STEPHEN OWEN

https://www.linkedin.com/in/stephen-owen-data-protection/

2023

What's our Annual Lost Expoure and probability of occurrence of these threats reaching and exploiting our asset?

CHIEF RISK OFFICER

Please demonstrate Return on Investment !

CHIEF FINANCE OFFICER

Ability to demonstrate request for resources in line with business risk tolerance.

CHIEF SECURITY OFFICER

Focus resources on use cases for TTP early in attack chain.

HEAD OF SOC

What governance and efficacy are the controls?

HEAD OF AUDIT

Are controls proportinate to risk?

DATA PROTECTION OFFICER

ARE WE SAFE?

Is it safe?

How good are they to inflict pain?

PYRAMID OF PAIN

Threat capability

Help prioritise efforts

'TEACH'

Travis Smith

(GitHub project no longer maintained)

Separating Techniques

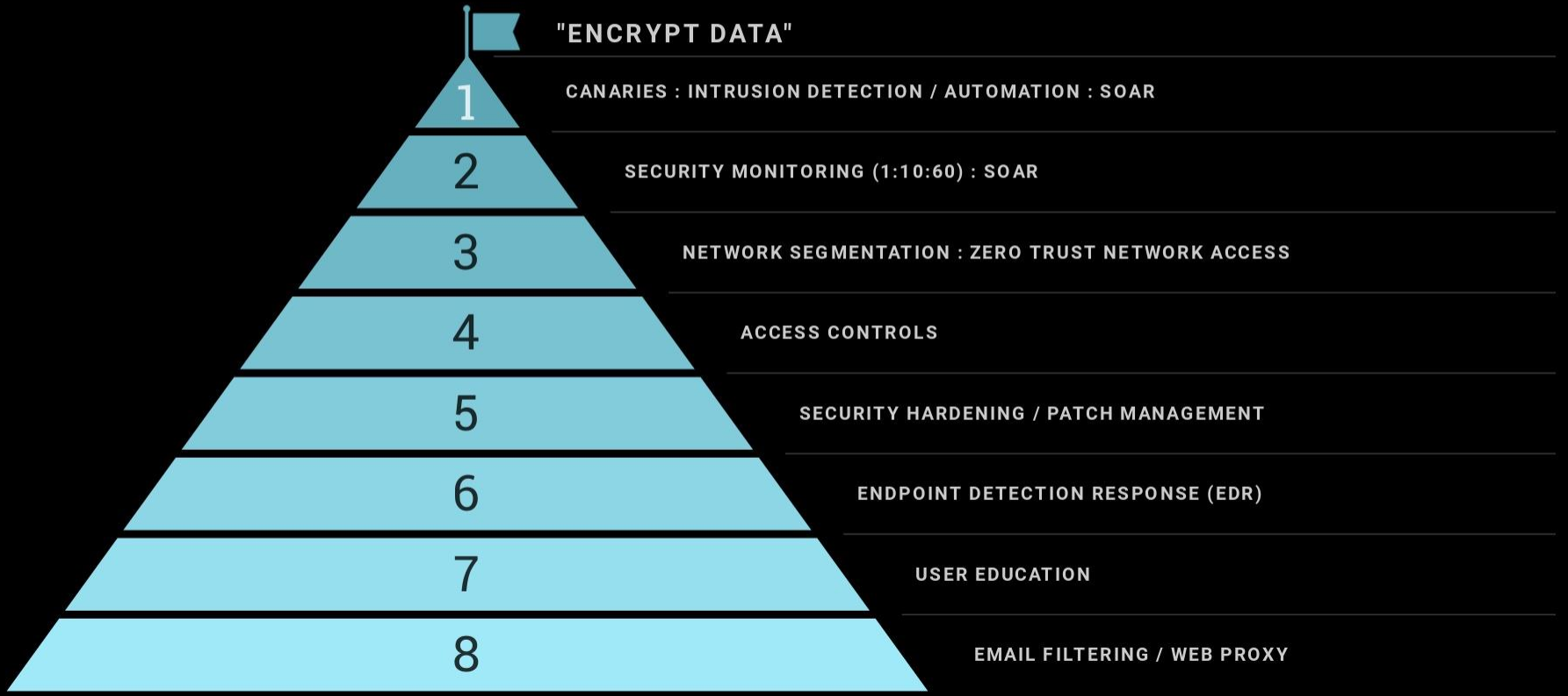
