HALL & WILCOX

THE 15 CYBER SECURITY LEADERSHIP QUESTIONS

3 NOVEMBER 2016

BENJAMIN MOSSÉ

Chief Executive Officer

MOSSÉ SECURITY
THREAT MATTERS

CYBER SECURITY INTRODUCTION

MOSSÉ SECURITY
THREAT MATTERS

Current State of Cyber Security

- Cyber (in)security has become an integral instrument of power for:
  - Criminals
  - Terrorists
  - Governments
  - Activists
  - Disgruntled Employees
- 2013: Europol announced that cyber crime was now more profitable than the drug trade.

For the most part, organisations are ill prepared to prevent, detect and respond to cyber attack.

Indicators of Insecurity

Industry Statistics	
+80%	Organisations have unknown threat actors on their networks
227	Number of days threats go undetected
20-30	Number of days it takes to remove an attacker from the network
80%	Think that cyber security is an IT issue
40-50%	**Organisations are not confident in their ability to detect a breach *at all*.**

Underground Market for Identities

Store History

Logged in as

You can use on paypal credit, prepaid cards etc. After buying try to search by address and u can see children, wife and all people at this address It's great for tax return method, because u can get $$$ for "your" children

Fill your query Search

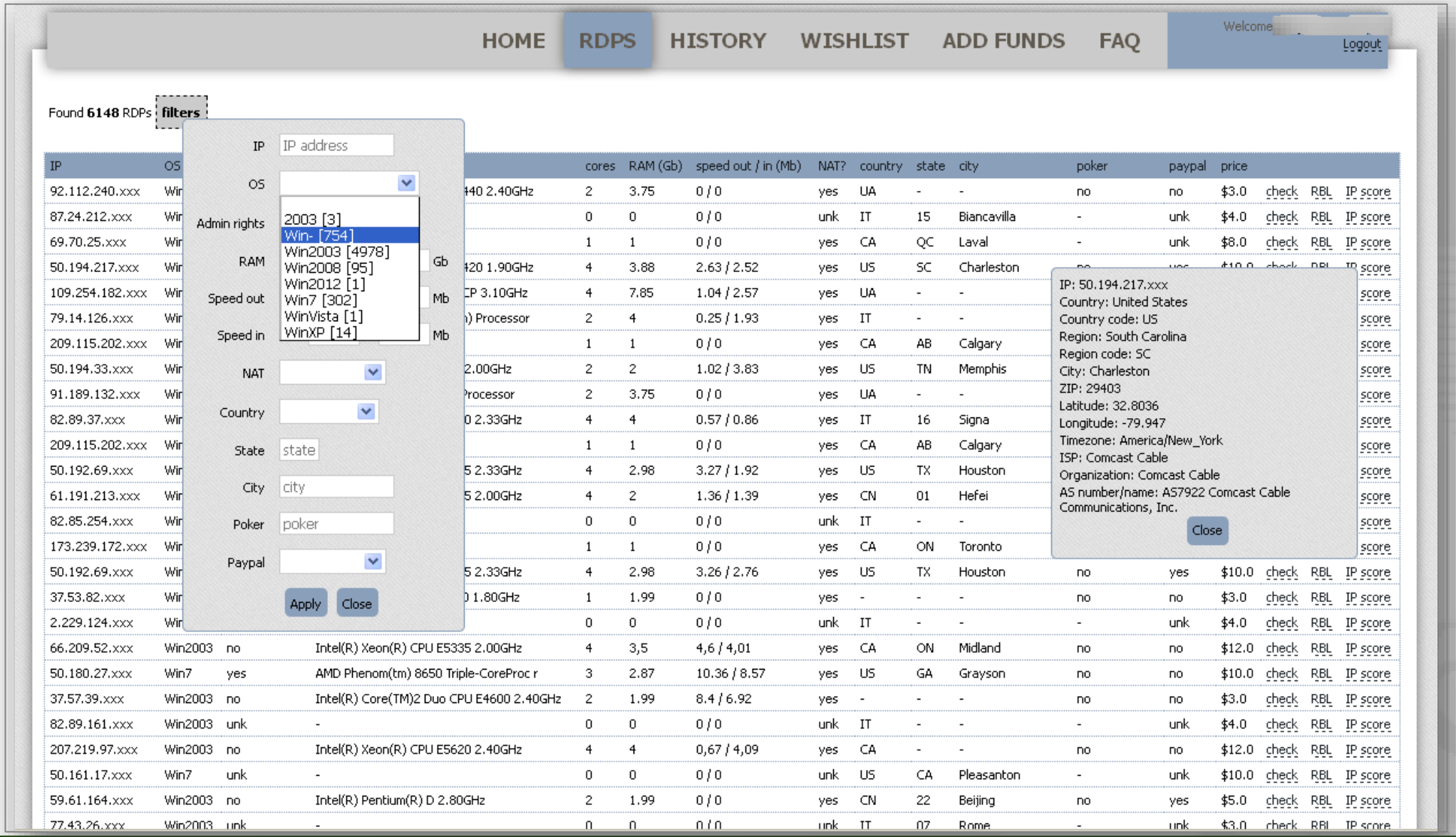
#	First Name	Last Name	State	Zip Code	DOB	Select ?
16	Rickey	B	TX	75602	7/14/	☐
25	Timothy Jr	L	None	66442	5/26/	☐
26	Kimber	L	None	66442	7/14	☐
67	Bryton	G	IL	62858	07.08	☐
68	Rylie	N	IL	62858	12.	☐
81	Lola Juanita	D	None	62854	11/	☐
85	Jamie	Du	Il	62846	01.	☐
96	James Nolan	F	IL	62839	9/	☐
98	Margaret M	Ch	IL	62838	01	☐
101	Amanda	Ph	IL	62838	01.0	☐
107	Clarence	H	IL	62824	08.0	☐
108	Charles	H	IL	62824	01.0	☐
117	Elinor	S	IL	62824	11/24/	☐
120	Casey	B	IL	62704	08.12.	☐
122	IBCCP	Log	IL	62656	11	☐

