RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: MASH-R03

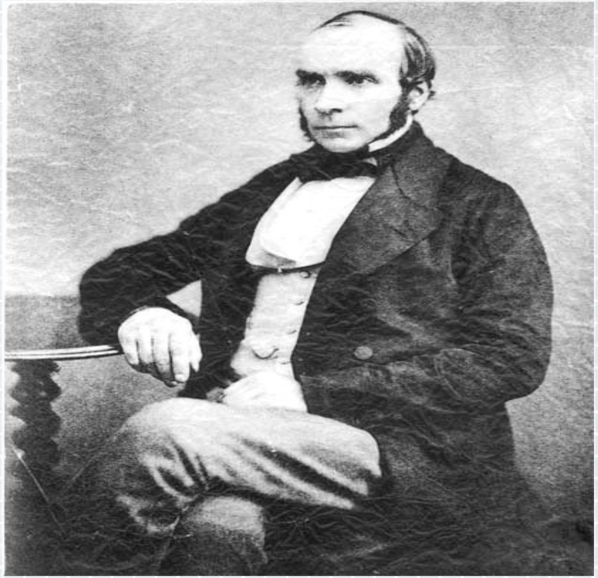
Epidigitalogy

Surveying for Digital Diseases like an Epidemiologist

Efrain Ortiz

Director, Market and Technology Innovation Group
efrain_ortiz@symantec.com
@ortizonline

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



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

Image Attribution: wikipedia.org., CDC.gov

What is Epidigitalogy?

- *“Epidigitalogy 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.”* *

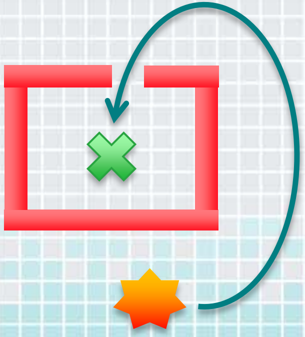
- *paraphrased from CDC*

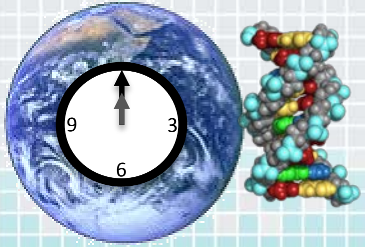
* Center for Disease Control and Prevention definition

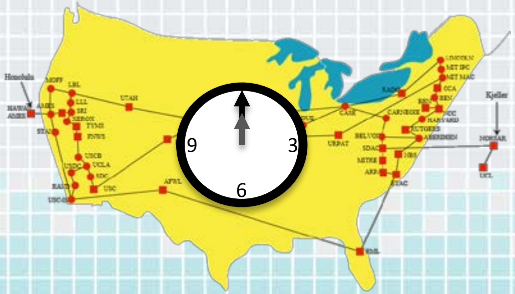
1+1=2

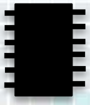
$$\begin{aligned} \partial_t u &= d_u^2 \nabla^2 u + f(u) - \sigma v, \\ \tau \partial_t v &= d_v^2 \nabla^2 v + u - v \end{aligned}$$

Epidemiology and Epidigitalogy
What are the similarities?