Categories

T	Techniques Only	• Not really an exploit • Requires the use of other techniques to be truly viable • Example – Graphical User Interface
E	Exploitable to Anyone	• Easy to exploit (my mom could probably do it) • No need for POC malware, scripts, or other tools • Example – Accessibility Features
A	Additional Steps Required	• Need some sort of tooling such as Metasploit or POC scripts • Could be more advanced than those found in green • Example – Exploitation for *
C	Cost Prohibitive	• Requires additional infrastructure to be able to exploit • Some are quite easy, some can be more advanced. • Example – Web Shell
H	Hard	• Might require custom DLL/EXE • In-Depth Understanding of the OS

What's your resistance...

Resistance layers

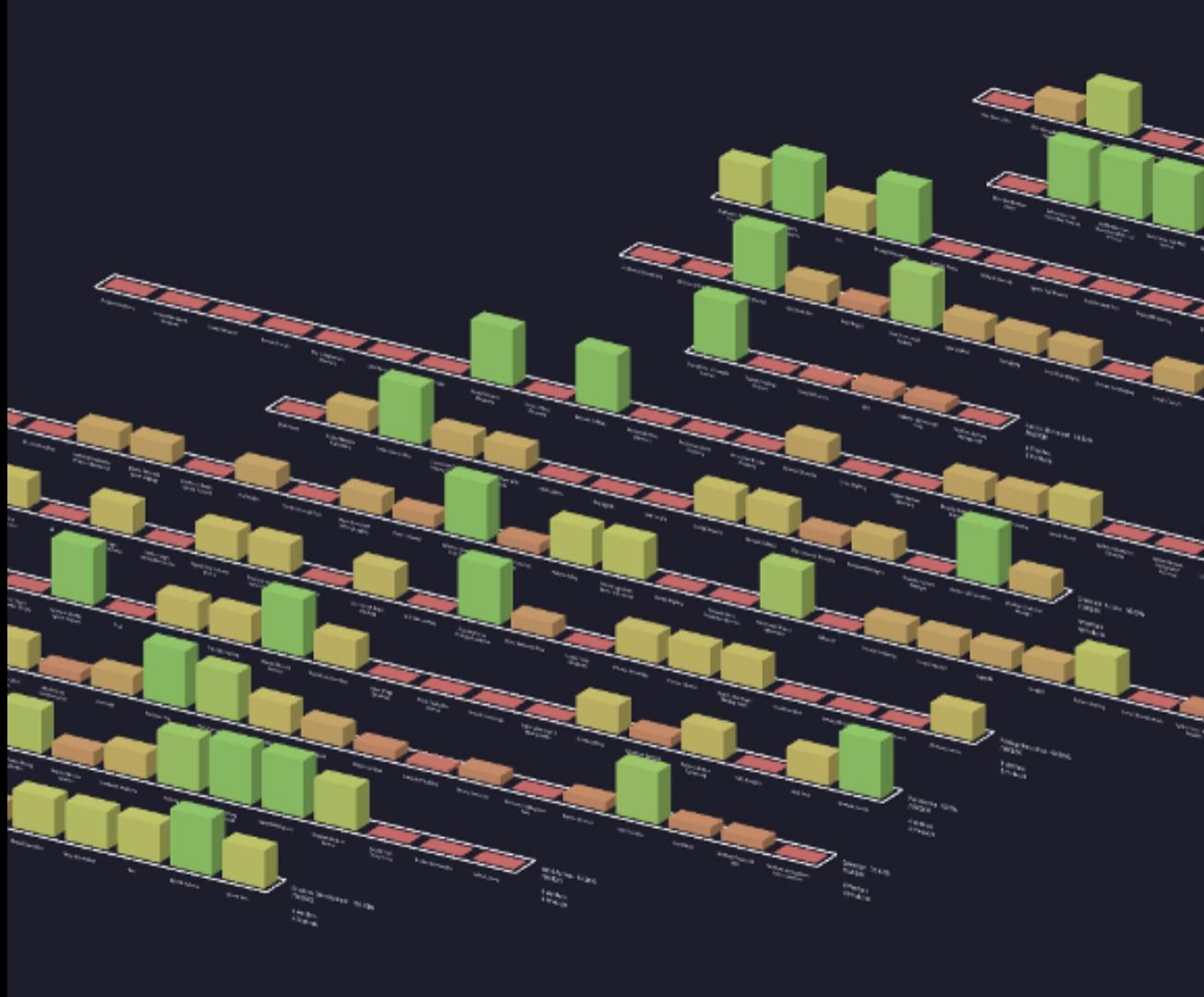
Example Ransomware defence in depth layers



