

Epidigitalogy

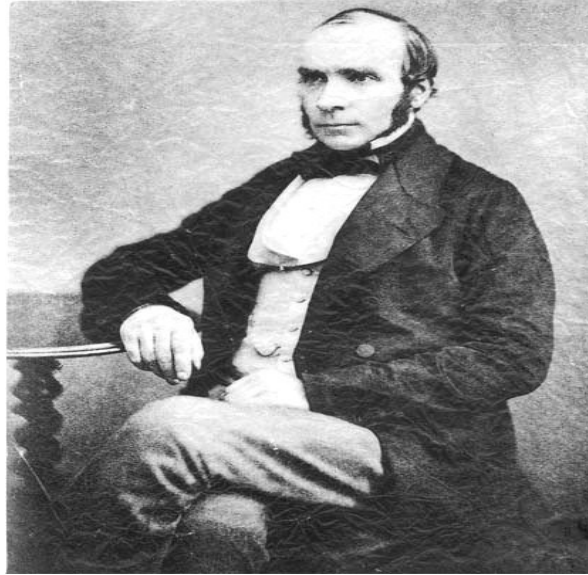
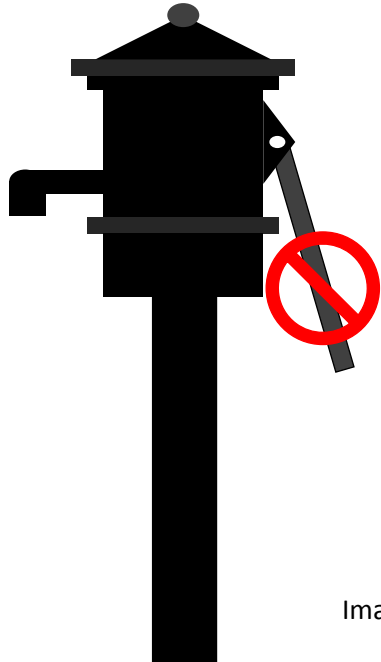
Surveying for Digital Diseases like an Epidemiologist

Efrain Ortiz, CISSP

Director, Market and Technology Innovation Group

Symantec

What does a 19th century doctor and CDC have to do with cyber security?



Centers for Disease Control and Prevention
CDC 24/7: Saving Lives, Protecting People™

What is Epidigitalology?

- “Epidigitalology is the **study** of the **distribution** and **determinants** of **digital-related states or events** in **specified populations**, and the **application** of this study to the control of digital diseases.” *

- paraphrased from CDC

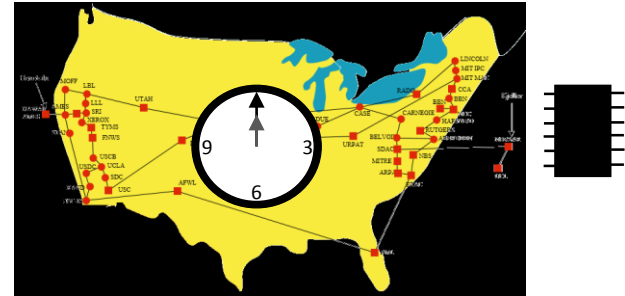
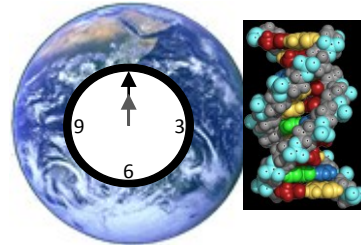
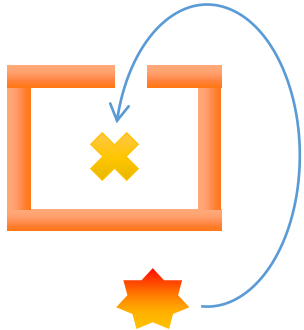
$$1+1=2$$

$$\begin{aligned}\partial_t u &= d_u^2 \nabla^2 u + f(u) - \sigma v, \\ \tau \partial_t v &= d_v^2 \nabla^2 v + u - v\end{aligned}$$

