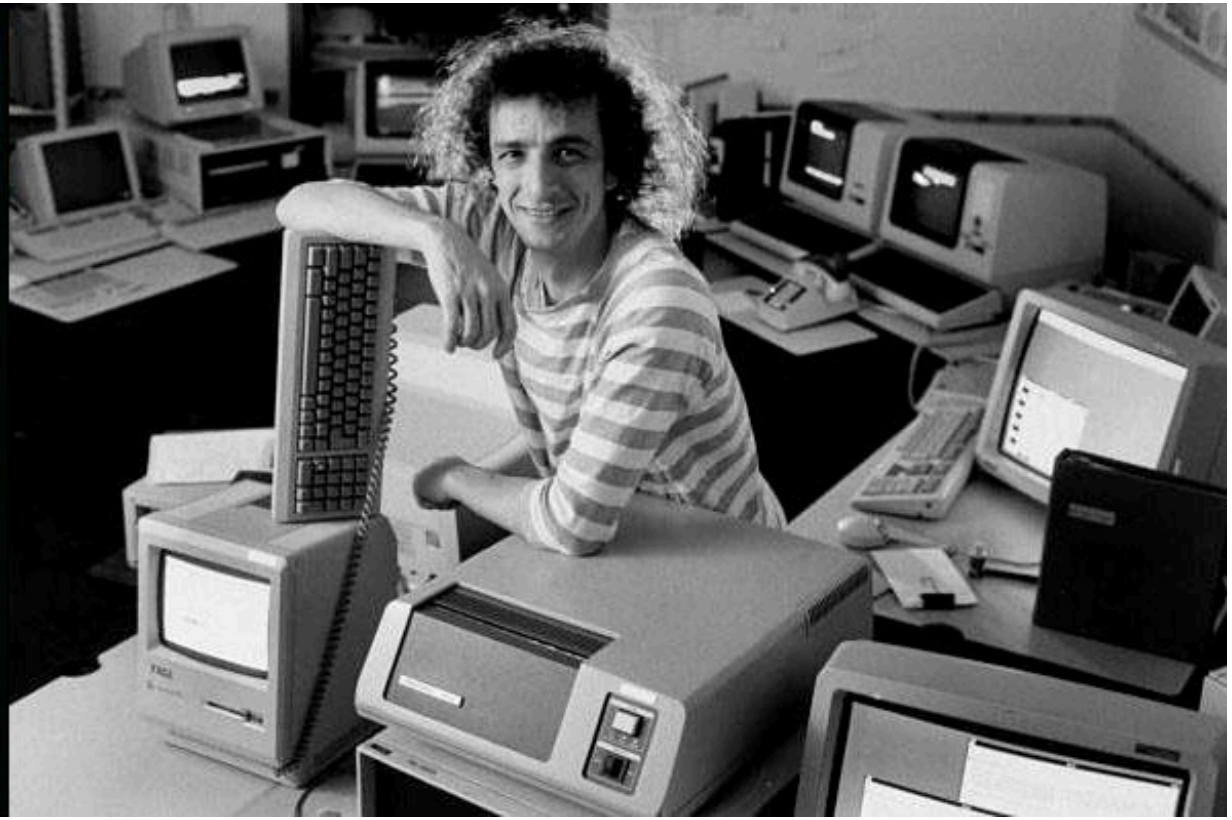
Ismael Valenzuela - イスマエル・バレンズエラ

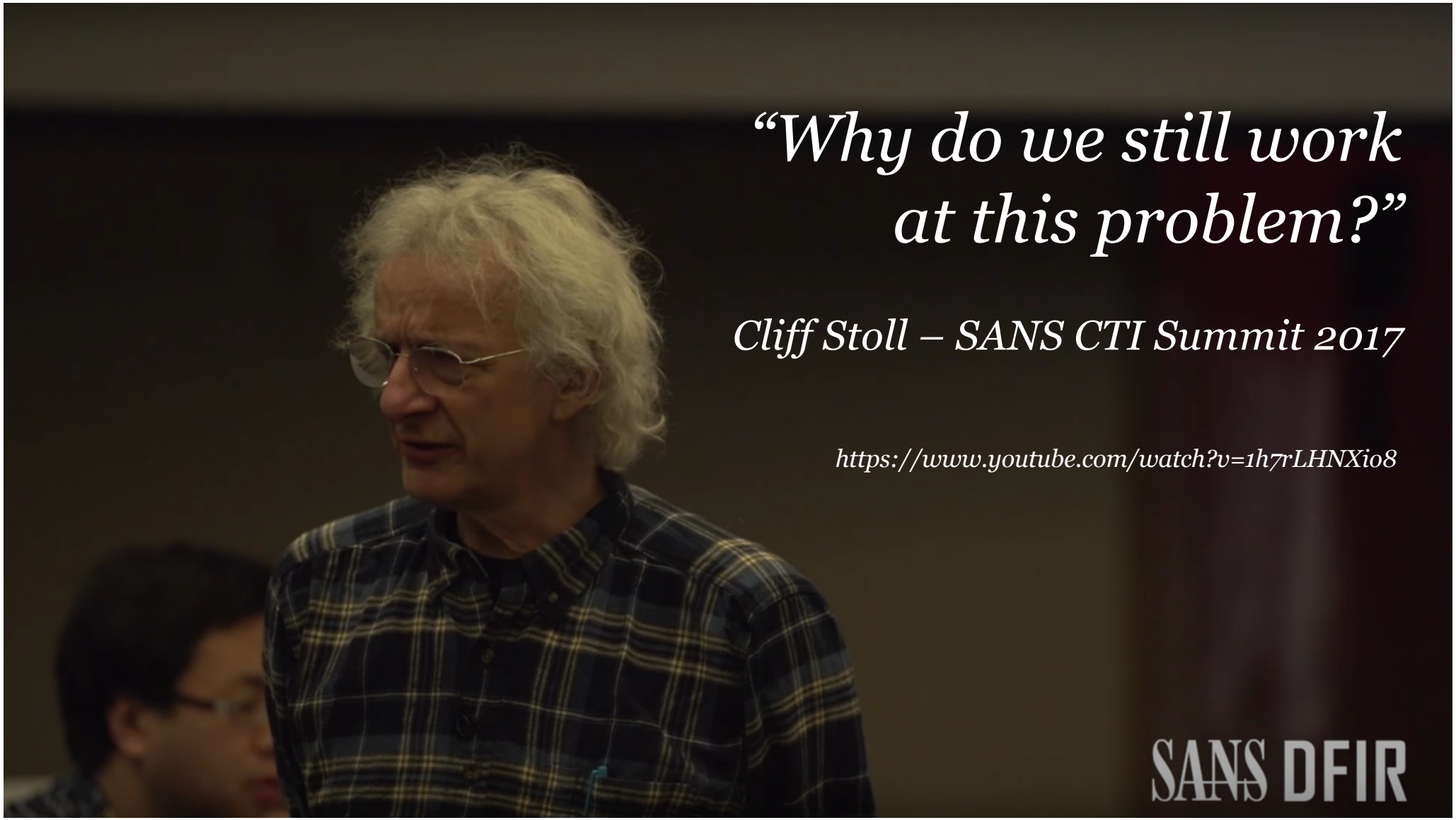
- SEC530 Co-author / SEC503 and SEC511 Instructor
- GSE # 132 and also a certification master
- Sr. Principal Engineer at McAfee
- **Twitter**: @aboutsecurity

Where were you in 1986?

Cliff Stoll - 1986






“Why do we still work at this problem?”
Cliff Stoll – SANS CTI Summit 2017
https://www.youtube.com/watch?v=1h7rLHNXio8
SANS DFIR

All Round Defender

Being an **all round defender** means you are the person responsible for:

- **Network Security**
  - Routers / Switches / Software defined networking
  - Flow data
  - Firewalls / IDS and IPS / Sandboxing
- **Cloud Security**
  - Hypervisors and central management
  - **I**nfrastructure/**P**latform/**S**oftware/**F**unction (**a**s-**a**-**S**ervice)
- **Endpoint Security**
  - Antivirus / Whitelisting / HIPS / EDR / Patching / Hardening / Logging / dare I go on?