Extract from ESProfiler

FOCUSED THREAT GROUPS

Behaviour against Mitre Att&ck TTP's

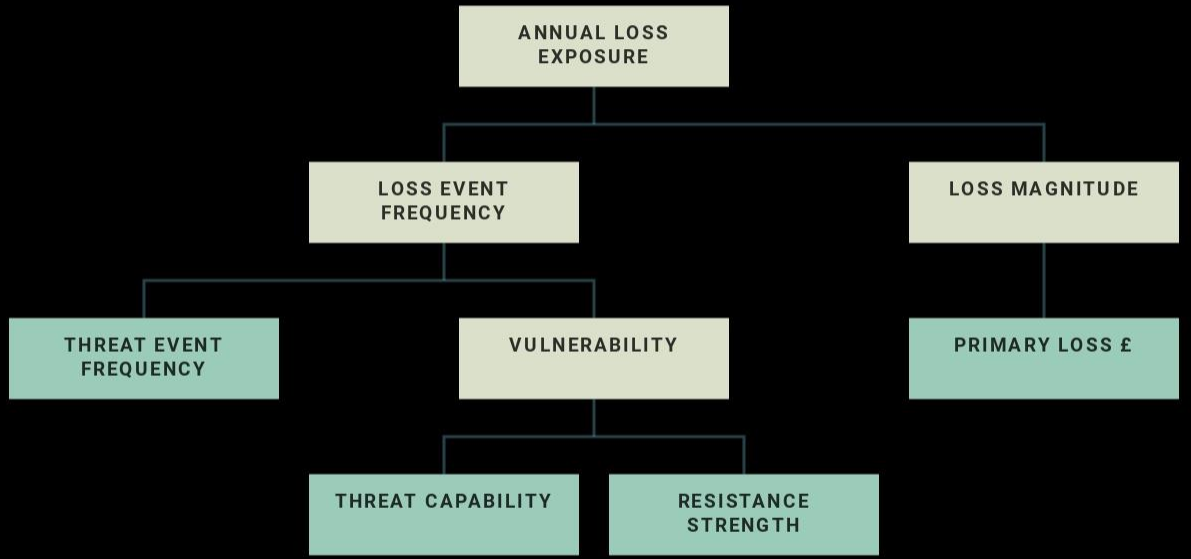


Resistance to attack group

Layer	Range	Min	Most Likely	Max
Canaries : Intrusion Detection / Automation : SOAR	0 - 5%	0	1	2
Security Monitoring (1:10:60) : SOAR	0 -10%	0	5	7
Network segmentation : Zero Trust Network Access	0 - 5%	0	0	1
Access controls	0 - 5%	0	1	2
Security hardening / patch management	0 - 30%	15	18	21
Endpoint detection response (EDR)	0 - 20%	14	16	18
User education	0 - 10%	5	6	7
Email filtering	0 - 15%	7	9	11
	100%	41%	56%	69%

Plug values into model.....

Factor Analysis of Information Risk (FAIR) Quantitative Model



Risk scenario

RANSOMWARE

Business impact

RANSOMWARE ATTACK BY CYBER CRIMINALS CAN LEAD TO LONG TERM UNAVAILABILITY OF IT INFRASTRUCTURE.

THERE IS A 38% PROBABILITY OF LOSSES GREATER THAN £7.6M WITHIN THE NEXT 12 MONTHS DUE TO RANSOMWARE; 1 IN 2.6-YEAR EVENT.

Risk summary

TYPICALLY, RANSOMWARE ATTACKS ARE DELIVERED VIA PHISHING EMAILS WHICH UNCHECKED CAN PROLIFERATE ACROSS IT NETWORKS AND ENCRYPT ASSETS AND DENY TO CORE BUSINESS APPLICATIONS. HISTORICALLY RANSOM DEMAND IS MUCH LOWER COST THAN LOSS OF DOWNTIME (WEEKS - MONTHS).