1 2 3 4 5 ... 786 787

Buy Selected

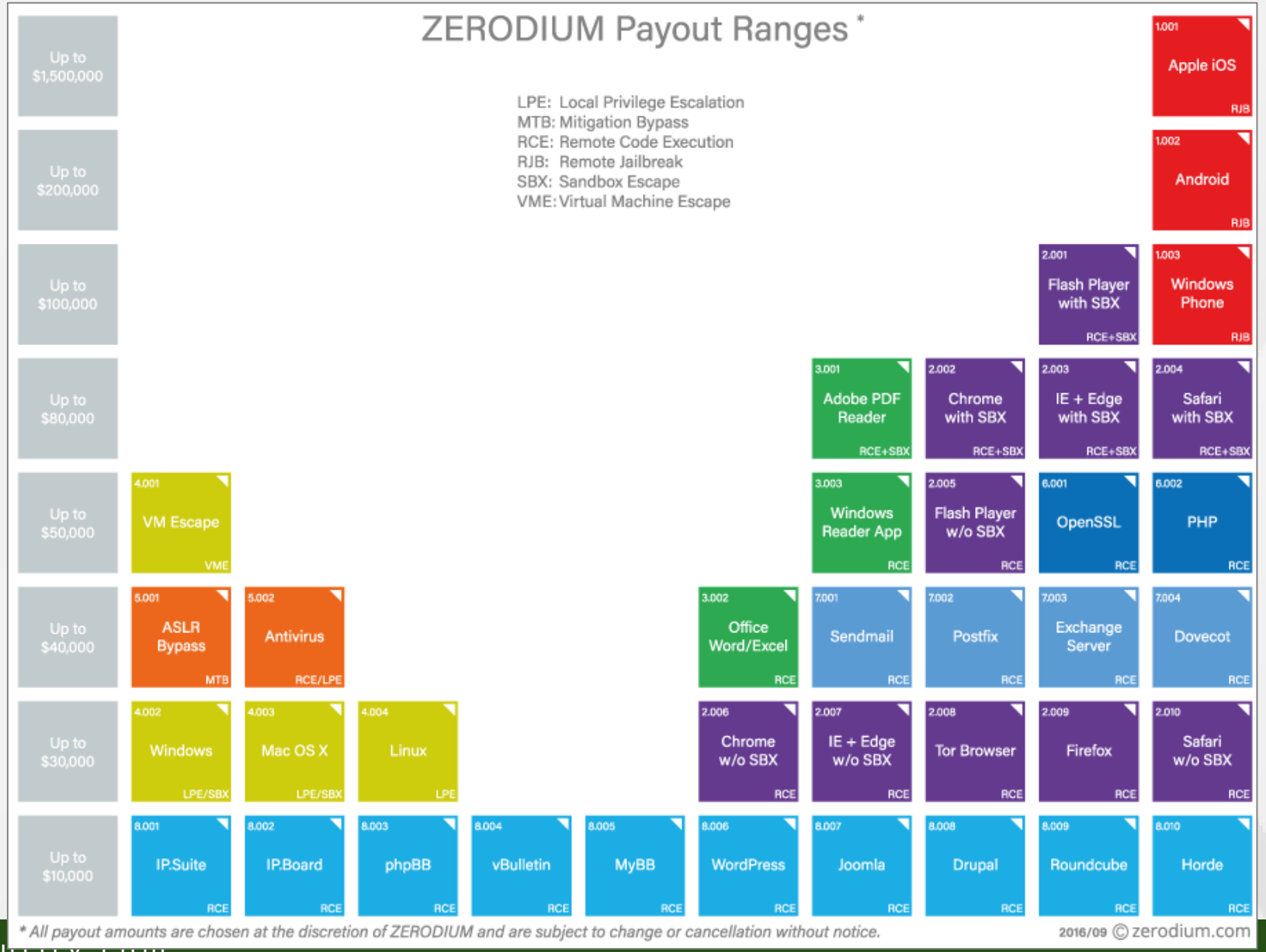
Select All

Buying Compromised Machines



IP	OS			cores	RAM (Gb)	speed out / in (Mb)	NAT?	country	state	city	poker	paypal	price			
92.112.240.xxx	Wir		440 2.40GHz	2	3.75	0 / 0	yes	UA	-	-	no	no	$3.0	check	RBL	IP score
87.24.212.xxx	Wir			0	0	0 / 0	unk	IT	15	Biancavilla	-	unk	$4.0	check	RBL	IP score
69.70.25.xxx	Wir			1	1	0 / 0	yes	CA	QC	Laval	-	unk	$8.0	check	RBL	IP score
50.194.217.xxx	Wir		420 1.90GHz	4	3.88	2.63 / 2.52	yes	US	SC	Charleston						IP score
109.254.182.xxx	Wir		CP 3.10GHz	4	7.85	1.04 / 2.57	yes	UA	-	-						score
79.14.126.xxx	Wir		) Processor	2	4	0.25 / 1.93	yes	IT	-	-						score
209.115.202.xxx	Wir			1	1	0 / 0	yes	CA	AB	Calgary						score
50.194.33.xxx	Wir		2.00GHz	2	2	1.02 / 3.83	yes	US	TN	Memphis						score
91.189.132.xxx	Wir		Processor	2	3.75	0 / 0	yes	UA	-	-						score
82.89.37.xxx	Wir		0 2.33GHz	4	4	0.57 / 0.86	yes	IT	16	Signa						score
209.115.202.xxx	Wir			1	1	0 / 0	yes	CA	AB	Calgary						score
50.192.69.xxx	Wir		5 2.33GHz	4	2.98	3.27 / 1.92	yes	US	TX	Houston						score
61.191.213.xxx	Wir		5 2.00GHz	4	2	1.36 / 1.39	yes	CN	01	Hefei						score
82.85.254.xxx	Wir			0	0	0 / 0	unk	IT	-	-						score