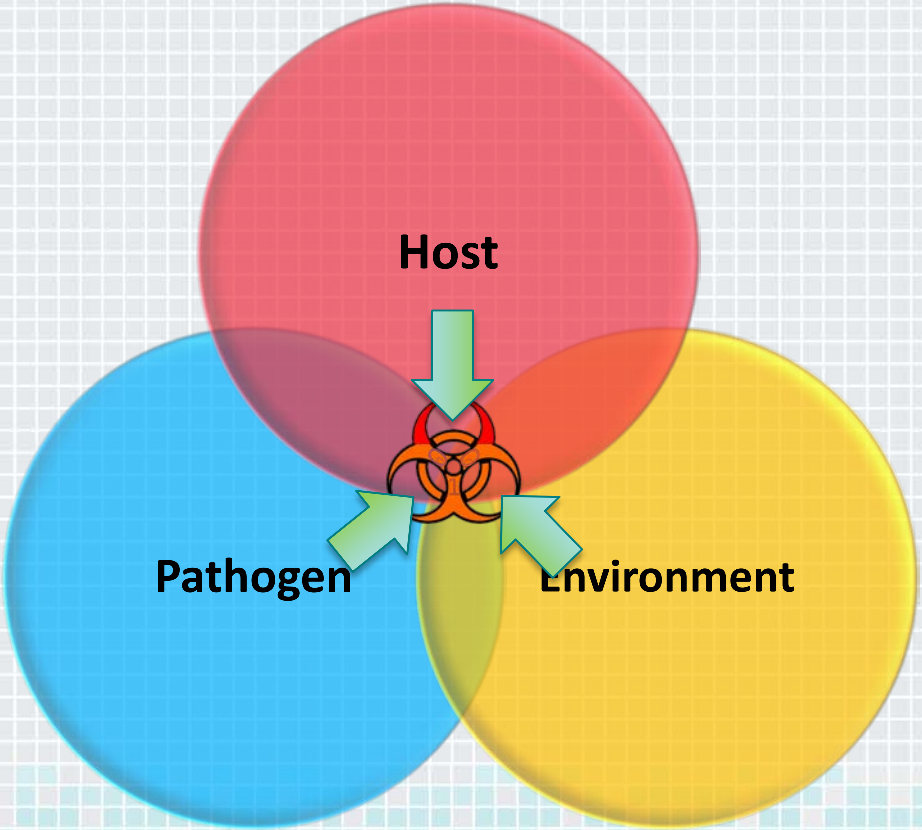








Epidigitalogical Triad

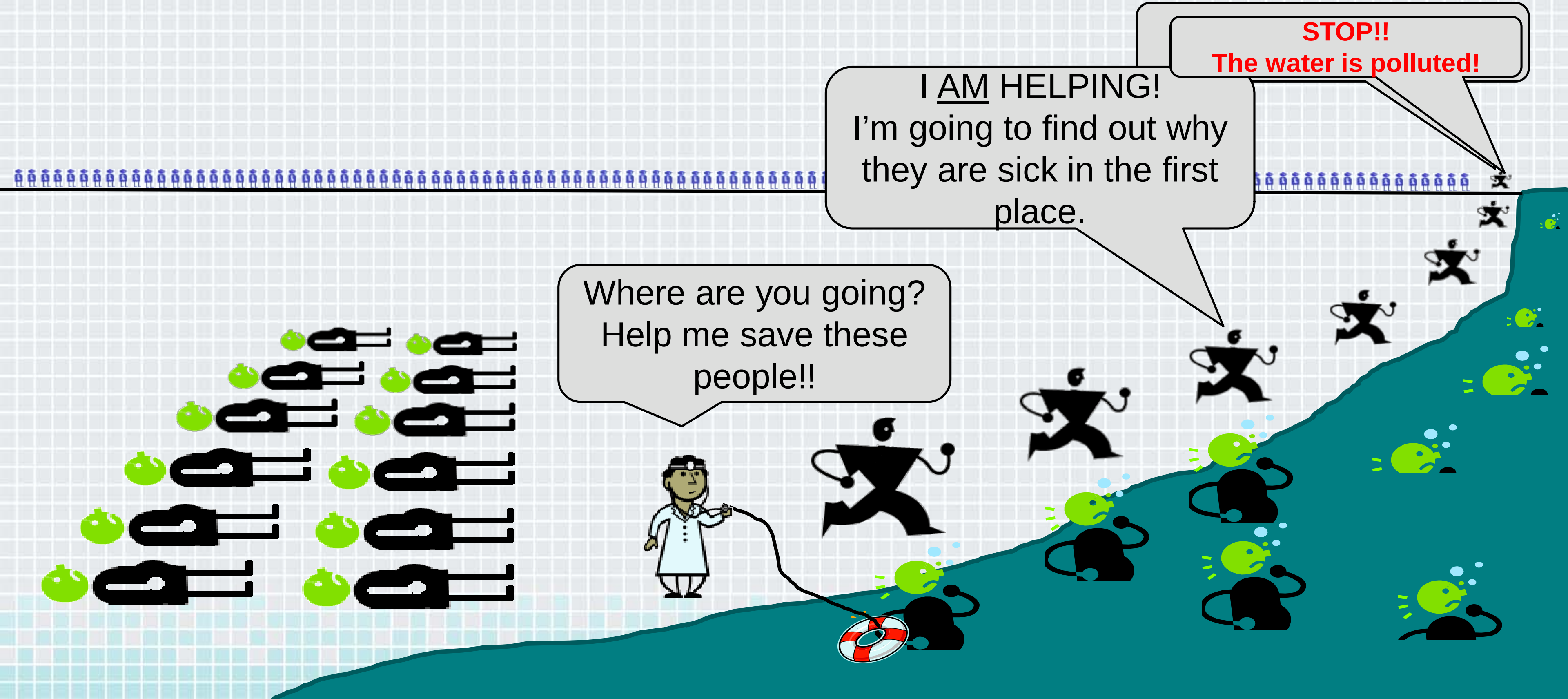


Host

Pathogen

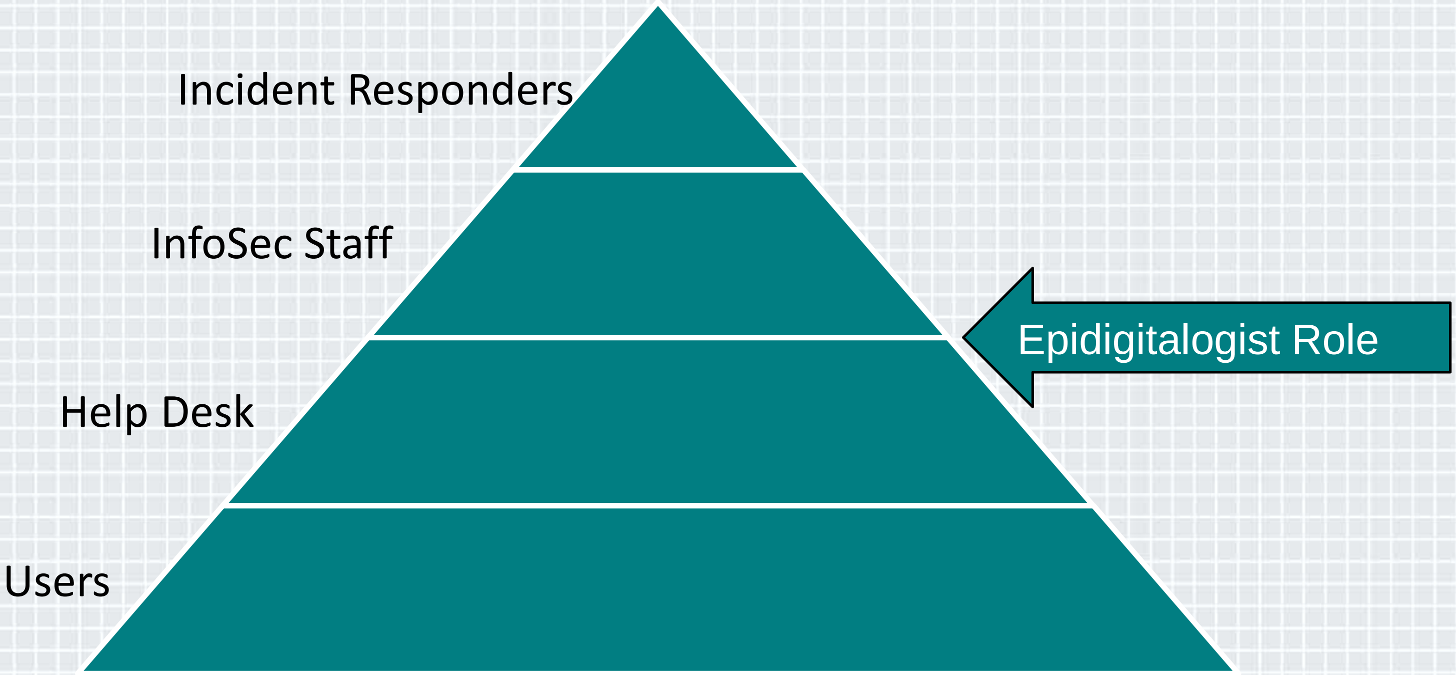
Environment

Why do you need an epidigitalogist?



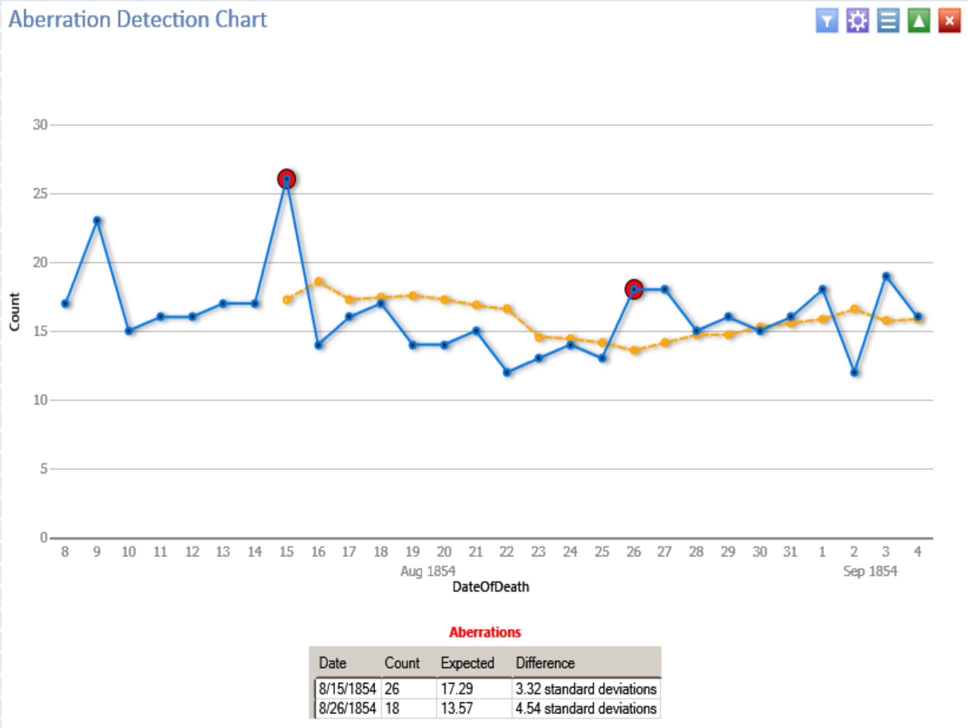
STOP!!
The water is polluted!
I AM HELPING!
I'm going to find out why they are sick in the first place.
Where are you going? Help me save these people!!

Where does an epidigitalogist fit in the organization?



