

eCTHPV2

Threat Hunting

BY: Ahmad Abdelnasser Soliman

abdelnassersoliman0@gmail.com



Index Of Content:

1- Introduction To Threat Hunting.....	1-12
2- Threat Hunting Terminology.....	12-50
3- Threat Intelligence.....	51-64
4- Threat Hunting Hypothesis.....	64-78

1- Introduction To Threat Hunting:

- هنتكلم فالجزء الخاص بال **Introduction** عن النقط دي ...

1.1 Introduction.....	1-5
1.2 Incident Response.....	6-10
1.3 Risk Assessment.....	11-12

1.1 Introduction:

- لازم نسأل نفسنا سؤال منطقي فالأول كذا ... ايه هو ال **Threat** **Hunting** وهيفدنا فأيه؟؟

- ال **Threat** معناها تهديد أمني وال **Hunting** معناها اصطيد التهديد اللي بيشكل خطر أمني عليك ... اللي بيميز ال **Threat** **Hunter** عن ال **Incident response** وغيره ان ال **Threat** **hunter** بيعمل **Hunt** لل **Threat** بشكل **Pro Active** يعني قبل مال **Attack** يحصل أو يتنفذ عند ال **target** بيكونوا قدروا يوصلوا لل **Threat** دا ويمنعوا التهديد من انه يشكل خطر ... بمعنى آخر مبيستناش أما المصيبة تقع ويشوفلها حل لاء دا بيسعى للحلول الممكنة لو المصيبة (**Incident**) كذا حصلت قبل متحصل ولو حصلت هنتعامل معاها ازاي ... فوظيفه ال **Threat Hunter** معاك فالشركة انهم يعرفوك ال **Defensive Tools** زي ال **Fire walls** وال **IDS&IPS** اللي عندك فالمؤسسة دول هيحموك ولالاء وهل لو اتعرضت ل **Attack** هيعرفوا يعملوا **Defense** ليه ولالاء ... وال **Threat hunters** باستمرار شغالين يعملوا **Search** على ال **Internet** بشكل مستمر عشان يشوفوا أي علامات لأي **Threat** جديد أو شركة مثلا مشهورة تم اختراقها بالطرق دي فال **Threat hunter** يشوف ايه الحل المناسب عشان لو اتعرضت الشركة أو المؤسسة بتعتك لنفس ال **Attack** دا هيتعاملوا معاها ازاي وهكذا ... أخواته اللي شغالين فال **SOC Level1** وظيفتهم انهم يمسكوا ال **Attack** فقط ويحللوا ال **Logs** اللي جياهم من ال **Siem Tools** ولو فيهم **Log** بيشكل **Incident** هتلاقيني طلعتهولك وال **SOC Level2** لما بيجيله ال **Alert** من ال **SOC Level1** بيعمله **Investigate** يعني بيحقق فيه ويتأكد ان ال **Incident** اللي جتله من ال **SOC Level1** هي بالفعل **Incident** وليس **False positive** .

- تعالى بقا لل **SOC Level3** اللى فحالتنا هنا ال **Threat Hunter** فانت بتاخذ وضع دفاعي بتمنع ال **Incident** أو ال **Attack** قبل ميحصل عالمؤسسه بتعتك وقبل ما **SOC L1** يمسكه و **SOC L2** يحقق فيه فانت بتمنعه من الأول ... فانت لو معندكش ال **SOC L3** اللى هو هنا ال **Threat hunter** تخيل انت بقا هيجيك كل يوم **Incident** وليكن هتمسكها هتعملها **Detect** و بعد كذا **Investigation** وماذا بعد هنتن فنفس اللفه دي لحد امتي !! طب متيجي ناخذ طريق تاني اننا نشوف ال **Attack** قبل ميحصل ونشوف هيصيب المؤسسه ازاي وناخذ حاجز دفاعي مسبق ضد ال **Threat** دا أو ال **Attack** ونمنعها ودا بيتم عن طريق ال **Threat Hunter** ومبيستناش **Alert** جايله من ال **Siem** وغيره لاء دا بطرق مسبقه هتلاقية شغال بيحاول يمنع المصيبه قبل حدوثها فوجود ال **Threat Hunter** عندك فالمؤسسه مهم لاغني عنه وأكثر الوظائف المطلوبه فالوقت حاليا ال **Threat Hunter** واحد منهم طبقا لكذا موقع زي اللى هرفقهملك دول .



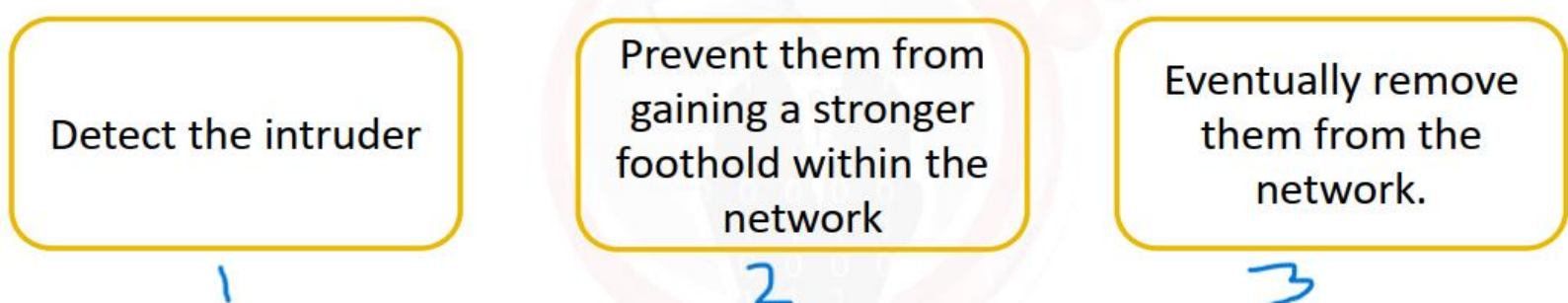
- ال **Search** اللى بيعمله ال **Threat Hunter** دا لازم يكون بشكل مستمر ويشوف آخر ال **Attacks** وال **Malware** من المواقع المخصصه للكلام دا وهنقولها قدام ... ف لازم تكون متابع كل جديد وزي مقولت متستناش ال **Attack** يحصل وتقول هنتعامل زعاه ازاي لاء انت لازم تكون سابق بخطوه وكمال عامل خطه احتياطي لو لقدر الله اتصبنا بال **Attack** دا هنتعامل معاه ازاي وهكذا.

- فلو مثلا انت ك **Threat hunter** بتقرء وتبحث فأحدي المواقع اللى هنذكرها قدام وليكن **The Hacker news** اللى بيحبلك آخر أخبار الاختراقات اللى تمت وال **Data Breaches'** وال **Vulnerabilities** الجديده اللى بيتم اكتشافها وال **Ransomwares** الجديده وازاي بتصيب ال **target** بتعها فانت لقيت ال **Ransomware** بيصيب الأجهزة مثلا اللى مفتوح عندها ال **Port** الخاص بال **SMB** فانت كدا تروح مسبقا للمؤسسه بتعتك وتعمل **Update** لل **SMB Service** وتقفل ال **Port** دا مثلا عشان تتلاشي ال **Attack** اللى بيحبلك من ال **Port** دا مش تستنى لما يحصل عليك ال **Attack** وتشوف هتتعامل معاه ازاى ...!! فانت علطول **Updated** ولازم تحصن نفسك دايم من ال **Attacks** وتشوف المؤسسات اللى اتصابت ازاى اتعاملت مع ال **Attack** دا عشان تروح لمؤسستك تنفذ نفس الكلام قبل متوقع فمحيط ال **Attack** وتخش فدايره تانيه .

- عندنا مصطلح اسمه ال **Dwell Time** ودا الوقت المحسوب مابين عمليه الاختراق أو ال **Attack** ومبين انه اتعمله **Detection** أو كشف لل **Attack** دا ... فلازم نقلل الوقت دا وكلما كان أقل كلما كان أفضل بالنسبه للمؤسسه عندك ... فتخيل ان عندك **Attack** مثلا فالمؤسسه بقاله احسن من 4 شهور تخيل عمل عندك ايه من **Privilege Escalation** و **lateral Movement** عندك فال **Network** وفتح كام **Back door** فالأجهزة اللى عندك فال **Network** عشان يستغلهم فيما بعد لو قفلت الثغره اللى دخلك منها ال **Attacker** وغيره كثير لأن ال **Attack** قد عندك مده طويله ... غير **Attack** تاني مثلا بقاله عندك أسبوع فأكيد بالمنطق مش هيكون عمل ال **Effect** بتاع ال **Attack** اللى بقاله عندك 4 شهور فال **network** فدا اللى بتكلم عليه كلما قل ال **Dwell Time** دا كلما كان فمصلحتك ك **Threat Hunter** وكلما كان فمصلحه المؤسسه بتعتك انها تعمل **Containment** لل **Attack** دا بشكل ميسببش ضرر كبير ليها .

- تقدر تقلل ال **Dwell Time** عن طريق ال **Pro Active Action** اللى هتاخده ك **Threat Hunter** قبل يحصل **Attack** عالمؤسسه بتعتك... ول لازم ال **Threat hunter** يكون عنده ال **Mindset** بتاعت ال **Attacker** يعني يفكر بطريقته عشان يفهم ال **Attack** دا ممكن يتنفذ عليه ازاي وساعتها هو بنفسه يوجد الطرق اللى ممكن نعمل بيها **Defense** لل **Attack** دا ... يعني نفكر بطريقة ال **Attacker** ومن خلال تحليلنا ليها ناخد ال **Actions** المناسبه للتصدي ليها فلازم ال **Threat Hunter** يكون فاهم ال **Hacking Techniques** وكمان ال **Cyber Kill chain** لازم تكون عارفها وفاهمها ك **Hunter** عشان تبقا عارف ال **Tools** وال **Techniques** اللى ال **Attacker** بيستخدمها فكل مرحله من مراحل ال **Cyber Kill Chain** ... فمثلا انت عارف ان ال **Attacker** فمرحله زي ال **Scanning** دي بيكون عاوز يعرف ايه هي ال **Vulnerabilities** اللى عندك فال **Network** عشان يستغلها فيما بعد في **Attacks** على المؤسسه بتعتك فأنت ك **Hunter** عارف المعلومه دي فتروح للناس بتاعت ال **Network Security** تعرفهم لو لقوا اي حد بيستخدم ال **Nmap** عندنا فال **Network** وقفوه أو بلكوا ال **IP** بتاعه فأنت كذا أخذت **Pro Active Action** قبل مال **Incident** تحصل عندك ... بالضبط دا اللى بكلمك عليه بس على نطاق أوسع ... فدور ال **Threat Hunter** بيتمثل فال **Diagram** دا .

The objective of the threat hunter is to:



- أول حاجه بتمسك ال **Intruder** قبل مينفذ عليك **Attack** بشكل مسبق زي موضحنا وبعد كذا بتمنعهم انهم ينتشروا فال **Network** بتعتك وبعد كذا تبتدي تسمحهم عندك من ال **Network** الخاصه بمؤسستك وطبعا الكلام دا كله فأقل وقت ممكن عشان نقلل ال **Risk** .

1.2 Incident Response:

- تعالى نعرف ال **Incident Response Process** طبقا لمعهد ال **NIST** الامريكي فهي عبارة عن **Process** مكونه من **4 Steps** .

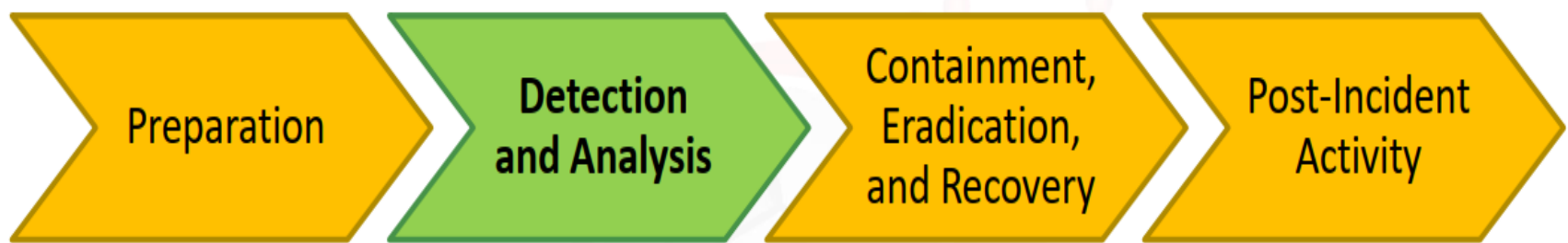


- تعالى ناخذ مرحله مرحله عالسريع ونفهم الغرض منها ايه ...



- ال **Preparation** الغرض منها تجهيز الناس اللى عندك فالمؤسسة الافراد اللى شغالين فال **SOC L2** ازاي لو حصلت اي **Incident** يعرفوا يتعاملوا معاها ويعملوها **Handle** ... بالاضافه الى مسؤوليه كل شخص عندك فال **SOC** ايه هي مسؤولياته مثلا ايه ال **Hardware** المسؤول عنها وايه ال **Tools** اللى هيستخدمها ومسؤول عنها وبكدا بنقل احتماليه وقوع ال **Incident** ... طبعا ال **Policies'** بتاعت ال **Incident** بتختلف من مؤسسه لأخري فلكل مؤسسه **Policy** معينه لل **Incident** دي لو حصلت ساعتها بتتصنف **Incident** ... مثلا احنا عندنا فالمؤسسه قايلين ممنوع حد يعمل **Scanning** فال **Network** عندنا فدي كدا **Policy** احنا حاطينها ... ال **SOC L2** طلعه من ال **Siem** ال **Alert** بيقوله ان فيه **IP** معين بيعمل **Nmap** عندنا فال **Network** وبكدا اتصنفت **Incident** طبقا لل **Rules** اللى احنا حاطينها .

- نيجي لتاني مرحله عندنا فال **Incident Response** ...



- احنا فال **Preparation** عرفنا كل واحد فال **IR Team** مسؤول عن ايه ... تعالى هنا فال **Detection & analysis** نعمل **Analysis** لأي علامه أو اي **Alert** أو مؤشر ان دي عمليه اختراق حصلت علينا ... اللي بيعمل ال **Detection** هو ال **SOC L1** واللى بيعمل ال **Analysis** هما ال **SOC L2** ... فال **SOC L1** يمسك ال **Thread** ويبعت لل **SOC L2** يحلله ونتأكد فعلا اذا كانت دي **Incident** ولا مجرد **Event** عادي واللى جالنا دا **False Positive** .

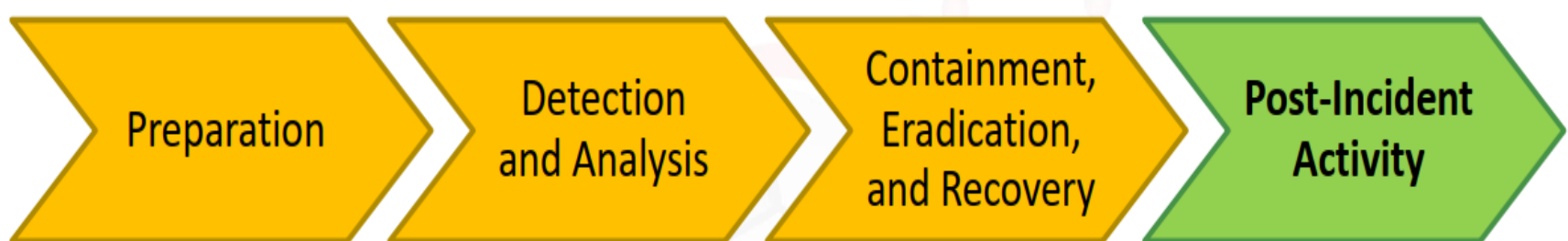
- تعالى نروح لل **Phase 3** اللي بعد ال **Detection & analysis** .



- دي ال **Phase** اللي بنعمل فيها احتواء لل **Incident** اللي عندنا فالمؤسسه يعني نمنع انتشارها فال **Network** لأجهزة أخرى أو لفرع آخر من ال **Network** التابع للمؤسسه مثلا ... ال **Phase** دي المسؤول عنها هو ال **SOC L2** واللى بيساعده فيها ال **SOC L3** اللي هو ال **Threat Hunter** بيدخل مع ال **Incident Responder** فعمليه ال **Containment** عشان يعرفه ال **Incident** دي ازاي نلهمها ونحتويها عشان هتنتشر لباقي ال **Network** بالطريقه اللي عارفها ال **Threat Hunter** عشان كدا بينصح ال **Incident Responder** انه ياخذ بعض ال **Steps** اللي هتساعده فال **Containment** وكمان هتقلل من ال **Risk** .

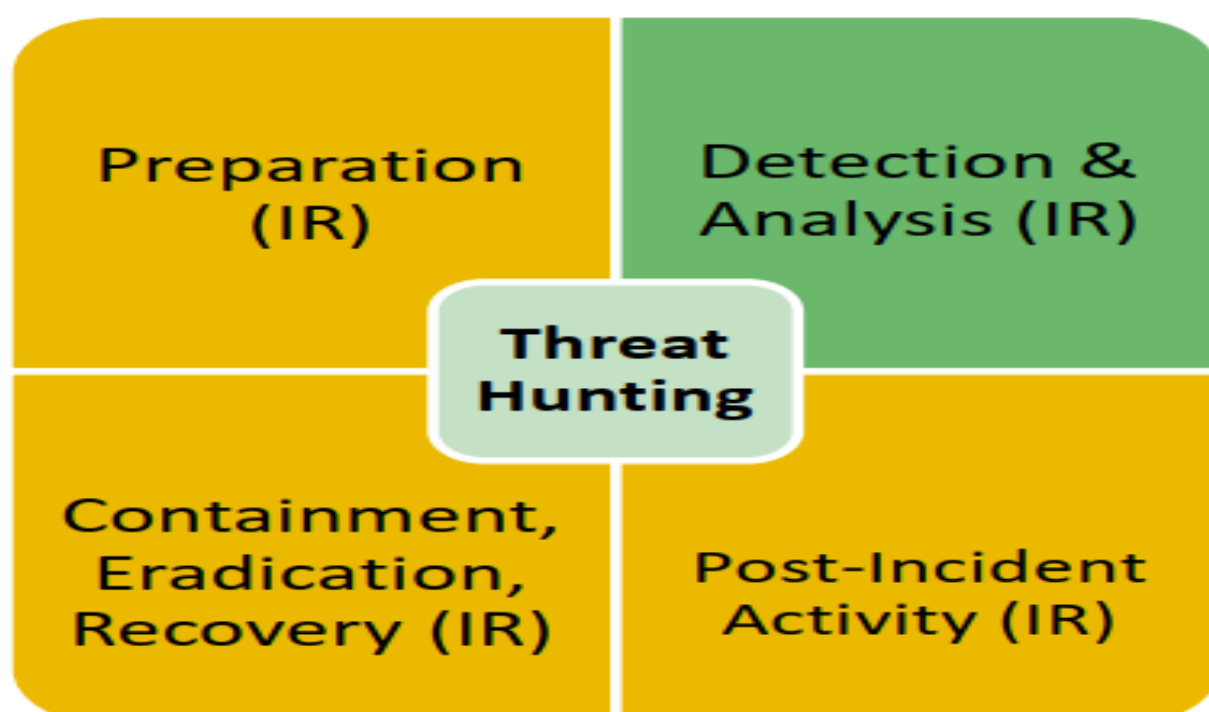
- ال **Containment** بتتمثل برضه فال **Create Signature** فال **Siem Tools** زي ال **IPS** عن طريق ال **Network Security** **Engineers** تعرفهم ي **Create** ال **Signature** المناسب لل **Attack** دا عشان لو اتكرر ال **Defensive Tools** بتعتنا تمسكه وميدخلش عندنا لل **Network** مره ثانيه .

- نيجي لل **Phase** الأخيره عندنا وهي ال **Post – Activity** .

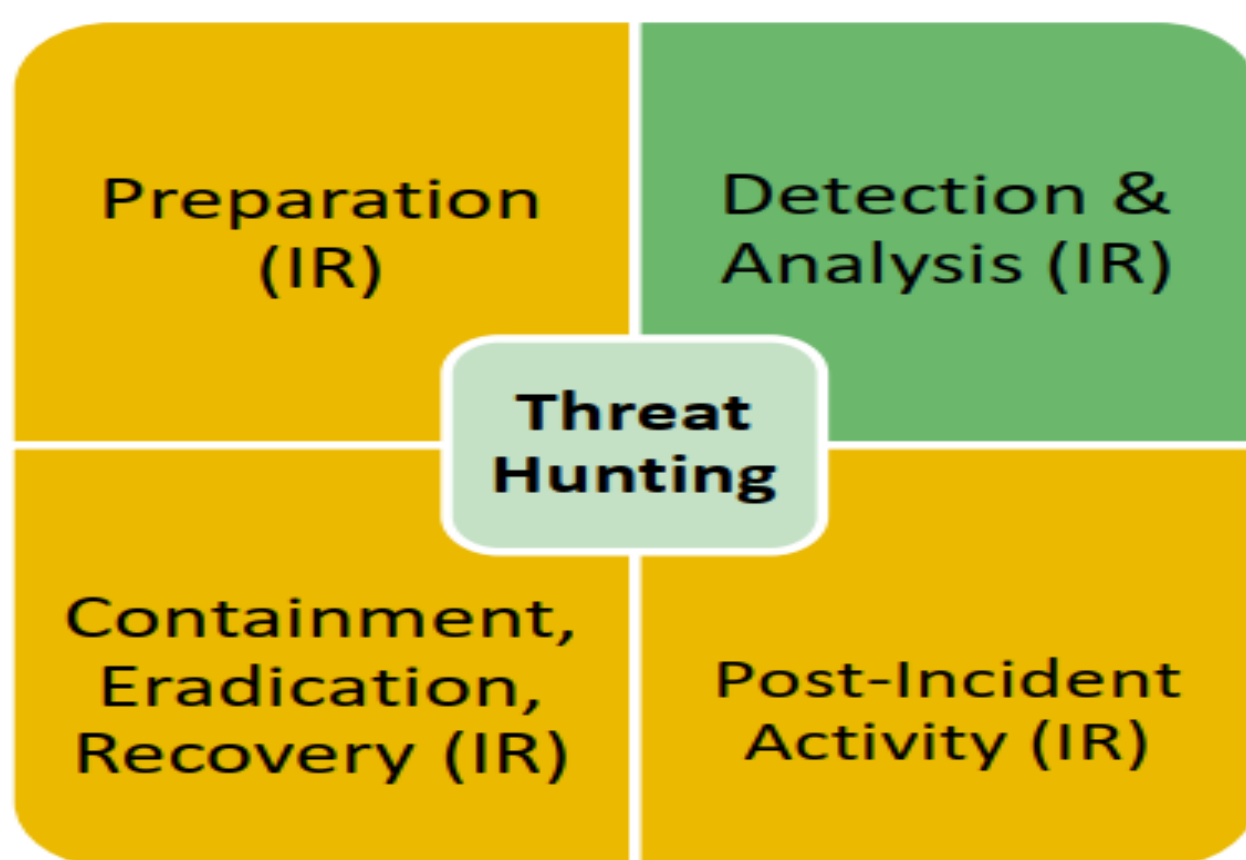


- هنا بقا نيجي للدروس المستفاده من ال **Attack** أو ال **Incident** اللى حصلت دي وازاي تمت علينا واتعاملنا معاها ازاى ك **IR Team** ودور كل واحد فينا كان ايه .

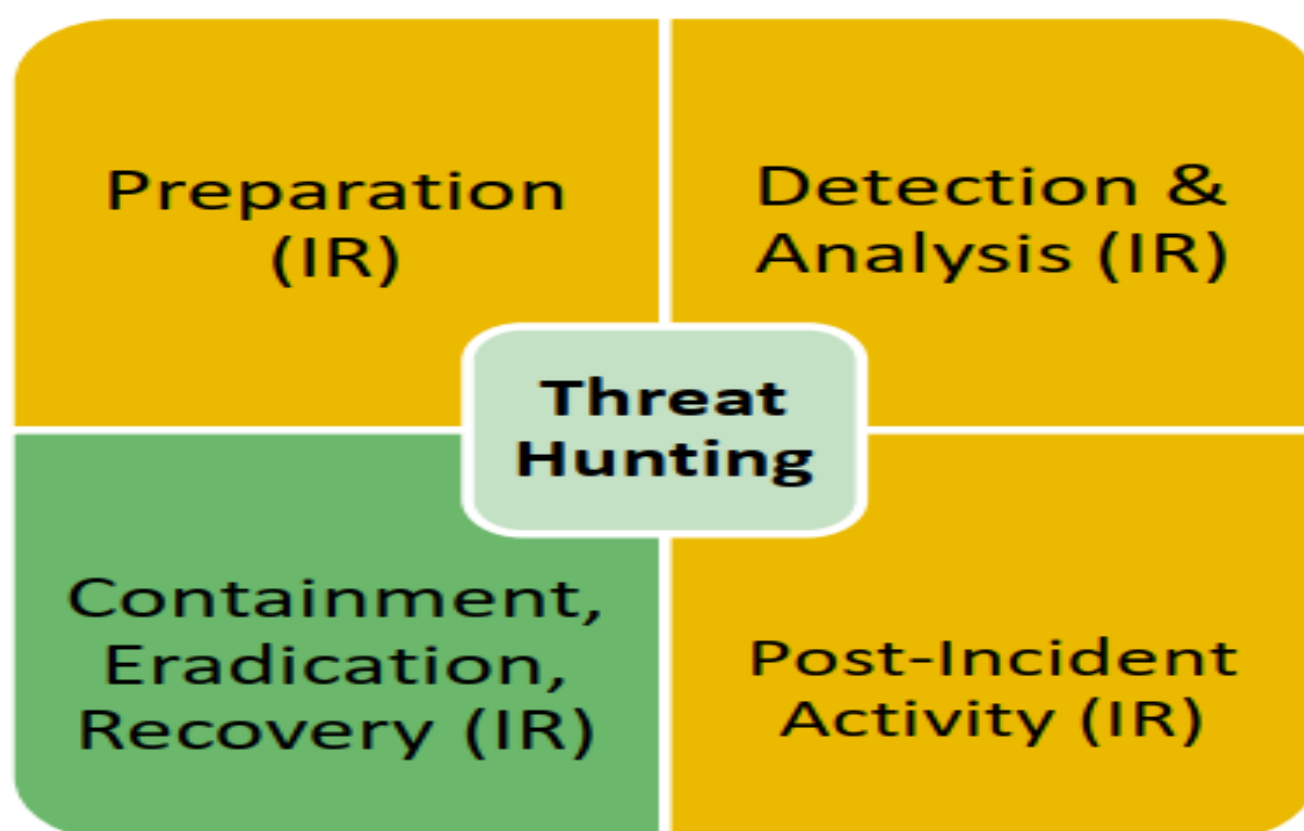
- جميل لحد هنا الكلام طب ايه علاقه ال **Threat Hunters** بالكلام بتاع ال **IR Team** اللى شغالين فال **SOC L2** ... احنا قولنا فيه بعض الحاجات المشتركه بين ال **L2** ال **Incident Responder** وال **L3** اللى هو ال **Threat Hunter** ... فتعالى نشوف دور ال **Threat Hunter** فكل مرحله من مراحل ال **Incident Response** .