173.239.172.xxx	Wir			1	1	0 / 0	yes	CA	ON	Toronto						score
50.192.69.xxx	Wir		5 2.33GHz	4	2.98	3.26 / 2.76	yes	US	TX	Houston	no	yes	$10.0	check	RBL	IP score
37.53.82.xxx	Wir		0 1.80GHz	1	1.99	0 / 0	yes	-	-	-	no	no	$3.0	check	RBL	IP score
2.229.124.xxx	Wir			0	0	0 / 0	unk	IT	-	-	-	unk	$4.0	check	RBL	IP score
66.209.52.xxx	Win2003	no	Intel(R) Xeon(R) CPU E5335 2.00GHz	4	3,5	4,6 / 4,01	yes	CA	ON	Midland	no	no	$12.0	check	RBL	IP score
50.180.27.xxx	Win7	yes	AMD Phenom(tm) 8650 Triple-CoreProc r	3	2.87	10.36 / 8.57	yes	US	GA	Grayson	no	no	$10.0	check	RBL	IP score
37.57.39.xxx	Win2003	no	Intel(R) Core(TM)2 Duo CPU E4600 2.40GHz	2	1.99	8.4 / 6.92	yes	-	-	-	no	no	$3.0	check	RBL	IP score
82.89.161.xxx	Win2003	unk	-	0	0	0 / 0	unk	IT	-	-	-	unk	$4.0	check	RBL	IP score
207.219.97.xxx	Win2003	no	Intel(R) Xeon(R) CPU E5620 2.40GHz	4	4	0,67 / 4,09	yes	CA	-	-	no	no	$12.0	check	RBL	IP score
50.161.17.xxx	Win7	unk	-	0	0	0 / 0	unk	US	CA	Pleasanton	-	unk	$10.0	check	RBL	IP score
59.61.164.xxx	Win2003	no	Intel(R) Pentium(R) D 2.80GHz	2	1.99	0 / 0	yes	CN	22	Beijing	no	yes	$5.0	check	RBL	IP score
77.43.26.xxx	Win2003	unk	-	0	0	0 / 0	unk	IT	07	Rome	-	unk	$3.0	check	RBL	IP score