Tools of the Epidemiology Trade

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

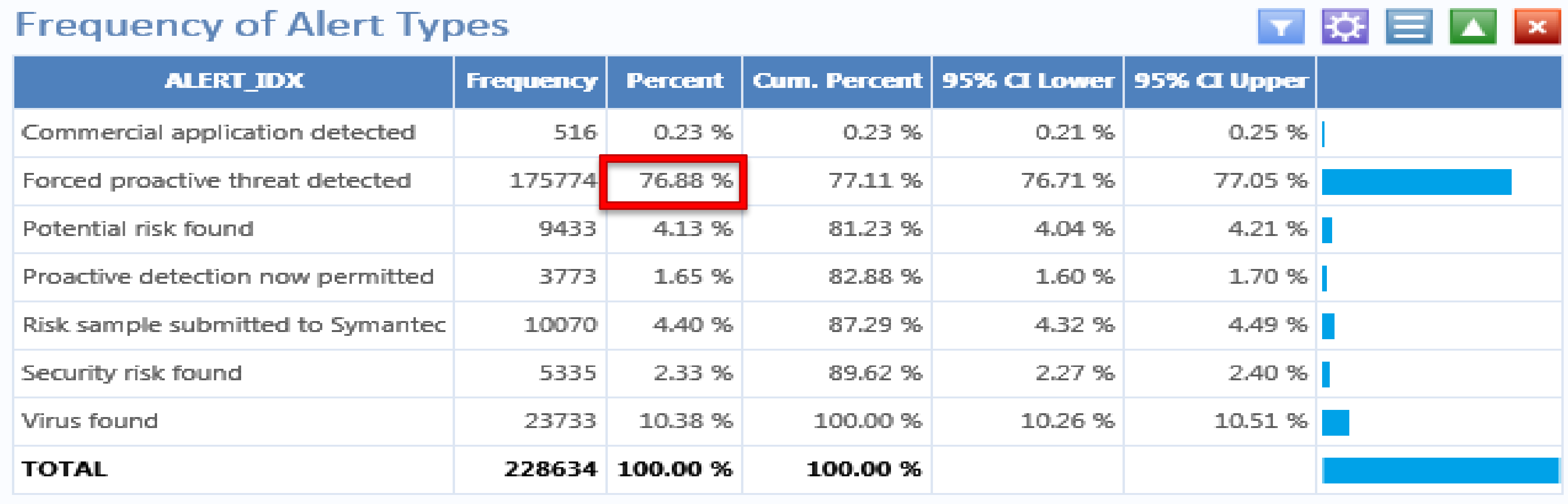


Aberrations

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?

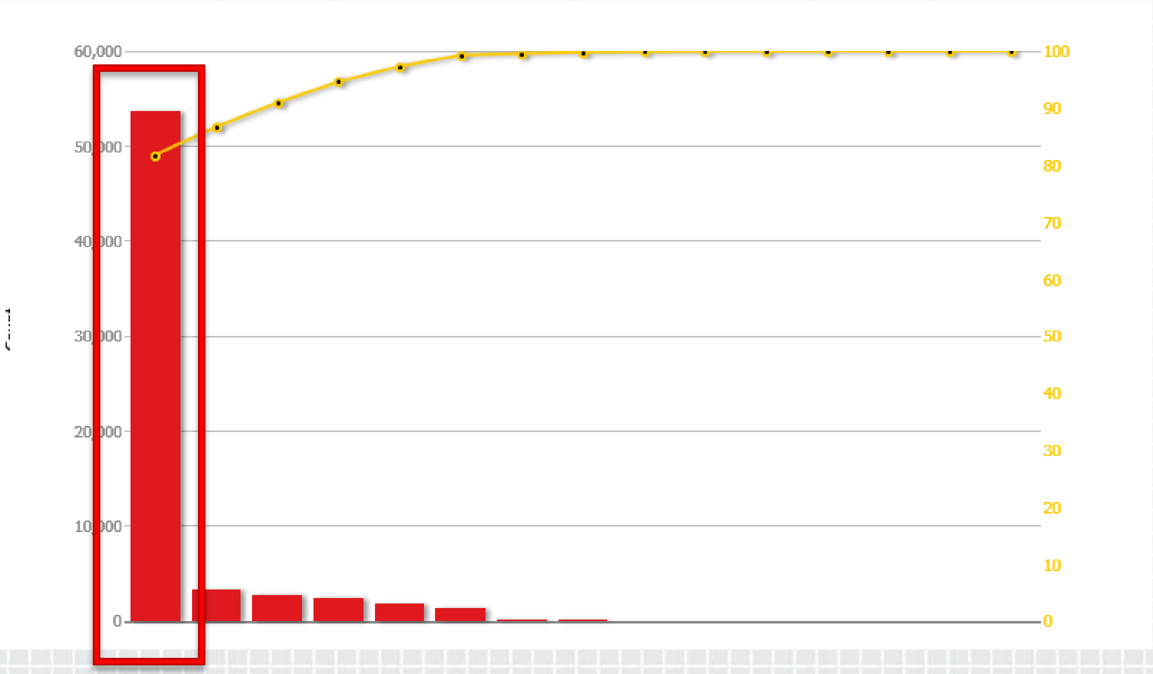
AV Log Events Frequency (Cases)