- أنت ك **Threat Hunter** لازم تكون ملتزم بال **Rules of Engagement** اللى هي قواعد الشغل بتاعك وهتم ازاي ... ف لازم أكون عارف مين معانا فال **SOC Team** من ال **Levels** الأخرى عشان أعرف اعمل **Assign** لل **Tasks** بتعتهم واعرفهم هما مسؤولين معانا عن ايه ... ف لازم يكون موجود ال **Threat Hunter** فمرحلة ال **Preparation** عشان يعرف كل شخص فال **Team** هيعمل ايه ودوره ايه فالشغل فال **Team** ... نروح للمرحلة التانيه .



- هنا ال **Threat Hunter** بيقرر يساعد في عملية ال **Investigation** ويقرر يحددك ال **Indicator** اللى مسكته عندك فال **Network** دا **Incident** وللااء ... نروح للمرحلة اللى بعدها .



- في بعض المؤسسات هتلاقي ال **Hunter** هو اللي عرف ال **Incident Responder** ال **Incident** دي يتعملها ال **Containment** ازاي ... فهتلاقي ال **Hunter** دايمًا بيعمل **Assign Task** دي لواحد من ال **IR Team** اللي هما ال **SOC L2** ... ودا على حسب المؤسسة بتعتك برضه ممكن تلاقيه هو اللي بيعمل ال **Containment** بنفسه عادي بس فالأغلب اللي ذكرناه ... تعالى نروح للمرحلة الرابعة والأخيره ونشوف دور ال **Hunter** فيها ايه .



- نيجي للمرحلة الرابعة والأخيره عندنا اللي هتلاقي ال **Threat Hunter** مشارك فيها بالفعل ... لأن لازم يكون عنده معرفه واسعه أو **Vast Knowledge** بال **IT Domains** وال **IT Security** وساعتها هو اللي بيقرر ايه هي ال **Recommendations** اللي هتم ايه بالضبط عشان ال **Incident** اللي حصلت عندنا فالمؤسسة دي متكرش مره ثانيه ... زي مثلا محتاجين نشترى **FW** جديد ال **Version** بتاعه أحدث بيعرف يمنع ال **Attacks** الحديثه وال **Advanced** ومثلا محتاجين نعمل **Install** ل **New AV** عندنا على أجهزة ال **Users** وهكذا من توصيات بيديها ال **Threat Hunter** لل **Incident Responder** هو شايفها من خبرته انها المناسبه فهو لازم هيشارك فال **Phase** الأخيره زي موضحنا ... وبكدا نكون وضحنا العلاقه مابين ال **Threat Hunter** وال **Incident Responder** .

1.3 Risk Assessment:

- باختصار المؤسسة بتعتك لازم كل فتره تعمل عمليه تقييم لل **Threats** وال **Vulnerabilities** وايه تأثيرها على ال **Assets** داخل المؤسسة عندك ... ال **Asset** يعني اي حاجه ذات قيمه عندك فالمؤسسة زي ال **Servers** وال **Data Center** وال **Network** **Devices** وال **PCs** وال **Laptops** وغيره من ال **Assets** الموجوده عندك فالمؤسسة ... فتلاقي الشركه بتعتك دايمًا بتعمل ال **Risk Assessment** من فتره لأخري عشان تعرف هل الدنيا جوا المؤسسة **Secure** وللااء ولو فيه **Threat** جديد تبدا تآخذ **Actions** للتعامل معاه مسبقًا وتعمل كذا **Plan** للتعامل معاه فحاله لو شكل **Risk** عالمؤسسة لأننا زي محنا عارفين عشان نقول دا على اي **Incident** دا **Threat** لازم يكون فيه **Vulnerability** واتفعلها **Exploit** من ال **Attacker** فشكلت **Threat** علينا ... وطبعًا لما ال **Risk Assessment** بيخلص بتعمل **report** بال **result** اللى وصلها ال **Team** ومن هنا بيبدأ يشارك ال **Threat Hunter** وبيأخذ نسخه من ال **Reports** دي ويكون **Road map** كدا فدماغه عن المؤسسة بأجهزتها بكل ال **Assets** اللى فيها ودي هتفيده فخطوه ال **Recommendation** بعد كذا لأنه هيفهم الدنيا ماشيه ازاي زي مثلاً ال **Threat Hunter** عرف ان أهم **Server** عندنا فالمؤسسة هو ال **Oracle Server** دا اللى عليه كل حاجه تخص المؤسسة فدا كذا بالنسباليه بشكل أهم شيء لازم يكون **Secure** بالنسباليه فكذا حطينا **Priority** يعني أولويه فشغلنا فلما تيجي تعمل **Hunt** انت ك **Threat Hunter** بما ان ال **Server** دا من أولوياتك فأنت كل تركيزك على ال **Threats** اللى بتهدد ال **Oracle Servers** عشان تتابعها وتقرء عنها وتشوف آخر ال **Vulnerabilities** الخاصه بيها وايه هي آخر ال **Ransomwares** اللى بتصيب ال **Oracle Servers** وازاي تحمي مؤسستك منها وبيتأكد ان **Server** بتعنا **Secure** .

- فدي هتوفر وقت على ال **Threat Hunter** عشان يعرف هيركز على ايه فشغله وهي عمل **Secure** لأنهو قسم أكثر من الآخر دا اللى هيحدده ال **Risk Assessment** اللى هياخد منها نسخه لأنه مثلا هيعرف ان قسم ال **HR** وليكن **Secure** ولكن قسم ال **data center** دا بييجي عليه **Attacks** أكثر فبص لقي ان ال **Server** اللى عندهم وشغالين بيه من النوع **Oracle** فيشوف **Updates** ينفذها زي انه يشتري ال **Version** الأحداث من ال **Servers** اللى بيعمل **Defense** لل **Attacks** دي أو أي حل تاني مناسب بحيث يقلل من ال **Attacks** اللى بتيجي عالمؤسسه عندك خصوصا على قسم ال **Data Center** .

- ولكن فالمؤسسات الكبيره زي **Google** مثلا مبتلاقيش ال **Threat Hunter** بيعمل ال **Risk Assessment** خالص لاء دي مسؤول عنها شخص آخر وال **Threat Hunter** بيتعاون معاه ولكن بتبقا وظيفه تانيه ليها ناسها وال **Threat Hunter** يركز فشغله ... أما لو كنت فشركه صغيره فهتلاقي ال **Threat Hunter** غالبا بيقوم بعمل ال **Risk Assessment** بجانب شغله الاساسي .

2- Threat Hunting Terminology:

- فال **Module** دا ان شاء الله هنتكلم عن أشهر المصطلحات الخاصه بال **Threat Hunting** فلازم تكون عارفها لأنك هتسمعها كثير ... وفال **Module** دا هنتكلم عن النقاط التاليه بالتفصيل ...

2.1 Threat Hunting Terms.....	13-41
2.2 Threat Intelligence.....	41-44
2.3 Digital Forensics.....	44-49
2.4 Threat Hunting Stimulations.....	50-50

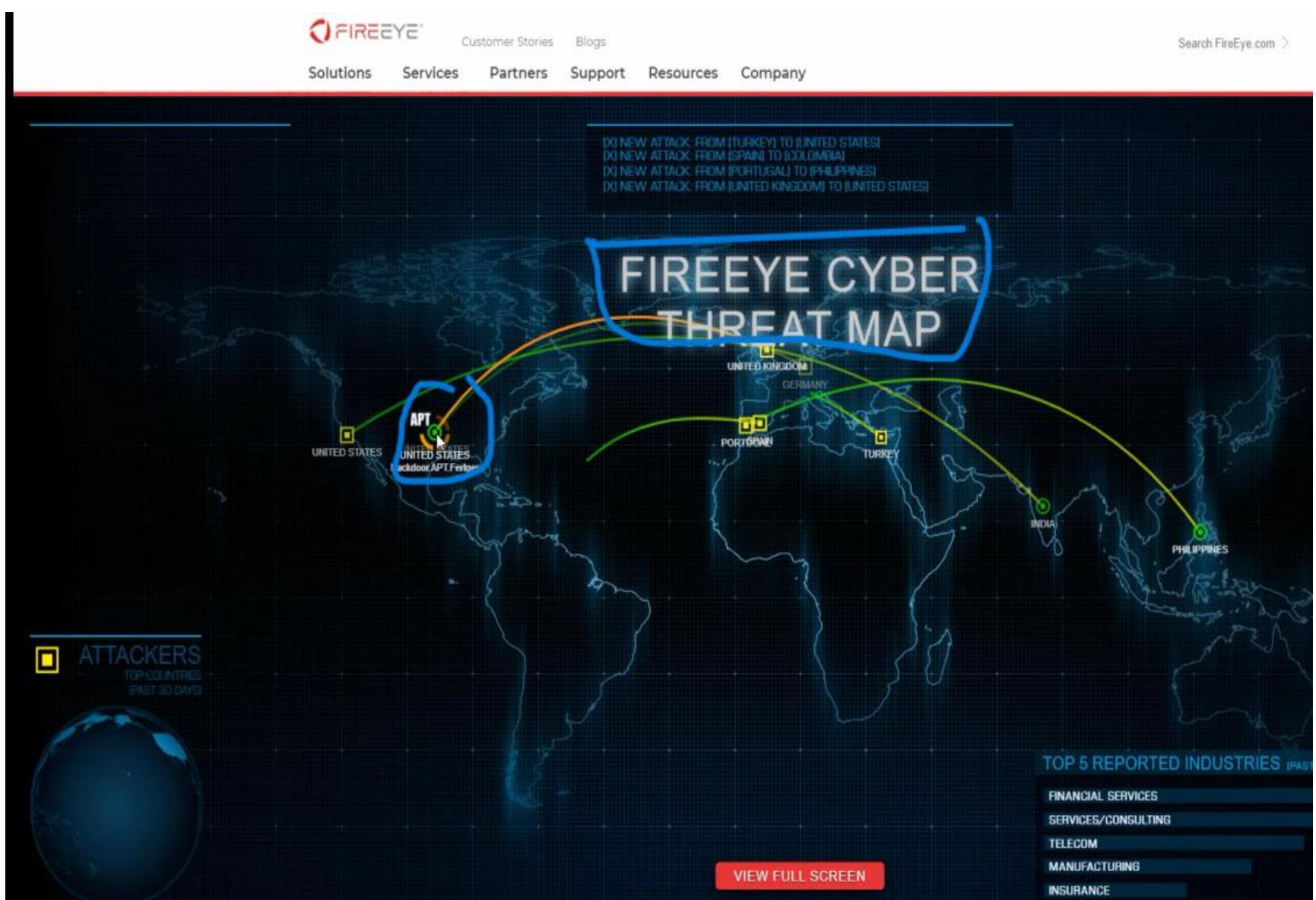
2.1 Threat Hunting Terms:

- أول مصطلح هتسمعه وانت شغال ك **Threat Hunter** أو حتى وانت بتعمل **Investigation** أو بتبحث عن آخر ال **Attacks** وغيره هو مصطلح ال **APT** اختصار ل **Advanced Persistent Threat** ... بمعنى آخر التهديدات المتقدمة المستمرة والمصطلح دا بنطلقه على ال **Attacks** اللى بتكون موجهه من جهه معينه وبطريقه مستمره لمدته شهور أو سنين وتلاقيها بتستهدف بنيه تحتيه او **Infrastructure** لمؤسسه ما أو غيره ودول بيبقوا عدد مش مجرد **Attack** من شخص معين ... فتلاقي الصين مثلا بتنفذ **Attacks** على ال **Infrastructure** الخاص بأمريكا وغيره ... خد بالك من نقطه وهي ان ال **Individual** لما بيحي يعمل **Attack** بيكون **Limited** لأن ال **resources** بتعته محدوده زى ال **RAM** وال **Processors** ... انما فال **APT** كل شيء متاح تقدر تاخد **Access** على كل شيء من ناحيه ال **resources** فانت تقدر تنفذ **Attack** وسط مجموعه معينه على دول زي مقولنا ... فتلاقي **APT** بيمثل **Iran** وليكن رايح بيترجت مؤسسات أو صناعات وبنيه تحتيه ل **USA** والعكس صحيح هتلاقي ال **APT** الخاص بالدوله الأخرى برضه شغال بيترجت دوله أخرى .

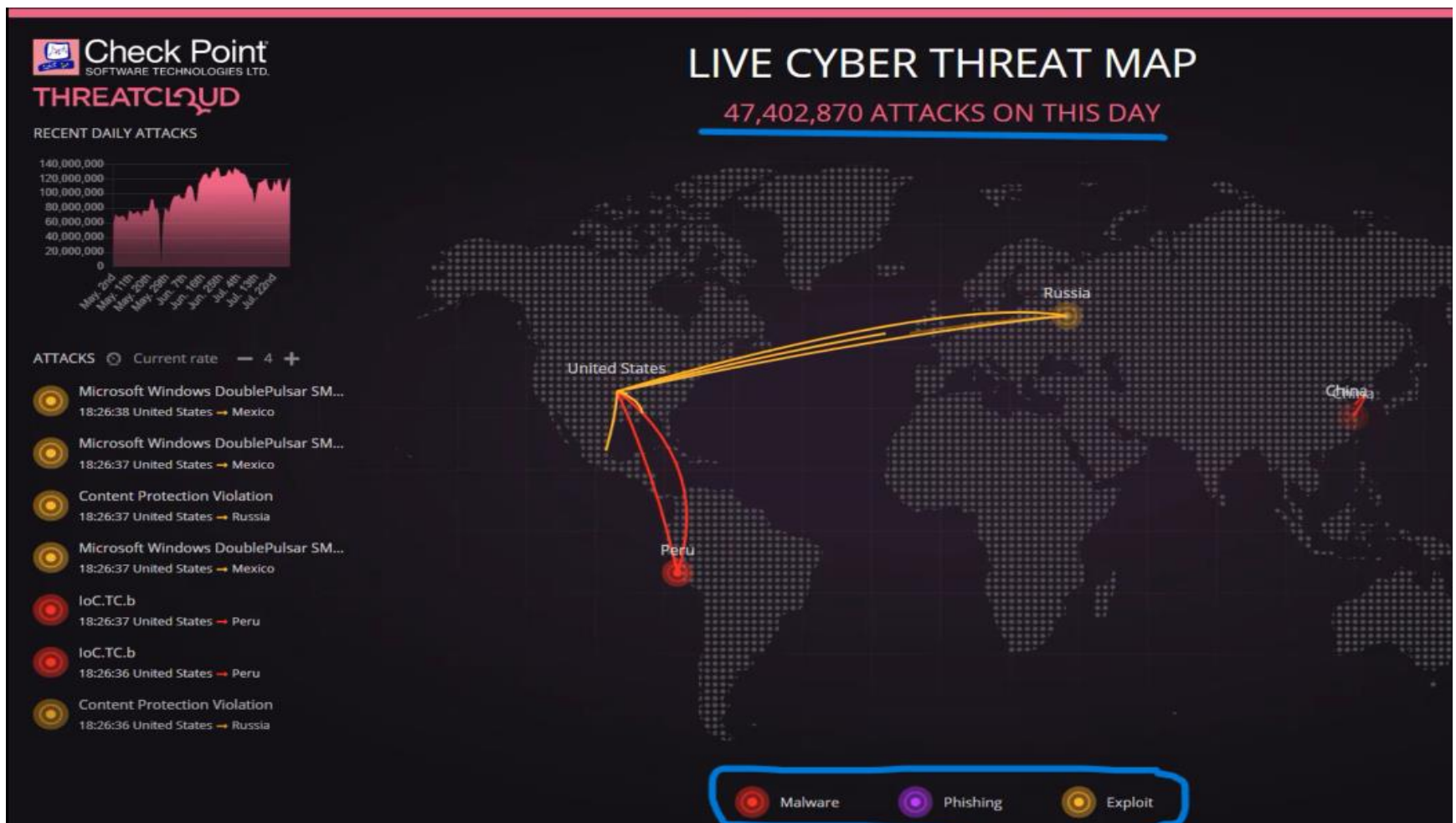
- تعالى ناخذ مثال وهو ال **Stuxnet** ودا كان **Malicious Software** ف 2010 كان بيترجت المفاعلات النوويه الأيرانيه وكان وراه **APT Group** من الكيان المحتل أو ال **USA** وكان وقتها ف 2010 متطور جدا ال **Malware** دا ... المفاعل النووي كان شغال ب **Software** من شركه **Siemen's** الألمانية اسمه **Step7** ودا كان المسؤول عن التحكم فال **Scada System** الخاصه بالمفاعل النووي وال **Scada** اختصار ل **Supervisory Control and Data Acquisition** ودا ال **Control System** اللى بتقدر من خلاله انك تتحكم بالأجهزة الموجوده فالمنظومه أو المؤسسه عندك .

- ال **Malware** بتاع ال **APT-Group** كان بيتلاعب فال **Values** بتاعت ال **Scada System** اللى كان **Step7** وقتها وتخليه يدخل قيم كتيره ومش مفهومه للمفاعل النووي ودا أدى لعلو درجه الحراره فالمفاعل النووي ودي كارثة لولا انها اتلحقت بدري كان هيحصل انفجار للمفاعل النووي ودا كان خير مثال يوضحك خطورة ال **Attacks** اللى بتيجي من ال **APTs Groups** .

- وانت ك **Threat Hunter** عندك **Service** من شركه **Fire eye** بتمكنك انت تشوف وتابع آخر تطورات ال **Attacks** من ال **APT Groups** وطالعه منين جايه لمين ونوعها كمان .



- وفكره ال **Cyber Threat Map** هتلاقى كذا شركه عامله الفكره دي مش **Fire eye** فقط ولكن عندك **Kaspersky** برضه و **Check point** وغيرهم من الشركات اللى بتقدم ال **Service** دي ... فلازم انت ك **Threat Hunter** تكون متابع الدنيا دي وآخر ال **APTs Attacks** عشان تحمي مؤسستك منها مسبقا لو كان فيه **APTs groups** بتهددها .



- طب بما انهم اسمهم ال **APT** اختصار **Advanced Persistent** **groups** هل دا معناه ان ال **Attacks** بتعتهم لازم تكون كلها **Advanced** ... لاء بالعكس ممكن تلاقيهم بيستغلوا **Attack** معروف ضدك عادي فالأسم مش شرط ولا ليه دلالة معينه ان كل ال **Attacks** بتعتهم دي **Advanced** وبيتعملها **Development** ودا برضه لا يمنع ان فيه منها هكذا ولكن مش الكل ... وبنسميها **Persistent** ودا عشان ال **Resources** اللى هي الفلوس والأدوات بتعتها اللى بتستخدمها فال **Attacks** زي **USA** كدا ال **Resources** الماليه والتكنولوجيه وال **Mans Powers** اللى هما الأفراد اللى شغالين عندك فهتلاقي ال **APTs** دايمًا مستمرين في هجماتهم لأن ال **resources** متوفره زي موضحنا .

- كل **APT Group** ليه اسم **Specific** بيحدده وبيميزه ومش شرط يكون ليه اسم واحد لاء انت ممكن تلاقي كذا **APT Group** ليه أكثر من أسم ودا نتيجة لمين من ال **Threat Intelligence Website** اللى بيطلق عليه الاسم فمثلا عندك **Mandiant** بيسمى ال **APT1** بتاع جيش تحرير الصين ودا **APT Group** مشهور فالصين بينفذ **Attacks** بشكل مستمر على دول تانيه زي **USA** .

- هتلاقيه بيسميه **Comment crew** وهتلاقي **Crowd Strike** بتسميه **Comment Panda** وهو هو ال **APT group** .

APT 1	Comment Panda	PLA Unit 61398	TG-8223	Comment Crew
-------	---------------	----------------	---------	--------------

- فلازم انت ك **Threat Hunter** تكون عارف أسامي أشهر ال **APT groups** دي وآخر تطوراتهم وآخر ال **Attacks** اللى بيقيموا بيها عشان تحصن نفسك منها أول بأول وتكون **Updated** بالكلام دا انت ومؤسستك .

- تاني مصطلح عندنا وهو ال **TTP** ودا اختصار ل **Tactics & Techniques & Procedures** اللى بيعملهم ال **Attacker** عشان ينفذ ال **Attack** ... ال **TTP** هي ال **Techniques** اللى ممكن يستخدمها ال **Adversary** عشان يدخل لل **Network** وازاي يعمل ال **Pivoting** فيها وياخد **Privilege Escalation** بالإضافة انك ممكن تطلعها عن طريق ال **IOCs** اللى هي ال **Indicator Of Compromise** اللى هي علامات عمليه الاختراق ... وال **IOCs** هي ال **Artifacts** يعني الحاجات المصنعه أو ال **Tools** اللى استخدمها ال **Attacker** عشان ينفذ **Attack** معين عال **Victim** ودي عباره عن الدلالات زي ال **Files** اللى بيرفعها ال **Attacker** عند ال **Victim** وغيره زي ال **MD5 Hashes** أو ال **Ip Addresses** أو **Names of EXE File** .

- تعالى ناخد مثال لل **IOCs** الخاصه بال **APT1** الخاص بالصين ونشوف ايه المميز فيه ... ال **APT1** كانوا بيستخدموا **2 Tools** بشكل كبير عشان يعملوا **Steal** لل **Victims Emails** وهما ال **Get mail** وال **Mapi get** .

- ال **Malware** اللى هو **Get mail** كانوا ال **Attackers** بيستخدموه عشان يعملوا **extract** لل **Email Messages** اللى كانت بتيجي فال **Outlook email** بتاع **Microsoft** ... وال **Malware** التاني اللى هو **Mapi Get** دا بيعمل **Extract** لل **Emails** اللى بتيجي على ال **Email Server** زي ال **Exchange Server** ... احنا ك **Threat hunters** لقينا عندنا على **Machine** معينه من اللى حصل عليهم ال **Attack** واتصنفت **Incident** واحنا بنعمل ال **Investigation** لقينا ملف زي دا اللى هو **IOCs** بالنسبالنا لأنه بيدل على حاجه **Malicious** احنا عارفينها .

Here is a snippet of the IOC for GETMAIL.

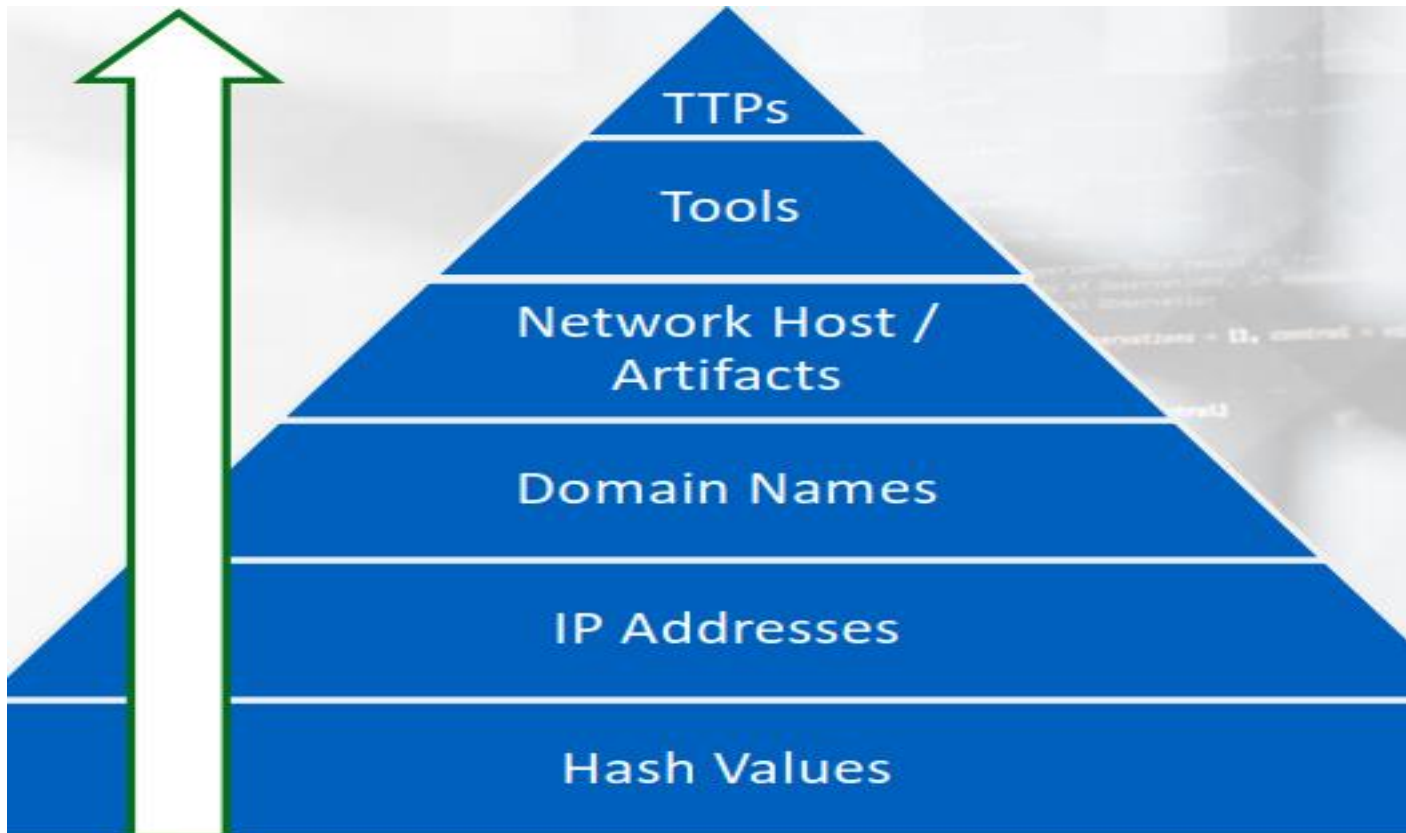
```
File MD5 is e81db0198d2a63c4ccfc33f58fcb821e
File MD5 is 909bef6db8d33854e983ebccdd71419f
File MD5 is 36ca55556280f715e2de8b4b997a26c9
File MD5 is e212aaf642d73a2e4a885f12eea86c58
AND
File Size is 86016
OR
File Name is getmail.exe
File Name is gm.exe
File Name is winps.exe
File Detected Anomalies is checksum_is_zero
OR
File Compile Time is 2005-01-05T01:38:18Z
File Compile Time is 2005-08-18T09:17:08Z
```

This is a snippet of the IOC for MAPIGET.