Buying and Selling Software Vulnerabilities



The Two Primary Mistakes

Too much technology, not enough people

No Data

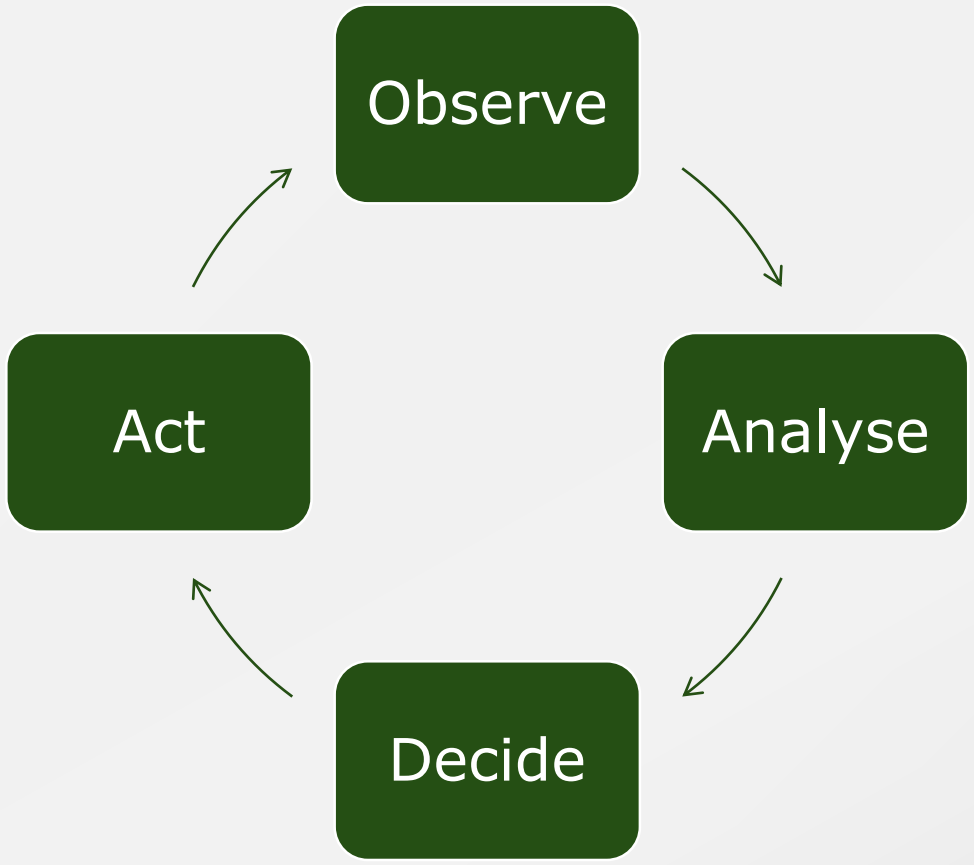
=

No Proof

Solution 1: The Culture of Learning

- Security investment philosophy that focuses on People
- "IT security starts with every person in the organisation"
- Train every person in the company on:
  - How they might be attacked
  - Practical tactics to defend themselves
  - Detecting and reporting attacks
  - Working as a team to protect themselves and your organisation

Solution 2: Data-Driven Security



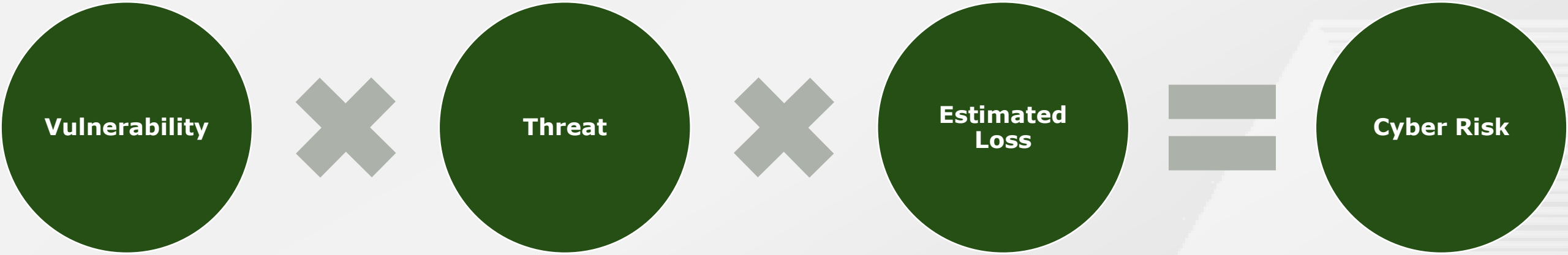
Stage	Action
Observe	• New vulnerabilities • Intrusions and breaches • Ongoing security testing
Analyse	Assess the effectiveness of current defences
Decide	Devise what the best approach is to improve defences
Act	Fine tune current security controls, and implement new ones (if necessary)

Focus on small, incremental, and rapid improvements.