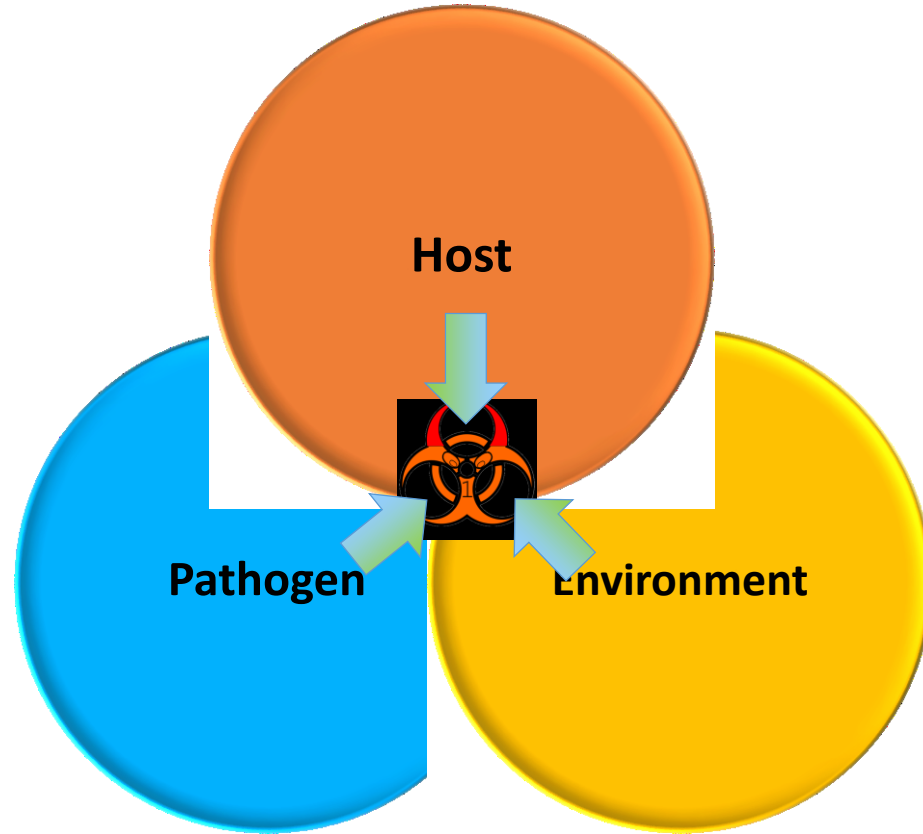


Epidemiology and Epidigitality

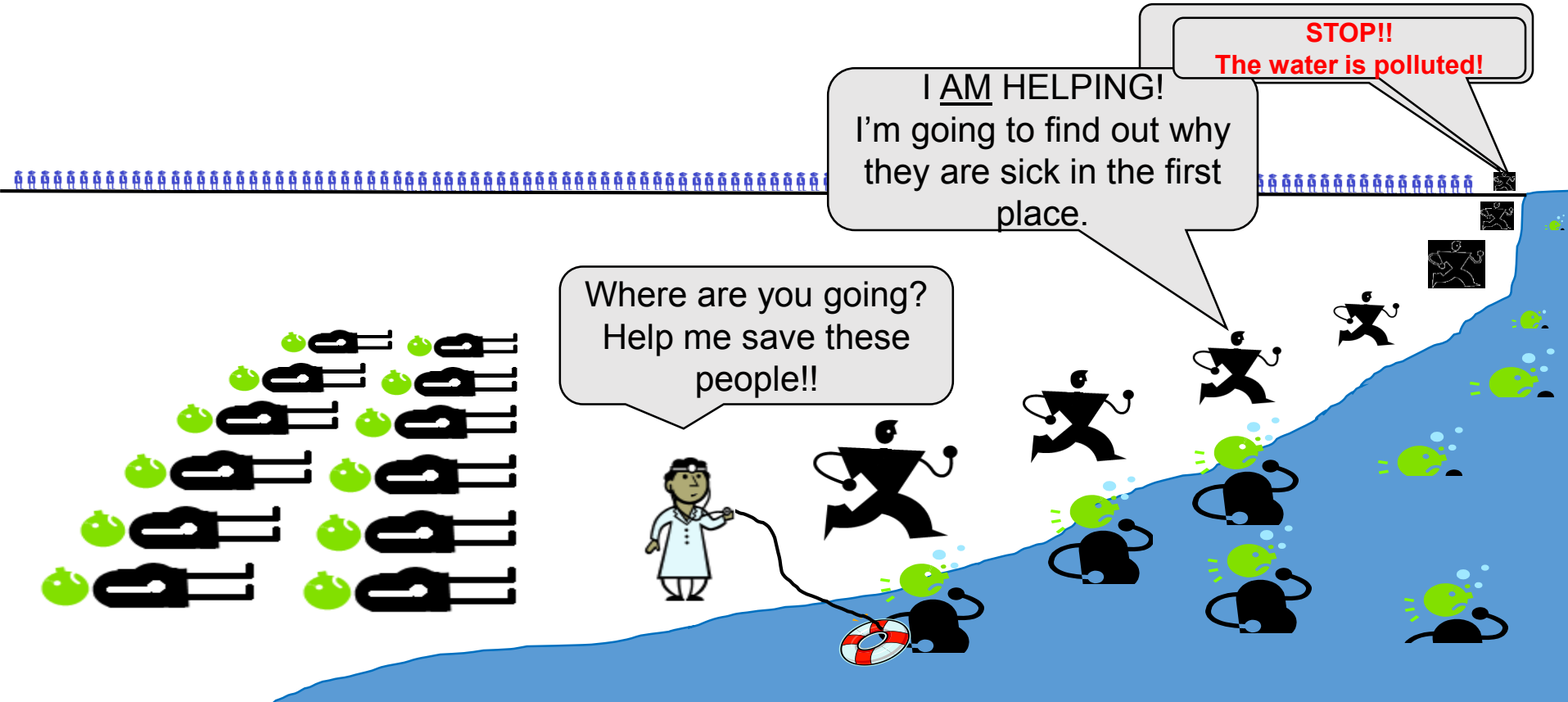
What are the similarities?



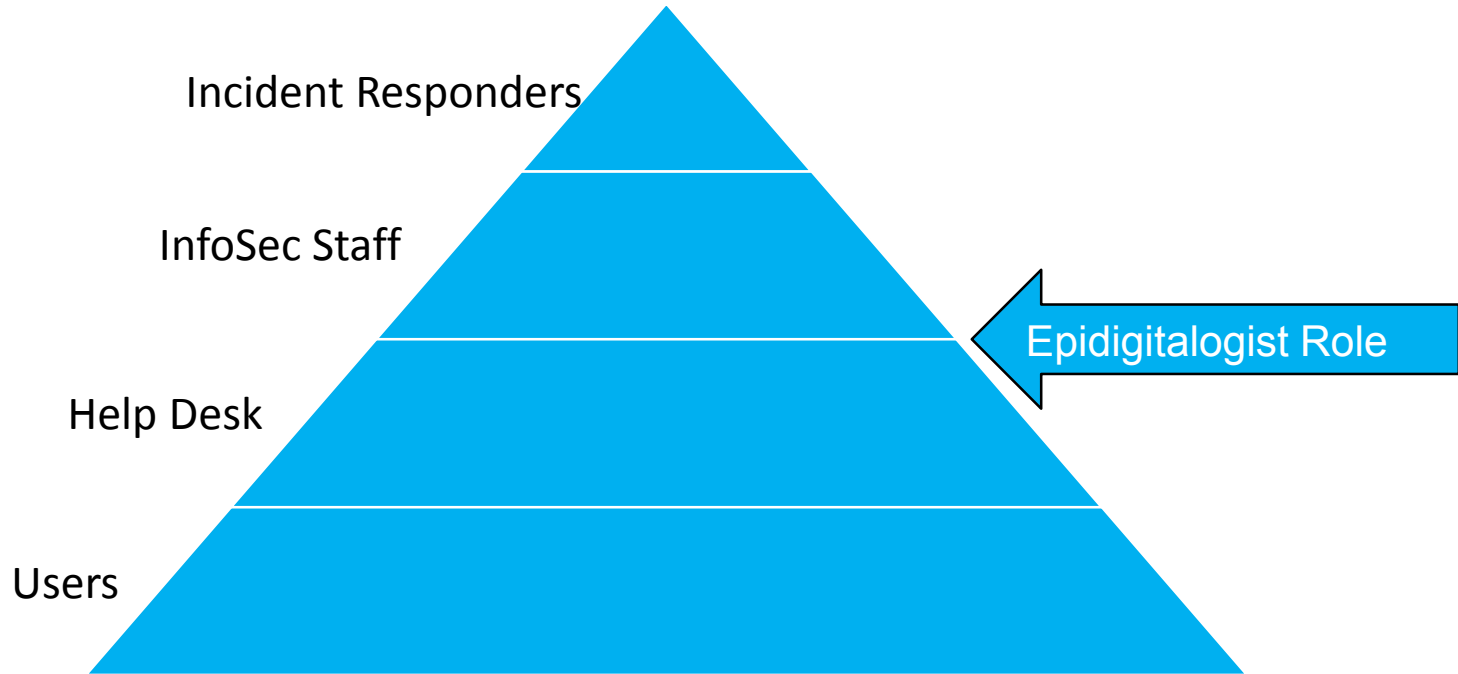
Epidigitalological Triad



Why do you need an epidigitalologist?