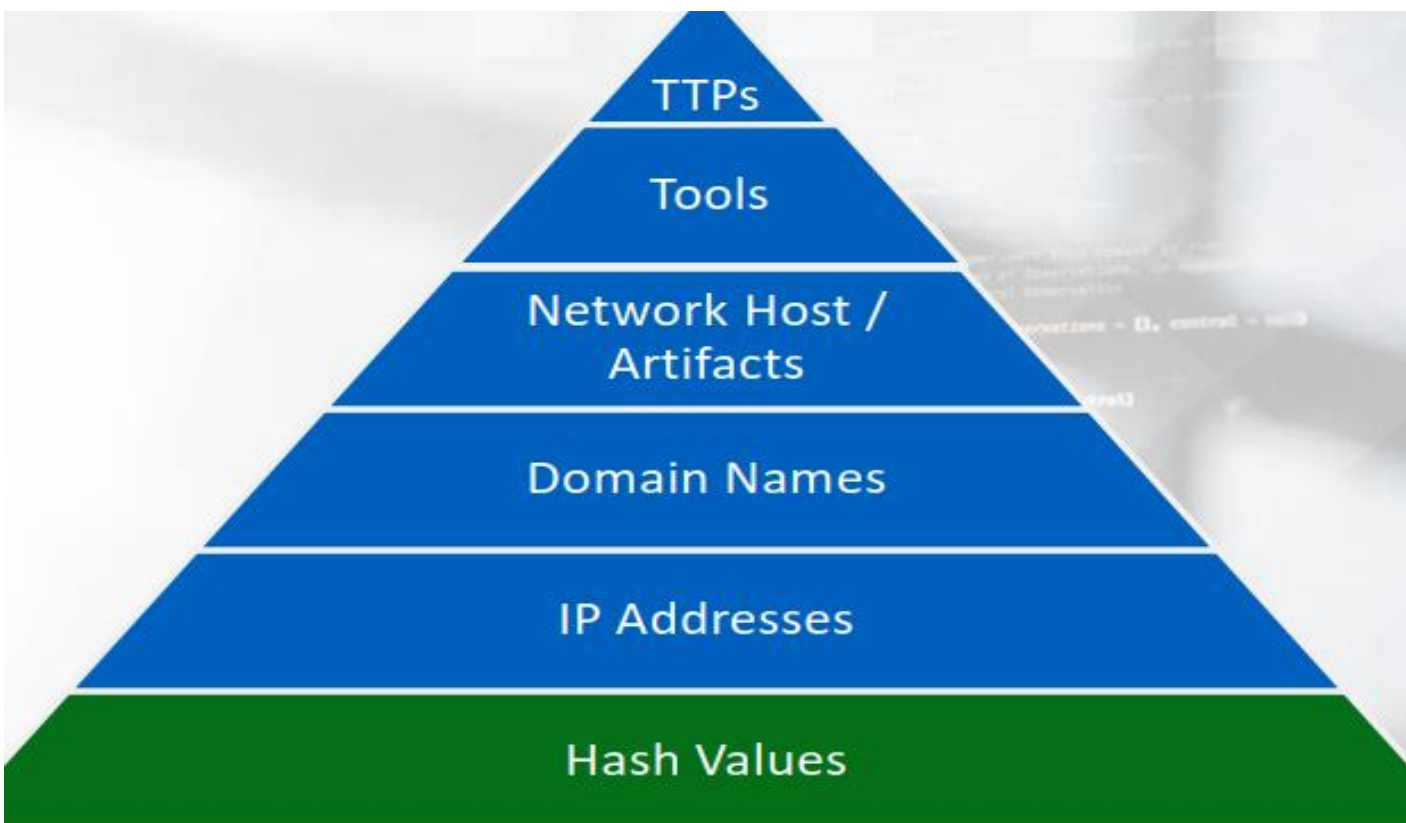
We'll discuss IOCs and various IOC-based tools in later modules.

```
File MD5 is c627e595c9ec6dc2199447aeab59ac03
File MD5 is f3c6c797ef80787e6cbeaaa77496a3cb
AND
File Size is 227840
File Compile Time is 2006-10-12T02:38:59Z
File Detected Anomalies is checksum_is_zero
OR
File Name is m1.exe
File Name is mapi.exe
AND
File Name is mapiget.exe
File Size is 62976
File Compile Time is 2006-10-12T00:34:06Z
File Detected Anomalies is checksum_is_zero
```

- المصطلح اللى بعد كدا عندنا وهو ال **Pyramid of Pain** ... ودي عباره عن بعض الخطوات اللى انت ك **Threat Hunter** بتتبعها وبتدور عليها فال **Incident** وانت بتعمل **Hunt** ولو لقيت الحاجات دي بتعرف تكتشف الخطوات اللى عملها ال **Attacker** عليك فال **Attack** وبنفس ترتيب الخطوات بتعتنا تبدء تدور عليها وتعملها **Hunt** .



- فانت أول حاجه تدور عليها عال **Machine** اللى حصل عليها ال **Attack** انك تجيب ال **Hash Values** وبعدها ال **IP Addresses** وبعدها ال **Domain Names** وهكذا الى نهايه ال **Pyramid** ... وكل خطوه من الخطوات اللى موجوده فال **Pyramid** عندك دول زي مقولنا لو عرفت تحصلها فانت عامل زي متكون بتضيق الطريق عال **Attacker** ... فانت فالحاله دي هتجبر ال **Attacker** انه يغير ال **Plan** بتعته لأنك ك **Threat Hunter** كشفت معظمها .



- واحنا هنبدء فال **analysis** من الأسهل للأصعب ... من قاعده الهرم لحد القمه وكل مبتطلع لفوق كل مالمعليه بتصعب أكثر فأحنا عاوزين نطلع ال **IOCs** الموجوده عندنا الأول اللى هتسهل علينا فالصعب اللى قدام ... فأول حاجه هنبدء بيها هي ال **Hash Values** .

- ال **Hash Value** هي طريقة نقدر نستخدمها فأثبات ال **IOCs** لكن غير اعتماديه بشكل كبير ودا بسبب ان ال **Hash** ممكن يتعمله **Change** من ال **Attacker** ... ال **Hash** دي طريقة بنأكد بيها ال **Identify** بتاعت ال **Data** اللى بتترسل مابين الطرفين أو طرف واحد فقط بيحملها زي الملفات الموجوده عالانترنت اللى بتعملها **Download** فدي ليها **Hash** عشان تتأكد ان دي النسخه الأصلية من ال **File** فلما بتنزله بتروح تقارن ال **Hash** دا بال **Hash** اللى الشركه صاحبه ال **File** منزلناه عندها عالموقع فلو لقيت ال **Hash** واحد والمفروض تلاقي كدا كدا يبقا انت تمام و **Secure** انما لو لقيت ال **Hash** مختلف عن بتاع الشركه الأصلي تعرف ان ال **Hash** دا اتلعب فيه من خلال **Attacker** فالسكه وهو بيوصلك ... زي ملف ال **ISO** اللى بتنزله لتوزيعه **Kali Linux** كدا ليها **Hash** فانت بعد اما تعمله **Download** من الموقع الأصلي اللى هو **Kali.org** المفروض تقارن ال **2 Hashes** ببعض عشان تتأكد انهم واحد وان ال **Data** تمام اثناء عمليه ال **Transfer** عن طريق انك تعمل ال **Calculate** لل **Hash** بتاع ال **File** اللى عملته **Download** وتقارنه بال **Hash** الموجود عالموقع الأصلي للملف ... دا كدا عالسريع حوار ال **Hash** عشان تبقا معايا فالجي .

- فلو لقيت اي ملف انت نزلته من مصدر غير معروف من مواقع ملهاش هويه الموجوده بكثره عالانترنت وفكيت ال **Hash** بتاعه وقارنته بال **Hash** الأصلي الموجود عالموقع الأصلي ولقيتهم مختلفين تعرف علطول ان الملف دا تم التلاعب فيه عن طريق زرع **Malicious code** فيه فتاخد بالك انت ك **User** من النقطه دي .

- تعالى نشوف مثال على **APP** اسمه **Putty** ودا بنستخدمه فال **Remote Connection** زي ان فيه شخص عاوز يدخل على جهازك **Remotely** عن طريق ال **Telnet** أو ال **SSH** .

Checksum files

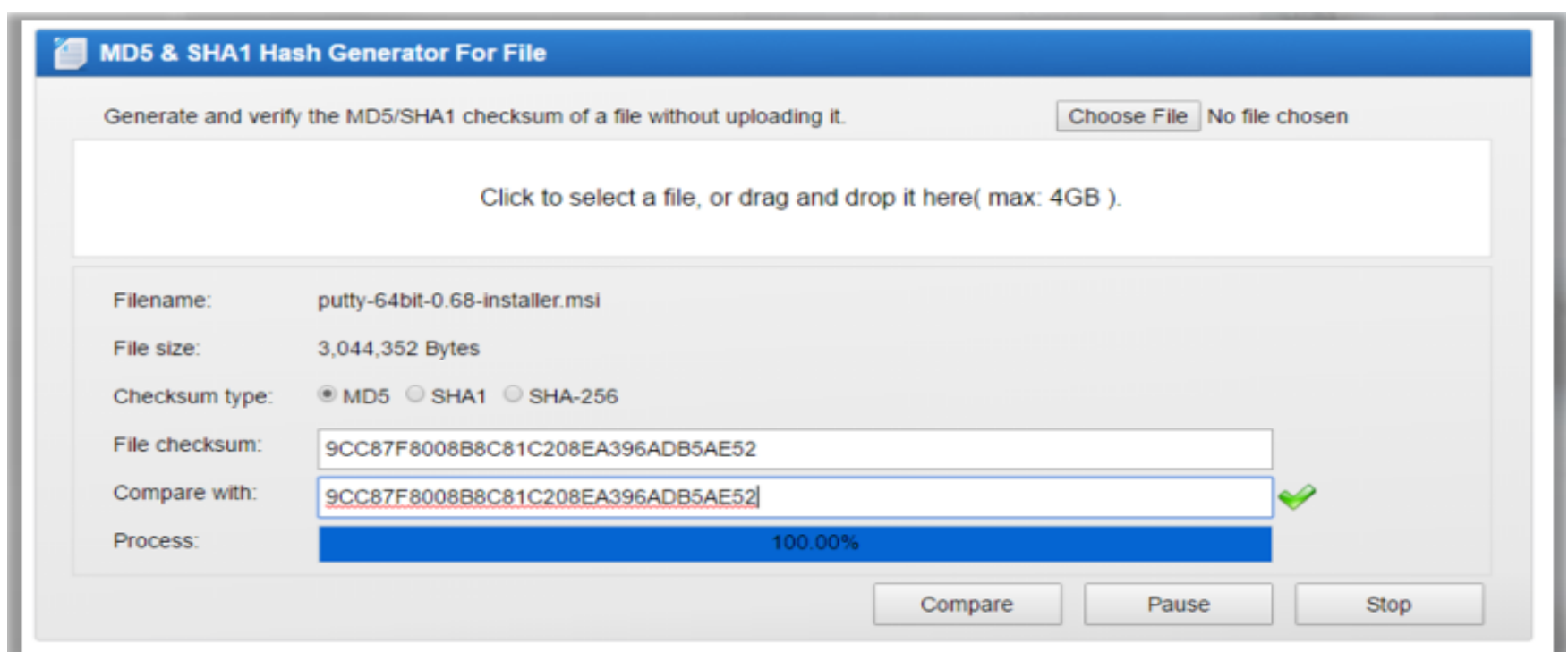
Cryptographic checksums for all the above files

MD5:	md5sums	(or by FTP)	(signature)
SHA-1:	sha1sums	(or by FTP)	(signature)
SHA-256:	sha256sums	(or by FTP)	(signature)
SHA-512:	sha512sums	(or by FTP)	(signature)

- ال **Checksum** الخاصه بال **Files** يعني ال **Hashes** الخاصه بال **Files** المختلفه اللى شركه **Putty** منزلها مع الملفات بتعتها عشان تعمل **Confirm** عالمفات اللى هتنزلها من عندهم أو اي مكان تاني .

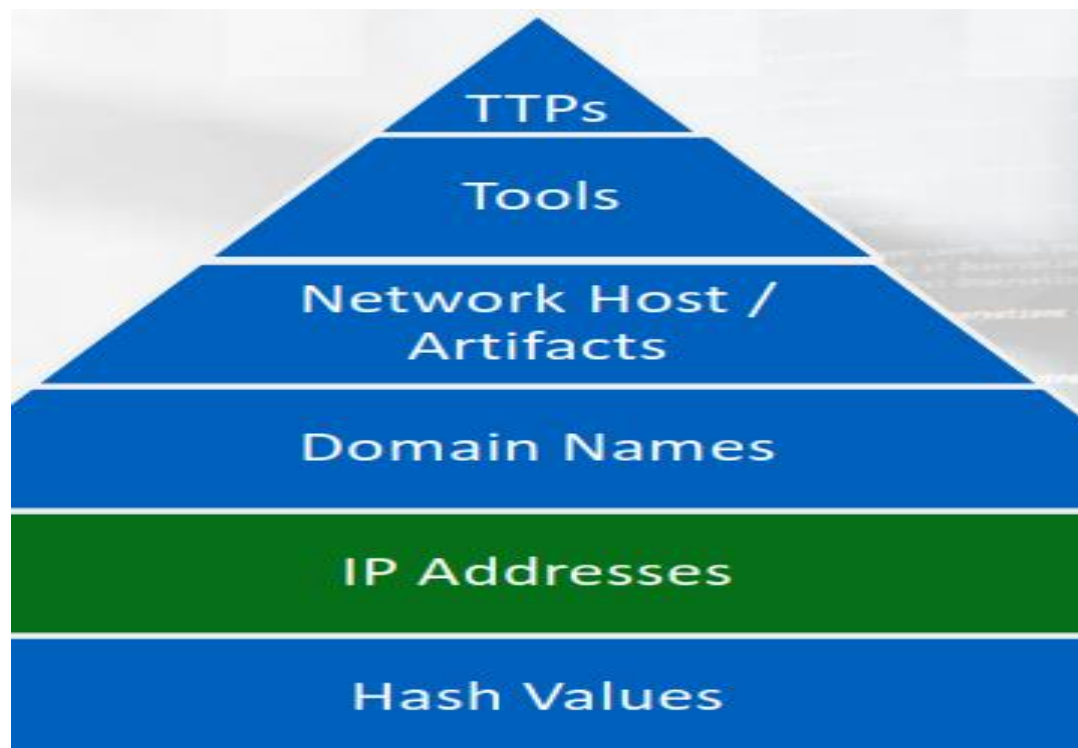
```
1c31b9d59c33124cf19aafe5ca4d8d77 w64/plink.exe
9206dae8b89a9e366b88f57a117068ea w64/pageant.exe
be183d872773a130efb8bf1f1c60b6db w64/puttytel.exe
caba0287018a2f1c0f4e7ba357f9072d w64/puttygen.exe
5ca0a9e56499c658d2790be7113930f1 w64/putty.zip
8ca5e64d33ff45f0278de27aa4994434 w64/pscp.exe
9cc87f8008b8c81c208ea396adb5ae52 w64/putty-64bit-0.68-installer.msi
a04e72503528dfc132c48e95fa3160ad w64/putty.exe
fc10492df39f9be3d8c139e2828a59da w64/psftp.exe
```

- اهوه بالضبط اللى قولناه هتلاقي لكل **File** ونسخه من ال **Putty** هتلاقي ال **Hash** بتعتها اللى تعمل بيه **Confirm** بعد اما تعمل **Download** للملف اللى انت عاوزه ... بعد كدا عندك مواقع **Online** كتير تقدر تحسبك ال **Hash** بتاعت الملف اللى عملته **Download** دا ترفعلها الملف وبعدين تحسبك ال **Hash** فانت تقوم واخذه مقارنه بال **Hash** اللى موجود عالموقع الأصلي وتعمل **Compare** مابينهم .



- دا هيفدنا فأيه ك **Threat Hunter** ... لما بنيجي نعمل **Hunt** فال **Incident** ولقينا **Malware** عال **machine** ال **Attacker** كان بيستخدمه فال **Attack** وحصلنا ال **Hash** بتاعه وروحنا شوفنا ال **Hash** دا بيدل على ايه لاقيناه دا **Unique Identify** ل **Malware** معين معروف فساعتها دا بمثابه ال **IOCs** فشغلك وساعتها عمله **Isolation** من ال **Machine** لأنه **Malicious** وكرمان هيعرفك ال **Attacker** بيستخدم انهو **Technique's** من خلال ال **Malware** اللى لاقيتها على ال **Victim machine** اللى حصلت ال **Hashes** بتعتها وتعرفت عليها أكثر من خلال عمليه ال **Search** هيخليك تبني عقلية عن ازاي ال **Attacker** بيشتغل ويستخدم انهو **Software** لما يجي يترجت **Victim** فانت تشوف ايه المفروض من ال **Defensive Techniques** اللى هتنفذها عال **Machines** اللى هتصد فالمستقبل نوعيه ال **Attacks** دي ... طب ليه مدام ال **Hash** كويس كدا بنصنفه انه **Unreliable** يعنى غير اعتمادي فشغلنا ك **Threat Hunters** ؟

- دا علشان ال **Attacker** يقدر يتلاعب فال **Hash** دا ويغيره بشكل مستمر ... بمعنى لو انت ك **Hunter** لقيت عندك **Malicious Software** عن طريق انك حصلت ال **Hash** الخاص بيه وبحثت عنه فعرفت انه **Malicious** ... طب لو ال **Attacker** نزل عندك **Malicious Software** معدل فالكوود بتاعه فلقيت انك بعد اما حصلت ال **Hash** دا مش عارف دا بيدل على ايه !! مش عارف تصنف ال **Hash** دا ايه أصلا !! لأن ال **Attacker** لعب فالكوود بتاعه فبالتالي غير ال **Hash** بتاعه فنتج عنه **Hash** جديد ... فهتلاقي عندك كميه من ال **Hashes** انت مش عارف دي ايه لا هي **Clean** ولا هي **Malicious** فانت هتقعد محتار وهتضيع وقت كبير ودا احنا مش عاوزينه فشغلنا أكيد ... علشان كدا لو لقيت **Hash** بيدل على حاجه **Malicious** وانت بتعمل **Hunt** فدا خير وبركه انما لو لقيت **hash** الدنيا فيه مش واضحه فساعتها هتبدء تروح للدرجه التانيه فال **Pyramid Pain** عندنا وهي ال **IP Addresses** علشان نكمل شغلنا.



- هتلاقي ال **Adversary** فجزءيه ال **IP** دي مبيدخلش ال **Network** بتعتك كدا بال **Real IP** لاء هتلاقيه بيدخل ب **Mask** عال **IP** بتاعه عشان يخفي العنوان الحقيقي ليه زي انه يستخدم ال **VPN** أو ال **Proxy** أو ال **Tor Browser** اللى بيستخدموه ال **Attackers** عشان يدخلوا من خلاله ال **Dark Web** ويبقوا مخفين فتعاملتهم دايمًا ودا عباره عن سلسله من شبكه ال **Proxy** مش مجرد **Proxy** واحد فانت بتطلع من **IP** فدوله معينه تروح للتاني واهي شبكه ماشيه ومحدث عارف يتتبع ال **IP** الحقيقي الخاص بيك فال **TOR** كل شويه بيغير الموقع بتاعك ل **IP** آخر كنظام تمويه وتشويش عشان لو فيه جهه أو شخص بيتتبع ال **IP** اللى انت متصل من خلاله حاليا ... ال **VPN** أو ال **Proxy** بيبقا أسهل فال **Detection** انما ال **TOR** بيبقا **More Secure** لل **Attacker** أكثر وطبعا ال **Detection** فيه بيبقا أصعب لأنك بتطلع من كذا **IP** من كذا دوله مختلفه .

- احنا ك **Threat Hunters** تعالى نشوف ازاي هنلاقي ال **Siem** بيطلعنا ال **IP Addresses** فال **Log** بتعته.

Dotted Decimal 192.168.1.1	Decimal 3232235777
Dotted Hex 0xC0.0xA8.0x01.0x01	Hex 0xC0A80101
Dotted Octal 0300.0250.0001.0001	Octal 030052000401

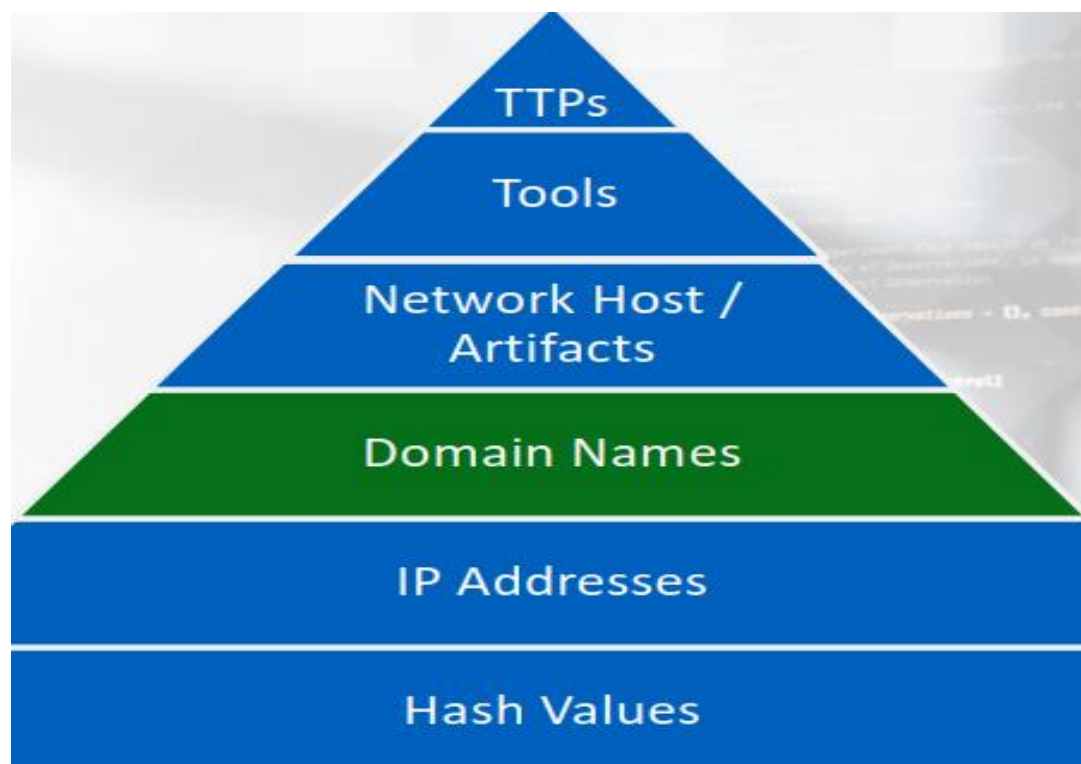
- ودي الأشكال اللي هتلاقي ال **Siem** مطلعهاك بخصوص ال **IP** بتاع ال **Attacker** لو عمله **Detect** بالفعل ... فممكن تلاقيه **Hex** وممكن **Octal** وممكن **Decimal** وممكن كل واحد من التلاته بس معاه الدوت (.). زي منتا شايف ... السؤال هنا هتعمل ايه لو لقيت **IP** زي دول انت ك **Threat Hunter** هتتعامل معاه ازاي؟؟

- أنت ممكن تعملها **Black list** انك تمنعها تدخل عندك فال **Network** مره تانيه ودا من خلال ال **Firewall** أو ال **Network devices** التانيه اللي عندك وطبعا دا بيبقا بالاتفاق مع باقي ال **SOC Team** اللي شغال معاك زي ال **IR** اللي بيتابعوا ال **Incident** هما اللي هيقولوك هل دا فصالح شغلنا انك تعمل **Block** لل **IP** دا دلوقتي ولا هنستنى عليه شويه لحد منوقعه فمصيده معينه مجهزنها ليه وبالتالي مينفعش انت ك **Threat Hunter** تاخذ قرار زي دا لوحدك لازم تشارك فيه ال **Team** بتاعك وتشوف أنهو حل أنسب فالوقت الحالي ... فحاله تانيه لو لقيت ال **Siem** بيقولك ان ال **IP** اللي مطلعهاك دا متصنف انه بيعمل حاجات **Malicious** عال **Network** فساعتها انت ممكن تعمله **Block** عادي مادون ذلك لازم تشارك ال **Team** بتاعك زي مقولنا ... وخذ بالك من نقطه فتحته ال **IP** قد يكون ال **Adversary** من ال **Internal network** !!؟ يعني ايه ...

- يعني موظف شغال معاك فالشرکه بس أخذ رشوه من ال **APT Group** وليكن اللي هتعمل عليك ال **Attack** ونزل من ال **Internet** ال **Malicious software** اللي متقف عليه وبعد كدا هما هيكملوا شغلهم وبتحصل كتير !! ... اللي أقصده انت لازم تراقب كمان ال **IP** اللي موجوده عندك فال **Internal Network** وتشوف خروجها عال **Internet** دا لحاجه ضروريه ولالاء وتشوف هي بتحمل ملفات ايه وهل بتدخل بال **Real IP** ولا من خلال ال **Proxy** أو ال **VPN** أو غيره.

- فساعتها دا يثير الشك حواليه وتبدء تراقبه بشكل مستمر وتحاول تربط مبین أي **Attack** يحصل عندك فالمؤسسه ومبین ال **Insider Attacker** دا وعلى هذه الطريقه من السيناريوهات لازم تاخذ بالك مش من ال **Attacker** اللى جايلك من برا فقط لاء من الموظفين اللى عندك لأنهم فكثر من الأوقات واتكررت فكثر من ال **Cases** بيكون ال **Attacker** اللى جي من برا أو ال **APT Group** أو اي مجموعه **Attackers** عموما بيساعدهم حد من جوا المؤسسه ودا أخطر!... ومجرد معرفتك ك **Threat Hunter** لل **IP** اللى جي من ال **Attacker** وتتأكد من دا خلاص انت تعمله **Block** فهتخلي ال **Attacker** لو عاوز ينفذ ال **Attack** بتاعه يبدء من جديد ب **IP** جديد تاني متعملهوش **Detect** .