Plus all the things that cross boundaries like data governance and identify management

Security Focus

So basically… find a control and make it work

- Having an idea of how to focus security application helps

Perimeter focus - Control data going into and out of the network

- Perimeter is not dead, but it is everywhere

Datacentric focus - Find important data and protect it

- Requires knowing what, where, when, why and then applying controls

Zero Trust focus - Trust nothing, verify everything

- Goal is to verify and authenticate all access

Case Study: NotPetya

- NotPetya is part of a family of malware based on the leaked (alleged) NSA hacking tools, including ETERNALBLUE
  - This exploit targeted Windows Server Message Block (SMB, TCP port 445) and was patched by MS17-010[1]
- This malware would typically enter an environment via SMB
  - It would then use Mimikatz to attempt to steal credentials and move laterally through a network via Microsoft PSExec and WMIC (Windows Management Instrumentation Console
  - Automated malware is now behaving like human penetration testers
- If an organization had one unpatched system and 999 patched: all 1,000 could become compromised
  - This is dependent on internet network segmentation, trust models, etc.

MITRE ATT&CK Matrix

- Provides a common language to describe adversarial tactics and techniques
- Applicable to real environments, allow mapping the attacker's behaviors to defenses
- Go-to model to plan & verify purple teaming exercises

ATT&CK™

https://attack.mitre.org/

Architecting for Network Visibility & Detection: NSM

Alert Driven Workflows vs. Data Driven Workflows

- Most security operations teams live in an alert driven world
- Alerts provide only the **initial** point for an investigation, but often additional context is needed to determine what to do next
- NSM provides additional data needed to "pull a thread" (go, hunt, explore) vs reactively waiting for an alert

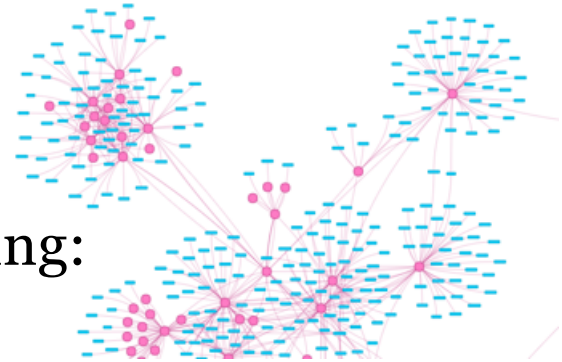
Behavioral Based NSM with Zeek IDS

Zeek[1] (Bro - 1995) enhances network visibility beyond traditional signature-based detection through protocol decoding.

- IDS++: a **Network Programming Language**
- Provides full context of all activity related to network events:
  - What domains a host queries
  - What SSL certificates are used
  - What files are downloaded
  - Any FTP/SMTP/IRC/SQL activity, etc
  - What User Agents are used

Provides a flexible framework that facilitates customized, in-depth monitoring beyond traditional IDS

Power of Network Metadata



IDS signatures look for known bad

- Network metadata is simply data

Allows for learning the environment and identifying:

- **Abnormal events**
  - Unusual/newly observed/random domains or user-agents
- **Unauthorized assets**
  - Computer DHCP but not in Active Directory or asset system
- **Vulnerable or misconfigured assets**
  - Old operating systems or applications on the network