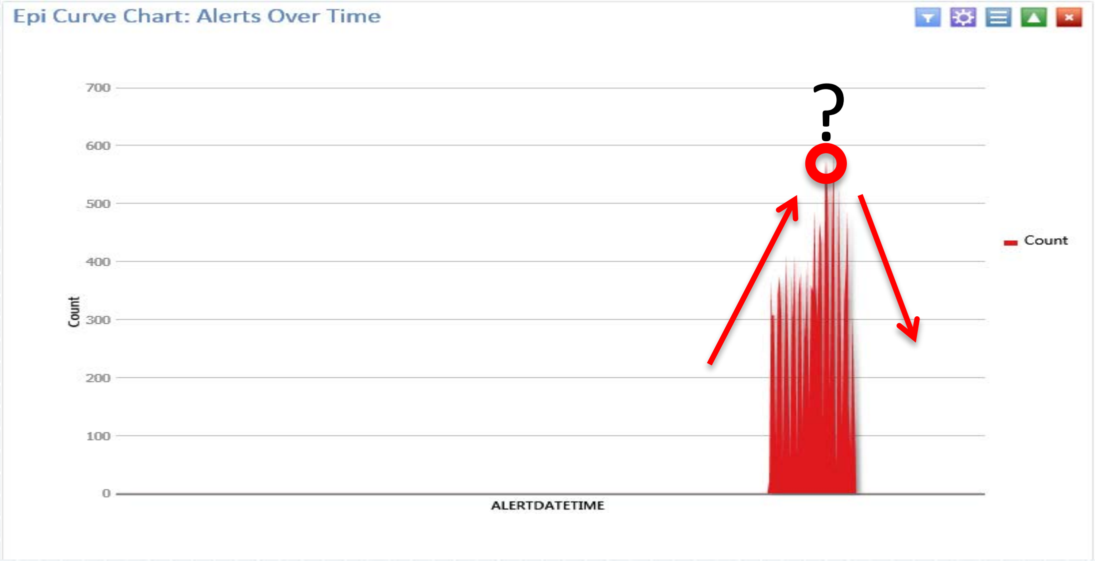
Frequency of Alert Types

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 %**			

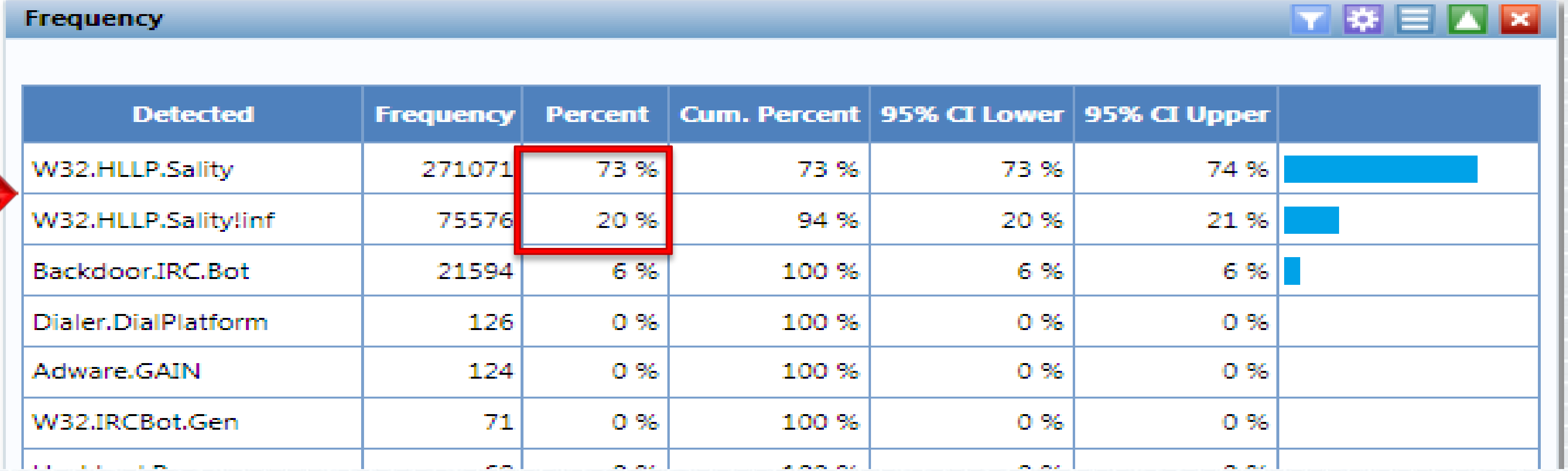
Pareto of Actions Taken (Cases)



EpiCurve of Events Frequency(Cases)



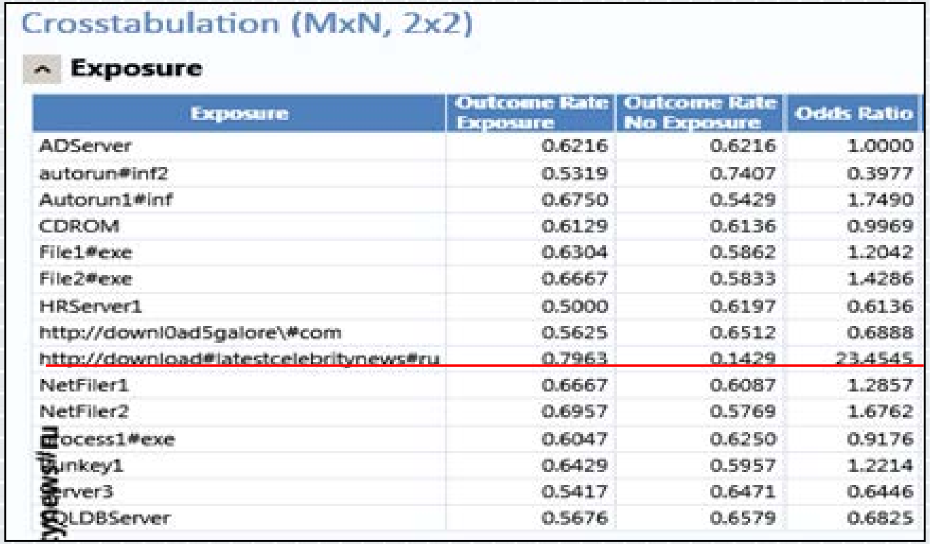
AV Risk Detected Frequency (Cases)



Frequency

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 %

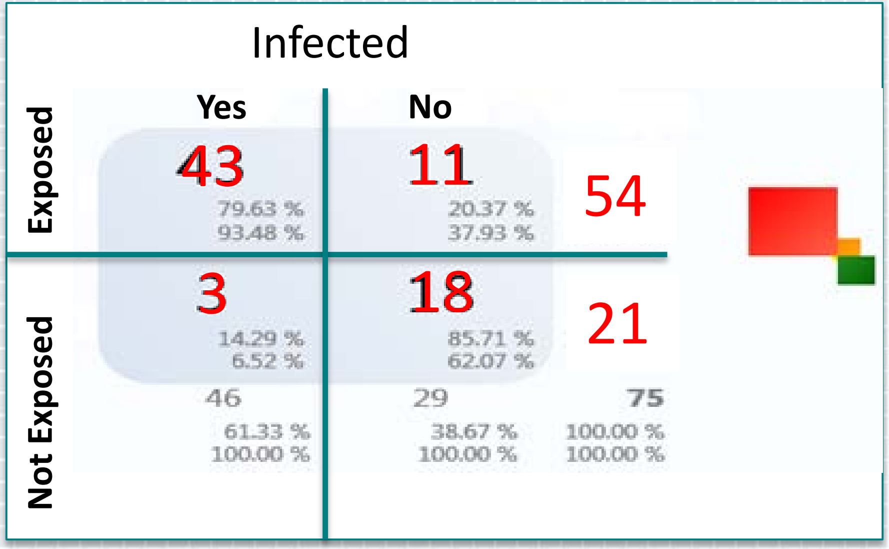
Epi Info 7.0 Visual Dashboard (Case Control study)



Crosstabulation (MxN, 2x2)

^ **Exposure**

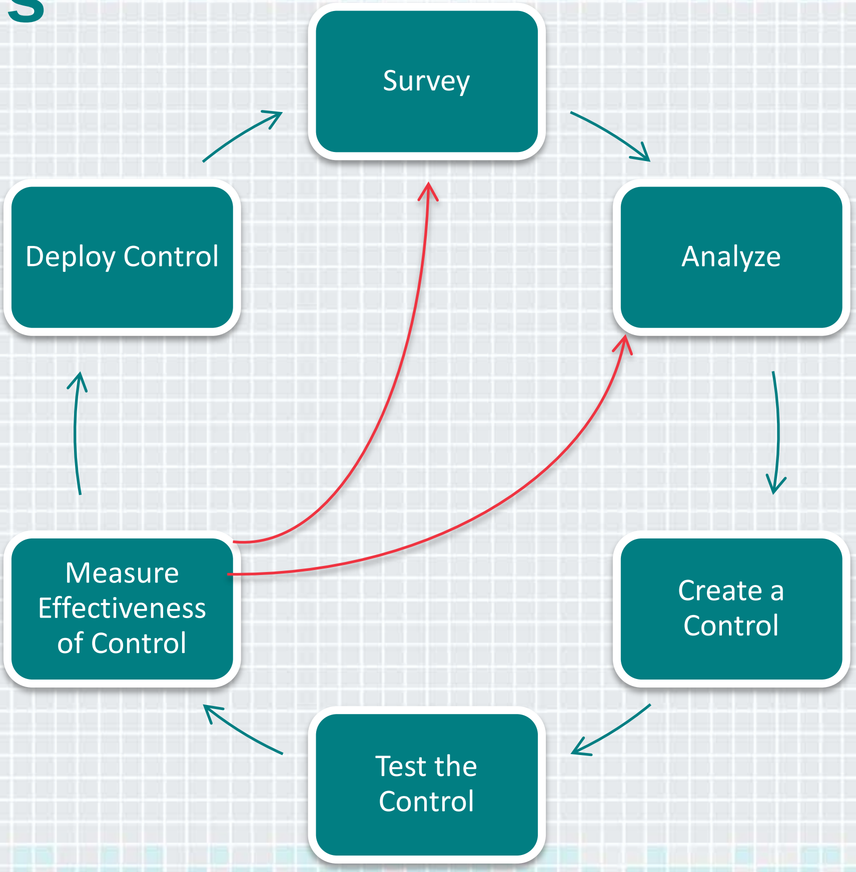
Exposure	Outcome Rate Exposure	Outcome Rate No Exposure	Odds Ratio
ADServer	0.6216	0.6216	1.0000
autorun#inf2	0.5319	0.7407	0.3977
Autorun1#inf	0.6750	0.5429	1.7490
CDROM	0.6129	0.6136	0.9969
File1#exe	0.6304	0.5862	1.2042
File2#exe	0.6667	0.5833	1.4286
HRServer1	0.5000	0.6197	0.6136
http://downl0ad5galore\#com	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
Runkey1	0.6429	0.5957	1.2214
Server3	0.5417	0.6471	0.6446
SQLDBServer	0.5676	0.6579	0.6825