- تعالى ندخل عالمرحله اللى بعدها فال **Pyramid Pain** وهي ال **Domain Names** .



- انت عارف انك عشان تطلع عال **Internet** لازم تعدي عال **DNS Server** الوسيط اللى بيوصلك بالموقع اللى انت عاوزه ... وال **DNS** علطول هتلاقيه **Update** بالمعلومات اللى تخص ال **Servers** اللى انت عاوز تتواصل معاها وليكن **Google** عشان تطلعه لازم تعرف ال **IP** واللى بيحول الاسم اللى بتكتبه فال **Browser** عندك لل **IP** بتاع **Google** فال **Background** هو ال **DNS Server** .

Unicode 邪悪なドメイン.com	Legitimate Domain rvasec.com
Punycode Xn—q9j5f9d1dzdq306auhtd.com	Malicious Homograph rvasec.com

- المشكلة عندنا ان لو كتبت اسم موقه بلغه زي الصيني مثلا ال **Browser** عندنا ميفهمش اللغه دي اللى هي صيغه ال **Uni Code** !! فكل **Domain** عندنا ليه **Puny Code** ترجمته يعني لصيغ تانيه ودا تمام مفيش مشكله ... انما المشكله عندنا بتدور حوالين حته ال **Punycode** انها بتحولك الموقع اللى ال **Browser** مش فاهمه لموقع يتفهم عادي بترجمه عادي لحاجه تتفهم ولكن مضمونها **Malicious** ودا اللى بيستغله ال **Attacker** انه يبعثك ال **Puny code** ف **Mail** مثلا وانت شايف ال **Domain** قدامك بتاع موقع موثوق فيه وانت عرفه وليكن **Google** ولكن دا عباره عن **Puny Code** لموقع تاني لما تضغط على ال **Link** دا هيحولك لموقع **Malicious** غير الأصلي اللى انت شوفته فال **Link** وضغطت عليه ... وال **Attack** دا حاليا بيتعمله **Detect** من ال **Browsers** لو لقيتكم بتفتح من خلالها **Link** وحست ان ال **Link** دا بيتعمله ترجمه لموقع آخر ساعتها هتوقفك وتديك **Alert** وتقولك الموقع دا بيحولك على موقع آخر قد يكون **Malicious** فالأحسن انك متفتحش الموقع دا ... يبقا الاختصار للكلام اللى فات عندنا ال **ASCII** دي اللغه اللى بيّفهمها ال **Browser** وال **Uni code** دي اللغه اللى مبيّفهمهاش ال **Browser** وبنستخدم ال **Puny code** عشان نحول ال **Uni code** لل **ASCII** .

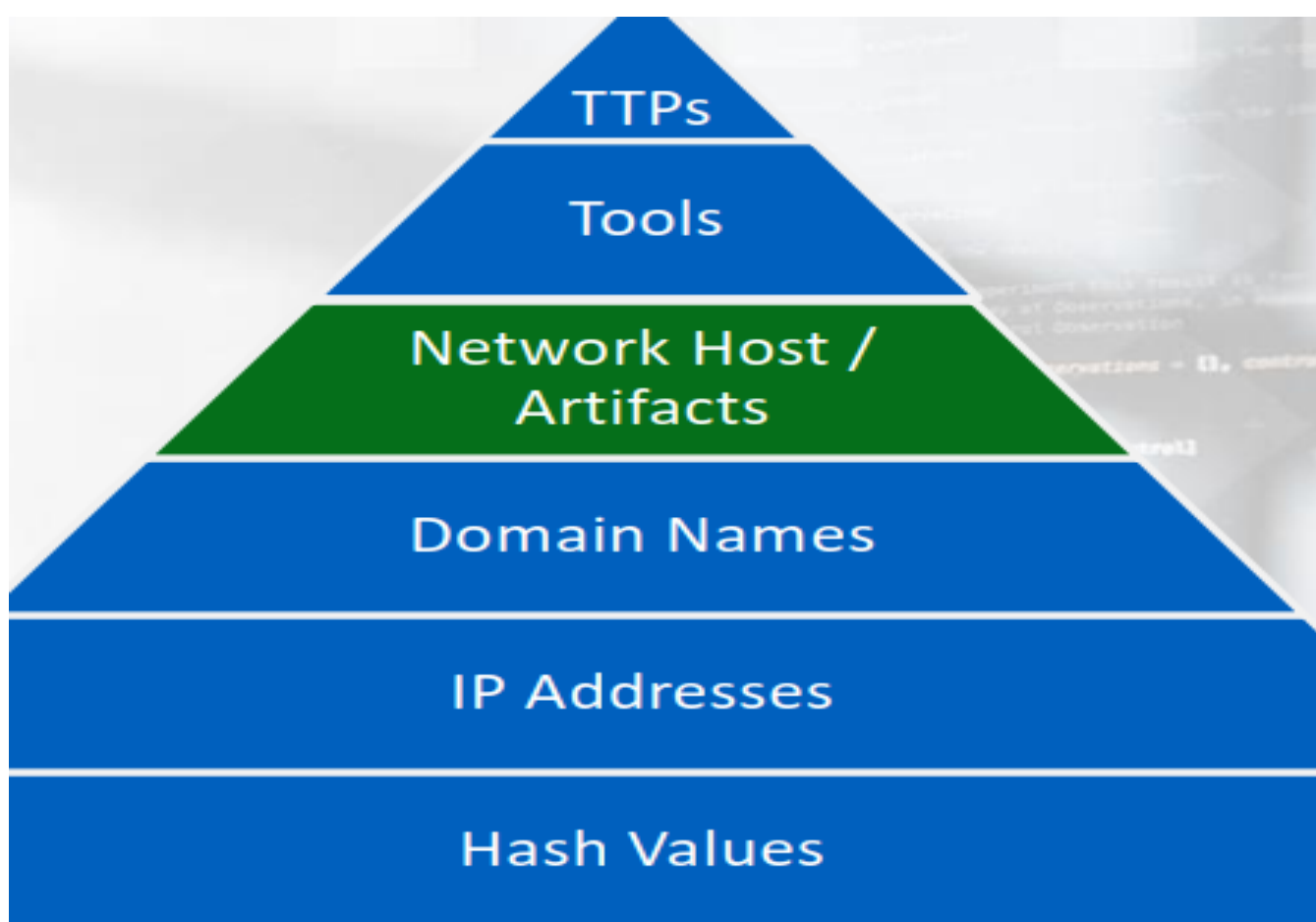
- خد مثال لموقع **Uni Code** حولناه لل **Puny Code** اللى يفهمه ال **Browser** عندنا .

Text	→	Punycode
Example: 點看		Example: xn--c1yn36f

- ودا اللي بينتج عن استخدام تقنيه ال **Puny code** ... موقعين بنفس الاسم واحد **Malicious** والثاني الأصلي .



- نيجي لل **Step** اللي بعد كدا عندنا فال **Pyramid of Pain** بتعنا وهي ال **Network Hosts & Artifacts** .



- وال **Artifacts** دي معناها ال **Tools** اللي استخدمها ال **Attackers** وهو عندك جوا ال **Network** ونسى يشيلها معاه أو يعمل **Delete** للأثار بتعتها ... فدي تعتبر ال **Clues** الادله اللي سابها ال **Adversary** وراه عال **Network** بعد أما نفذ ال **Attack** أو حتى هتلاقيه سلبها عال **End point system** ... زي مثلا ال **Attacker** عمل **Scanning** كتير عندك عال **Network** ...

- فال **Logs** عندك بتاعت ال **Siem** سجلت انه فيه **IP** معين دخل عندنا عال **Network** وعمل **Scan** كتير بشكل غير اعتيادي فال **IP** دا يعتبر هنا **Artifact** وبرضه لو ال **Attacker** ف **End point** بعد معمل عليها ال **Attack** نسي يحذف ال **Malware** من ال **End point**

فنقدر ساعتها نروح ناخذ ال **Malware** دا ونعمله **Analysis** ومن خلال ال **Analysis** نوصل لل **Attacker** ... ناخذ أمثله تانيه .

Network Artifacts	Host Artifacts
Rare User-Agent strings	Specific Registry key
Traffic on non-traditional ports (i.e. 6667)	Process connected on port 80 that is not a browser

- ال **Network Artifacts** زي منتا شايف هتلاقي ال **Attacker** بيستخدم ال **rare user** وهو داخل عندنا فال **Network** بالإضافة لأنك هتلاقيه شغال على **Non-traditional Port** يعني بورتات غير اعتياديه أو معروفه عندنا فال **Network** زي **6667** ... يعني ببساطه احنا ك **Threat Hunter** لما جينا نعمل **Hunt** عال **Incident** اللى عندنا لقينا ال **Attacker** داخل عندنا من **Agent** يعني متصفح غريب مش معروف زي **Google** أو **Edge** أو **Yahoo** أو غيره ... لقينااه داخل عندنا من متصفح غريب فدي أول نقطه فال **artifact** فال **Network** ... وتاني نقطه هتلاقيه جي يعمل عليك **Attack** من خلال ال **Port number** زي **6667** !!! ودا **Non-Traditional** بالنسبه لينا فالمؤسسه اي حد جايلنا من ال **WAN** داخل لل **LAN** عندنا مبيجيش من ال **Port** دا فدا تاني **Artifact** يخلينا نعرف ان فيه **Attack** حصل لل **Network** عندنا .

- عندنا بعد كدا ال **Host Artifacts** زي ال **Registry Keys** اللى بينساها ال **Attacker** عال **End point machine** اللى عملها أختراق بالفعل ... بالنسبه ل **Machine** ال **Windows** أي حاجه بتعملها عليها بتتسجل فمكتبه ال **Registry** عال **System** عندك .
- فلقينا فال **Registry** واحنا بنعمل **Hunt** لل **Incident** انه فيه **Specific Key** متسجل فال **Registry** وشكله غريب فساعتها دا بنصنفه **Artifact** لل **Attacker** ك **Host** فال **Network** عندنا .

- ثاني حاجة معانا هي انك وانت بتعمل **Hunt** لاقيت **Process** شغاله على **Port 80** ومش متصله بال **Browser** والمفروض انها تكون **related** بال **Browser** واي حاجة شغاله من خلال ال **Browser** هتلاقيها شغاله على ال **HTTP** أو ال **HTTPS** اللى هما **80** أو **443** فأنت لقيت **process** شغاله عندك على ال **Host** فال **End point** على **Port 80** ومش **related** بال **Browser** فتعرف علطول ان دي تابعه لل **Attacker** تابعه لل **Attack** اللى كان بيعمله ونساها عال **Host** ... وبرضه هتلاقي **Port 80** شغال عادي ولكن مفيش **Traffic** خاص بال **HTTP/S** أو اي **Traffic** خاص بال **Web** فتعرف تميزه علطول انه **Host Artifact** ... نشوف مثال عالكلام دا .

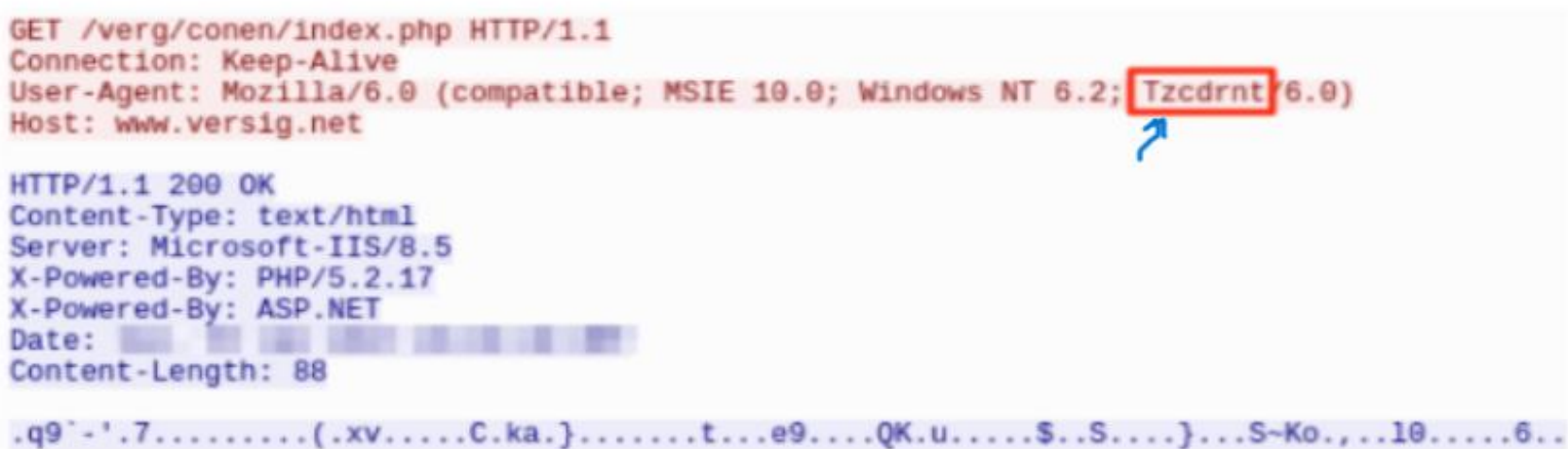
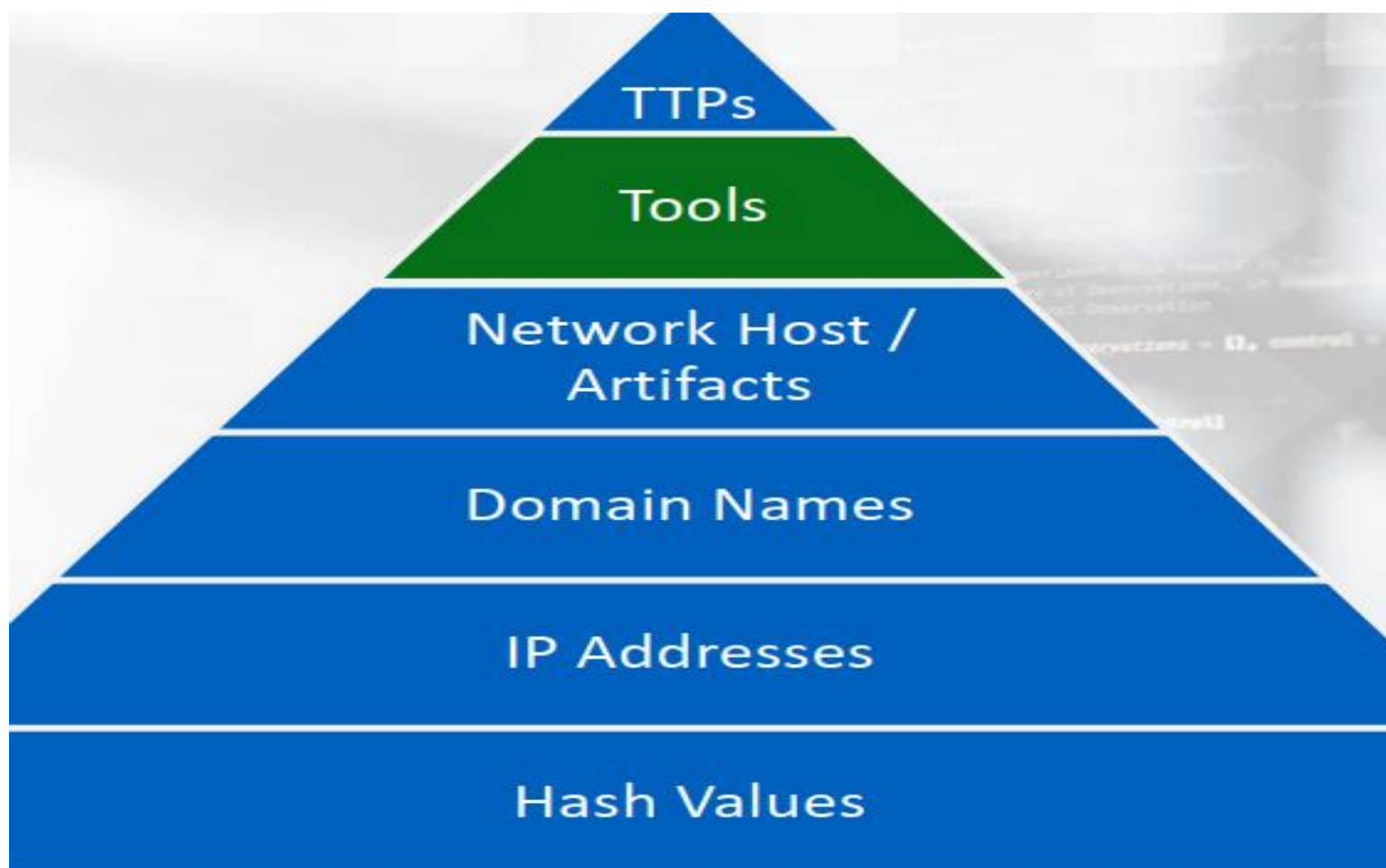


Figure 9: ZeroT initial beacon over HTTP requesting URL configuration

- واخد بالك من ال **Agent** اللى بيستخدمه ال **Attacker** هتلاقيه زي مقولنا مش مألوف بالنسبه لينا ودا **Real World Scenario** ... فدا مثال على ال **Network Artifact** عشان توصلك المعلومه أكثر ... ندخل بعد كدا على ال **Step** اللى بعد كدا فال **Pyramid Pain** وهي ال **Tools** اللى بيستخدمها ال **Attacker** ...

- لو تاخد بالك احنا شغالين خطوه خطوه نفصص فكل جزء من ال **Pyramid pain** عشان ضروري ك **Threat Hunter** تكون عارف كل جزء فيه بيمهد للى بعد ازاى وتكون عارف لما تقابل **Incident** هتتعامل معاها ازاى وتوقفها بدري قبل أي **Risk** ممكن تضر المؤسسه بتعتك .

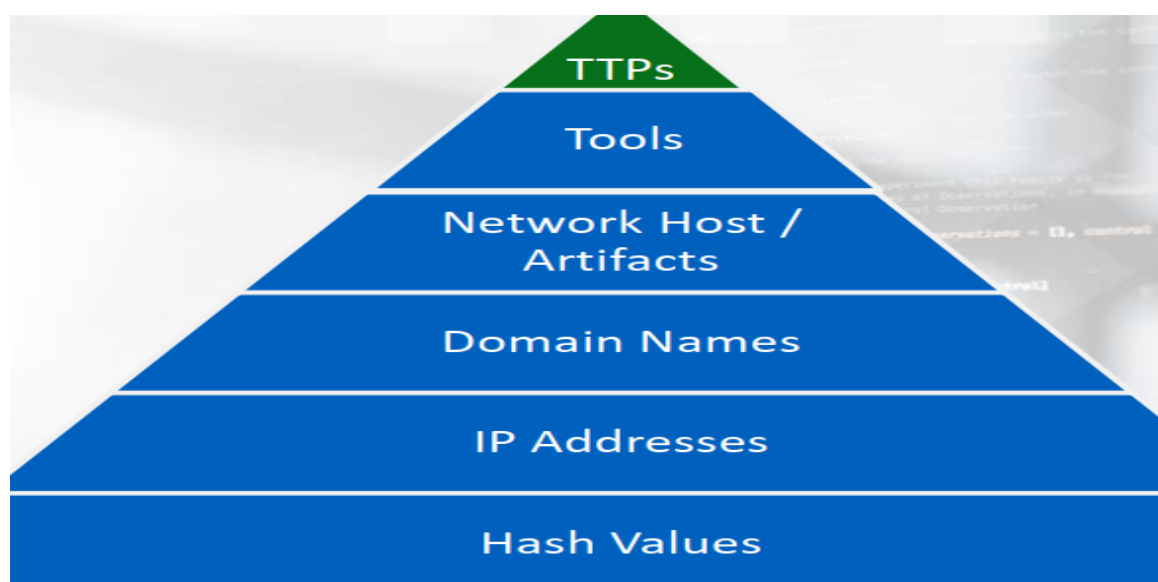


- وأنت بتعمل **Hunt** لقيت بعض ال **Tools** اللى ال **Attacker** بيستخدمها وانت من خبرتك المفروض عارفها فأول متشوفها على **Machine** حصل عليها **Incident** تعرف علطول ان هنا عال **End point** دي حصل **Attack** لأن ال **IOCs** واضح قدامك ... فلو لقيت ال **tools** المعينه دي زي ال **Nmap** اللى ال **attacker** بيعمل بيها **Scanning** أو ال **Metasploit** اللى بيستخدمها فال **Exploitation phase** أو اي **Tool** ليها علاقه بال **Attack** عموما دي دليل كافي يعرفك ان هنا كان فيه **Attack** حصل عال **Machine** دي ...

- أي **APT Group** أو حتى **Individuals Attackers** هتلاقهم بيستخدموا بعض ال **Tools** بشكل اعتيادي فال **Attack** بتعم وبيفضلوها عن اي **Tool** تانيه زي ال **Nmap** مثلا زي موضحنا فال **Scanning Phase** عال **Target** بتعم ... وزي ال **SQL map** فال **SQL Injection Attacks** برضه عندك **Tools** كتير ولكن ال **Pen tester** أو ال **Attacker** بيفضل ال **Tool** دي فعلشان كذا لازم انت ك **Threat Hunter** تكون عارف ال **Tools** دي وعارف ال **Attacker** بيشتغل ازاي وايه هي أدواته عشان تعرف تعملة **Hunt**

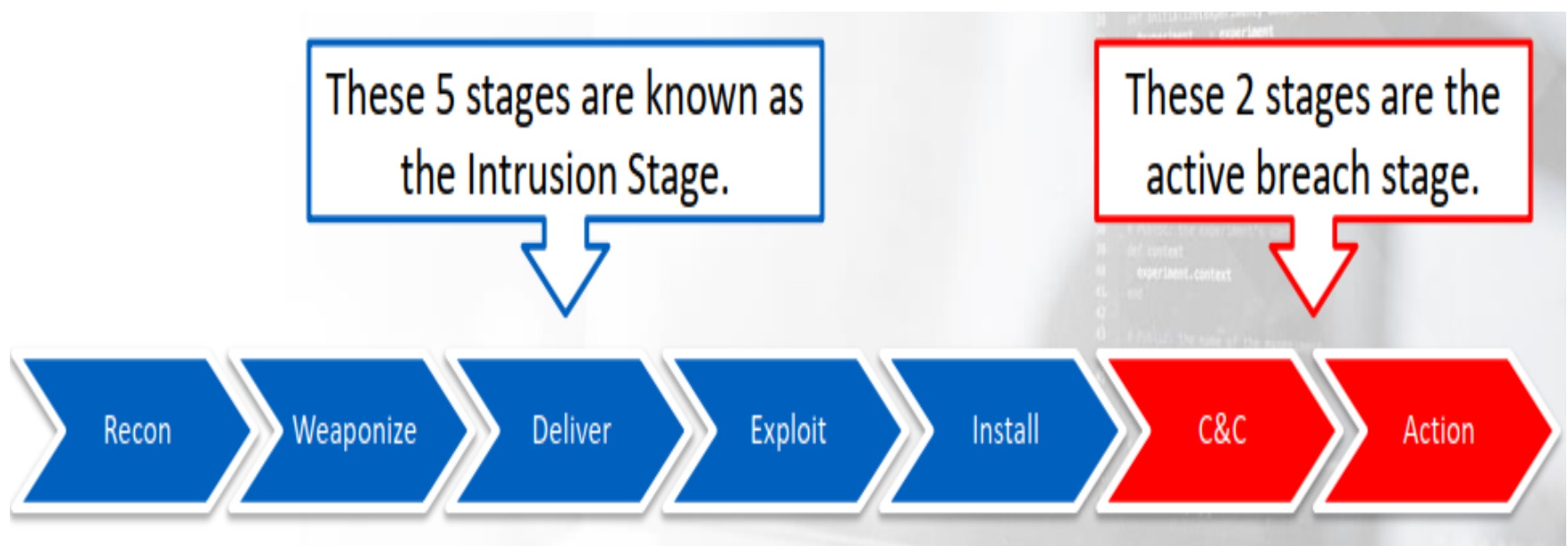
- فانت ك **Threat Hunter** عرفت ال **Tool** اللى شغال بيها ال **Adversary** عندك فال **End point** وعملت لها بلوك من عندك دا يفيدك فأيه أو يفيد مؤسستك فأيه !!؟؟ لو جه ال **Adversary** يستخدمها مره تانيه هيلاقىها ممنوعه فانت كدا أجبرته انه يغير طريقه شغله ويستخدم **Tool** تانيه من أول وجديد وضيعتله وقته ومجهوده دا غير ان ممكن مبيكنش يعرف يستخدم **Tools** تانيه الا اللى عارفهم فال **Attack** بتاعه مش هيتم مره تانيه فانت كدا منعته بخطوات بسيطه أو مش متعود عال **Tools** دي فدا كله فمصلحتك انك تأخره .

- تعالى نروح للسلمه الأخيره فال **Pyramid of pain** عندنا وهي ال **TTPs** اللى كنا اتكلمنا عليها قبل كدا فوق أرجعلها ولكن هنذكرها عالسريع .



- من الآخر عشان تتعرف عال **TTPs** اللى هي طرق ال **Adversary** فال **Attacking** حلها ال **Training** الكثير !! عشان تعرف آخر ال **Techniques** وال **Tactic's** وال **Procedures** اللى هما اختصار ال **TTPs** لازم يكون عندنا ناس شغالين فال **SOC** يكونوا **Qualified** يعني **Updated** بشكل مستمر بأخر ال **Attacks** وآخر ال **APT Group Attacks** وال **Scenario's** المختلفه والجديده بتعتهم ... فلازم الناس دي تهتم بيها وتديها **Training** علطول متستخسرش فالأشخاص اللى عندك انت هتستثمر فيهم فانت هتحفظ مؤسستك وعملك من الأنهار لازم تصرف عالأشخاص تماما وتزودهم معرفيا زي المؤسسه بتعتك تماما .