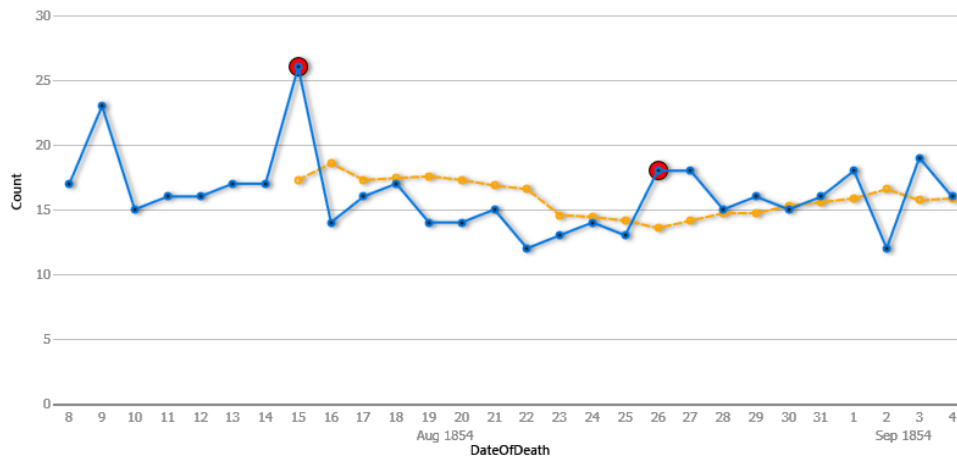
Where does an epidigitalologist fit in the organization?



Tools of the Epidemiology Trade

Let's get visual for faster time-to-know.

Aberration Detection Chart



Aberrations

Date	Count	Expected	Difference
8/15/1854	26	17.29	3.32 standard deviations
8/26/1854	18	13.57	4.54 standard deviations

What happens when we feed Epiinfo 7 endpoint security data?

AV Log Events Frequency (Cases)

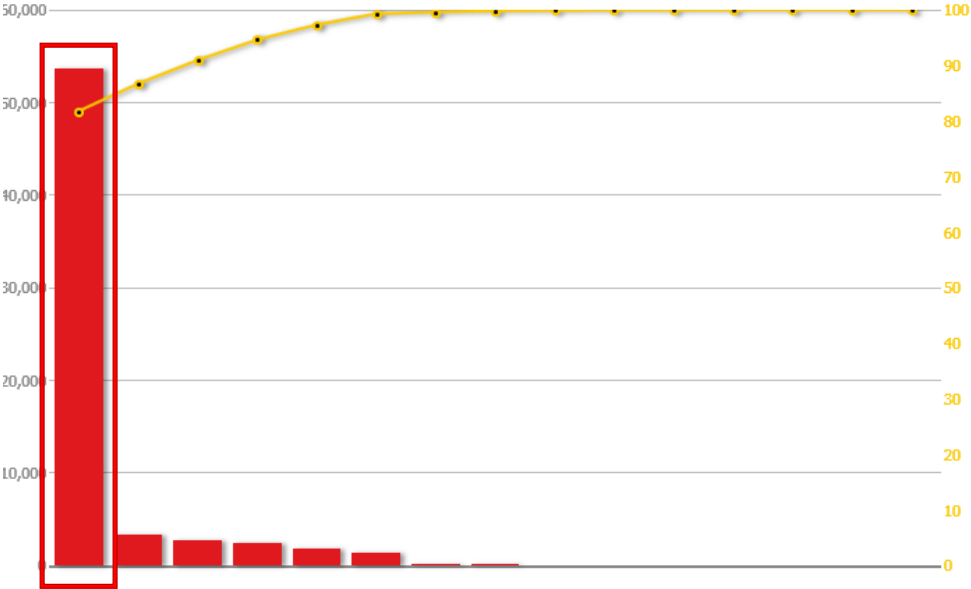
Frequency of Alert Types



ALERT_IDX	Frequency	Percent	Cum. Percent	95% CI Lower	95% CI Upper	
Commercial application detected	516	0.23 %	0.23 %	0.21 %	0.25 %	
Forced proactive threat detected	175774	76.88 %	77.11 %	76.71 %	77.05 %	
Potential risk found	9433	4.13 %	81.23 %	4.04 %	4.21 %	
Proactive detection now permitted	3773	1.65 %	82.88 %	1.60 %	1.70 %	
Risk sample submitted to Symantec	10070	4.40 %	87.29 %	4.32 %	4.49 %	
Security risk found	5335	2.33 %	89.62 %	2.27 %	2.40 %	
Virus found	23733	10.38 %	100.00 %	10.26 %	10.51 %	
TOTAL	228634	100.00 %	100.00 %			

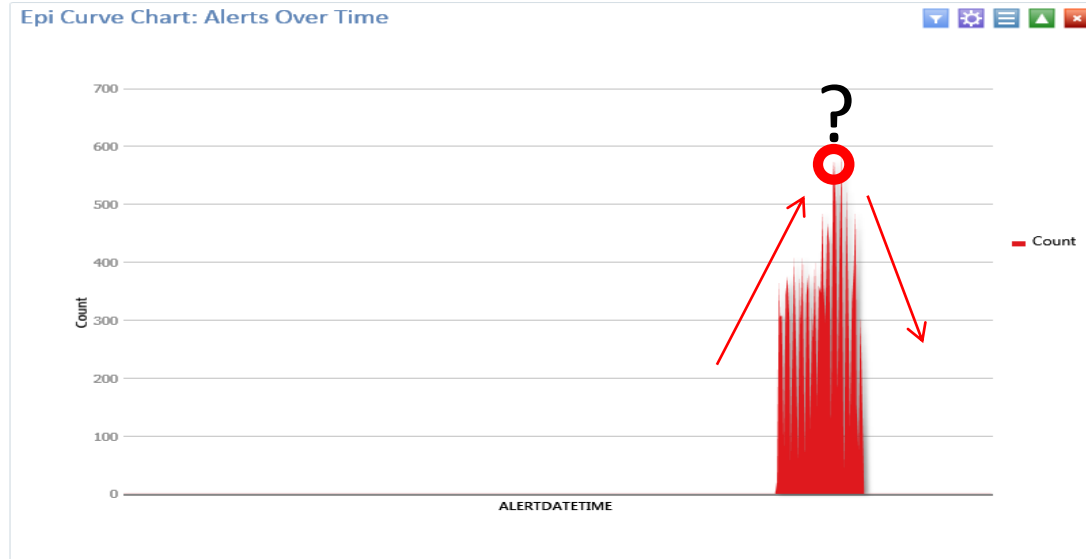
Pareto (80/20 Rule) of Actions Taken (Cases)

Chart: Action Taken on Identified Threats







ACTUALACTION_IDX

EpiCurve of Events Frequency(Cases)



