**Palo Alto Training**

NGFW

Prevention ( ngăn chặn )

Endpoint : 3 huong lam

* Tao bo chu ky ( malware …) tao bo AV
* Detection and Respond
* Ngan chan

Mo hinh tam giac bao mat Palo Alto

* Wildfire ( cloud )
* NGFW ( network)
* Endpoint protection

Yeu cau 1: co the su dung dich vu tren mang mot cach an toan

User - > Application ->Content

Design rule Palo Alto : Define by Appplication

Palo Alto co dich vu danh gia Rule firewall cho users

TCP port -> Application

Note : Default enable check Application ( App ID )

Policy by Users ( Users ID )

User ID + App ID

Check SSL Decryption

Yeu cau 2 : Tap trung ngan chan cac hiem hoa

Tuong minh – Giam thieu nguy co – Ngan chan hiem hoa da biet – Ngan chan hiem hoa chua biet

* Tuong minh :

Decryption SSL theo 2 chieu

Define User ID

* Giam thieu nguy co

Chan web

Gioi han file

App ko hop le

* Ngan chan hiem hoa da biet

Malware ( dung AV va Cloud )

Exploits

CC

Web

* Ngan chan hiem hoa chua biet

Sandbox phan tich

Nen tang bao mat Palo Alto

3 thanh phan

NGFW

Endpoint

Cloud

Hardware Palo Alto

PA-800

PA-5200

PA-220

SSL Decryption

Flexible I/O

Lisence :

Wildfire : sandbox nhieu loai file khac nhau( apk,email,office,pdf .. ), cap nhat tu cloud 5p

Voi file pet hi ko can liénce

Threat prevention : gan nhu full tinh nang

URL Filtering :

GlobalProtect : Lisence cho VPN,mac dinh co tren firewall

Chip Palo Alto ko dung chip x86

Palo Alto dung Asic

Kien truc Palo Alto :

Control plane + Data plane

Goi tin di qua 1 lan

SSL/TLS :

Firewall Decryption types

Lab :

<https://use.cloudshare.com/Ent/Course.mvc/StudentLogin/COkWn79RsiKRUKqpgmCgH7Hw2>

DTS IS THE BEST

Trong Palo Alto bao gio cung uu tien phan Application

-Enpoint

Giai phap chong khai thac lo hong va thuc thi ma doc tren may tram

AV : KAV,Bitdefender,….

So sanh file ,hash voi database voi AV

Voi nhung loi zero day,thay doi cau truc -> gap kho khan

Next gen protection : ngan chan

2 xu huong

EDA : tap trung sau khi tan cong,truy vet

Advance protection : chan tan cong nhu the nao ? ngay tu dau ,ngan chan su chong thuc thi

Exploits >< Malware

Exploits : doan ma thuc thi de khai thac lo hong phan mem

Khai thac vao cac phan mem pho bien : office,adobe pdf,web browser

Malware : ma doc

La mot chuong trinh chay ( .exe .dll .. thuc thi cac tac vu,hanh dong xau

Cac ky thuat de khai thac lo hong phan mem :

Control panel protection

Data execution prevention

Uaslr

Dll-hijacking protection …

CAc tinh nang ngan chan Exploit

Chong do quet lay thong tin + ngan chan cac ky thuat khai thac + bao ve kernel

Malware :

Chan ma doc

* Giam bot diem tan cong
* Ngan chan ma doc da biet
* Ngan chan ma doc chua biet
* Phat hien cac tan cong phuc tap

Cac ky thuat chong ma doc

Wildfire intelligence -> phan tich local tren may +phan tich dong tren wildfire ->ngan chan cac tien trinh xau ->chong ma hoa du lieu

Mo hinh trien khia Trap

Endpoint security manager

ESM server + ESM database + Admin Console