Zeek Use Cases: Spotting the C2

- 'Pulling a thread' with X.509 certificates and DNS logs
- Samples available at
  - https://github.com/aboutsecurity/Bro-samples

```
$ cat ssl.log | bro-cut server_name, subject, issuer_subject

www.seu4oxkf6.com CN=www.tl6ou6ap7fjroh2o.net CN=www.tbajutyf.com
www.fjpv.com CN=www.vklxa6kz.net CN=www.ohqnkijzzo5vt.com
www.pdpqsu.com CN=www.5rthkzelyecfpir56.net CN=www.qbboo7mcwzv7.com
www.vkojgy6imcvg.com CN=www.dctpbbpif6zy54mspih.net CN=www.m6hoayo5cga.com
www.dbyryztrr7sui3rskjvikes.com CN=www.getvdkk6ibned7k3krkc.net CN=www.7pz4gaio6
www.xqwf7xs6nycmciil3t5e4fy5v.com CN=www.hstk2emyai4yqa5.net CN=www.wc62pgaaorhc
www.rix56ao4hxldum4zbyim.com CN=www.icab4ctxldy.net CN=www.wmylm3gln.com
www.uabjbwhkanlomodm5xst.com CN=www.bnbhckfytu.net CN=www.w4rlc25peis46haafa.com
www.dl2eypxu3.com CN=www.e6nbbzucq2zrhzqzf.net CN=www.cbj5ajz4qgeieshx32n.com
www.ebd7caljnsax.com CN=www.cvapjjtbfd6yohbarw5q.net CN=www.brbqn4rqhscp4rdq.com
```

```
$ cat dns.log | bro-cut query | sort -u

a37fwf32k17gsgylqb58oylzgvlsi35b58m19bt.com
a47d20ayd10nvkshqn50lrltgqcxb68n20gup62.com
a47dxn60c59pziulsozaxm59dqj26dynvfsnw.com
a67gwktaykulxczeueqf52mvcue61e11jrc59.com
axgql48mql28h34k67fvnylwo51csetj16gzcx.ru
ayp52m49msmwmthxoslwpxg43evg63esmreq.info
azg63j36dyhro61p32brgyo21k37fqh14d10k37fx.com
cvlslworouardudtcxato51hscupunua57.org
cyh44jud50g33iuarlzgqbup22fqisixf62kr.org
d10h34othyp62b18lyfwnzazj26p42fud50gzc49.biz
d20iwe51ftitg53lvl18a27hvlqjyjtd20gue61.com
dqhzhtbto21h14lvp12iqhtlrnxasarcte61.biz
drp42i25ati55m69pvgza57nyh34hwk57i55m19n60.ru
iqcqmrn30iuoubuo11crfydvkylrbtmtev.info
iqo11c69mud20krk57j16fqnrfwgva67oraql48.com
isjqn30a27hwgqbxnxksi65hrnsgyc49mylt.biz
iupqhxfwpylxm29jsexovj16cqfybwb68aw.org
iwpslvesj26i65oynxhtoyc39o41asdvnqc59.com
j36lxf52hsj56itc49lqayoveymwfzosi15jw.org
```

Architecting to Protect the Crown Jewels: Data-Centric Security

Identify and Prioritize Critical Assets

- The answer to: "*what are you trying to protect?*" can't be *everything*
- A security architect needs to understand the mission(s) of the organization and work with business owners to identify the associated critical assets needed to support them
- Create a list of defensible assets and classify them from most critical to least critical
  - If your organization has a BCP, start there
- Consider different network zones and user tiers
- Align different security levels to zones & tiers

Know Thy Organization

A defensible architecture requires organizational awareness

- What are critical assets?
- Where are the critical assets?
- Why are they considered critical assets?
- What do these assets need to function?

