EDR/XDR

Intro for CISO Alliance chapter meeting

BACKGROUND

McAfee, Symantec, Microsoft, Trend, Cybereason, CrowdStrike

Challenges

- Diversity of products
- Features now vs roadmap
- Support for diverse environment
- Dependence on internal skills we may not universally have
- Integration of service capability
- Ability to identify and deal with sophisticated attackers
- Tick box with all the “cool” features vs what really counts
- Rapid changes in network topology (WFH/WFA)

CONSIDERATIONS

- Size of estate
- Diversity of estate (Windows vs Solaris vs AIX vs Linux etc)
- Need to support outdated assets (OS and agents going EOL)
- Levels of function (RFM)
- Managed detection vs response vs eviction
- Roles and responsibilities (maintenance of agents)
- SLAs
- Classification of assets (and permission to act)
- Reporting and customization
- Tenanting and hierarchy
- Triage after detection
- Incident response
- Nation state capability

CONSIDERATIONS

- Integrations
  - To SOC and development of use cases
  - To service management platform
- Organization / divisions ability to deal with volume of detection on a timely basis (Classification)
- Cloud hosting (USA vs EU vs Other)
- Threat hunting and Threat Intelligence
- Detection of nearby undefended hosts (complicated by WFH)
- Organization appetite to Isolate hosts

Confidential : CrowdStrike Falcon Complete | Current State

Node Count post eviction (May ‘21) : 28 578
Current Node Count (EU) : 31 181
License Allocation : 32 087

We continue to onboard additional devices identified through Falcon's Discover feature which identifies neighbouring nodes without CrowdStrike

4/100

CrowdScore

CrowdScore is a cloud-based analytics and AI feature of CrowdStrike that provides CxOs with a single view of an organisation’s threat exposure and ability to detect and prevent threats aligned to the 1-10-60 rule. CrowdScore is ranked on a scale of 0-100. The higher the CrowdScore, the greater the risk exposure*. CrowdScore as @ March ‘21 was 87/100

*https://crowdstrike.wistia.com/medias/n2x7ld83sd

Posture	Description	Node Count
Active	All remediation actions without Organisation intervention	20551 (66%)
Measured	All non-disruptive remediation actions without Organisation intervention	10331 (33%)
Cautious	Remediation requires Organisation intervention	307 (<1%)

- >99% of nodes are able to be remediated without Organisation intervention

Incident/Detection Count – Week 40	Total	New	In-Progress	Remediated by Falcon Complete
CrowdStrike Falcon Detections (Endpoint Protection and Response Technology)	**1,956**	1,057	7	**892**
CrowdStrike Overwatch (Threat Hunting Incidents)	**11**	2	0	**9**
Escalated Incidents (by CS requiring Organisation Intervention Cautious/Measured)	**25**	0	4	**21**

- There has been a significant improvement (+- 80%) in reducing the number of detections per week since the service was commissioned

Region	# Current EU Cloud Node Count	# Nodes in RFM
MENA		
xxxxxxx	882	87
xxxxxxx	771	70
SEA		
xxxxxxx	30	0
xxxxxxx	443	10
xxxxxxx	78	6
xxxxxxx	572	130
xxxxxxx	12,060	171
xxxxxxx	124	11
xxxxxxx	1,981	100
xxxxxxx	605	11
xxxxxxx	62	4
WECA		
xxxxxxx	1,010	248
xxxxxxx	1,691	103
xxxxxxx	3,043	57
xxxxxxx	1,076	23
xxxxxxx	216	58
xxxxxxx	247	19
xxxxxxx	297	2
xxxxxxx	598	8
xxxxxxx	4,996	55
N/A Sensor Tags	344	40
3rd Party Service Providers	56	1
Grand Total	**31,181**	**1214**

RFM (Reduced Functionality Mode or safe mode) is a Falcon agent safety feature that occurs when the agent is unable to identify or does not support the system kernel (regardless if the OS is supported)

Data @14/10/21