AV Risk Detected Frequency (Cases)



Detected	Frequency	Percent	Cum. Percent	95% CI Lower	95% CI Upper	
W32.HLLP.Sality	271071	73 %	73 %	73 %	74 %	
W32.HLLP.Sality!inf	75576	20 %	94 %	20 %	21 %	
Backdoor.IRC.Bot	21594	6 %	100 %	6 %	6 %	
Dialer.DialPlatform	126	0 %	100 %	0 %	0 %	
Adware.GAIN	124	0 %	100 %	0 %	0 %	
W32.IRCBot.Gen	71	0 %	100 %	0 %	0 %	

Epi Info 7.0 Visual Dashboard (Case Control study)

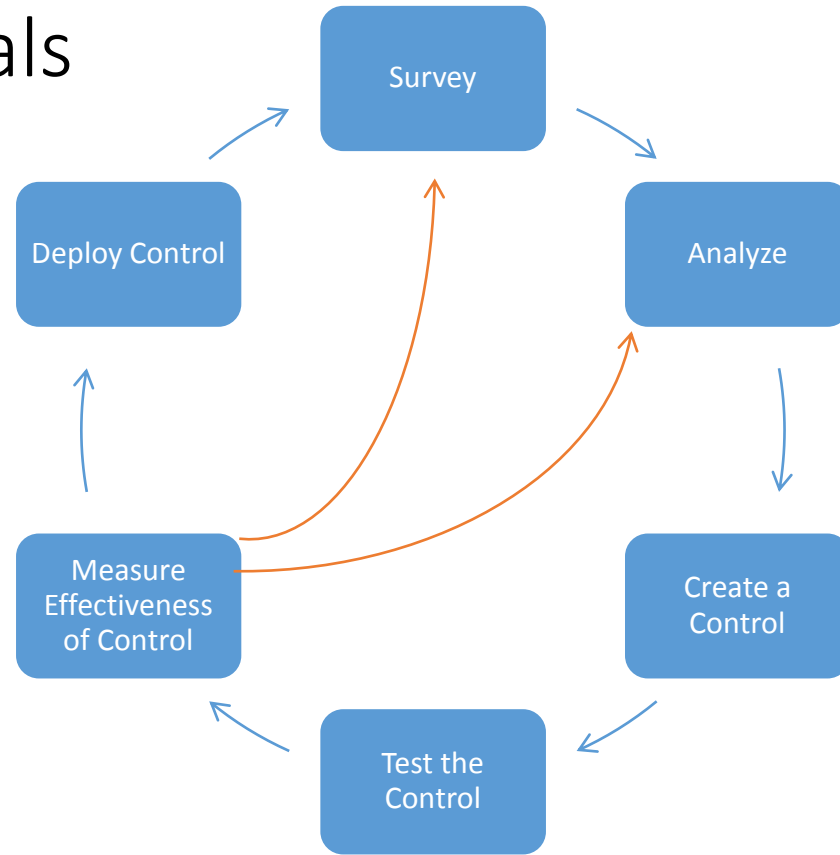
Crosstabulation (MxN, 2x2)

Exposure

Exposure	Outcome Rate Exposure	Outcome Rate No Exposure	Odds Ratio
ADServer	0.6216	0.6216	1.0000
autorun#inf2	0.5319	0.7407	0.3977
Autorun1#inf	0.6750	0.5429	1.7490
CDROM	0.6129	0.6136	0.9969
File1#exe	0.6304	0.5862	1.2042
File2#exe	0.6667	0.5833	1.4286
HRServer1	0.5000	0.6197	0.6136
http://downl0ad5galore\#com	0.5625	0.6512	0.6888
http://download#latestcelebritynews#ru	0.7963	0.1429	23.4545
NetFiler1	0.6667	0.6087	1.2857
NetFiler2	0.6957	0.5769	1.6762
Process1#exe	0.6047	0.6250	0.9176
Unkey1	0.6429	0.5957	1.2214
Server3	0.5417	0.6471	0.6446
SQLDBServer	0.5676	0.6579	0.6825

		Infected		
		Yes	No	
Exposure	Exposed	43 79.63 % 93.48 %	11 20.37 % 37.93 %	54
	Not Exposed	3 14.29 % 6.52 %	18 85.71 % 62.07 %	21
		46	29	75
		61.33 % 100.00 %	38.67 % 100.00 %	100.00 % 100.00 %