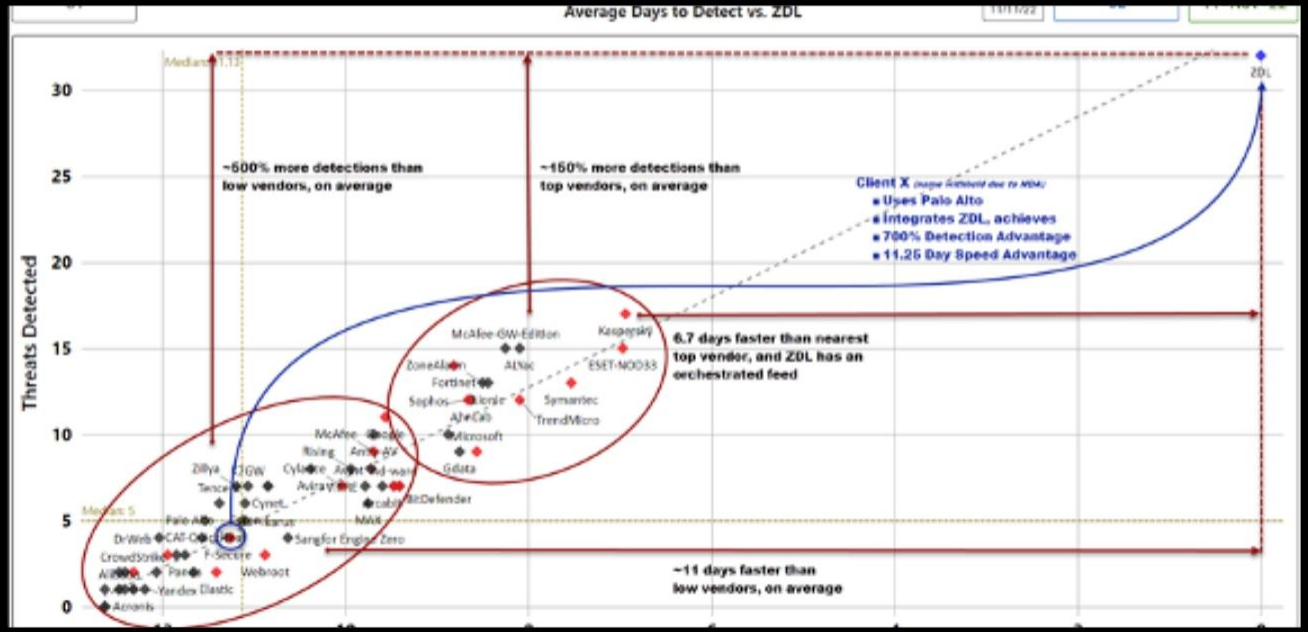
Questions?

Appendix

Venture if you dare !

Extract from Blackwired Threat Intelligence data platform

Threat Intelligence feeds - All are not equal!



THREAT INTELLIGENCE FEEDS MAY INCREASE RESISTANCE ACROSS MULTIPLE LAYERS OF DEFENCE WITH A GOOD RETURN ON INVESTMENT

What improves Resistance?

PEOPLE TRAINING

ENRICH WITH THREAT INTELLIGENCE

FEEDBACK FROM CONTROL FAILURE

METRICS (KRI/KPI) FROM CONTROL

FREQUENCY OF CONFIGURATION REVIEW

RED TEAM TESTING OF CONTROL

INTRODUCTION OR CHANGE OF CONTROL

KISS

Resistance influence	Weight	Simple	Example of control efficacy"Most Likely"
People training on control	10%	CMMI	Level 3 - Defined = 6%
Metrics (KRI/KPI) from control	5%	CMMI	Level 1 - Initial: Processes are ad hoc = 0%
RED team testing of control	10%	CMMI	Level 5 - Optimizing = 8%
Enriched with threat intelligence	8%	Optional	Level 3 - Defined = 4.8%
Frequency of Configuration review with vendor	7%	CMMI	Level 4 - Quantitatively Managed = 5.6%
Maturity of CIS Critical Security Controls (CIS Controls) mapped against control area	10%	CMMI/NIST CSF	Level 4 - Quantitatively Managed = 8%
Control efficacy against TTP/Threat	50%	ESProfiler	35%
	100%		67.40%