- عندنا مصطلح جديد أسمه ال **Cyber Kill chain Model** ودا عباره عن رسم توضيحي ودا عباره عن **Model** بيوضحك ازاي ال **Attack** بيتم بالخطوات اللى بيمشي عليها ال **Attacker** بال **Stages** عشان انت ك **Threat Hunter** تبقا عارف ال **Methodology** بتاعت ال **Attacker** وتعرف تعمل **Detect** لل **Attack** دا بدري ... فأنت هتتسأل ك **Threat hunter** ازاي ال **Attack** حصل بعد اما ال **Incident** تخلص وتيجي تعمل فيها ال **Investigation** وتكتب ال **report** بتاعك ... من خلال ال **Cyber Kill Chain Model** هتقدر ك **Threat Hunter** تعرف ال **Attack** تم ازاي عالمؤسسه بتعتك بتفاصيله ... فتعالى نتعرف عال **Cyber Kill Chain** مع بعض .



- ال **7 Stages** دول هيفسرولك ازاي ال **Attack** تم عندك عالمؤسسه وفيه منهم **5 Stages** ال **Attacker** بيعملهم عندك عشان يعرف يعملك ال **Infection** يعني يعمل لجهازك أصابه بال **Exploit** بمعنى بيتدي ف عمليه الاختراق اللى هما ال **Intrusion Stage** وبعد كدا عندك ال **2 Stages** التانيين اللى بنسميهم ال **Active Breach** **Stage** ودي المراحل اللى من خلالها ال **Attacker** هيعرف ياخد **Remote Access** عليك يتحكم فيك عن بعد ... مهم تعرف كل مرحله منهم لأنك هيقابلك بعض ال **Incident** هتلاقىها ف واحده من ال **Stages** دول فمثلا هتلاقي ال **Attacker** فعلا عمل **Exploit** للتغره اللى عندك فال **Network** أو ال **PC** ودخل لجهازك وبيثبت ال **Exploit** لسه وانت ك **Threat Hunter** اكتشفت دا ؟!! .

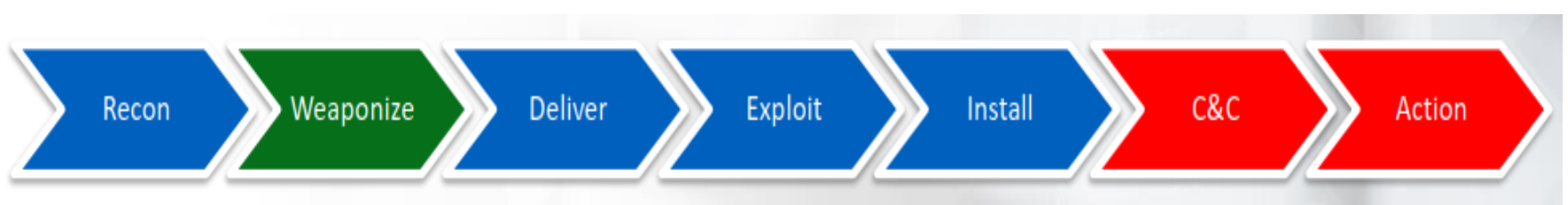
- فدا معناه انه عملك ال **5 Stages** كلهم اللى ذكرناهم ولسه بيعمل **Install** فانت تحاول توقفه هنا بدل مياخد ال **2 Stages** التانيين وتبقا العملية أصعب عليك ... واحنا اتكلمنا فموضوع الوقت دا قبل كدا وذكرنا أهميته بالنسبة لل **Threat Hunter** فكل موقفك ال **Incident** وعملت **Detect** لل **Attack** بدري كل مالمؤسسة بتعتك تفادت خساره كبيره ووفرت عليها مجهود كبير و دا بيقلل ال **Risk** اللى اتعرضت ليها المؤسسة من ال **Attack** دا طبعا كل مقدرت على حسب خبرتك تتحكم فالوقت وتعمله **Detect** بدري فأهم حاجه فأي **Incident** هو عامل الوقت ودا مجرد مثال للتوضيح وعندك كتير .

- تعالى ناخد **Phase Phase** منهم زي ال **Pyramid of pain** بالضبط ونفهمها مع بعض .



- **أول Phase** معانا هي ال **Recon** ... اللى هي ال **Information** **Gathering** عال **Target** بتاعك فقبل ماي **Attacker** او **APT** group يترجت المؤسسة أو الفرد اللى هينفذ عليه ال **Attack** بيجمع عنه معلومات الأول بطريقه **Passive Scanning** اللى هو بيجمع عنك معلومات من غير ميتواصل معاك بشكل مباشر مش زي ال **Active Scan** اللى بيتعمل بال **Nmap** كدا ... فهتلاقيه بيروح لل **OSINT** اللى هي ال **Open source intelligence** اللى هي الحاجات الموجوده **Public** عال **Internet** فال **Attacker** بيستخدمها عشان يقدر من خلالها يجمع معلومات عن ال **Target** بتاعك ... زي ال **Social Media Accounts** مثلا **LinkedIn** أو **Facebook** وال **Search engine** ومعاها ال **Dorks** بتاعت **Google** مثلا ... وهتلاقي ال **Attacker** بيعمل برضه ال **Active Scan** اللى هو ال **Attacker** بيستخدم **Tools** عشان يعمل عال **Network** ال **Scanning** عن طريق ال **Nmap** وغيرها من ال **Tools** .

- فانت فال **SOC** مثلا لقيت **IP** معين بيعمل على ال **Network** بتعتك **Scanning** بشكل متكرر وحجم ال **Traffic** بتاعه كبير فتعرف ان دا **Malicious IP** بيحاول يشوف ايه هي ال **Ports** المفتوحة عندك عشان يشوف ال **Services** اللي شغاله عليها وبعد كدا يعملها **Exploit** او استغلال فدي كلها معلومات لازم تاخد بالك منها وانت شغال فال **SOC** فتعمل **Block** لل **IP** دا وعندك سيناريوهات كثير جدا تقدر تشوفها عملي كمان على موقع زي **Cyber Defender** اللي بتقدمك تدريبات متنوعه وسيناريوهات مختلفه لل **Attacks** وطريقه حمايتها ... نروح **لتاني Phase** معانا وهي ال **Weaponize** .



- ودي المقصود منها التسليح لعملية ال **Exploitation** اللي هينفذها عال **Attack** بمعنى ... ايه هو ال **Technique** اللي هتمشي عليه عشان تنفذ ال **Attack** بتاعك ... فمثلا انت عارف ان ال **Target** بتاعك وانت بتجمع عنه معلومات فمرحلة ال **recon** انه عنده فالمؤسسه **Servers** بتاعت **Microsoft 2019** مثلا ... يعني منزل عنده عال **Servers** نسخه **Microsoft Windows 2019** فدي معلومه فانت ك **Attacker** هتبدء تطور **Exploit** مناسب لل **Attack** دا ال **RAT** اختصار ل **Remote access Trojan** وتبعته لل **Victim** على ثغره فنسخه ال **Windows Server 2019** منتا لما عرفت انه شغال بيها روجت بحثت عن نقط الضعف وآخر ال **Exploits** فالنسخه دي من على موقع **Exploit database** مثلا وجبت ال **Exploit** بتعتك وهتبعته لل **Target** بتاعك ... فال **Weaponization** بتعتك هنا هي ال **RAT** الطريقه اللي هتبعته بيها ال **Payload** بتعتك اللي بتبعته مع ال **Exploit** عند ال **Target** عشان تشكل **Thread** عالمؤسسه ... طبعا بنختار ال **Weaponization** على حسب المعلومات اللي جمعناها من مرحله ال **Recon** وعلى حسب المعلومات بنختار السلاح المناسب .

- عرفنا ال **Special Weapon** بتعنا ايه اللي هنستخدمه عند ال **target** نيجي للى بعده وهي ال **Phase الثالثة** ال **Deliver** .

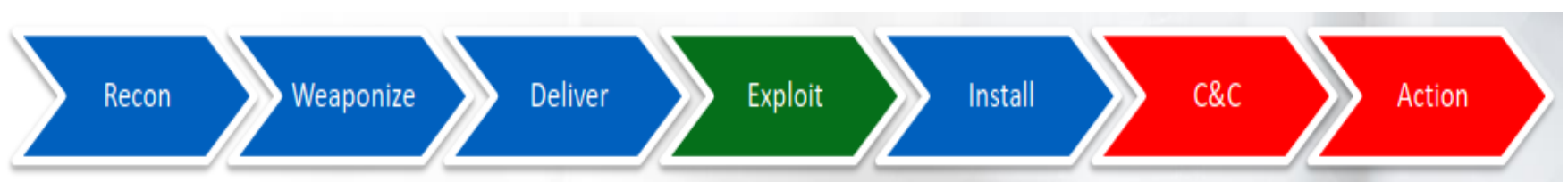


- ودي المرحلة اللي عندنا ال **Attacker** فيها بيعمل **Delivery** لل **Weaponized Tool** اللي قرر ال **attacker** انه هستخدمها من خلال عمليه ال **Recon** اللي عملها عال **target** ... مش احنا معانا ال **RAT** اللي هي ال **Weaponize** بتعنا اللي هيبعتها مع ال **Exploit** لل **Target** طب هل سألت نفسك هيبعتها ازاي !!؟؟ ... لازم يكون عند ال **Target** بتعنا **Vulnerability** يعني نقطه ضعف يقدر ال **Attacker** يدخل من خلالها عند ال **Victim** ... يعني لازم الثغره الموجوده عند ال **Target** عشان يبعثه من خلالها ال **Exploit** اللي بيشيل ال **Payload** فسكته ... فالثغره دي هي بالنسبه لل **Attacker** ال **Delivery Method** ... وبرضه ممكن ال **Delivery** دا يكون ال **Email** أو **Port** مفتوح عند ال **Target** أو من خلال ال **social media** أو من خلال ال **Water Hole Attack** ودي مرحله **Advanced** شويه لأنها بتحتاج ان ال **Attacker** يكون أخترق ال **Victim** بالفعل ونزل عنده عال **Server** الملف ال **Malicious** اللي هيعمل **Infection** لأي حد يخش عليه فأني حد هيتواصل مع ال **Server** دا هيتم أصابته بال **Malware** اللي موجود عالملف .

- دا مثلا ممكن يحصل عال **Active Directory** انه يثبت عليه **Exploit** ما وأي شخص جوا المؤسسه يتعامل مع ال **Active Directory** فيتصاب بال **Exploit** دا ... ودا لأن هو دا ال **Server** اللي بينظملك التواصل مابين الأجهزة فالمؤسسه عندك سواء أي **Request** أو **Responds** فال **Server** دا المسؤول عنها ... دا مجرد مثال .

- خد بالك من نقطه فال **Cyber Kill Chain** الترتيب مهم بين ال **Phases** وبعضها فمثلا مينفعش ال **Deliver** تتنفذ قبل ال **Weaponization** ف لازم ال **Attacker** يمشي على نفس الترتيب اللى ذكرناه ... كل دا لازم يكون حاضر معاك وانت بتعمل **Hunt** لأنك وانت بتعمل **Investigation** لقيت مثلا ملف **Malicious** مخفي على **Machine** ما فكدا انت بالمنطق استنتجت ان ال **Attacker** نفذ ال **3 Phases** عال **target** بتاعه عمل ال **recon** وال **weaponization** و كمان عمل ال **Deliver** بدليل الملف الموجود قدامك دلوقتي عال **Machine** و داخل على **Phase 4** اللى هي ال **Exploit** ... و لازم تفكر بعقليه ال **Attacker** الأول وتحط نفسك مكانه عشان تعرف عمله **Hunt** وما دون ذلك فأنت بتبصمج **techniques** وبتنفذها زي ال **Tasks** الروتينيه كدا تماما.

- نيجي لل **Phase الرابعه** معانا اللي هي ال **Exploit** واللى بيحصل فيها ال **Actual Exploitation** الأختراق الفعلي لل **Target** بتاعك .



- ودا بيحصل لما ال **User** اللى انت بعته ال **Malicious Attachment** يفتحه من خلال **Gmail** اللى انت بعتهوله عليه أو يضغط على **Link** معين ... طب لو طلع واحد قلك احنا عندنا **NGFW** بيمنع ال **Attacks** اللى من النوع اللى ذكرناه بتاع ال **Attachment** دا لو لقي اي **Attachment** فال **Mail** بيصنفه انه **Malicious** وبيمنع وصوله لل **User** ... ال **Attacker** هتلاقيه بيتفادى الكلام دا بأنه بيعتلك ال **Loader** فالأول اللى هو بيكون ملف **exe** وبيكون **Clean** فأنت دا كدا هيعدي من ال **NGFW** ... أول مال **user** يضغط عال **Loader** دا المبعتهوله فال **Email** بيقوم محمل من ال **Internet** ال **Actual RAT** على جهاز ال **User** وبكدا يكون ال **attacker** تخطى حته ال **Firewall** دي .

- بعد أما تمت مرحله ال **Exploitation** عال **Target** بتعنا ... تعالى نشوف ال **Phase** اللى بعدها وهي **الخامسه** ال **Install** .



- وال **Phase** دي بتقع فحيز ال **Persistence** اللى هي الاستمراريه لل **Attacker** عندك عال **Machine** اللى عملها اختراق ... فتلاقيه يزرع عندك **Keylogger** عندك عالجهاز عشان يسجله كل الضغوطات بتاعت ال **User** عالكيبورد ... فتلاقيه زارع عندك **Backdoor** مثلا عشان منين ميحب يرجع لجهازك ميفقدش ال **Connection** ويرجع يعمل ال **Attack** من أول وجديد من تاني ... لاء بيضمن استمراره على جهازك حتى فحاله خروجه أو ان ال **User** يعمل **Shutdown** لجهازه أو **restart** كل دا ليه **Techniques** عند ال **Attacker** بتقع فحيز ال **Persistence** زي مذكرنا ودا ممكن هنشوفه قدام فحاجه زي ال **Malware Persistence** ان ال **Malware** اللى بيعته ال **Attacker** لل **Victim** هتلاقي ال **Malware** بيخبي نفسه فملفات ال **Registry** الغير معروفه لل **user** عشان يعمل منها **AutoStart** من ال **Location** اللى خفا نفسه فيه وعندك طرق تانيه كتير لل **Persistence** زي ال **DLL Hijacking** ودا هنبقا نناقشه فموضعه باءذن الله فجزء ال **Malware Hunting** .

- نيجي لل **Phase** **السادسه** معانا من ال **Cyber Kill Chain** **Model** وهي ال **C&C** اختصارا ل **Command & Control** .



- هنا ال **Attacker** يقدر يخلى ال **Victim** ينفذ **Commands** معينه بطريقه **Remotely** ... فال **Victim** كدا أصبح فرد من جيش ال **Attacker** .

- نيجي لل **Phase** الأخيرة معنا وهي ال **Action** .



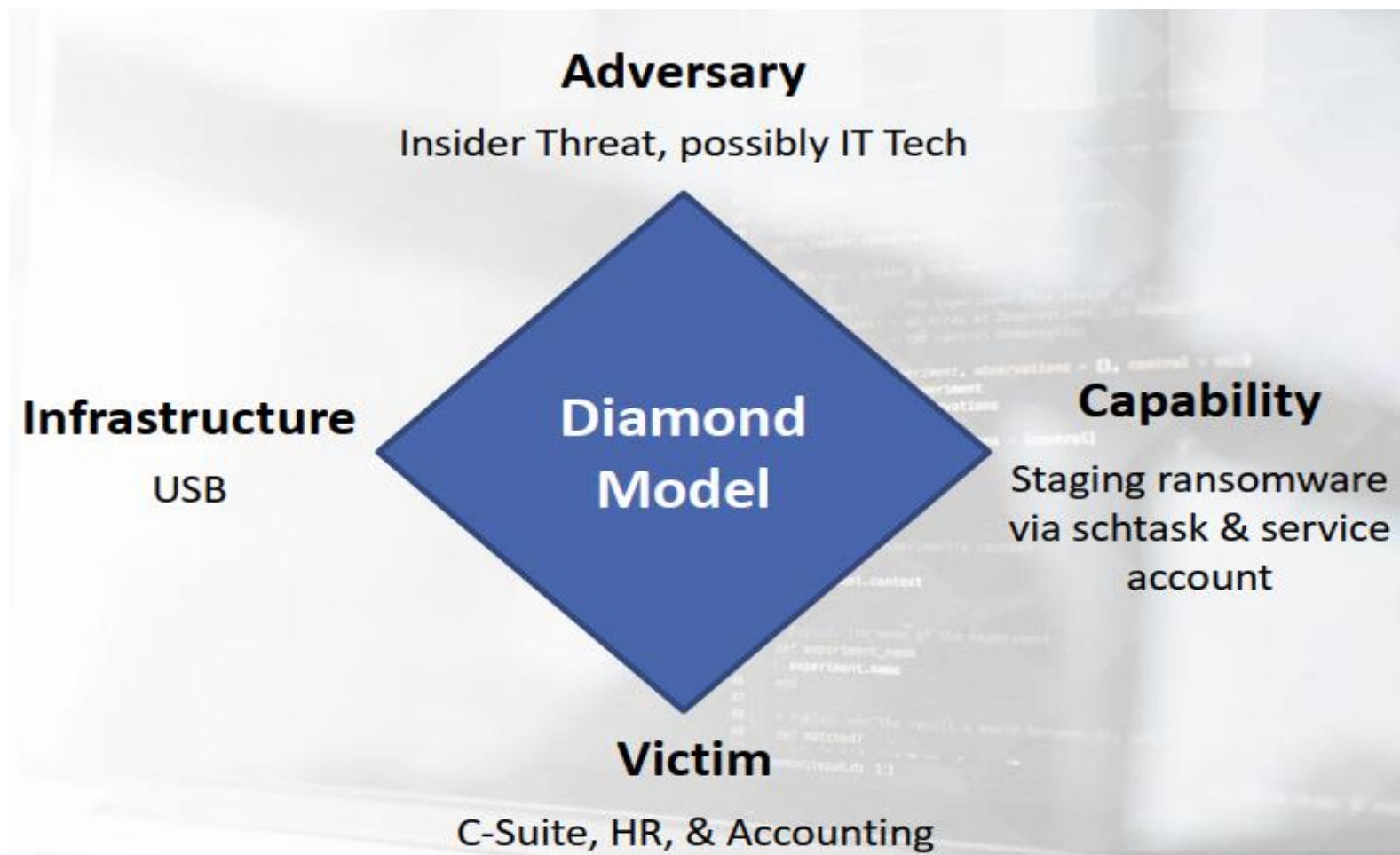
- فالمرحلة دي ال **Attacker** خلاص بيبقا وصل لل **Target** بتاعه اللى عاوزه من الأول زي انه ممكن يكون كان عاوز يعمل **Data Exfiltration** مثلا من عند المؤسسة بتعتك ... بمعنى فيه **Sensitive data** تخص المؤسسة بتعتك هو وصلها وهيسربها ويبعها عال **Dark Web** دا واحد من ضمن **Targets** كتير عند ال **Attacker** ... وممكن تلاقي ال **Attacker** بيستخدم جهاز ال **Victim** عشان يعمل **Pivoting** لباقي ال **Devices** الموجودة عندنا فال **Network** ... بمعنى انه يتنقل من جهاز لآخر عن طريق جهاز ال **Victim** اللى عمله **Exploit** انه يعمل **Scan** لباقي ال **Network** ... والكلام دا اتشرح تفصيلي فملفات ال **eCPPT V2** الموجودة عندي على **LinkedIn** اللى شرحنا فيها ال **Section** الخاص بال **Network Security** بشكل كامل تقدر ترجعلها لو محتاج تفاصيل وتوضيح أكثر... فال **Attacker** مثلا ال **target** بتاعه النهائي هو ال **Server** ولكن صعب الوصول ليه عشان هو جايه من ال **WAN** لل **LAN** وهيلاقي **Defensive Network Devices** كتير فسكته هتوقفه فيروح لافف حواليه بمعنى ... يروح يشوف جهاز جوا ال **Network** ويعمله ال **Exploitation** ويخرقه بالفعل ويبقا واحد من الأجهزة الموجودة فال **LAN** وياخد الجهاز دا ك **Bridge** كوبري يوصل منه لل **Server** اللى هو الهدف النهائي بتاعه وهو اللى يهمله انه يوصل لل **Server** فالنهايه ازاى دي بقا ! تنفع بكذا **Method** المهم توصل لل **Target** وهو دا باختصار ال **Pivoting** ... فأخر مرحله من ال **Cyber Kill Chain** اللى بنتكلم فيها حاليا ال **Data** بتاعت مؤسستك اللى كنت بتحميها هتشوفها هنا وهي بتتسرب أو موجودة بالفعل على مواقع بيع ال **Dark Web** الخاصه بالتسريبات فمعتش هنا هينفعك الندم ... وعلشان كذا كنت بقولك عامل الوقت مهم جدا جدا .

- في حاجتين مهمين مهم تعرفهم عن ال **Cyber Kill Chain** بعد أما خالصناها وهي انها **Cyclic Process** وكمان **non-linear** !!؟؟

- معنى **Cyclic** يعني ال **Phases** دي متكرره ال **Attacker** ممكن يكررها كثير مش بيعملها مره واحده وخلص ... فال **Attacker** عمل ال **Recon** عال **Target** بتاعه واختار ال **Weapon** بتاعه وبعد كدا راح يعمل **Deliver** وفشلت معاه العمليه !! هيروح يعيد ال **Phase** الأولي من تاني وهي ال **Recon** ويجمع معلومات أكثر عن ال **Target** ويشوف **Weapon** تاني ويجرب بيه لحد معمله ال **Exploitation** تنجح بالفعل فعلشان كدا سمناها **Cyclic** ... النقطه الثانيه وهي **Non-linear** بمعنى مش عمليه بتمشي على استقامه يعني مش خطوات يتنفذها وتنقل على اللى بعدها كدا وخلصنا لاء دي **Cyclic** زي موضحنا ... فأنت عندك كل **Phase** من اللى ذكرناهم ممكن تتكرر أكثر مره ودا زي موضحنا وكله فسبيل عمليه ال **Exploitation** تنجح عند ال **Target** بتعنا ... وبرضه الفكره ان ال **Attacker** بيعمل ال 7 **phases** بتوع ال **Cyber Kill Chain Model** فكل **Target Machine** يروحله ال **Attacker** هيجتايج ينفذ عليه ال **Phases** بتعتنا فال **Process** بتعتنا بتكون **Cyclic** واحنا عرفنا ان ال **Attacker** بيستخدم **Technique** اسمه ال **Pivoting** فال **Post Exploitation Techniques** عشان يروح من جهاز لجهاز فال **Network** اللى أخترق جهاز واحد فيها فهو محتايج يتنقل ولما يتنقل هيجتايج يعمل ال **Process** بتعتنا من أول وجديد .

- أنت بقا ك **Theat hunter** دورك ايه فالليله دي ؟؟ اننا نعمل **Detect** لل **Adversary** من قبل مال **Attack** بتاعه ينجح بال **target** اللى عاوزه يتحقق ... قبل مال **Adversary** ينفذ حاجه أصلا لأن زي مقولنا وظيفتنا فال **L3** اننا نمنع ال **Attack** قبل ميحصل مش زي باقي ال **Defender Team** انهم يحاولوا يمنعوا ويوقفوا ال **Adversary** من تنفيذ باقي ال **Cyber Kill Chain** !!.

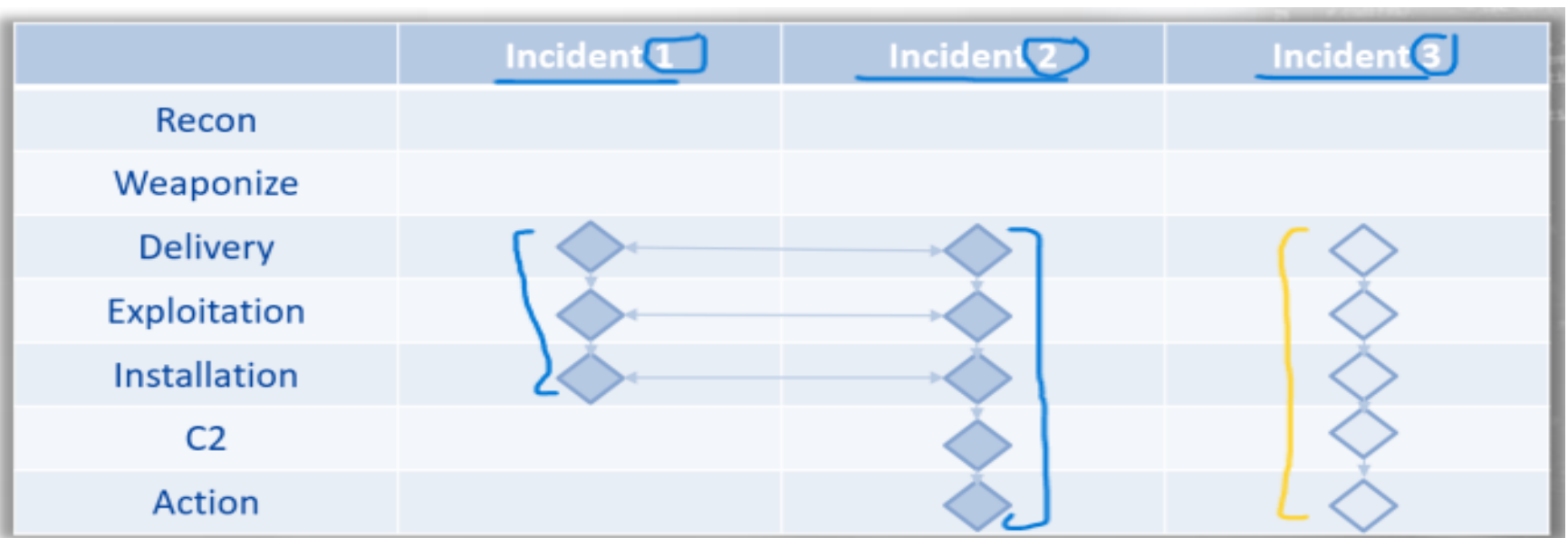
- ال **Diamond Model** دا ال **Model** الثاني معانا عشان يورينا ال **Attacker** ازاي بينفذ عملية الاختراق عال **target** بتاعه ... فال **Diamond** ببساطه بيوضحك مين ال **Adversary** ومين ال **Victim** ومين ال **Infrastructure** اللى حصل عليها ال **Attack** وايه هي طرق الاختراق اللى اتنفذ أو تمت بيها عملية ال **Attack** .