15 CYBER SECURITY LEADERSHIP QUESTIONS

MOSSÉ SECURITY
THREAT MATTERS

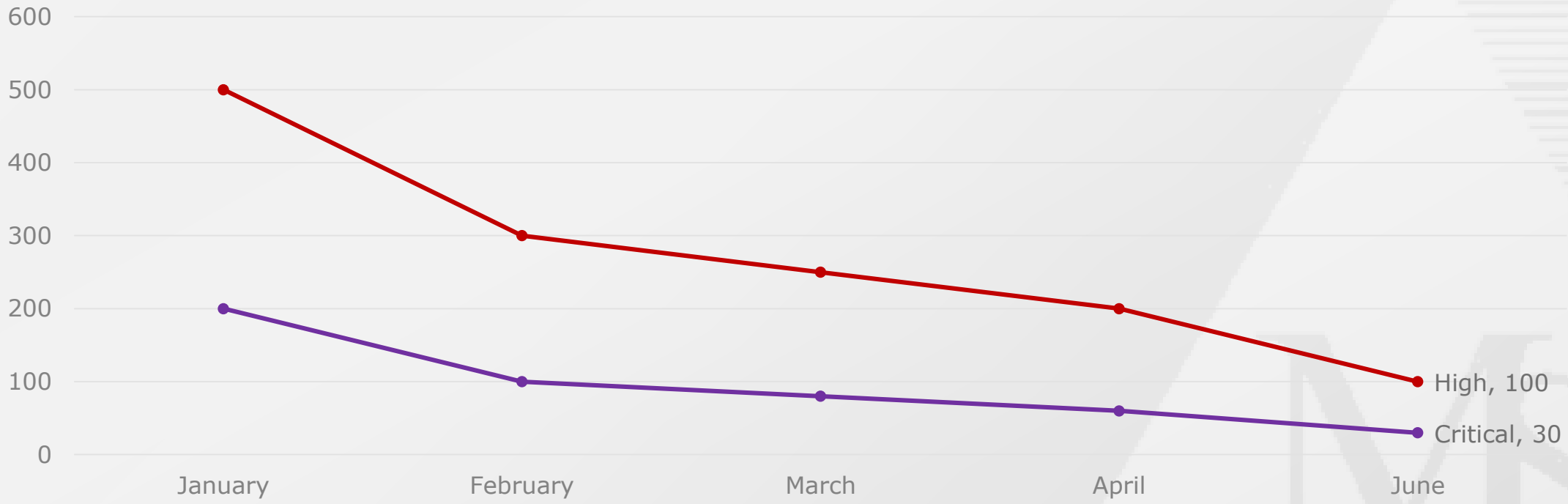
Cyber Risks 101



CYBER RISK is
Your most critical vulnerabilities, exploited by your greatest adversaries, in the worst case scenario possible.

Rule 1: Manage Your Vulnerabilities

- How many critical and high risk vulnerabilities do we have today?
- How many vulnerabilities can we mitigate in the next 90 days?
- What resources are required to fix those vulnerabilities? (Calculate in dollars)