Infected

	Yes	No	
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 61.33 % 100.00 %	29 38.67 % 100.00 %	75 100.00 % 100.00 %

Clinical Trials


Survey

Analyze

Create a Control

Test the Control

Measure Effectiveness of Control

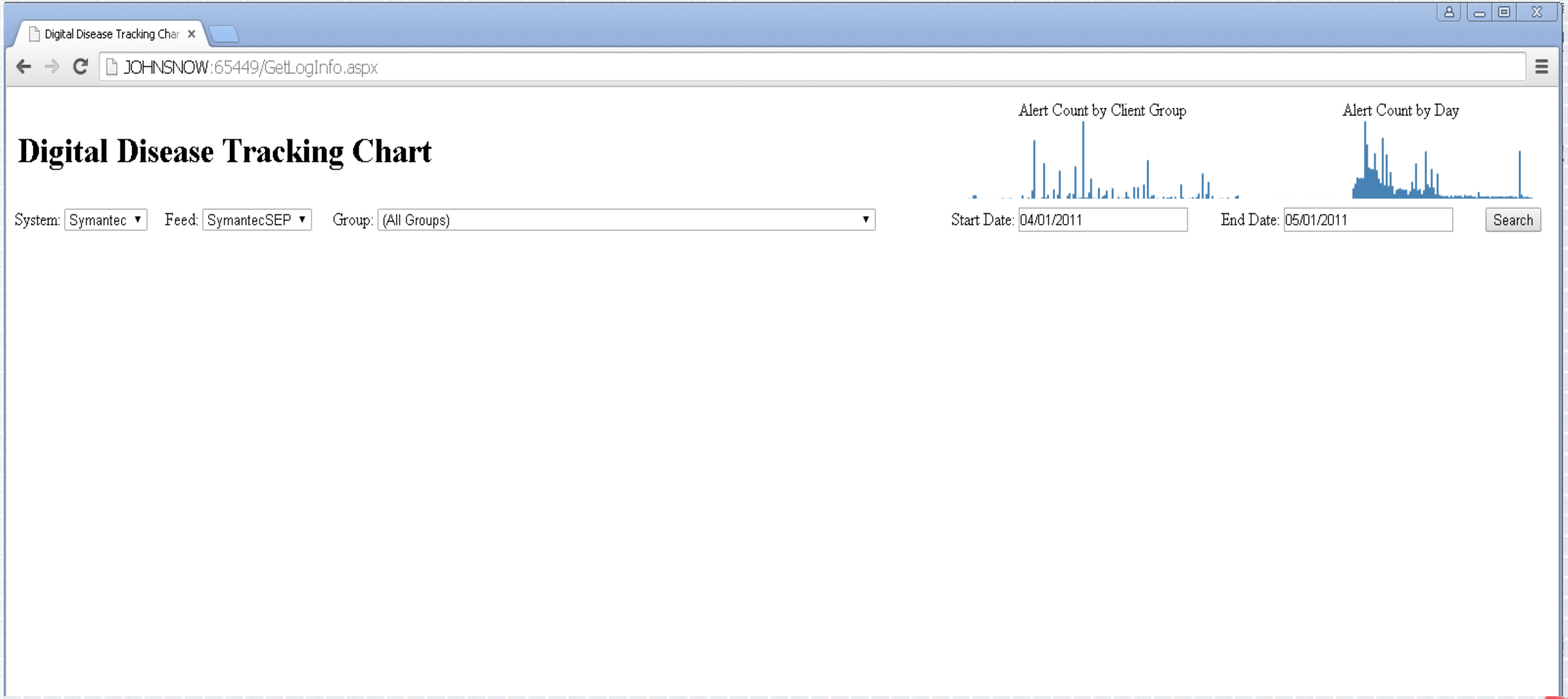
Deploy Control

Digital Disease Tracking Web Portal

Proof of concept

Programming by David_Ewall@radius180.com

Digital Disease Tracking Web Portal



Digital Disease Tracking Char
JOHNSNOW:65449/GetLogInfo.aspx

Digital Disease Tracking Chart

Alert Count by Client Group
Alert Count by Day

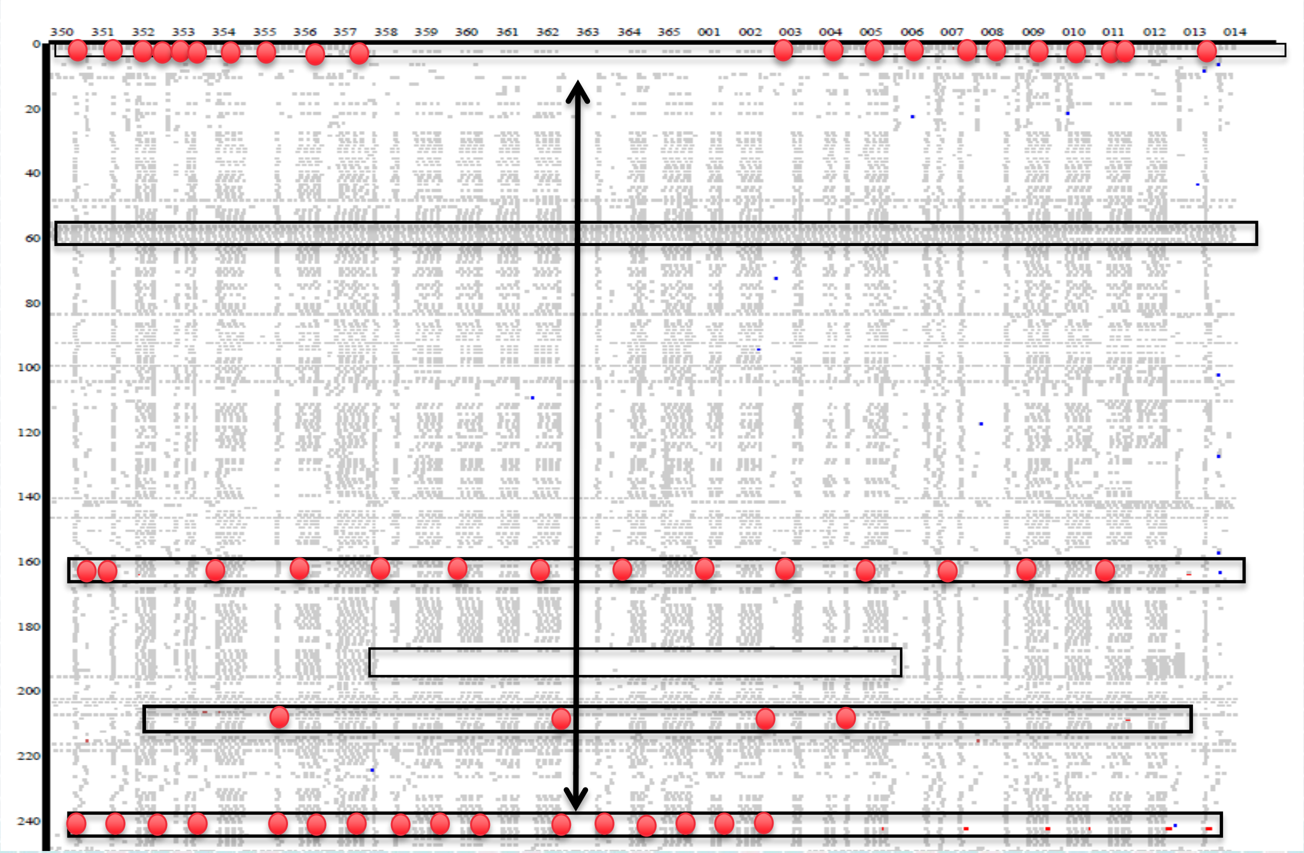
System: Symantec ▾ Feed: SymantecSEP ▾ Group: (All Groups) ▾ Start Date: 04/01/2011 End Date: 05/01/2011 Search