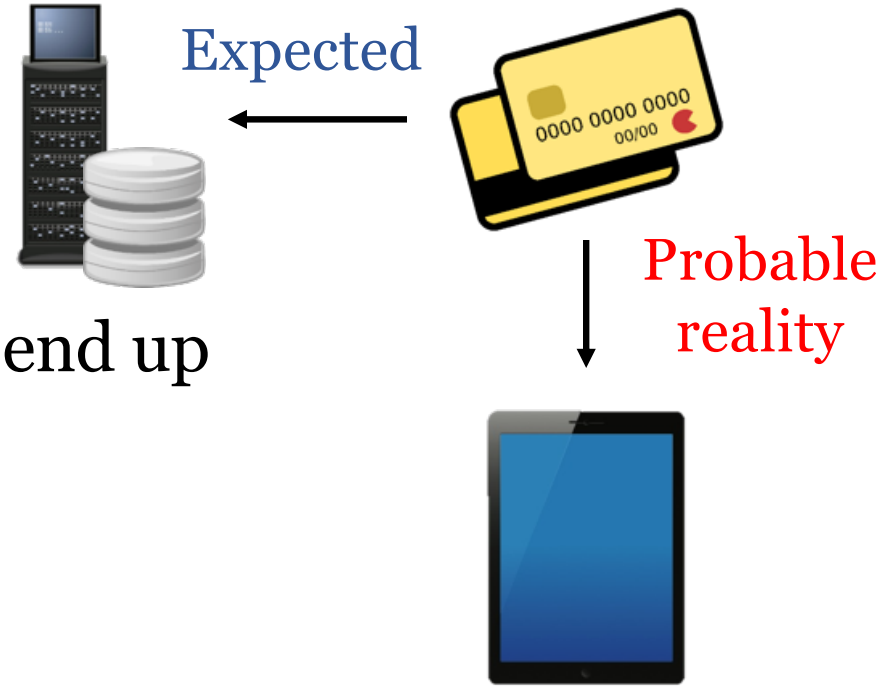
Knowing the above questions allows defenses to be built

- **Network-centric** defenses build a security moat
- **Data-centric** defenses secure the treasure in the castle

Acceptance

First task is to identify key data and where it is expected

- File servers
- Database servers
- USB drives



Next, is to realize where it may end up

- Laptops
- Mobile phones
- Personal USB devices

File Classification

To control and audit sensitive files requires classification

`D:\pci_share\530_backup.xlsx` <- Contains PCI

Maybe files in **pci_share** are expected to have PCI data

- File server is properly segmented and intended for PCI
- Yet user with read access can copy it to local box

Assume you saw a file called **530_backup.xlsx** on a desktop

- Would you assume it had credit card data?
- File classification adds tags to identify and control files

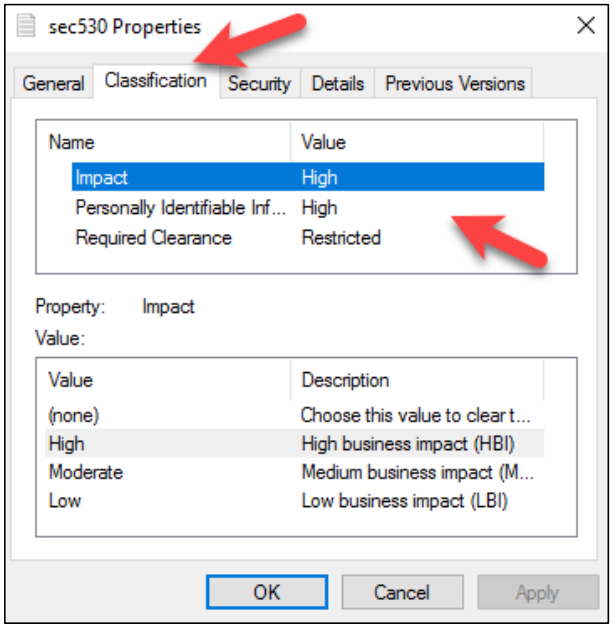
Windows File Classification Infrastructure (FCI)

Server 2008 R2 and later supports file classification

- Requires File Server Resource Manager (FSRM) role

Allows assigning properties to files

- Properties can be anything
  - Clearance required
  - Level of PII
  - Whether something is PCI or EPHI
  - Date something occurred
  - Impact of disclosure



File Properties

2008 R2 only supports local file properties

- After 2008 R2 properties can be local or in AD

Properties added in Active Directory Administrative Center

- Dynamic Access Control -> Resource Properties
- Includes many file properties that can be enabled