- فزي منتا شايف على سبيل التوضيح ال **Adversary** اللى هو ال **Attacker** يعنى اللى هو ممكن يكون **Insider Threat** ... وال **Victim** ممكن يكون ال **HR Department** قسم ال **HR** هو اللى مستهدف فال **Attack** ... وال **Capability** اللى هو ازاي تمت الأصابه أو ال **Infection** للأجهزة أو ال **Network** عند المؤسسه ودا زي المثال اللى قدامك ان فيه **Ransomware** انتقل ليهم أو عن طريق **Service Account** جديده اتعملها **Create** عالأجهزة ... وال **Infrastructure** اللى هي ايه ال **Tools** اللى تم نقل ال **Attack** من خلالها واللى هي قدامك ال **USB** .

- فتقدر تجمعها فالجمله دي ... ان عندك ال **Insider Threat** أو شخص من ال **IT** استخدم ال **USB** عشان يترجت أو يصيب قسم ال **HR** بال **Ransomware** اللى هيذرعه عندهم .

- افكر ان ال **Target** بتعناك **Threat Hunter** اننا نمنع ال **Adversary** انه يوصل لل **Goal** بتاعه !! فأنت عندك ال **Cyber Kill Chain Model** ممكن تستخدمها لوحدها أو مع ال **Diamond Model** والعكس صحيح كله على حسب ال **Case** اللى قدامك وطريقه تعاملك معاها ... فأنت على حسب ال **Case** بتقرر هتستخدم ايه فخد عندك المثال دا بيوضح بعض ال **Cases** على شكل رسم بياني اننا استخدمنا فال **Incident** الاول والثانيه ال **Cyber Kill Chain** وفالتاليه استخدمنا ال **Diamond** وزي موقلتك اهم حاجه توصل لل **Target** بتاعك انت ك **Threat Hunter** .



- انت من كتر شغلك فال **SOC** ومن كتر ال **Cases** اللى هتقابلها هتبقا عارف ال **Case** دي تتعامل معاها بأنھو طريقه سواء ال **Diamond** أو ال **Cyber Kill Chain** ... فأنت عدت على **Case** قبل كدا وشوفت ان ال **APT Group** اللى عامل عليك ال **Attack** دا بيمشي بالطريقه دي بيستخدم ال **Weaponized** المناسب بالطريقه دي وبيعمل **Delivery** بالطريقه دي وال **Tools** بتعتهم معروفه عندك من كتر ال **reports** اللى بتقراها وال **Cases** اللى اتعرضتلها ... فأنت اكتشفت فيما بعد **Incident** جديده بنفس الطريقه بالضبط عاملين **Deliver** بنفس الطريقه وال **Exploit** بنفس الطريقه فخلاص انت كواحد شغال فال **SOC** عندك خبره هتلاقي ان بالعين فقط هتعرف ال **Attack** دا جي من انهو **APT Group** لأنك عارف **Cases** وسيناريوهات كثير عدت عليك فعندك خبره مسبقه بالكلام دا ودي فايده انك تطبق عملي وتشوف **Cases** كثير وتتعامل معاها .

- فانت ك **Threat Hunter** على حسب المؤسسه بتعتك فهتختار ال **Methodology** الخاصه بيها واللى هتتفع معاها ... فالبنيك الشغل فال **SOC** فيه غير المؤسسات والشركات والقطاعات الحكوميه وهكذا كل مكان ليه الطريقه المناسبه ليه فانت تشوف ال **Methodologies** الموجوده وتتعلم منها وتشوف الأنسب لشغلك ومؤسستك ايه .

2.2 Threat Intelligence:

- الجزء دا بيتم بكذا طريقه عشان ننفذ ال **Hunting** ممكن بعض ال **Hunters** يقولك أنا هشتغل عن طريق ال **Threat Intelligence** عن طريق ال **OSINT** وغيره زي مهنشوف ... وواحد تاني يقولك اديني ال **Tools** بتعتي وانا هشتغل عن طريق ال **Digital Forensics** اللى هو هدخل بال **Tools** بطريقه **Manual** وانفذ ال **Hunting** عال **Incident Machine** عن طريق ال **Tools** بتعتي مش بطريقه ال **Threat Intelligence** .

- تعالى ناخذ طريقه ال **Threat Intelligence** فالأول ... دي بتبقى عباره عن معلومات أو **Data** عن ال **Threats** بأشكال مختلفه من مصادر مختلفه زي المعلومات اللى ممكن تجمعها عن طريق ال **OSINT** وال **Social Media Accounts** وال **Vendor Reports** الى آخره ... واحد من أهم المصادر اللى تعتمد عليها فتحته قرايه ال **Reports** واخر ال **Data Breaches** اللى حصلت وأخر ال **Attacks** اللى قام بيها **APT Group** معين وأخر ال **Cyber Attacks** وأخر ال **Malwares** وغيره من ال **data** اللى هتفيدك ك **Threat Hunter** هو موقع **The Hacker News** ... بس خد بالك ال **data** اللى هتطلعها من ال **Threat Intelligence** زي ال **Hashes** أو ال **Netblocks** أو ال **Domains** ...

أو **IP Addresses** أو ال **Cybercrime Groups** هي **Data** فقط ...
... فين بقا ال **intelligence** هنا !!؟ محنا هنعملها **Analyze** بعد
كدا هنحللها ومن خلال التحليل دا هنعرف أجوبه بعض الأسئلة عندنا
ومن هنا هنعول ل **intelligence** ... زي مثلا لو سمعت **APT**
Group ما عمل **Attack** على احدي الشركات فأنت دي كدا معلومه
معاك طب تحولها ازاي ل **Intelligence** ؟ اننا نحللها ونطلع منها
معلومات زي ال **Methodology** اللى تم بيه ال **Attack** دا وايه هي
نقاط الضعف اللى عند الشركه دي اللى من خلالها ال **APT Group** دا
قدر يستغلها وينفذ ال **Attack** بتاعه وهكذا ... يبقى انت معاك معلومه
بتستخرج منها معلومات تفيدك انت ك **Threat Hunter** فشغلك
والبحث بتاعك ... عشان نطبق ال **Threat Intelligence** عندنا 3
أنواع منه وكل واحد منهم ممكن تعتبره سؤال مطروح المفروض انك
تجاوب عليه عشان تبقا نفذت ال **Process** دي بشكل مضبوط .

- أول نوع هو ال **Strategic** بمعنى **Who, why, where** والنوع
الثاني معنا هو ال **Tactical** ودا بنجاوب بيه على سؤاين اللى هما
What , Where والنوع الثالث معنا هو ال **Operational** واللى
بنجاوب بيه على سؤال **How** ... وهنشوفهم بالتفصيل فالجي .

- أول نوع وهو ال **Strategic** ودا لو اشتغلنا بيه هيبقا مهم لل **SOC**
Manager أو حد من المديرين اللى فوقك المسؤولين عن المؤسسة
النوع دا هيفدهم جامد ... هتلاقيه بيقولك ال **APT Group** أو ال
Adversary اللى نفذ ال **Attack** مين هو أو مين الجهة المسؤوله
وعمل ال **Attack** دا علينا ليه وايه الدوافع اللى خلته يعمل كدا
وبالأضافه فين حصل ال **Attack** دا قبل ميحصل عندنا فالمؤسسه ودا
عشان يشوفوا ال **Budget** بتاع المؤسسه ويشوفوا هل يزودوا مثلا
Security Hardware زي ال **NGFW** مثلا فأماكن وأقسام معينه
اللى هتذكرها انت ك **Threat Hunter** فال **Report** ...

زي ال **HR Department** مثلاً فيبتدوا ياخدوا قرارات بتكثيف ال **Security Hard ware** فالمكان دا أو يدوا دورات **Security Awareness** بشكل **Updated** لأحدث الهجمات للموظفين اللى شغالين فالقطاع دا عشان يبقا عندهم الوعي الكافي للتعامل فالمستقبل وهكذا .

- النوع الثاني من ال **Threat Intelligence** معانا هو ال **Tactical** ودا هنجابوب على سؤالين وهما **What , When** وهنا هنجأ اننا نستخدم ال **Cyber kill chain Model** وال **Diamond Model** عشان نجابوب عالمطلوب مننا وبرضه مطلوب مننا نعرف أكثر عن ال **TTPs** اللى ال **Techniques** وال **Tactics** بتاعت ال **Adversary** ودا كنا اتكلمنا عنه بالتفصيل فوق أرجعله ... يبقا هنا عاوزين نعرف ايه هي ال **Tools** اللى استخدمها ال **Attacker** وامتأ اتنفذ ال **Attack** دا علينا اللى هو توقيت حدوثه ولو بتقرء **Reports** كتير هتلاقي بعض ال **APT Group** بتستهدف عنصر التوقيت دا زي الحرب تماماً يعني فيوم معين فساعه معينه وموظفين معينين موجودين فالمؤسسه هيبدا ال **Attack** وبنك بنجلاديش وعملية اختراقه سنه **2016** كانت خير دليل فحاول تقرء **Reports** كتير على قد متقدر هتطلع بأفكار جديده .

- النوع الثالث معانا وهو ال **Operational** ودا بيجاوبنا على سؤال واحد وهو **How** بمعنى ازاي ال **Attack** دا حصل علينا ودا ممكن تستعين بيه من خلال معرفتك لل **IOCs** واللى كنا اتكلمنا عليها فالأول فالمصطلحات الخاصه بال **Threat Hunting** أرجعلها ... احنا ك **Threat Hunters** هنركز فشغلنا على ال **Tactical** وال **Operational** من ال **Threat Intelligence** .

- وانت ك **Threat Hunter** بتعتمد فشغلك على ال **known bad** **Information** اللى هي أي معلومات مش تمام ومشكوك فيها وانت بتعمل **Hunting** لازم هتركز عليها وتعملها **Analyze** عشان هتفيدك قدام فال **Incident** ووانت بتكتب ال **Report** عنها ... فمثلا انت أجهزة المؤسسه بتعتك شغاله ب **Software** من شركه **Cisco** وليكن فأنت ك **Threat Hunter** مدام مسمعتش عن أي تهديد وانت بتقرء **Reports** يخص شركه **Cisco** ومنتجاتها مثلا فأنت كدا فالأمان ... انما لقيت مثلا **Report** عن ثغره جديده فأجهزة **Cisco** فهنا تبتدي تتحرك وتقلق لأن مؤسستك شغاله بأجهزة **Cisco** فتبدء تبحث وتعمل ال **Threat Intelligence** بتاعك عشان لو عندك فأجهزة المؤسسه الثغره دي تلحق تعملها **Patching** قبل ميتعملك **Infection** ب **Malware** ولا حاجه ونقعوا فحيز ان ال **Incident** حصلت ودا احنا مش عاوزينه ... تعالى نشوف الطريقه التانيه وهي ال **Digital Forensics** .

2.3 Digital Forensics:

- ال **Hunter** الثاني دا هتلاقيه بي **Focus** على ال **Host** وال **Network** وال **memory Forensics** ... هنا هتلاقي العكس بتستخدم الطريقه دي لو عاوز تشتغل **Unknown** بمعنى انت بتشك فحاه زي لقيت مثلا ال **Traffic** بتاع ال **Network** على فجأه بشكل غير مسبوق فأنت تبتدي تشك ممكن يكون **Malware** نزل على الأجهزة فالمؤسسه واحنا منعرفش عن طريق **Attack** من **APT** **Group** معين فخلي ال **Traffic** على فال **Network** فتبتدي تاخذ ال **Tools** بتعتك وتعمل ال **Threat Hunting** عن طريق ال **Digital Forensics** .

- فهنا العملية لو عندك معلومات **Unknown** على عكس ال **Threat Intelligence** كان لازم تكون عارف معلومه وبتكون **Bad** وتخص المؤسسه بتعتك فتبدء ت **Search** عليها عشان تتأكد ان مؤسستك فإلسليم .

- فحاله ال **Digital Forensics** ال **Data** بتعتنا نقدر نجيبها منين ؟ من خلال ال **Network** أو **VPN & Firewalls Logs** أو انك تعمل ال **Disk Forensics** أو ال **Memory Forensics** أو روت تشوف ال **Passive DNS Requests** وتحللها وطبعا كله عن طريق ال **Tools** زي موضحنا قبل كدا ... وبرضه مش معنى انك شغال بال **Digital Forensics** انك تهمل ال **Threat Intelligence** لاء انت ممكن تشغل الاتنين مع بعض عادي وكله برضه على حسب ال **Case** ... ولكن فال **Digital Forensics** انت بتعمل **Hunt** بشكل **Proactive** فتقدر تقول ان فال **Digital Forensics** ال **Human Based Detection** هو ال **Based Detection** فهي معتمده عليك بشكل رسمي ... وانت عارف انك فال **SOC L3** مبتستنش ال **Alert** بتاع ال **Incident** يحصل عشان تتحرك وتحل المشكله أو مش زي ال **IR** بتاع **L2** اللى مدام ال **Siem** مطلعطهوش **Alert** يبقا تمام وزى الفل ... لاء احنا شغلنا كله بشكل **Proactive** مال **Incident** تحصل وعشان كدا شغلنا كله معتمد بشكل أكبر عال **Digital Forensics** اننا ندخل بشكل **Manual** نعمل **Investigation** عشان نتأكد بشكل مسبق ... يبقا علشان ال **Threat Hunter** يعرف يعمل ال **Digital Forensics** لازم يكون بيعرف كام حاجه منهم ... يكون عنده ال **Knowledge** بال **Data Resources** وال **Data Logs** وكمال يكون عنده ال **Knowledge** بال **Attacks** المتنوعه اللى هيقابلها والطرق المختلفه بتاعت ال **APTs Groups** ودا انت تقدر تعرفه من خلال قرايتك لل **Reports** الخاصه بال **Incidents** المختلفه ومصدر زي اللى ذكرناه اللى هو **The Hacker news** هيساعدك فالجزءيه دي .

- وبرضه يكون عندك ال **Knowledge** بتاعت ازاي تفهم ال **Different Attacks** اللى بيتعملها **Detect** من ال **Different Data Sources and Logs** ... وكمان تتابع ال **Logs** أول بأول وتشوف هل مثلا فيه **User** جديد اتعمله **Create** وتشوف كمان ال **Process Masquerading** اللى هو عندك **Process** جديده اتعملها **Create** ولا لاء عال **System** عندك وهل ممكن يكون ال **Attacker** دخل من **Process** معينه وعملها **Migrate** ل **Process** تانيه وتشوف هل فيه **Process** معينه عندك عال **System** كانت واخده رقم وبعد كدا اتغير مثلا !! وحاجات من هذا القبيل ... وبرضه يكون عندك خبره مسبقه بالتعامل مع ملفات ال **exe** وانك تعرف لو انت شاكك فملف ما عندك عال **System** تعرف تعمله **Reverse Engineering** اللى هو هندسه عكسيه للملف دا وتفككه وتشوف ال **Content** بتاعه ودا هيجي من الخبره وكتر ال **Cases** اللى هتعرضلها فشغلك ... وبرضه تعمل **Locate** بال **Sources** وتكون على صله بيها دايمه اللى ممكن يحصل عليها **New Attack** فتاخذ بالك منها ودا برضه هيجي من قرايه ال **Reports** وتعرضك أثناء العمل ل **Cases** كتير وكمان التطبيق العملي على **Cases** كتير وتشوف سيناريوهات أكثر ودا هتلاقيه ممتاز جدا فمصدر زي **Cyber Defender** المنصه دي ممتازة فالتطبيق العملي عال **Cases** .

- خلاص جبت ال **Data** من ال **Sources** بتعتك عندنا نوعين من ال **Hunting** ممكن ننفذهم عال **Data** دي ... وهما ال **Attack** **based Hunting** وال **Analytics based Hunting** فتعالى نشوف الفرق بينهم !.

- ال **Attack- Based Hunting** دا بيبقا عباره عن ال **data** اللى جمعتها عن طريق ال **Digital Forensics Tools & Resources** وعاوزين نطلع من ال **data** دي ال **Attack** .

- يبقا احنا هنا بنعمل Search على اي دليل أو Evidence يقول ان حصل عندنا هنا Attack عال Machine ... كأنك بتسأل نفسك هل ال Attack الفلاني دا حصل عندنا على ال Network بتاعت المؤسسه وللااء ... مثال ... هل ال Attack اللي هو Pass the Hash حصل عندنا فال Network ?? هل ال Attack اللي هو Create Local Account حصل عندنا عال Machine ?? هل حصل عندنا سرقة لل Credentials عندنا فال Network وللااء ??

- طبعا انت ك Threat Hunter بتجمع المعلومات بتعتك بال Digital Forensics زي مقولنا وليكن على سبيل المثال لقيت ان فيه ثغره ما بتتسبب فال Create Local Account عال Machines !! فأنت ك Threat Hunter وظيفتك انك تفتش فال Logs اللي عندك وتشوف فعلا عندك الثغره دي وهل فيه Account جديد اتعمله Create فالوقت القريب دا عال Machines ... ودا اللي بنسميه بتطبق ال Hunting بناء على ال Attack اللي انت بتتوقعه أو شاكك يكون عندك عال machines أو ال Network عموما .

- الطريقه الثانيه عندنا فال Hunting بعد أما جمعنا المعلومات بتعتنا هي ال Analytics'-Based Hunting ... هنا انت بتبدي تمسك مثلا ال Logs وليكن بتاعت ال Firewall وتقدر تعمل Analysis لل traffic اللي جي عندك فال Network وتبدي تمسك فالحاجه اللي انت شاكك فيها وتحلل أكثر عشان تتأكد ان الدنيا تمام ... مثال ... حصل عندك عال Network وليكن Un encryption Detected ال Traffic مكنش مشفر واتعمله Detect مثلا عندك عال Network فتاخذه تعمله Analysis ... شخص مثلا بيحاول ياخد Access عال data الخاصه بال HR ... عندك مثلا Work Station عملت Connect ب 10 أجهزة تانيين فدا Behavior تصنفه مش Normal فتشك فيه علطول وتعمله Analysis .

- مثلاً برضه عندك **Multiple Process** من ال **Wininit.exe** معمولها **Running** على **Host** واحد ... فتأخذ الكلام دا وتعمله **Analysis** وتشوف هل الكلام دا **Incident** أو **Thread** مثلاً أو الكلام دا عادي وحاله منفردة عندنا ... فأنت لازم تتأكد من ال **Case** المشكوك فأمرها .

- برضه انت ك **Threat Hunter** لازم وانت بتعمل ال **Hunting** تكون محدد الوقت بتاعك اللي هت **Hunt** فيه ... وعندنا **3 Periods** وهما ال **Point time** وال **Real Time** وال **Historic** ... تعالى نشوف الفرق بينهم .

- ال **Point Time** معناه انك عاوز تعمل **Hunting** فيوم معين فوقت معين دقيق مثلاً يوم الخميس 3 مايو الساعة 10 وربع صباحاً هتروح على **Machines** معينه انت شاكك فيها وتعمل عليها ال **Hunting** سواء كان بالطريقه ال **Attack - Based** أو بال **'Analytics - Based** ... بس خد بالك ممكن بعض ال **Data** يحصلها **Volatile** يعني تتبخر من ال **Machine** ودا بسبب التوقيت المحنك اللي انت جي فيه بيحصلها **Missing** فتوقيت ما قبله أو بعده ودا بسبب ال **Hunting** فتوقيت **Specific** .

- التوقيت الثاني معانا هو ال **Real Time** اللي هو فالوقت الحالي بشكل **Live** تدخل تعمل **Hunt** عال **Machine** ودا بيتم عن طريق ان يكون فيه **Agent** هناك عند ال **Machine** أو ال **Server** اللي عاوز تعمل عليها **Hunt** وبيكون متصل بال **SIEM** اللي بيعتلك ال **Alerts** ... فا فيه بعض ال **Configurations** اللي المفروض تعملها عال **Machines** اللي عاوز تنفذ عليها **Hunt** بشكل **Real** فالعيب هنا انه لازم يكون عندك **Agent** عال **Machines** اللي هت **Hunt** عليها

- التوقيت الثالث عندنا وهو ال **Historic** اللى هو هنروح نعمل **Hunting** لحاجات حصلت عندنا فال **Past** حصلت قبل كدا يعنى مش فالوقت الحالي ... فمثلا تروح تجيب الحاجات اللى حصل آخر شهر عندك من ال **Logs** وتحللها وتعملها **Hunt** ... فأنت هنا بتروح لل **SIEM** **Solution** بتاعك وتطلع حاجات قديمه وتعملها **Investigation** من أول وجديد وتشوف هل فيها حاجات **Malicious** أو **Attack** متنفذ عندك بالفعل وانت مش واخد بالك وهو شغال عندك فال **Background** فالنوع دا هيفيدك فالحاجات اللى شبه كدا.

- وفي بعض الأحيان يفضل يكون عندك ال **Techniques** الخاصه بال **Reverse Engineering** علشان في بعض ال **Cases** بيكون عندك ملف **exe** أو **binary** شاكك فيه ممكن يكون **malicious** أو حاجه شبه كدا فأنت بتحتاج تعمله ال **Reverse Engineering** علشان تتأكد منه .

- للعلم الكلام دا بيحصل فالمؤسسات الصغيره اللى بيكون ال **Threat Hunter** ليه علاقه بال **Reverse Engineering** أما فالمؤسسات الكبيره بيكون ال **Threat Hunter** ليه تخصصه فقط وشغله وال **Reverse Engineering** دا قسم تابع لل **Malware Analysis** اللى هو برضه قسم عندنا فال **SOC L3** زي زي ال **Threat Hunting** بس كل واحد ليه شغله .

- وبكدا نكون ذكرنا أهم النقاط الخاصه بال **Digital Forensics** **Hunting** وقبلها اتكلمنا عن ال **Threat Intelligence** ولكن دا ليه كلام تفصيلي جاي قدام باءذن الله .

2.4 Threat Hunting Stimulations:

- اللى هو طول منتا شغال فالتخصص بتعنا اللى هو ال **Threat Hunting** فانت شغال تتعلم وتتدرب بأستمرار.

- ال **Threat Hunting** فالعموم بيحتاج كذا **Skills** لازم تكون عندك بشكل مسبق زي معرفتك بال **Attacks** وال **Attacking Techniques** عموما زي كورسات ال **Pen testing** عموما وقبل كل دا لازم تكون عديت بال **IR** وعرفت ال **Technique's** بتعتهم ايه ومعرفتك بال **Fire walls** وال **Network** وال **Network Traffic's analysis** ومفيش مانع لو شويه **Programming** معاهم فمممكن تحصلهم من كورسات منفردة وأهم حاجه تحصل ال **Skills** اللى فيهم ... فانت بتفكر بنفس تفكير الجنود فالحرب دايمما فتدرب مستمر استعدادا لأي حرب قادمه والحرب عندنا هي ال **Attack** اللى ممكن يتم عالمؤسسه عندك ... فانت دايمما بتقرء **Reports** ل **Incident** حصلت فمؤسسات تانيه وال **Write up** بتاعت ال **Hackers** أو ال **Pen testers** وتحللها وتشوف ال **Methodology** بتعتها ازاي بتم وازاي اتعملها **Hunting** من الناس الأعلى منك خبره وتتعلم من ال **Cases** بأستمرار وتشوف **Cases** وتتدرب وتحل كتير فانت دايمما فحاله تعلم مستمر وتطوير لنفسك و **Updated** بكل جديد ... وتكون برضه بتحضر ال **CTF** اللى هي مسابقات ال **Capture The flag** أو بتحل التحدي بشكل **Online** على منصه زي **Try Hack Me** دي هتقوى ال **Skills** بتعتك فال **Penetration testing** عموما وكمان فال **Defensive Side** ... وبكدا نكون أنهينا ال **Module** دا الخاص بال **Threat Hunting Terminology** وذكرنا كل المصطلحات اللى متعلقه بال **Threat Hunting** وفصصناها جزء جزء .

3- Threat Intelligence:

- تعالى هنا نتكلم عن أهم المصطلحات التي ذكرناها قبل كذا وهي ال
Threat Intelligence ونفصلها كلمة كلمة لأنها فغايه الأهميه
وخلال ال **Module** دا هنتكلم عن النقاط التاليه :

3.1 Introduction.....	51-54
3.2 Threat Intelligence Reports & Research....	54-58
3.3 Threat Research & Exchanges.....	59-61
3.4 Indicators of Compromise.....	61-64

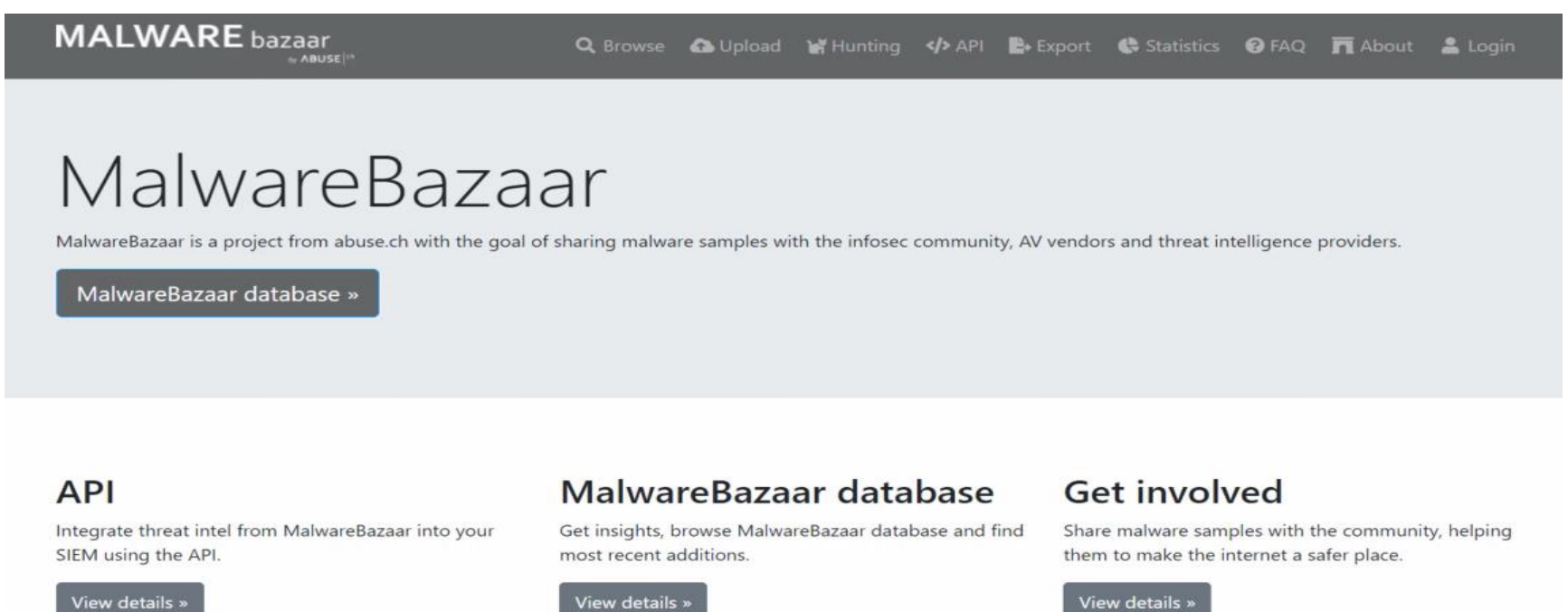
3.1 Introduction:

- كنا اتكلمنا قبل كذا اننا لو عاوزين نعمل **Threat Hunting** عندنا
طريقتين وهما ال **Threat Intelligence** وال **Digital**
Forensics ... فال **Threat Intelligence** باختصار هي ال
Data الموجوده فال **Threats** ... المعلومات التي نقدر نستخرجها من
ال **Data** الموجوده عندنا والمواقع وال **Resources** الموجوده عال
Internet زي مهنشوف ... وقولنا عشان نقول عال **Data** دي انها
Intelligence لازم يتعملها **Processing** معالجه وكمان
Analyze يعني نحللها ونطلع منها التي يفدنا وكمان نخليها
Actionable يعني تبقا قابله للأستخدام عشان نعرف نمنع بيها
Attack هيحصل علينا ... يعني انت عملت **Detect** وليكن ل **IP**
عندك ل **APT Group** معروف انها من روسيا فانت تحول ال **Data**
التي لقيتها دي ل **Intelligence** لما تعرف ال **IP** دا جايلك من انهي
جهه أو مقاطعه ف روسيا وتعرف ال **Location** بتاعه والمدينه وهكذا
فمجرد معلومه بسيطه عاديّه عرفت تستفاد بيها .