*Programming by David_Ewall@radius180.com

Proof of Concept: Endpoint Product 1

X-Axis = Date

Y-Axis = Hosts



⬜ Virus Def Update

🟦 Check in Time

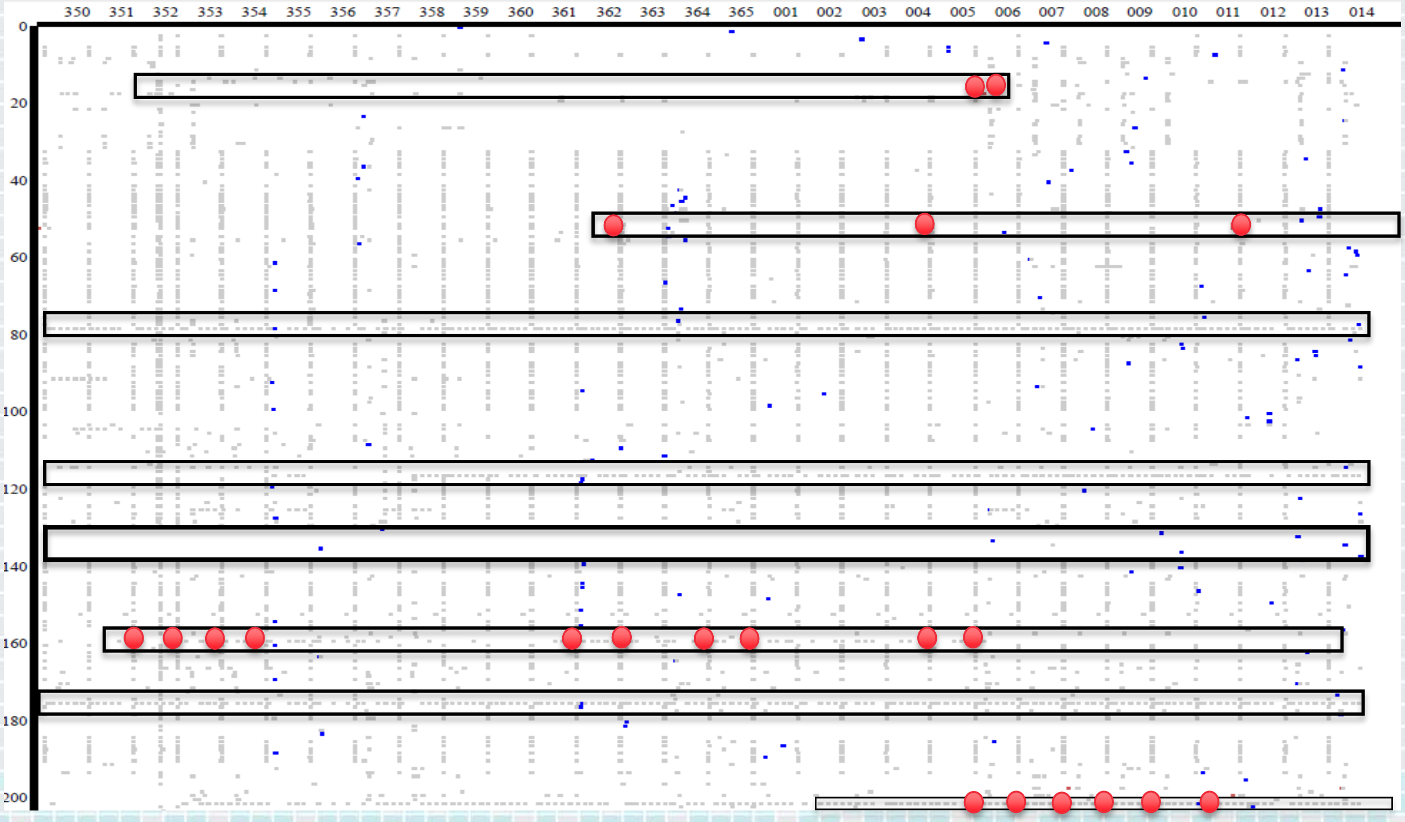
🟥 Infections

*Programming by David_Ewall@radius180.com

Proof of Concept: Endpoint Product 2

X-Axis = Date

Y-Axis = Hosts



⬜ Virus Def Update

🟦 Check in Time

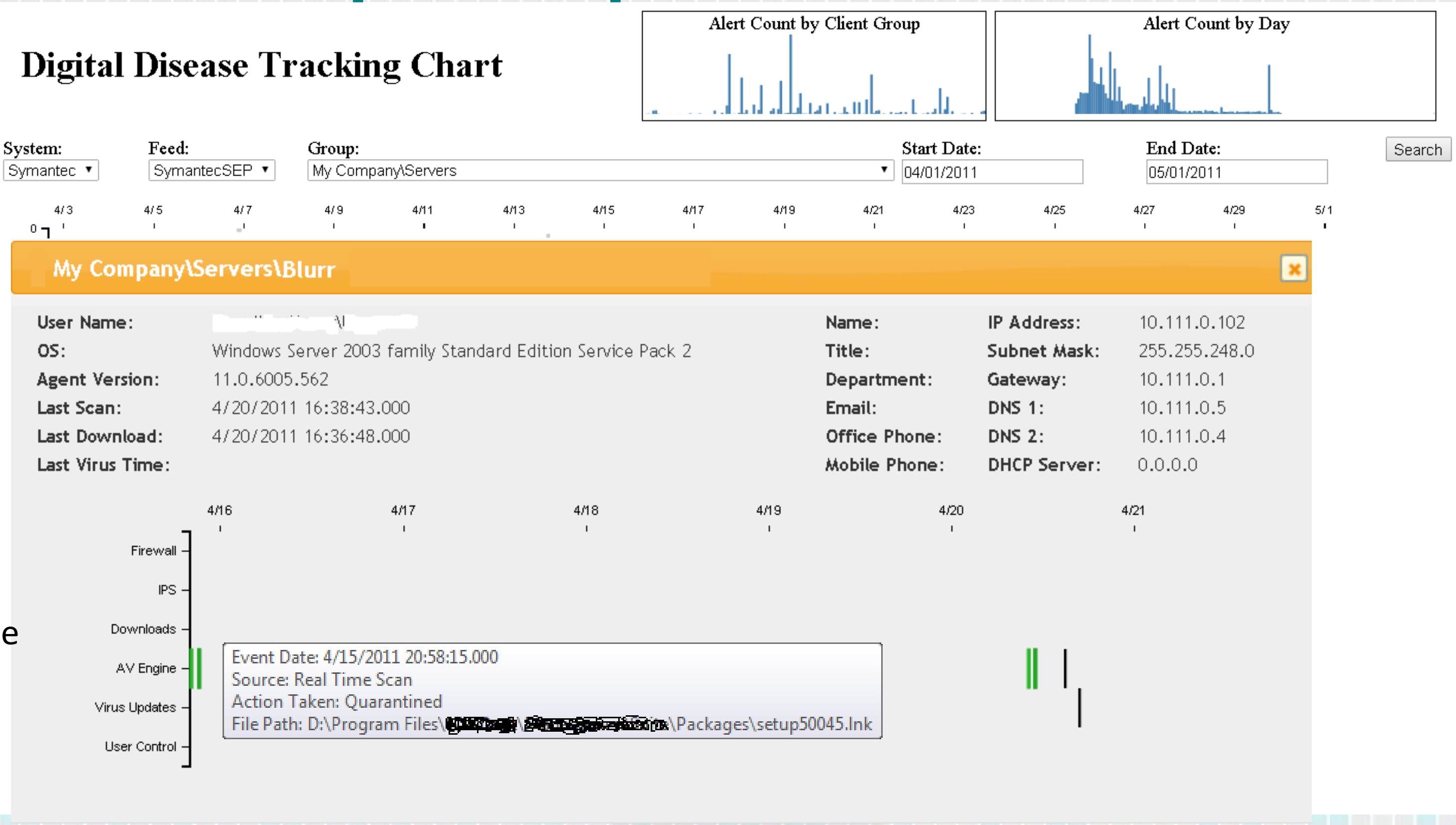
🟥 Infections

*Programming by David_Ewall@radius180.com

Proof of Concept: Endpoint Product 3

X-Axis = Date

Y-Axis = Hosts



Digital Disease Tracking Chart

System: Symantec

Feed: SymantecSEP

Group: My Company\Servers

Start Date: 04/01/2011

End Date: 05/01/2011

Search

My Company\Servers\Blurr

User Name:	[redacted]	Name:	IP Address:	10.111.0.102
OS:	Windows Server 2003 family Standard Edition Service Pack 2	Title:	Subnet Mask:	255.255.248.0
Agent Version:	11.0.6005.562	Department:	Gateway:	10.111.0.1
Last Scan:	4/20/2011 16:38:43.000	Email:	DNS 1:	10.111.0.5
Last Download:	4/20/2011 16:36:48.000	Office Phone:	DNS 2:	10.111.0.4
Last Virus Time:		Mobile Phone:	DHCP Server:	0.0.0.0

Event Date: 4/15/2011 20:58:15.000
Source: Real Time Scan
Action Taken: Quarantined
File Path: D:\Program Files\[redacted]\[redacted]\Packages\setup50045.lnk