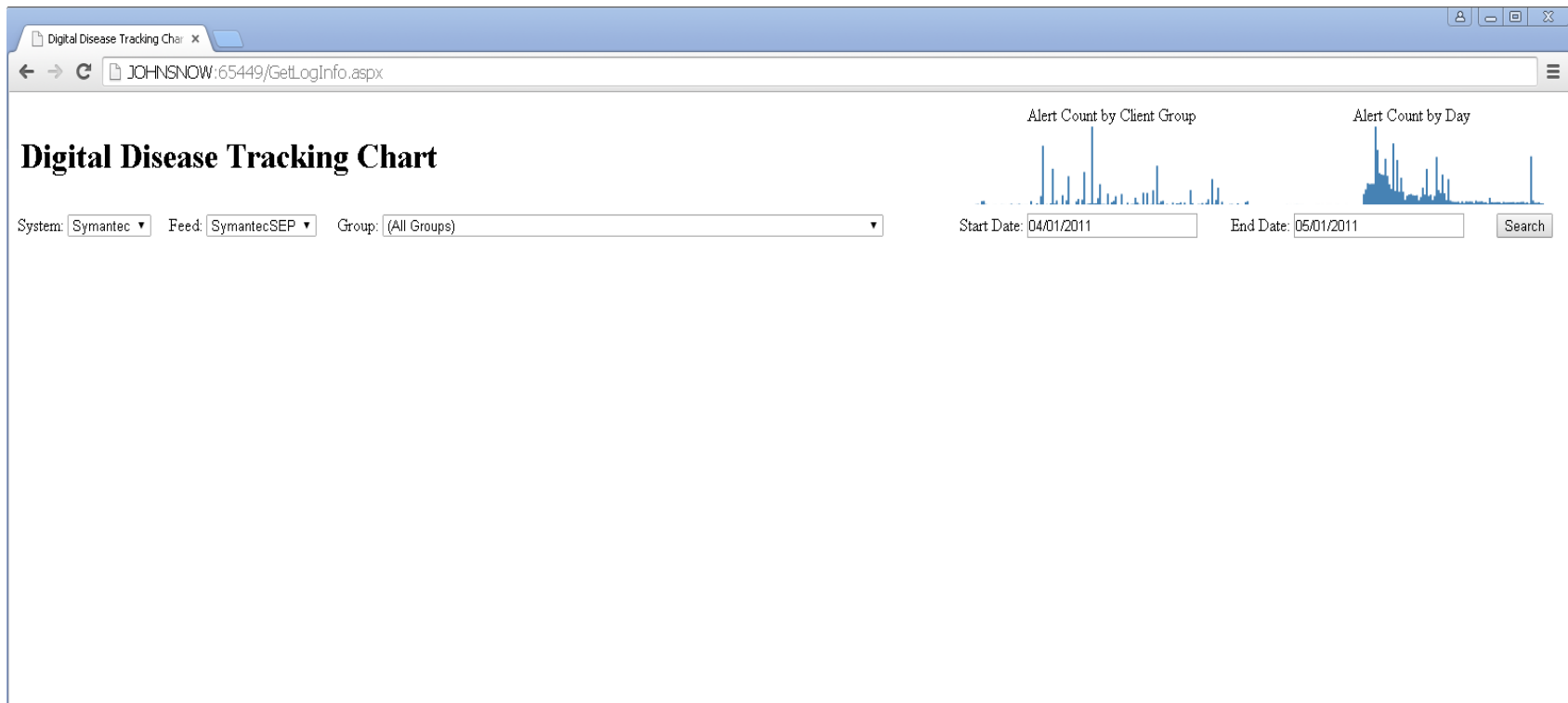
Clinical Trials



Digital Disease Tracking Web Portal

Proof of concept

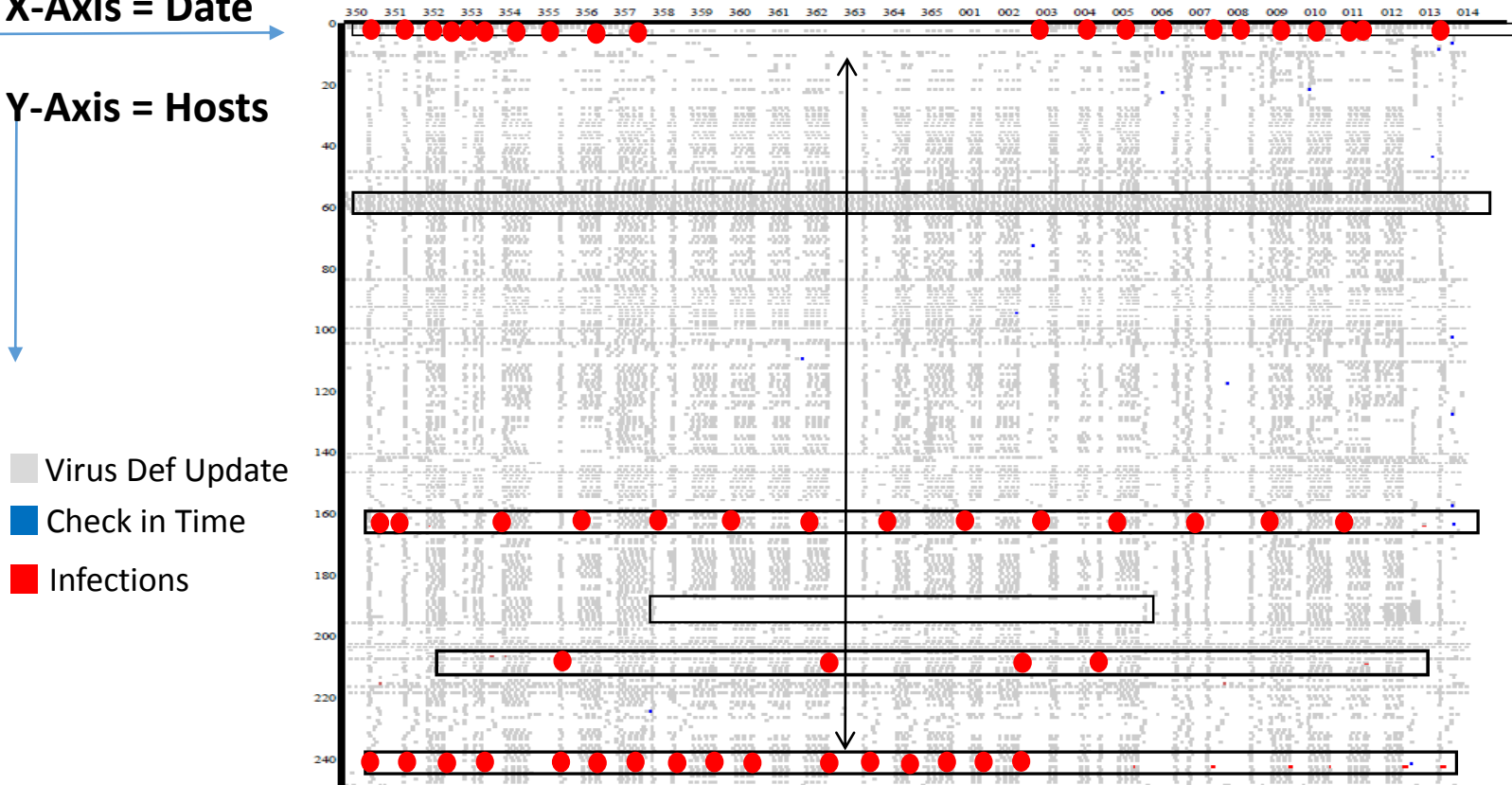
Digital Disease Tracking Web Portal



Proof of Concept: Endpoint Product 1

X-Axis = Date

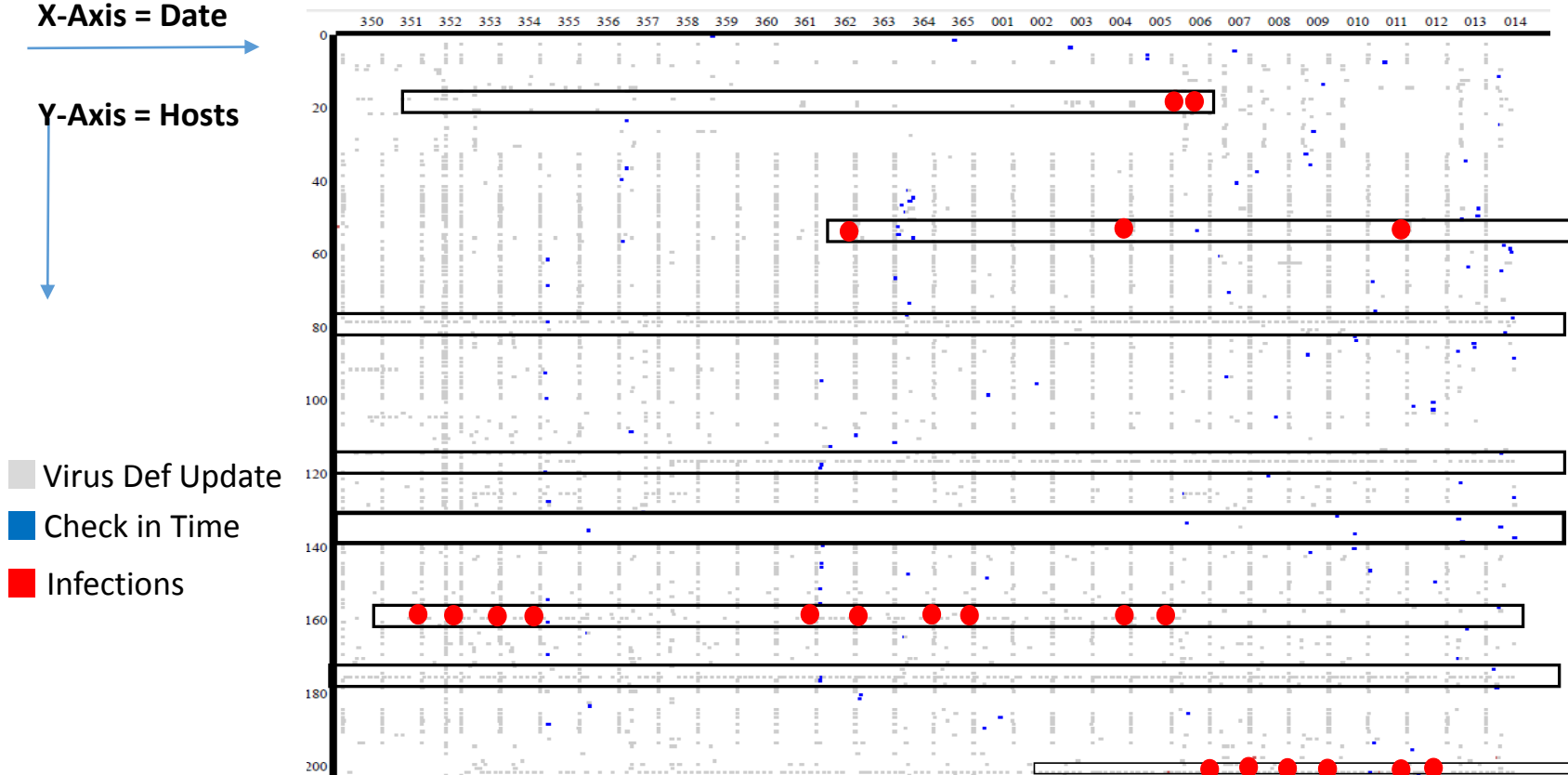
Y-Axis = Hosts



Proof of Concept: Endpoint Product 2

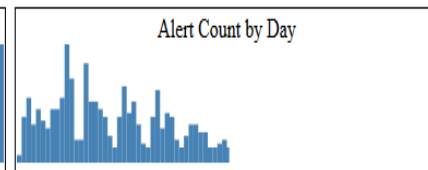
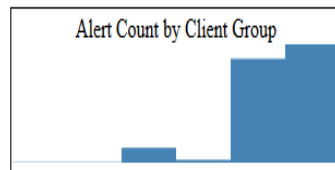
X-Axis = Date

Y-Axis = Hosts



Proof of Concept: Endpoint Product 3

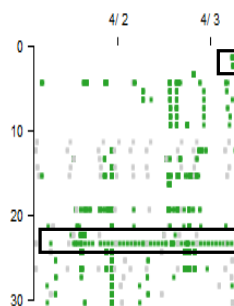
Digital Disease Tracking Chart



System: Symantec Feed: SymantecSEP Group: (All Groups) Start Date: 4/1/2015 End Date: 4/16/2015 Search

X-Axis = Date

Y-Axis = Hosts



My Company\Servers\Soundwave

User Name:	LOCAL\domadmin	Name:	255.255.255.2
OS:	Windows Server 2008 R2 Standard Edition Service Pack 1	Title:	Subnet Mask: 255.255.255.0
Agent Version:	12.1.5337.5000	Department:	Gateway: 255.255.255.1
Last Scan:	4/13/2015 21:44:58.000	Email:	DNS 1: 255.255.255.2
Last Download:	3/2/2015 18:12:28.000	Office Phone:	DNS 2: 255.255.255.4
Last Virus Time:	3/16/2015 09:51:35.000		0.0.0

Event Date: 4/11/2015 05:01:31.000
Event Type: Application Control Rules
Action Taken: continue
User: NETWORK SERVICE
Description: This rule will log all applications that writing files to any USB device that add a drive letter to your system.
Caller Process: C:\Windows\System32\wbem\WmiPrvSE.exe
Parameter: D:/
Rule Name: Log files written to USB drives | [AC5-1.1] Log writing to USB drives