-بالاضافه لأن ال **Threat Intelligence** مش مجرد **IP** فقط لاء دا ممكن يكون **Hash** ... فلو **Attack** حصل عليك هتلاقي فالأغلب ال **Adversary Group** بيستخدموا **Malicious Programs** ال **Malwares** يعني فال **Attack** بتعهم ... فكل **Malware** بيبقا ليه **Hash** معين مميز ليها يميزها عن باقي ال **Malwares** ... ودا ممكن تشوفه من خلال موقع زي **Virus Total** تقدر تديه **Hash** أو **IP** معين انت شاكك فيه وهو يقولك اذا كان دا مصنف **Malicious** ولا لاء ودا بيتم من خلال ال **Signatures** اللى مخزنها عنده فال **Data bases** الخاصه بيه واللى بيقارنها بلى انت بتديهوله وساعتها بيرد عليك .



- وعندك **Resource** ممتاز فالحته دي وهو **Malware Bazaar** ودا موقع بيوفرلك أخر ال **Malwares** بال **Signatures** بتعتها اللى اتعملها **Detect** ف **Incidents** معينه فتقدر تستعين بيه فحته ال **Threat Hunting** عن طريق ال **Threat Intelligence** .



- كمان ال **Threat Intelligence** من خلالها هنقدر نعرف ال **Tactics** وال **Techniques** وال **Producers** الخاصه بال **Attacker** عشان نعمل **Stop** لل **Attacker** ... فال **Threat Intelligence** معتمد اعتماد كلي على ان ال **Hunter** يجمع معلومات عن ال **Threats** المعروفه ال **Known** زي مذكرنا قبل كدا فال **Module** السابق ... يعني **threat** معروفه وحصلت عند مؤسسه أو جهه ما وسمعت بس لسه مجتش صابت المؤسسه عندك فأنت بتبحث بعد أما يجيلك ال **Threat Report** وتجمع المعلومات عنها عن طريق ال **Threat Intelligence** عشان تحمي نفسك منها فالمستقبل ... فأحنا هنا فالجزء دا هنعرف ازاي ال **Threat Hunter** بيجمع ال **Data** دي وايه هي ال **Resources** اللى بيجمعها منها ... وهنا مش هنعتمد على ال **SIEM** هو اللى يعرفنا ال **Threats** بعد اما يعملها **Detect** زي ال **IR** ... لاء احنا هندخل **Manual** ونشوف آخر ال **Threats** عن طريق ال **Research** بتعنا واحنا اللى هنجيب ال **Resources** وندور عليها وهو دا شغلنا .

- طب عالسريع ال **SIEM** نفكر الناس بيه هو اختصار ل **Security Information & Event Management Solution** ودا عباره عن نقطه مركزيه بمعنى **Centralize Collection Point** بيجمع كل ال **Logs** الخاصه بال **Fire walls** وال **Network** وال **Application** وال **Events** اللى بتحصل عال **Machines** وياخد كل ال **Data** دي بعد كدا ويعملها **Analyze** ويصنفها ويطلعك منها ال **Malicious** اللى بيقولك هنا فيه **Incident** فال **Logs** الخاصه بال **Fire wall** مثلا لأنه زي مقولنا بيحتوي على **Network Devices** كتير ... فهو بيشيل عنك جزء كبير من المجهود فشغلك ودا عن طريق ال **Engines'** اللى موجوده فيه بتساعده عال **Tasks** دي وبينظملك ال **Output** بتاعك .

- بحيث انت ك **IR** أو **TH** تعرف تستفيد من ال **Data** دي ... احنا بقا ك **Threat Hunters** نقدر نعلم عال **SIEM** فال **Internal Threat Intelligence** فقط مش ال **External** ... بمعنى هو بيجمعلك ال **Data** اللى جتله فقط انما احنا عاوزين نجيب ال **Data** الموجوده فال **Websites** وال **Resources** الأخرى وعن طريق قرايه ال **Reports** برضه هنقدر نجمع كميه **Data** مهمه نعملها **Analyze** ونطلع منها ال **Intelligence Data** وبكدا يبقا احنا استفدنا من ال **Internal** وال **External** فال **Threat Intelligence** .

3.2 Threat Intelligence Reports & Research:

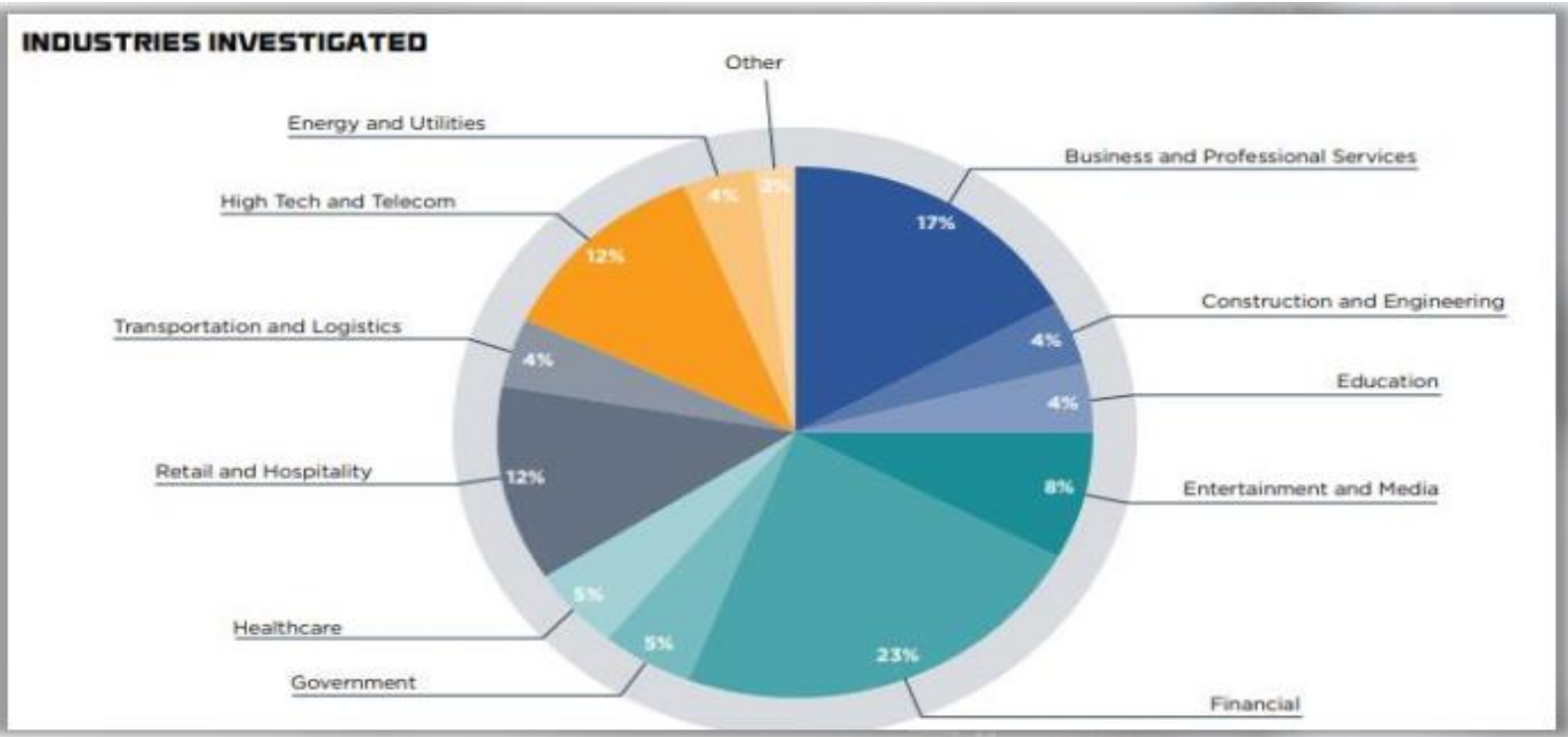
- هنا هنتعرف على ال **Resources** اللى بنجيب منها ال **Data** بتعتنا الخاصه بال **Threat Intelligence** وازاي نكتب ال **Report** بتاع ال **Incident** بشكل صحيح ... عندنا ال **Trusted Third party** اللى الشركات الخارجيه المتخصصه فال **Threat Intelligence** زي **Fire eye** و **Palo Alto** و **Crowd Strike** و **Cylance** و **Trust Waves** و **Verizon** و **F-Secure** وغيرهم كتير ... الشركات دي بتجمعلك ال **Data** عشان تكونلك فالآخر ال **Threat Report** الخاص بال **Incident** ... نوعيه ال **Report** دي بتحتوي على آخر ال **Threats** و آخر ال **Malicious Activity** ... المطلوب منك **Threat Hunters** اننا نتابع ال **Third Party** دي وتقرأ كل **Report** هما بينزلوه عندهم وتبقا **Updated** بالكلام دا علطول وآخر ال **Attacks** واوزي بتم وال **Reports** الخاصه بيها ... كل **Third party** هتلاقيه مسمى الجاه اللى نفذت ال **Attack** بأسم مختلف عن التانيه مش مهمه أوي دي انما تبقا عارف ال **Attack** تم ازاي ومين المسؤول عنه ودا هتجمعه من خلال قرايتك لل **Reports** .

- هناخد شركة **Fire Eye** كمثال عندنا الشركة دي بتطلع كل سنه ال **M-Trends** بمثابه **Threat Report** بينزل بشكل سنوى مجمع كل ال **Threats** وال **Attacks** وازاي تعملها **Hunt** وكمان ال **Latest Defensive Strategies** تقدر تحمله من موقع **Fire Eye** وتستفيد منه فال **Threat Intelligence** عموما كقرأه ومعرفه لأخر ال **Threats** وال **Attacks** وازاي تتعامل معاها واحصاءيات ال **Attacks** فكل سنه ويقارنها بلي قبلها ويديك التقرير النهائي ورسم توضيحي لأنواع ال **attacks** ونسبتها وهكذا ويكون بالشكل دا .

On the surface, not much has changed over the past 10 years. 2018 was much like 2017, and 2017 like the preceding years. We continue to see large impactful incidents, though fewer high-profile public disclosures. Extortion cases are on the rise, assisted by cryptocurrency and other forms of non-attributable payment. Cryptocurrencies are also directly targeted via wallets, payment systems and miners.

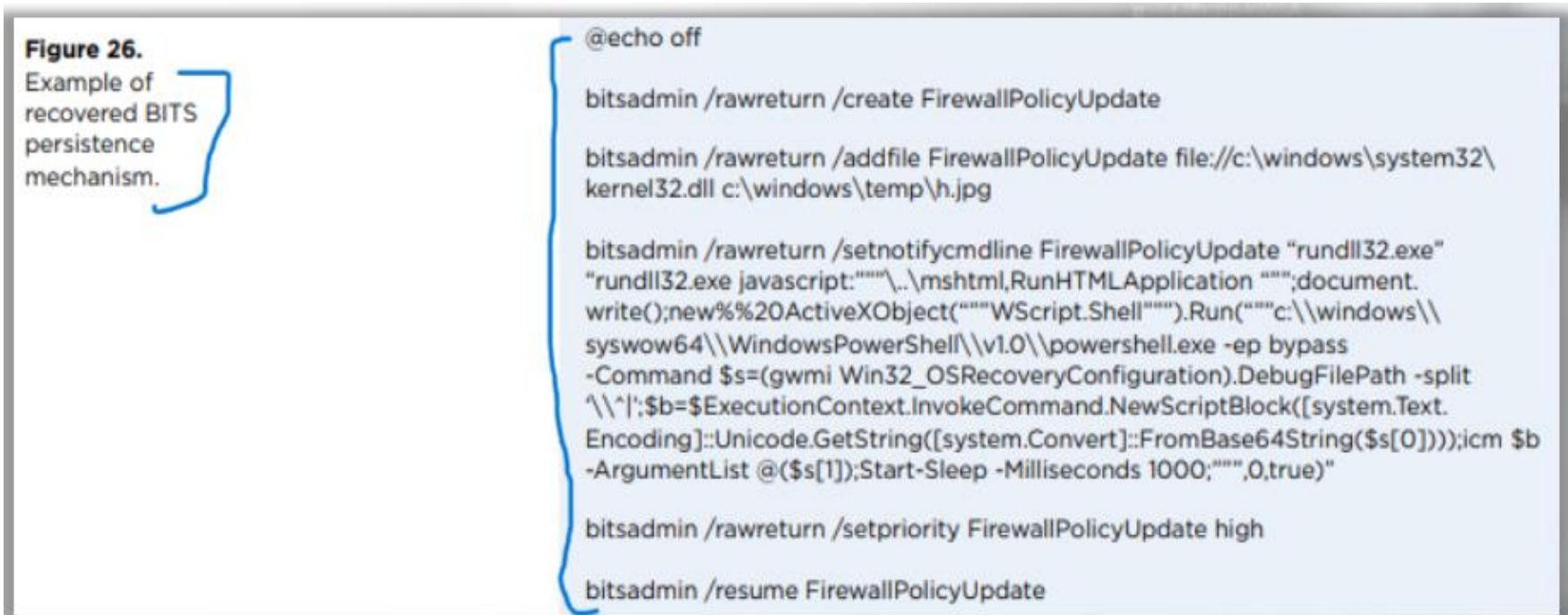
The significant trends or shifts we saw in 2018 were:

- A significant increase in public attribution performed by governments. Recent years have seen a significant increase in private sector attribution of attack activity, but the past year saw a significant number of attacks publicly attributed by way of indictments from the U.S., U.K., Netherlands and Germany. Some of these were assisted by data from private sector companies such as FireEye. Governments have not changed their operational rules of engagement, but they are combating threats publicly through indictments.
- As more and more customers move to software as a service and cloud, attackers are following the data. Attacks against cloud providers, telecoms, and other organizations with access to large amounts of data have increased.



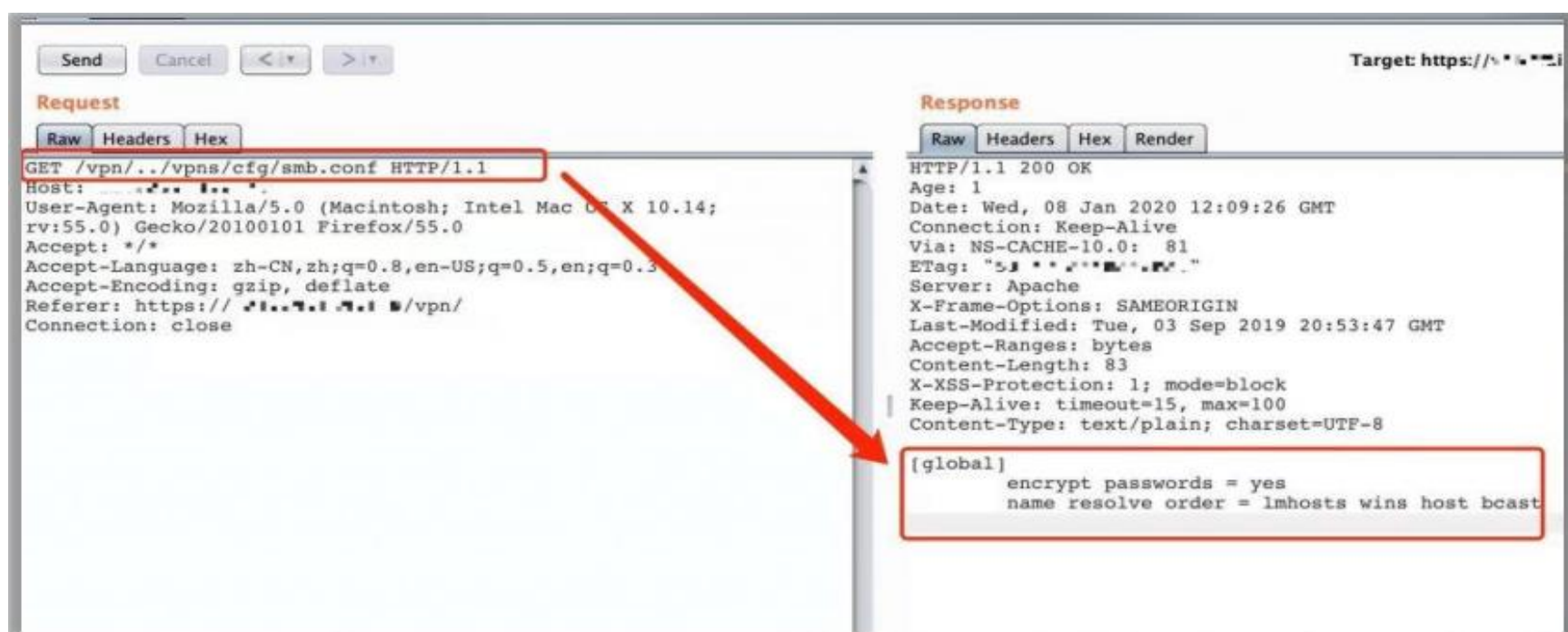
Retargeted incident response clients, by region.		
Region	2017	2018
Americas	44%	63%
EMEA	47%	57%
APAC	91%	78%
Global	56%	64%

- برضه هتلاقي عندك فال **Report** بيتكلم عن **Attacks** معينه و **Technique's** معينه حصلت وهتلاقيه بيشرحك ال **TTPs** بتعتها بالتفصيل وال **APT Group** المسؤوله عنها ... زي كدا .

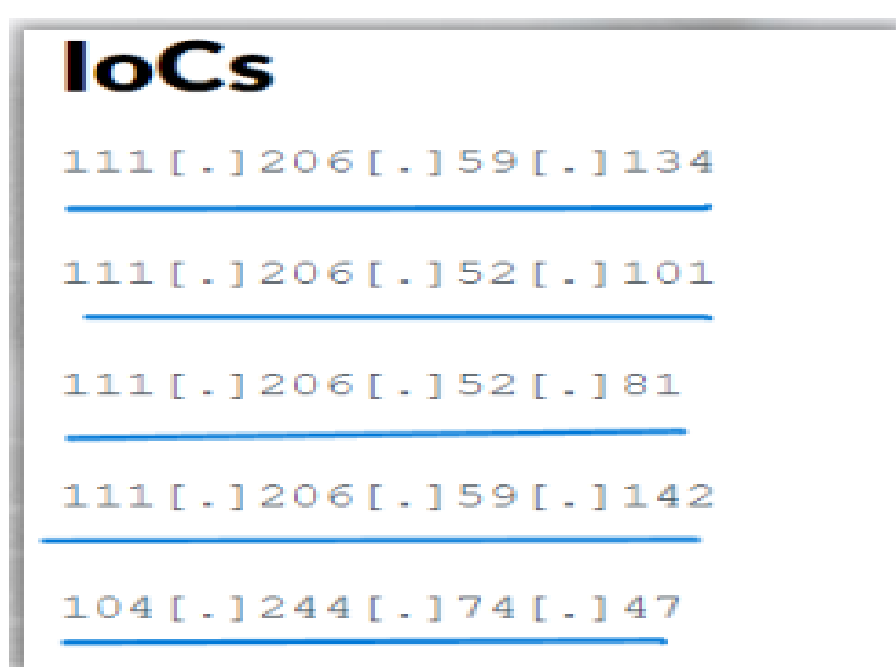


- وكمان عندك بعض ال **Reports** اللى بتطلعها ال **Third Party** أمثال **Fire Eye** اللى بنتكلم عليها هنا وواخذنها كمثال بتكون ال **Reports** دي عباره عن قطاع معين جوا ال **Industry** .

- فمثلا **Fire Eye** عندها **Threat Intelligence Reports** لقطاع ال **Education** فقط يعني تجبك ال **Attacks** اللى حصلت عالقطاع دا فقط لو عندك قطاع مالي أو مصرفي برضه نفس القصة تتواصل مع ال **Third Party** وهي تطلعك ال **Report** الخاص بيك ... وفيه بعض ال **Security Researchers** بيطلعوا ال **Reports** دي بشكل منفرد عن ال **Third Party** فتقدر تتابعهم برضه على **LinkedIn** و **Twitter** وال **Blogs** الخاصه بيهم و **Medium** عشان تستفيد من خبراتهم وتعرض نفسك ل **Cases** أكثر ... وكمان هتلاقيه عاطيلك فال **Report** ال **Proof Of Concept** اللى هو **POC** اللى هو أثبات وجود ال **Vulnerability** بالتطبيق العلمي ... ودا اللى هتلاقي كتير من ال **Researcher's** بيعملوه حتى فال **Bug Hunting** اللى هو مجال اصطياد الثغرات وتبلغها وتاخذ مكافأه ماديه لازم أثبات وجود للثغره وتوريها له عملي ف فيديو أو **Screenshot** فدا يوضح أهميه ال **POC** فشغلك انت حتى ك **Threat Hunter** .



- برضه هتلاقي من ضمن محتويات ال **Report** ال **IOCs** ال **Indicators of compromise** اللى هي علامات وجود الاختراق ... مثلا مجموعه **Ips** خاصه **APT Group** معين واتعملها **Detect** هتلاقيها نازله فال **Report** اللى زي كدا وبيقولك لو لقيت **IP** من دول عندك فال **Network** دا **Malicious** تعمله **Block** علطول أو من الأول تعمله **Block** وتريح دماغك وتحطه فال **Blacklist** ... ودا بيبقا حل مؤقت عشان ميحصلش عندك **Incident** فالمؤسسه فنلحق الدنيا قبل ميحصل حاجه ونعمل لل **Ips** دول **Block** .



- فلما نيجي ال **Report** بتاع ال **Incident** أو اللى طلعتة ال **Third Party** لازم بعض النقط كدا نعرفها ونطلعها ؟ ... أولهم ايه هو هدف ال **Attacker** من ال **Attack** دا وايه اللى عاوز يوصله سواء كان **Adversary** أو **APT Group** ... تاني حاجه معانا وهي اننا ازاي نقدر نعمل **Detect** لل **Malicious Activity** دي عندنا فالمؤسسه فحاله تعرضنلها ونحمي نفسنا منها ازاي فالمستقبل .

- النقطة الثالثة معنا وهي هل ال **Malicious Activity** بتاعت ال **Attacker** دي حصلت عندنا فالمؤسسه قبل كذا ولا دي أول مره ؟ لازم تسأل نفسك الكام سؤال دول وتدورلهم على حل وتقدر تقول دول بمثابه ال **TTPs** اللى نفذهم ال **Attacker** فأنت محتاج تجاوب عليهم .

- فال **SOC** عموما بيكون عندنا **Dashboard** فيها كذا **Resource** لكذا موقع وكذا **Third party** انت متعاون معاهام بتجبلك دا قدامك فالشاشات الكبيره متقسمه ل **Categories** على حسب كل قسم ومعلوماته عندك فبتلاقي ال **Reports** طالعه وآخر ال **Incidents** وآخر ال **Malwares** وآخر ال **Attacks** اللى قاموا بيها **APT** **Group** معين اسمه كذا ... كل دا متجمع قدامك فشاشه واحده بحيث المعلومات تبقى ملمومه قدامك فمكان واحد مش هنقعد نلف على كل موقع شويه لأن دا مضيعه للوقت ولو انه بيحصل ولكن فحاله شاده عن القاعده الأساسيه ... تعالى نشوف شكل ال **Dashboard** .

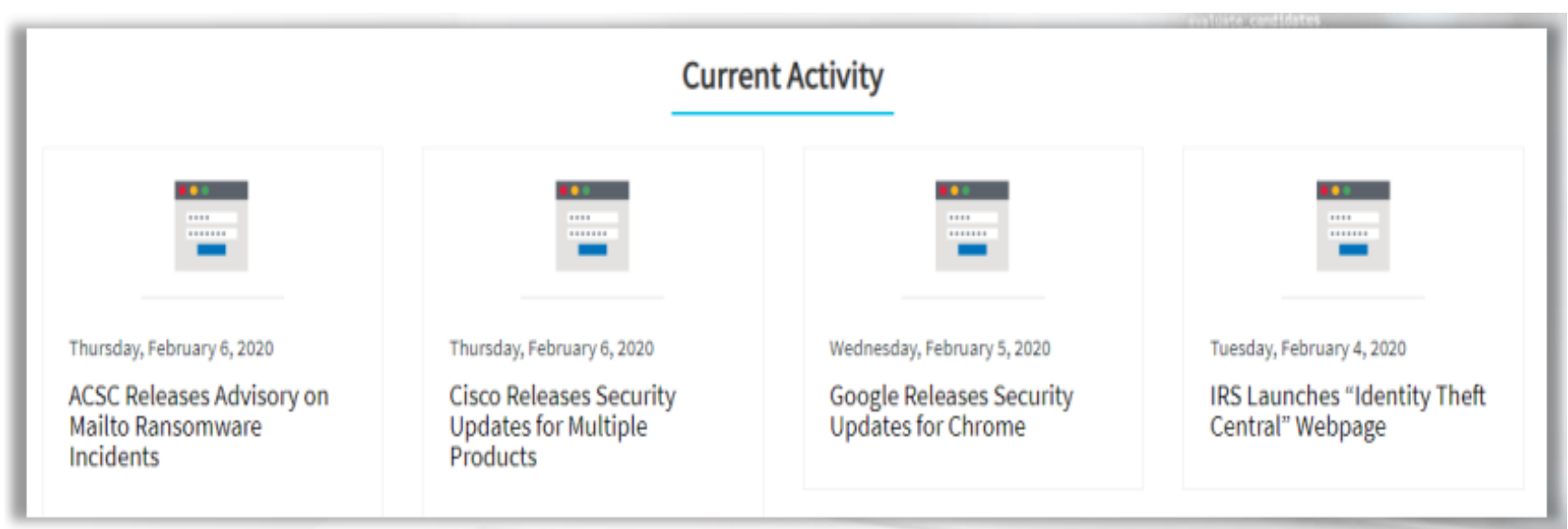


- طب احنا هنجيب المواقع دي منين اللى هتجبلنا المعلومات اللى عاوزينها فال **Threat Intelligence** عشان نعملها **Analysis** ونطلع منها ال **Intelligence** عشان نستفيد بيه ... دا اللى هنشوفه فالجزء الجي المهم جدا عشان نشوف هنطبق عملي ال **Threat Intelligence** ازاى.