PowerShell can export and import properties and settings

Display name	ID	Referenced	Value Type
Discoverability	Discoverability_MS	No	Single-valued...
Folder Usage	FolderUsage_MS	No	Multi-valued C...
Immutable	Immutable_MS	No	Yes/No
Impact	Impact_MS	No	Ordered List
Intellectual Property	IntellectualProperty_MS	No	Single-valued...
Personal Use	PersonalUse_MS	No	Yes/No
Personally Identifiable Info...	PII_MS	No	Ordered List

Alternate Data Streams (ADS)

File classifications are stored in alternate data streams

- Feature of NTFS that allows data to be attached to existing data

```
C:\>streams64.exe C:\test\sec530.txt

C:\test\sec530.txt

   :FSRM{ef88c031-5950-4164-ab92-eec5f16005a5}:$DATA 234

PS C:\> get-content -path C:\test\sec530.txt -Stream
"FSRM{ef88c031-5950-4164-ab92-eec5f16005a5}"

îC8àBŠ>«N±a$íh,Î%!Ò|n|Ì‰Óê   8          h*Á‘ny<Ô¬È5Û mB…üyËxN²
@  .   $   I m p a c t  M S   3 0 0 0       @  (   P I I _ M S   5 0 0
0       @  D   :   R e q u i r e d C l e a r a n c e _ M S   3 0 0 0
```

Automatic Classification Rules

Multiple methods to set properties on files

- **Manual** - User sets properties on one or more files at a time
- **Location-based** - Automatically sets properties if file exists in a folder (Folder classifier)
- **Content-based** - Automatically set properties based on content or regex pattern within file (Content classifier)

Automatic classification can run in continuous mode or on schedule

- Continuous mode is not real-time but fairly quick

Regex and basic pattern matching is used to set classification rules

Azure Information Protection[1]

Microsoft file classification is integrated into multiple cloud products

- Office 365 and SharePoint Online support FCI

Microsoft is pushing Azure Information Protection (AIP)

- Similar to AD Rights Management Services (RMS) (on premise)
- Neither Azure Information Protection or AD RMS are free
  - But Azure Information Protection may be part of your subscriptions

Information Protection classifies data similar to FCI

- But properties and content are handled completely different

Classification Is Not Protection

Classification does not equal protection

- Each serves different purposes

Classification - Labels a file to help set limits on use

- Similar to a file system Access Control List (ACL)
- Physical access to disk makes ACL and classification pointless

Protection - Uses encryption to protect data and classifications

- May be overkill for all files and can break software
- But highly recommended for key files

Trust No One: Zero Trust Security

Zero Trust Mandates

1. All traffic must be secured
   - Traffic must be authenticated
   - Traffic must be encrypted
2. Least privilege must be enforced
   - Trust must be factored into least privilege
   - Trust is no longer binary (yes or no)
3. All data flows must be known and controlled
4. All assets must be scanned, hardened, and rotated

Trust Nothing
Verify Everything

Variable Trust

Access controlled by **variable trust**

- Similar to real-life credit scores

User authentication with username/password	10 points
Device authentication	10 points
Known device and location	10 points
Access to PCI database requires	**40 points**
Multifactor authentication with smart card	20 points
Access to PCI database	**GRANTED**

Electric Fence

Mick Douglas refers to dynamic access as an electric fence

- Behave as normal, and you have full access
- Touch the fence, and a digital shock occurs

Electric shock results in an **automated digital response**

- Quality controls (QoS) slows access
- ACLs remove access
- PCAP recording kicks in
- User is notified of digital shock

Solid Detection Required

Scripting or commercial solutions update the control plane

- But dynamic access necessitates custom trust levels
- Cannot be done without low false positive detection

Level of detection maturity and capabilities required

- Integration between disparate solutions necessary

Examples:

- NSM + Sandbox + Flow Data + NGFW + Scripts
- Security Incident Event Management (SIEM) + NAC

Dynamic Authorization

Abnormal conditions should be monitored and reacted to

- **Temporal** - Access outside normal user window
- **Geographical** - Access from different location
- **Behavioral** - Access to resource user does not normally use
- **Frequency** - Last access or volume of device/user use
  - Or number of requests over time