Firewall 4/2 4/3 4/4
IPS
Downloads
AV Engine
Virus Updates
User Control

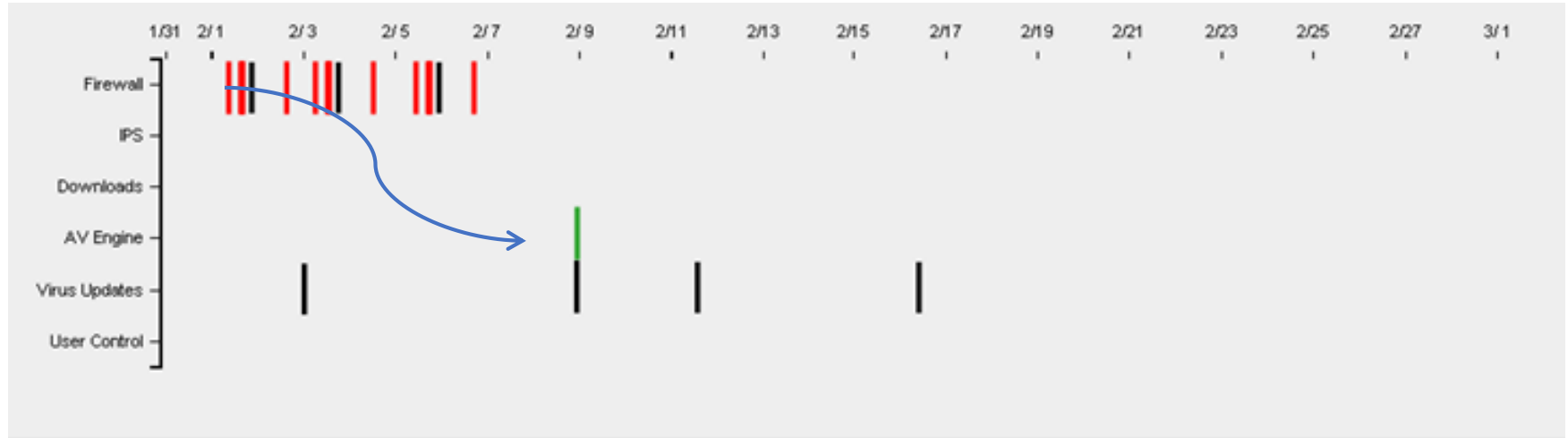
Virus Def Update

Check in Time

Infections or Violations

User Control Violation

Possible Network Borne Digital Disease Pathogen

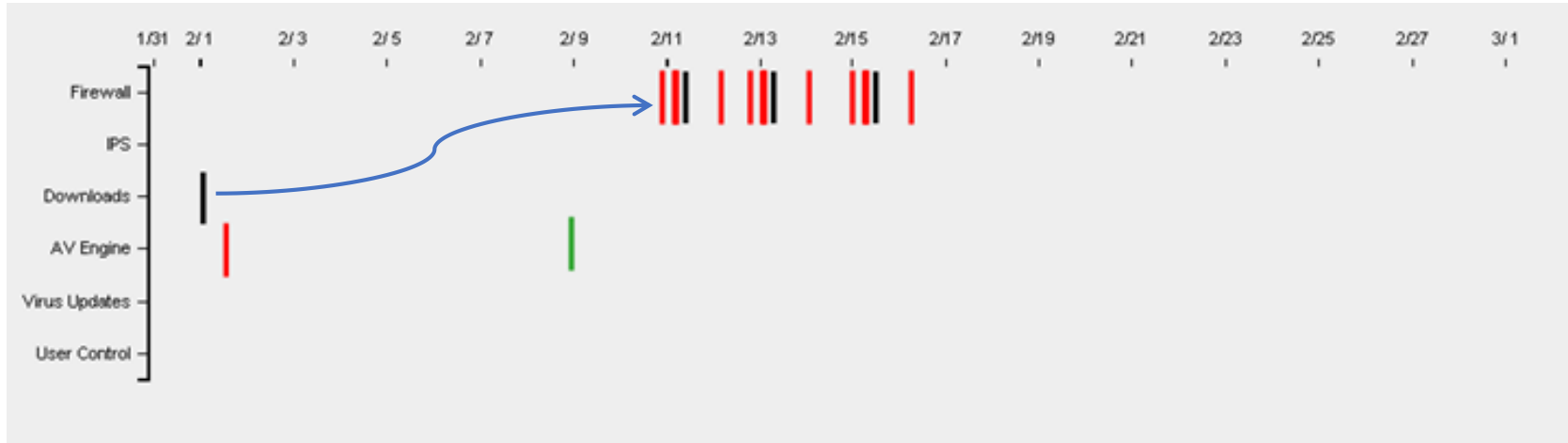


■ Threat Detected but stopped

■ Informational

■ Violation or Failed to Stop

Possible Download Borne Digital Disease Pathogen

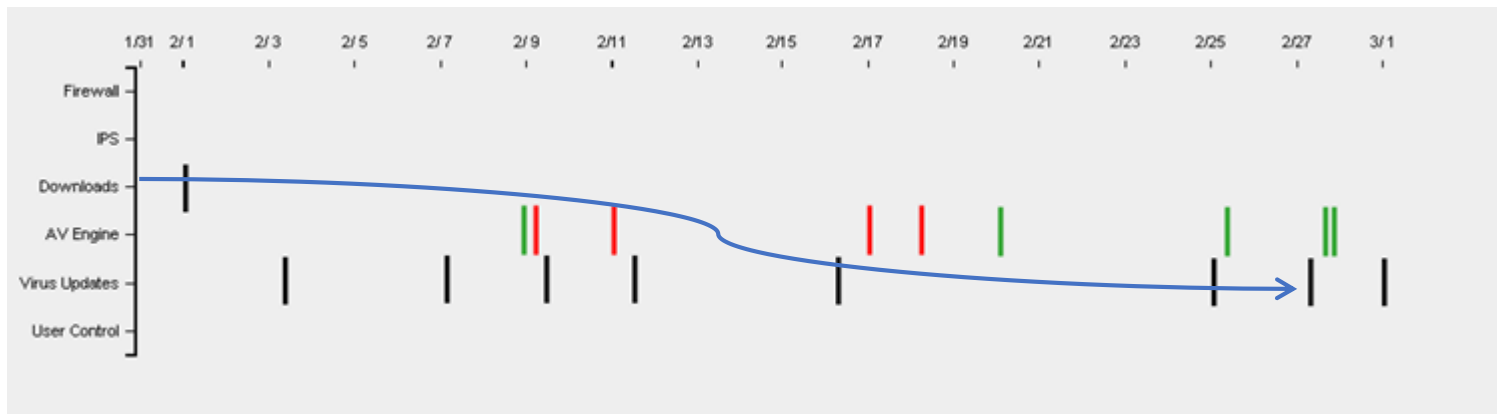


■ Threat Detected but stopped

■ Informational

■ Violation or Failed to Stop

Possible Downloader Borne Digital Disease Pathogen

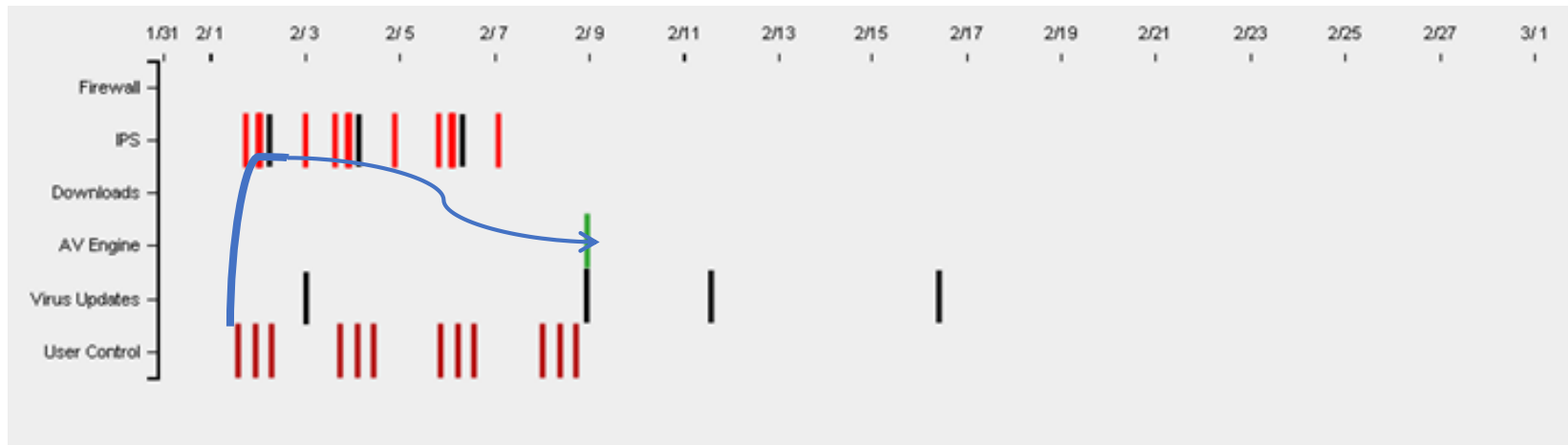


■ Threat Detected but stopped

■ Informational

■ Violation or Failed to Stop

Possible USB Borne Digital Disease Pathogen



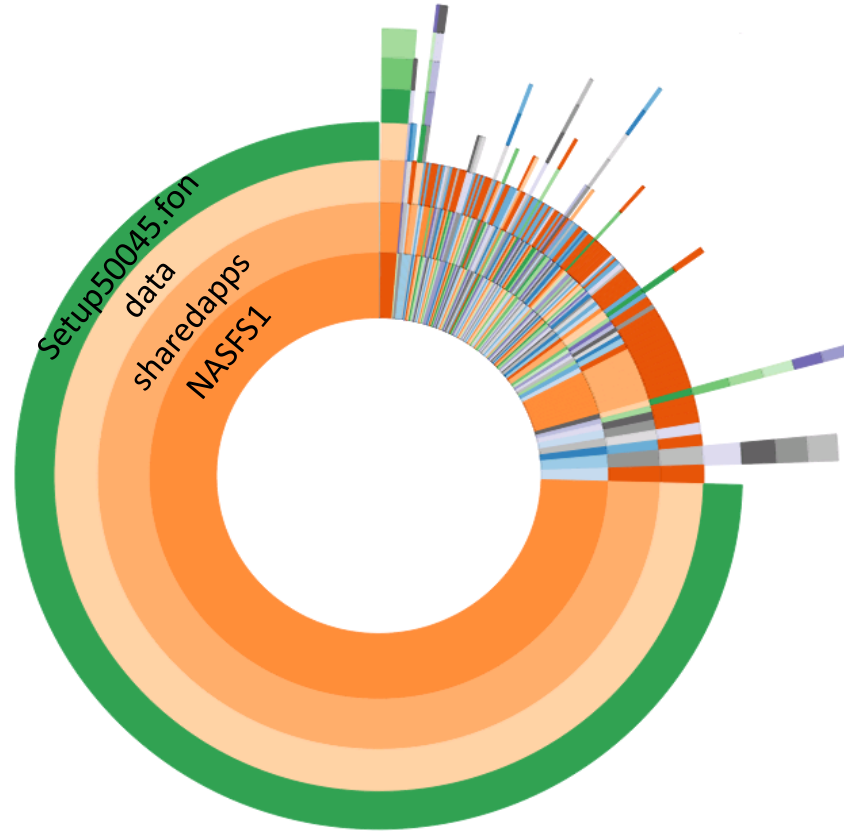
■ Threat Detected but stopped

■ Informational

■ Violation or Failed to Stop

■ Policy Violation

NAS Borne Infections Visualization



Digital Disease Flare Comparator

Digital Disease Flare Comparator

Search

System:
Symantec ▼

Feed:
Anti-Virus ▼

Group:
(All Groups) ▼

Start Date:
06/08/2015

End Date:
06/16/2015

Category 1: ☒ Show Text
(Select One) ▼

Category 2: ☐ Show Text
(Select One) ▼

Category 3: ☐ Show Text
(Select One) ▼

Chart Type:
Sunburst ▼

Search

Comparing Group Name Count to Virus Count in Sunburst

Digital Disease Flare Comparator

Search

System:

Symantec

Feed:

Anti-Virus

Group:

(All Groups)

Start Date:

01/08/2015

End Date:

06/16/2015