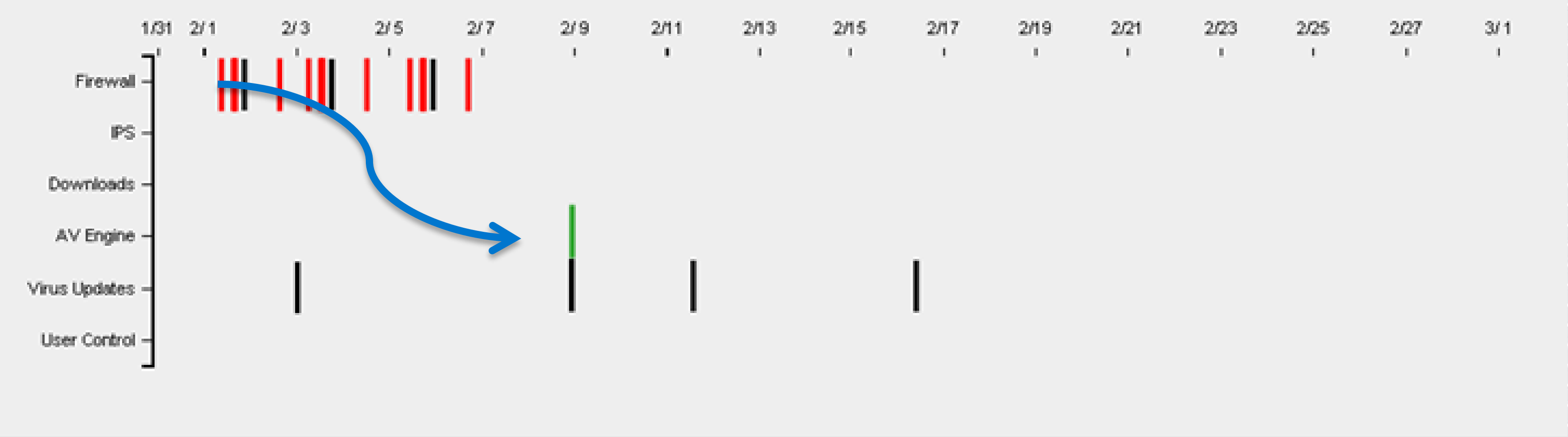
⬜ Virus Def Update

🟦 Check in Time

🟥 Infections

Programming by David_Ewall@radius180.com

Possible Network Borne Digital Disease Pathogen

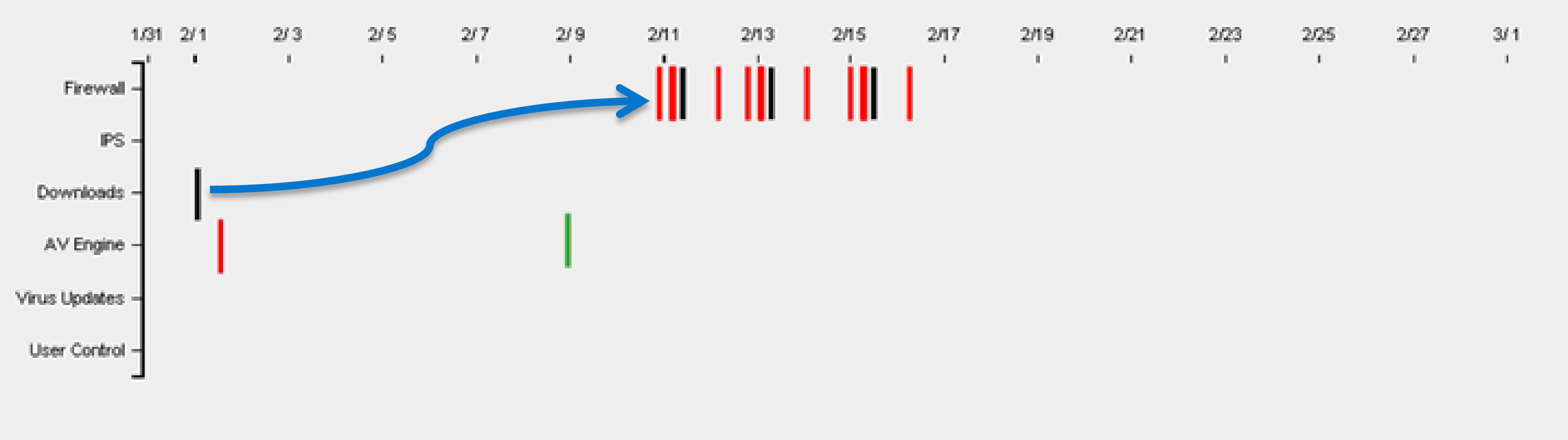


🟩 Threat Detected but stopped

■ Informational

🟥 Violation or Failed to Stop

Possible Download Borne Digital Disease Pathogen

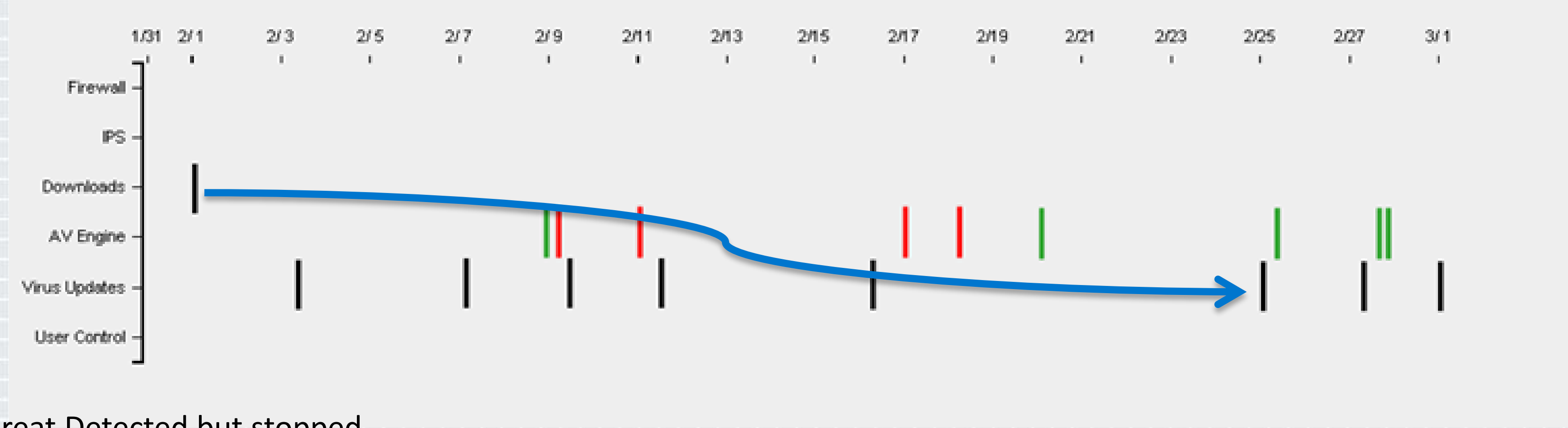


🟩 Threat Detected but stopped

⬛ Informational

🟥 Violation or Failed to Stop

Possible Downloader Borne Digital Disease Pathogen

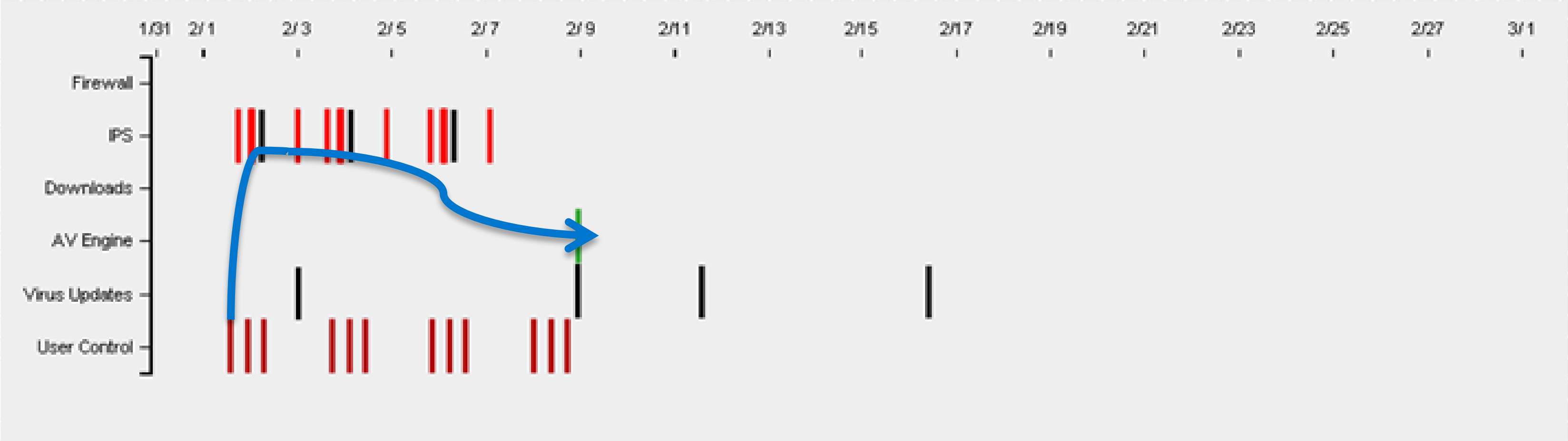


🟩 Threat Detected but stopped

⬛ Informational

🟥 Violation or Failed to Stop

Possible USB Borne Digital Disease Pathogen