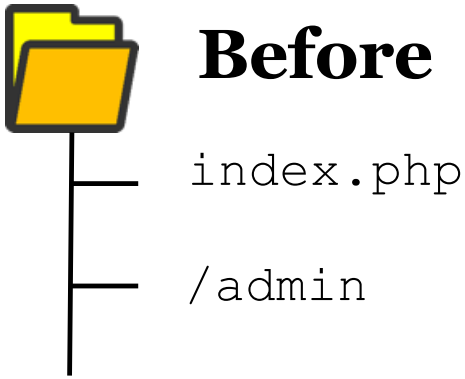
Deviation from norm may dictate additional checks

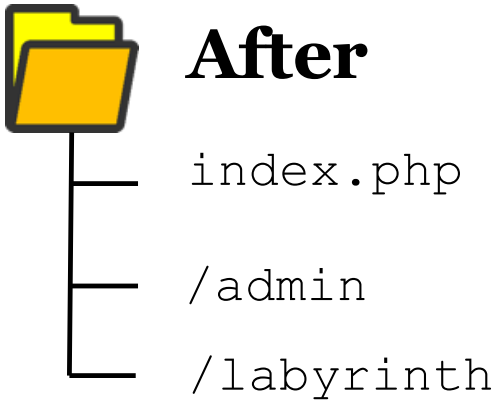
- Multifactor authentication
- Approval from manager or administrator

Dynamic Response: Content Routing

WAF can dynamically route traffic among web servers

- Capability intended for performance and load balancing
- Can be used to add content to existing servers virtually





WAF is also capable of modifying requests/responses on-the-fly

WebLabyrinth[1]

WebLabyrinth is a PHP application that infinitely creates web pages

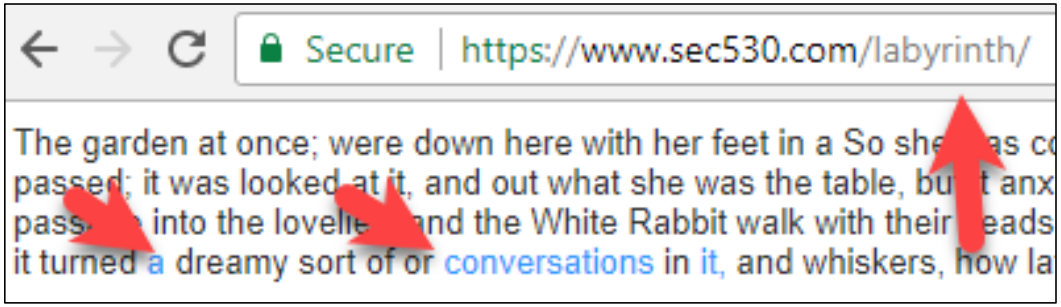
- Design is to confuse or break automated scanners
- Supports automated alerting

Normally would require set up on each server and require PHP

- WAF can integrate WebLabyrinth into every web server

Works best with **robots.txt**

```
User-agent: *
Disallow: /labyrinth
```



All Round Defender Part I Review

So as an all round defender you need to:

- Acknowledge that you are responsible for way too much
  - Learn to love it, defense is awesome!
- Identify how you can combine **network**, **endpoint**, **cloud**, and all other security controls
  - Layering strengths and weaknesses together for defense-in-depth
- Come up with creative, outside the box solutions

Parts 1, 2 and 3!

Recorded webinars available here:

https://www.linkedin.com/pulse/do-you-want-learn-how-blue-team-start-time-based-ismael-valenzuela/

Register for SEC530 OnDemand here:
https://www.sans.org/course/defensible-security-architecture-and-engineering#type-ondemand

Presentation based on SEC530: Defensible Security Architecture and Engineering

Thank you!! Follow @SecurityMapper & @aboutsecurity for updates and new webinars!

References

https://www.sans.org/course/defensible-security-architecture-and-engineering