Category 1:

☒ Show Text

Group Name

Category 2:

☒ Show Text

Virus Name

Category 3:

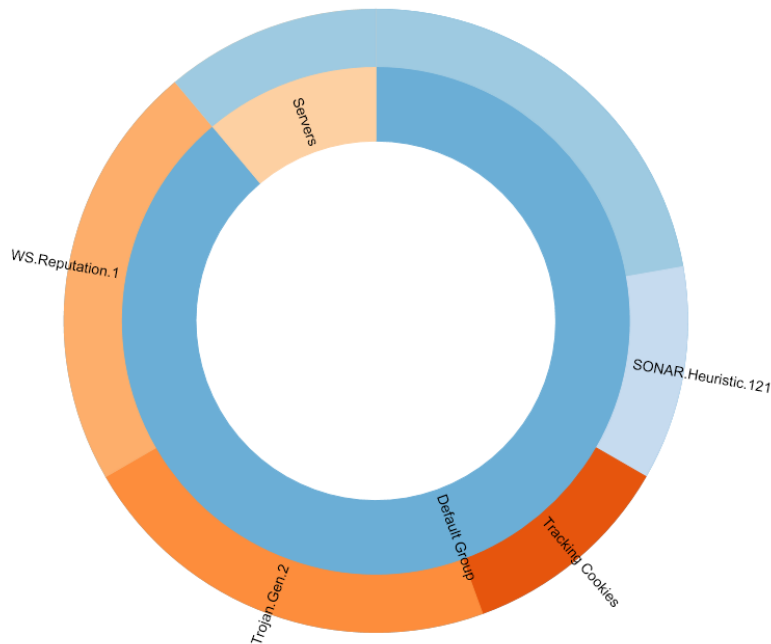
☐ Show Text

(Select One)

Chart Type:

Sunburst

Search



Summary

- Actively Survey Population thinking like an epidemiologist
- Case/Control Studies
- Clinical Trials
- Visualize Your Data
- Repeat Process Ad Infinitum

Apply Epidigitalogy

- Within a week you should:
 - Read Epidigitalogy blog link at <http://www.epidigitalogy.com/>
- In the first three months following this presentation you should:
 - (1) Download (2) Customize and (3) Install Digital Disease Tracking Web Application and (4) Attach or customize to your endpoint environment.
- Within six months you should:
 - Assign someone to the epidigitalogist role.
 - Commence routine surveying of endpoint data in your environment using epidemiological survey techniques.

Existing Literature Mentioning Epidemiology and Security

Title	Author(s)
Microsoft Exec: Infected PCs should be quarantined	Scott Charney's RSA Keynote 2010
Applying Epidemiology in Computer Virus Prevention: Prospects and Limitations	By Weiguo Jin Univ of Auckland
A genetic epidemiology approach to cyber-security	Santiago Gil, Alexander Kott & Albert-László Barabási
The Application of Epidemiology to Computer Viruses	W.H. Murray (1988)
Computer Viruses- Theory and Experiments	Fred Cohen (1984)

Thank You

Director, Market and Technology Innovation Group

Efrain_Ortiz (at) Symantec (d0t) com

@ortizonline