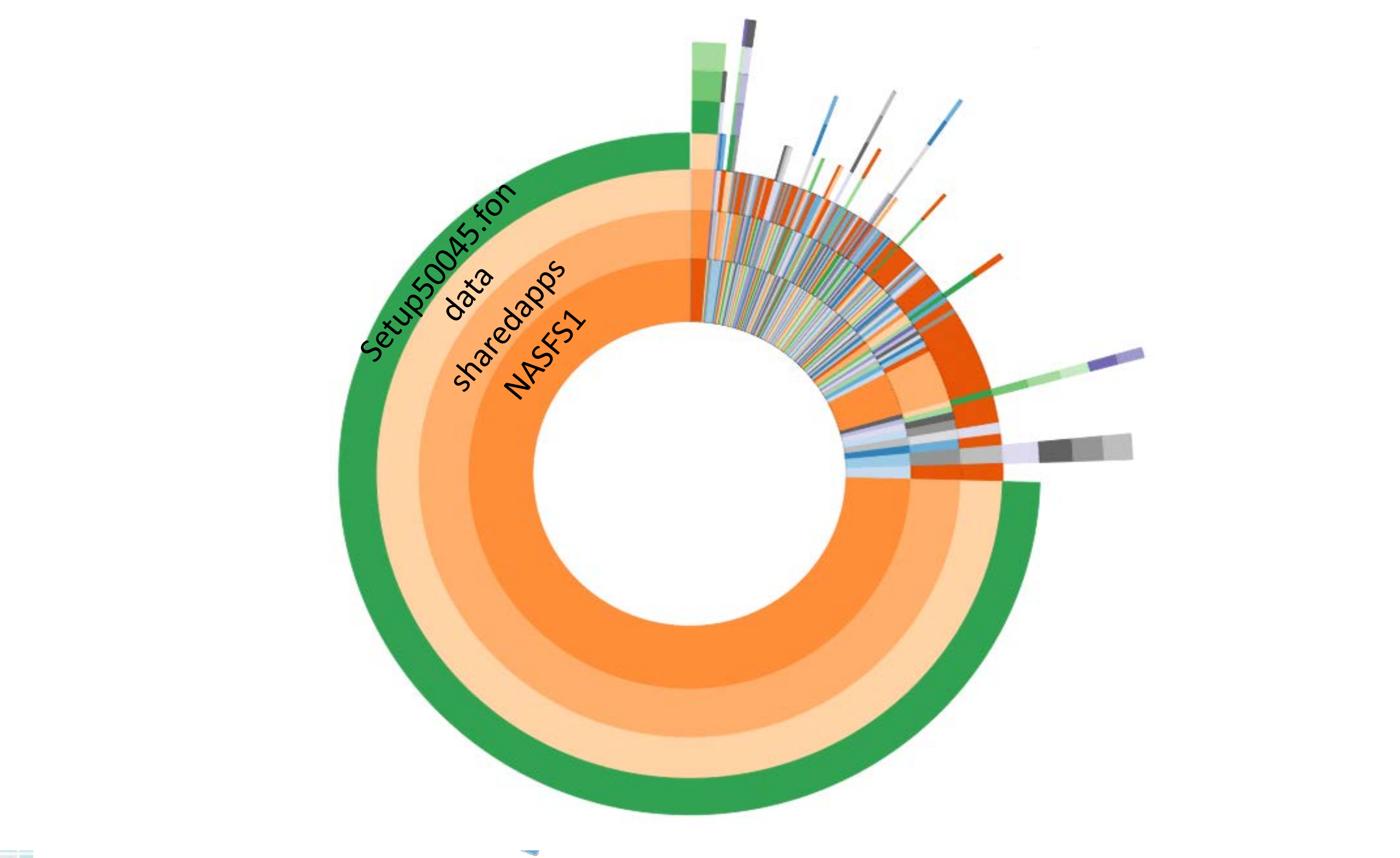
🟩 Threat Detected but stopped

⬛ Informational

🟥 Violation or Failed to Stop

🟫 Policy Violation

NAS Borne Infections Visualization



Summary

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

Existing Literature on Epidemiology and Security

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

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:
  - Commence routine surveying of endpoint data in your environment using epidemiological survey techniques.

RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: MASH-R03

Q&A

Efrain Ortiz

Director, Market and Technology Innovation Group
Efrain_Ortiz@Symantec.com
@ortizonline