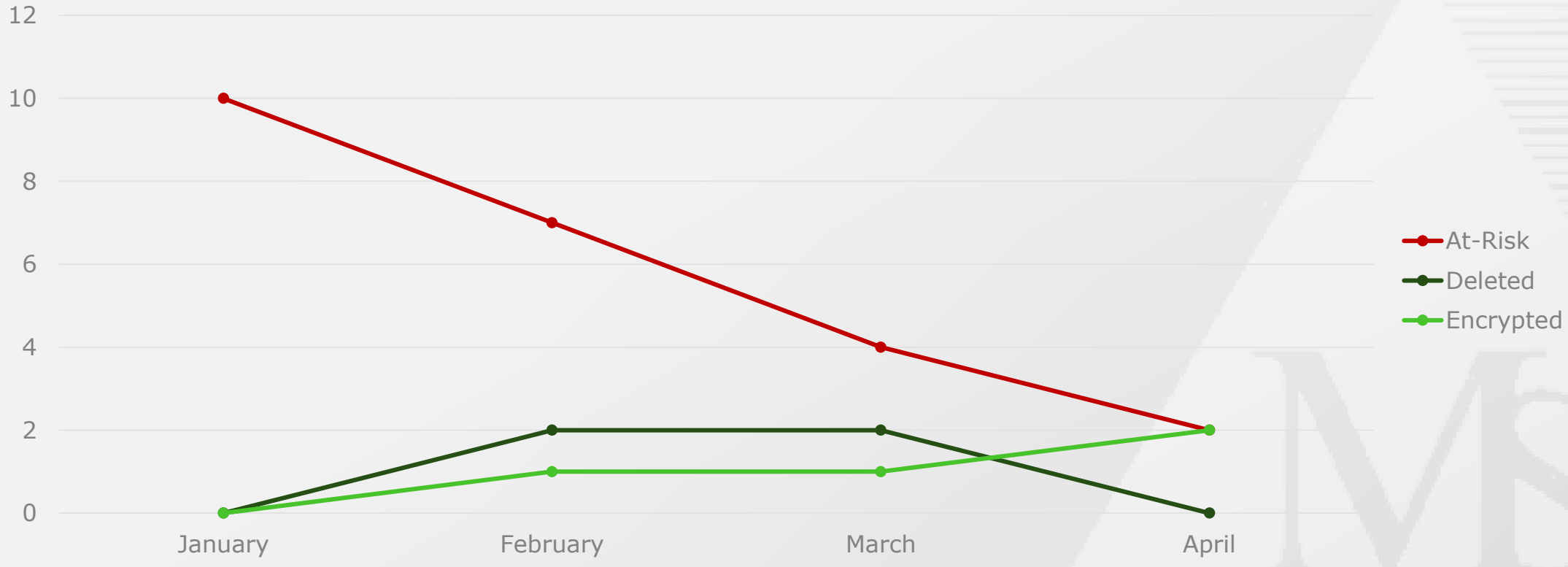
Rule 2: Disrupt Your Enemies

- How many threat actors breached into our network in the last 90 days?
- For each intrusion, what risks were we exposed to? (Calculate in dollars)
- How much time did it take us to detect the intrusions and recover?
- What resources are required to prevent the attackers from coming back?

Metrics	Current Status	Goals
Number of intrusions	+10	Less than 3
Skill level used to breached in	Basic techniques	Complex techniques
Detection time	227 days	Less than 10 days
Response time	25 days	Less than 48 hours
Impact generated / Value stolen	$250,000.00 AUD and above	Less than $10,000.00 AUD

Rule 3: Limit Your Exposure

- How much data at risk do we have today?
- How much data can we safely remove in the next 90 days?
- How much data can we safely encrypt and archive in the next 90 days?



Rule 4: Making Sure The Plan's Solid

	Question
Cost Saving	How are we leveraging our existing investments to solve today's challenges?
Data Driven	How are we going to measure the effectiveness this round of investment?
Long Term	How are we making sure this round investment will continue to yield results in 12 months?
Feasible	How do we know if we have people with the right knowledge to implement the plan?
Backup Plan	How will we address things if we find we're off track?

Goals

Achieve those goals within 12 to 24 months:

- Train 100% of your staff members on cyber security
- Review 100% of your network for active or dormant threat actors
- Remove or encrypt 70% of your data
- Stop and detect the top 200 tactics and techniques employed by attackers
- Patch 80% of all your critical and high risk missing security patches

CONCLUSION

MOSSÉ SECURITY
THREAT MATTERS

Conclusion

- Commit to becoming a Cyber Security Champion
- Progress in small steps
- Implement a feedback loop to monitor your progress
- Use the 15 Cyber Security Leadership Questions
- Investment ratio should be:
  - People: 40%
  - Process: 30%
  - Technology: 20%

CONTACT US

Benjamin Mossé

Chief Executive Officer

Mossé Security

Mossé Cyber Security Institute

1300 730 035

contact@mosse-security.com

MOSSÉ SECURITY
THREAT MATTERS