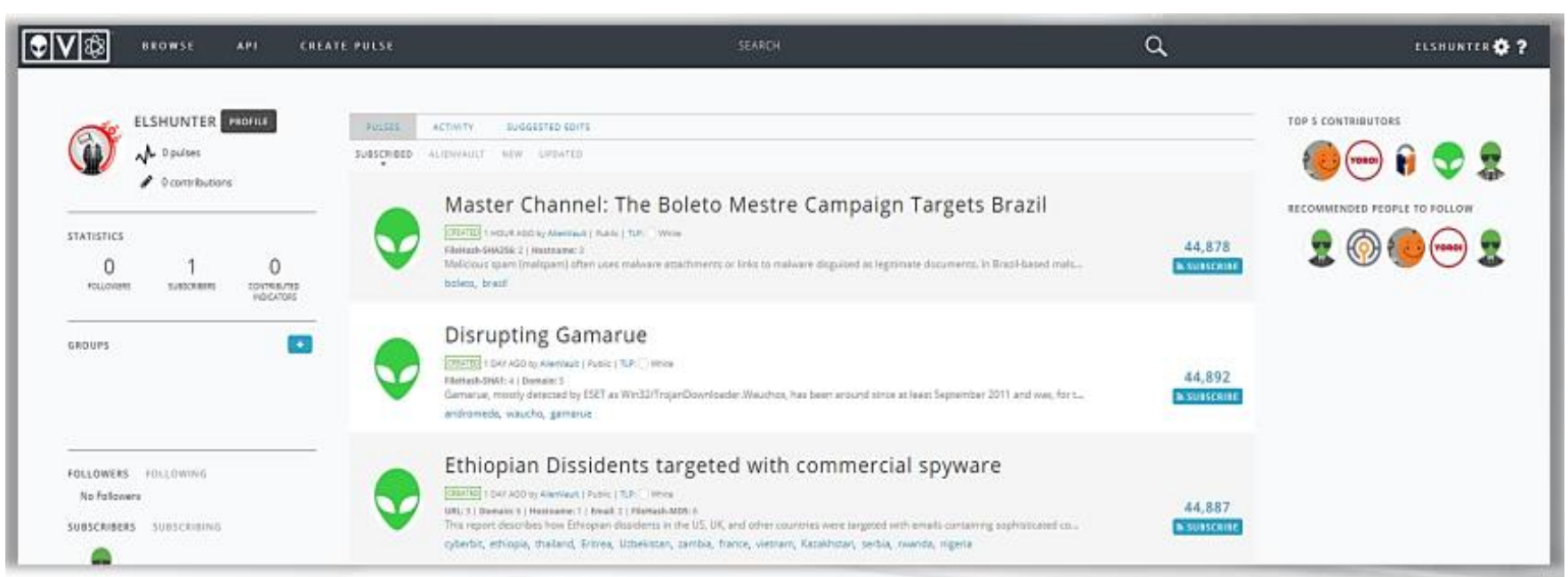
3.3 Threat Research & Exchanges:

- أنا دلوقتي عاوز أعرف آخر ال **Threats** عاوز أعرف آخر ال **APT Groups** اللى بتعمل ال **Attacks** عالمؤسسات عندنا **أول حاجه** وهي **ISACs** ودي اختصارا ل **Information Sharing & Analysis Centers** ... ودي عباره عن مؤسسه زي مقولنا مسئوله عن انها تمد ال **Threat Hunters** بأخر ال **Threats** وكمان ال **Mitigation** الخاصه بيها اللى هي طرق التعامل معاها وال **Defensive Techniques** للتعامل معاها ازاي ... دا مش **Technique** خد بالك دا اسم كذا جهه أو مؤسسه مع بعضهم كدا مسؤولين عن انهم يطلعولك معلومات عن ال **Threats** وكمان ال **Mitigation Information** الخاصه بيها عشان تساعد بيها ال **Threat Hunters** اللى شغالين فالمؤسسات ...

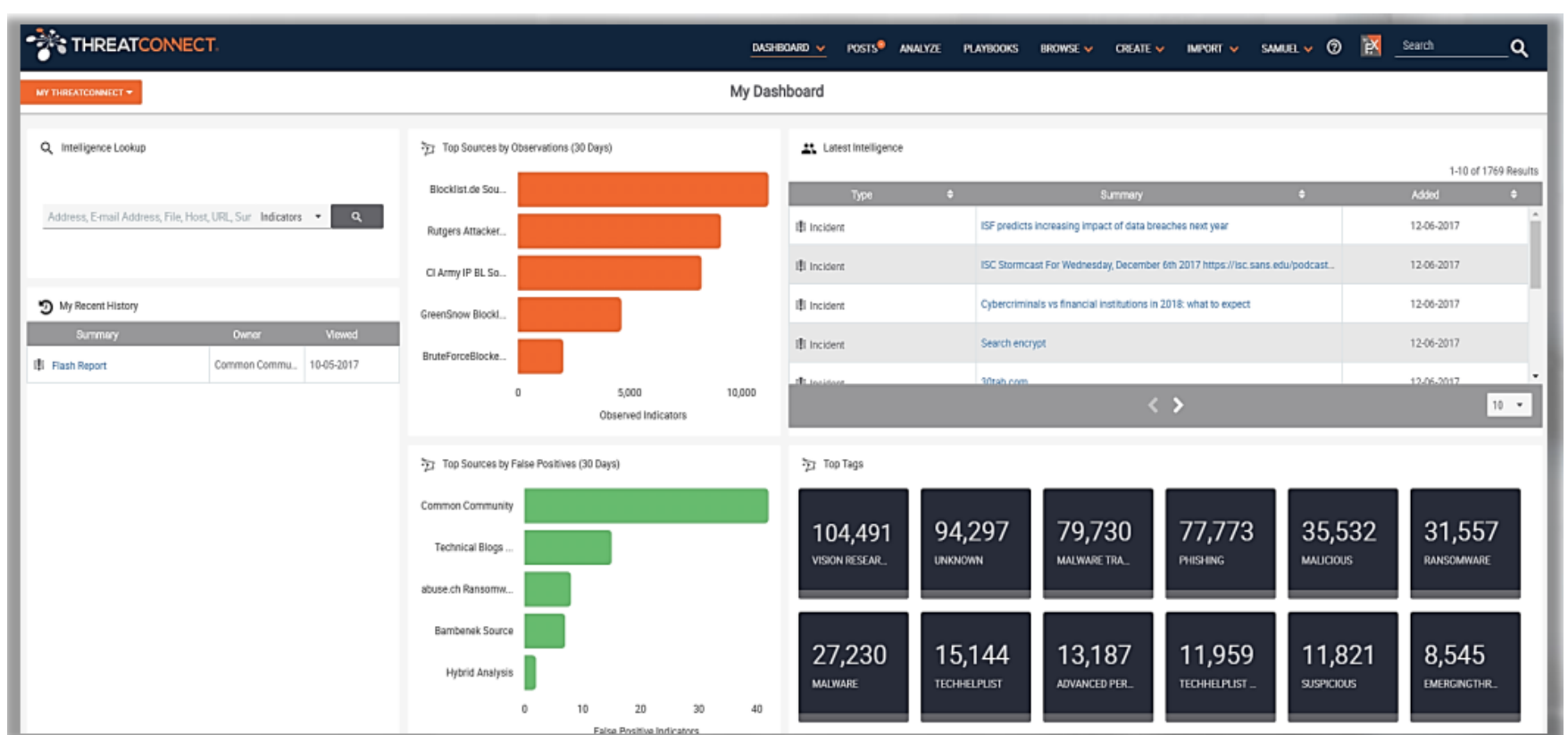
- **الجهه التانيه** اللى ممكن تعرف منها معلومات **Trusted** هي ال **US-CERT** ودي اختصار ل **United States Computer Emergency Readiness Team** ... ودا **Resource** محترم تقدر تعتمدة فال **Threat Intelligence Process** بتعتك فيه قدر موثوق من ال **Reports** وال **Alerts** وبيتم عمل **Update** ليها بشكل مستمر فدي من حكومه **USA** فتقدر تضيفها لشغلك ... ودا بالمناسبه هتلاقية فكل الدول كل دوله عندها ال **CERT** الخاص بيها اللى دايمًا بينصحها وبيمدها بالمعلومات الكافيه فال **Threat Intelligence Process** بس نصيحتي دايمًا خليك مركز و **Updated** بالدول اللى مهتمه بالتكنولوجيا زي الدول العظمى روسيا والصين وامريكا وهكذا عشان تبقا مواكب آخر ال **Updates** بشكل حقيقي يخدمك فشغلك .



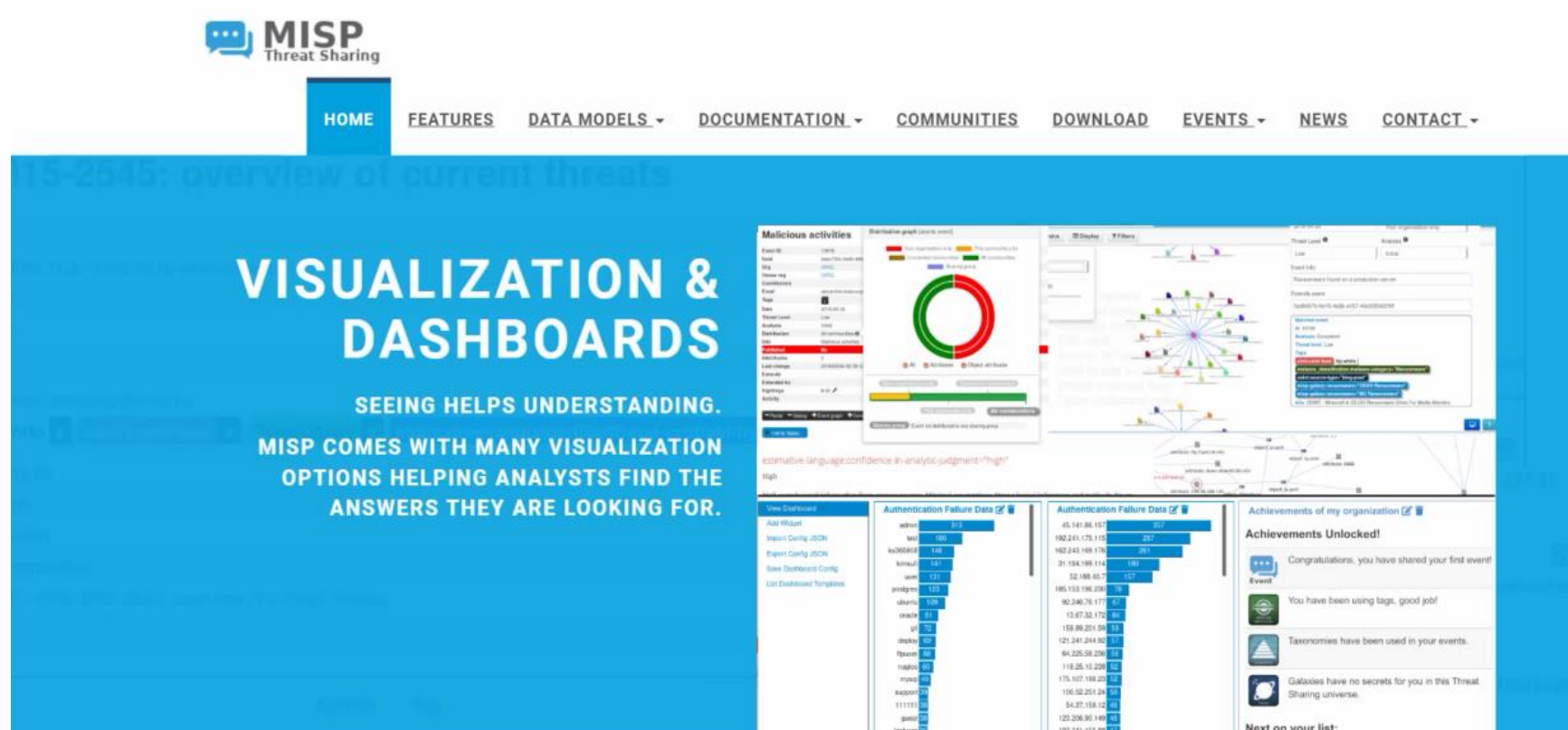
- عندنا **الجهة الثالثة** برضه نفس قصه الى سبقوها تقدر تستخرج منها المعلومات الى هتعمك فال **Threat Intelligence Process** و الى ممكن تعتمد عليها وهي **Open threat intelligence** يعني مجانيه بشكل كامل ال **OTX** وهي اختصارا ل **Open Threat Exchange**.



- برضه الى شبيه ال **OTX** ومجاني برضه تقدر تستعين بيه هو موقع **Threat Connect**.



- **الجهة الرابعة** عندنا هي ال **MISP** ودي اختصارا ل **Malware** **Information Sharing Platform** ... عباره عن **Open-Source Software Solution** بيعملك **Collect** و **Store** و **Distribute** و **Share** لل **Cyber Security Indicators** وآخر ال **Threats** وآخر ال **Incidents** وآخر ال **Malwares** وطرق ال **Attack** ال **Advanced** وآخر ال **APTs Groups Attacks** وهكذا وكل دا على شكل **Report** محترم منظم بشكل مجاني ودا برضه مصدر محترم تقدر تعتمد عليه .



3.4 Indicators of Compromise:

- ال **IOCs** كنا تكلمنا عنها عالماشي كدا فمواضيع مختلفه فوق كل مجت سيرتها ذكرنها ... انما هنا بالتفصيل ... دي عباره عن قطع **Information** تلاقيها وانت بتعمل **Forensic Data** فال **System Log** مثلا أو **Files** أو ال **SIEM** أو أي **Network Devices** تاني عندك فال **Network** والمعلومات دي كلها تعرفك اذا كان حصل **Malicious Activity** حصلت هنا ولا لاء سواء عال **System** او ال **Network** المهم تربط ال **Piece's** دي ببعضها عشان توصل لنتيجه واضحه هل حصل هنا **Malicious Activity** !.

- بمعنى ثاني ايه هي علامات حدوث أي حابه **Malicious** هنا عال **System** بتاع الأجهزة أو المؤسسه عموما أو ال **Network** برضه ... هل فيه علامات عندنا هنا تدل على ان فيه **Attack** حصل بدون منعرف أو ال **Attack** شغال فال **Background** واحنا نايمين فالعسل فكل دا اللي بيجاوبنا عليه هي ال **IOCs** ... مثلا أجهزة بتعمل **Download** بكميات كبيره فسحبت ال **Bandwidth** فدي علامه شكوك و أجهزة ثانيه فال **End points** بيحصلها **Restart** كل شويه لوحدها وال **Hard Disks** اللي عالجهزة بتتملى بسرعه أو بيتم استهلاكها بشكل مش مسبوق ومش طبيعي بالنسبه للمعتاد فهنا بقا انت تشك لأن دي علامات أو **Indicators** تدل ان فيه حابه مش طبيعيه هنا !! ... طب عاوزين نتأكد انها **Compromise** يعني خاصه بأختراق فعلا حصل ولا شكوك فالفاضي وأي كلام؟؟ دا بيتم عن طريق النوع الثاني من ال **Threat Intelligence** وهو بال **Digital Forensics** اللي هو الشغل ال **Manual** بتعنا المعتاد اللي بندخل جوا ال **Machine** اللي شاكين فيها بال **Tools** بتعتنا ونعمل ال **Investigation** عشان نتأكد من العلامات اللي شوفناها .

- نقطه ثانيه ال **Indicators Of Compromise** بتساعد ال **Information Security** وال **IT Professional** انهم يعملوا **Detect** لل **Data Breaches** اللي التسريبات وكمان ال **Malware Infections** وال **Other Threat Activity** ... فمن خلال اننا بنعمل **Monitoring** مراقبه لل **IOCs** المؤسسه بتعتنا تقدر تعمل **Detect** لل **Attack** وتعرف تاخذ **Action** بسرعه عشان نمنع ال **Breach** انه يحصل لل **Data** بتعتنا فبدل ميكون ال **Damage** كبير لاء هنعمله **Limit** ونخلي ال **Damage** يكون أخف ودا عن طريق اننا بنعمل **Detect** لل **Attack** فمرحله بدري شويه من مراحل ال **Attack** .

- وال **IOCs** ممكن تجبها من المنصات اللى ذكرناها فالجزء السابق زي **ISACs** و **OTX** وغيرهم من اللى اتذكروا ... بتبقا بامتداد **Open IOC Format** ودا بيخدها وينزلها ال **Threat Hunter** وبيكون قادر انه يعملها **Read** ويشوف المحتوى بتاعها ايه عشان يعرف عمله **Analyze** ويطلع منه الحاجات ال **Intelligence** ... وفيه **Tools** معينه بتمكنك انك تعمل **Download** لل **IOCs** فحاله انك معندكش البرامج اللى بتفتح الأمتداد بتاعها فدي محلوله لا تقلق هتنزل البرنامج المخصص لملف ال **IOCs** اللى نزلته وتفتح بيه الملف عشان تعرف تقرأه ... وأغلب الجهات أو المؤسسات اللى بتديك ال **IOCs File** بتديهولك بامتداد ال **Open IOC Format** وعشان نقرأ الملفات دي محتاجين يكون عندنا ال **IOC Editor** اللى كنا قولنا عليه هتحمله ودي زي **Tool** بتعملك **Manage** لل **Data** اللى بتجيلك فال **IOCs** ... وال **IOCs** بتبقا عبارته عن **XML Documents** بمعنى زي لغه ال **HTML** هتلاقي الكلام مكتوب بين **<>** ال **tags** دي ودا عشان تساعد ال **Threat Hunter** يحللوا ال **Data** دي ويعدلوا فيها بحيث تطلعهم ال **Malicious Files** فقط وعندك **Feature's** كتير بتقدمها ال **XML** اللى مكتوب بيها ال **IOCs** ودي هتقدنا كتير .

- ال **Indicator's** دي بتحتوي على **Malware Signatures** زي ال **MD5 Hashes** بتاعت ال **Malware Files** وكمال ال **IP Addresses** وال **URLs** وكمال ال **Domains** بتاعت ال **Botnet** اللى متمثله فال **C&C** ال **Command and Control Servers** .

- عندنا **Tool** تانيه اسمها **Redline** ودي برضه بتساعدنا نعرف نقرأ ال **IOCs** وكمال بتساعدنا أكثر فحته ال **Memory Analysis** وعندنا **Tool** تانيه اسمها **Yara** ودي بتساعد أكثر ال **Malware Researcher** انهم يطلعوا معلومات أكثر من ال **Malware Sample** اللى اتعمله **Detect** ...

عشان تطلع ال **Description** بتاعه ايه وال **Family** بتاعته ايه
وممكن نستخدمها احنا ك **Threat Hunters** عشان نعرف نطلع ال
IOCs بتعتنا .

- وبكدا نكون أنهينا الحديث فال **Module** دا عن ال **Threat**
Intelligence بشكل عام من خلال ال **Topics** اللى ناقشناها وهي
ان اتعرفنا على ال **IOCs** وكمان ال **Format** الخاص بيها وازاي
نستخدمها ونطلع من خلالها ال **Information** اللى علوزينها وكمان
اتعرفنا على ال **Threat Intelligence** بشكل عام وعرفنا ايه هي
اهم ال **Resources** اللى نستخدمها فشغلنا ك **Threat Hunters**
أثناء ال **Threat Intelligence Process** وعرفنا ازاي نطلع
معلومات **Intelligence** من معلومات **Raw** وعرفنا ازاي نجيب ال
Reports ومنين ال **Sources** الخاصة بيها وبس كدا .

4- Threat Hunting Hypothesis:

- تعالى هنا فآخر جزء ف **Section 1** نشوف ايه هنبء نعمل ال
Hunting منين أو ايه هي الافتراضيات أو ال **Steps** اللى المفروض
نمشي عليها أثناء تطبيق ال **Threat Hunting** ... وهنتكلم هنا عن
النقط دي بشكل تفصيلي باءذن الله .

4.1 MITRE & Attack.....65-68

4.2 Data Collection & Analysis.....69-75

4.3 Hunting Hypothesis & Methodology.....75-78

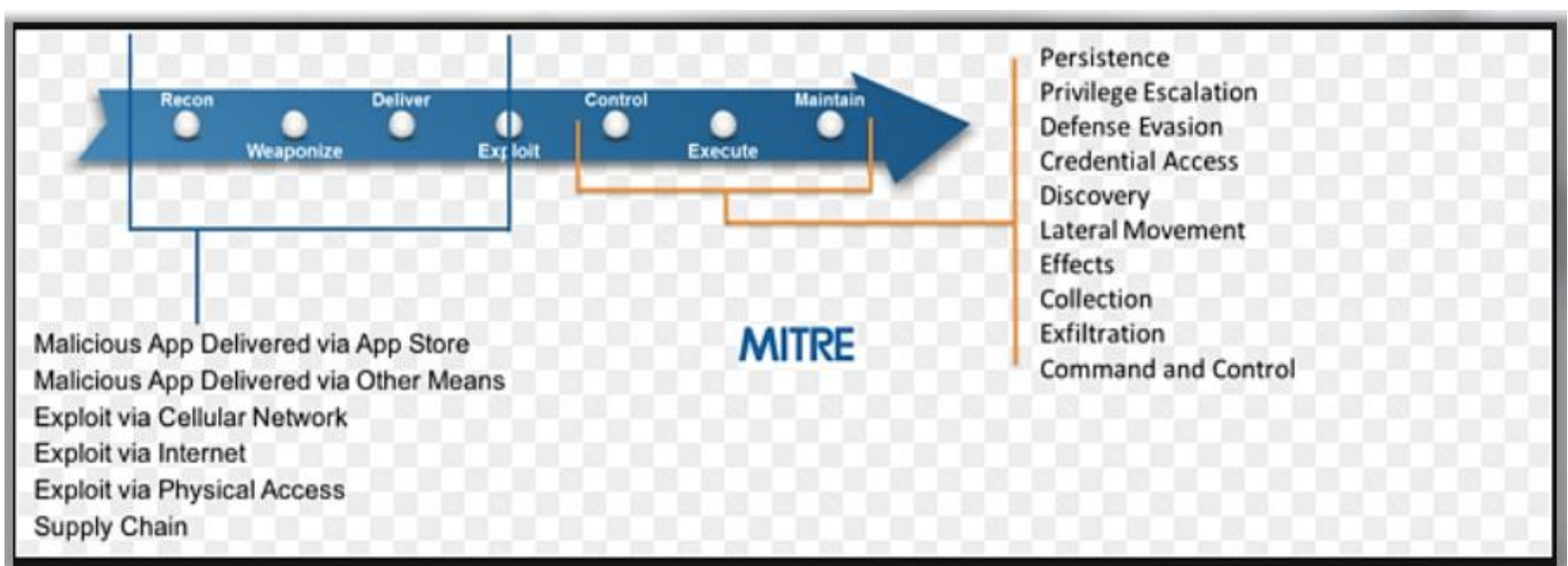
4.4 Hunting Metric's.....78-78

4.1 MITRE & Attack:

- زي مقولنا قبل كدا لازم انت ك **Threat Hunter** يكون عندك ال **Knowledge** الخاصه بال **Penetration Testing** وال **Attacks** اللى بييقوم بيها ال **Attacker** علشان تبقا عارف ازاي هتعمل **Detect** ال **Attacks** دي فال **Network** عندك فطبيعي يكون عندك الجانب الخاص بال **Offensive** قوي وعارف أنواع ال **Attacks** وتكون فاهم **Deep Understanding** ليهم مش مجرد أدوات وتطبق بيها وخلاص لاء لازم تكون فاهم ال **Attack** والغرض منه ايه وازاي بيحصل وايه ال **Steps** اللى بيعملها ال **Attacker** عشان ينفذ ال **Attacks** دا وازاي بتم عال **Endpoints** مثلا وهكذا فلزام تعملى **Stimulation** لل **Attack** اللى انت متوقع حدوثه دا أو شاكك انه عملنا **Infect** لازم تثبت الكلام دا بشكل عملي وتوريني ال **Steps** اللى مشى عليها ال **Attacker** عشان ينفذ ال **Attack** دا ويأكد الكلام اللى بتقوله ك **Threat Hunter** لمديرك فالمؤسسه وعشان فالنهايه تعرف تعملها ال **Detection** وأنت فاهم هتنفذ الكلام دا فين وازاي .

- ال **Detection Methods** دي معتمده انك تشوف الدلالات اللى عندك عال **Machines** اللى فال **End points** أو ال **Network Traffic** ... فأنت بتقول ان فيه **Attack** حصل هنا على **Machine** معينه فال **End point** !! ايه اللى يثبت ان ال **Attack** دا حصل بالفعل ساعتها انت ك **Threat Hunter** تقولي مثلا لقيت **2** **Processes** شغالين بنفس الاسم على **Machine** واحده فدا مقصدي بالمثال دا انك تثبت اللى بتقوله بشكل عملي ... طب احنا عاوزين نشوف نظره كامله عن ال **Attacks** وازاي ال **Attacker** بينفذها بال **Steps** عشان نعرف نبني الكلام اللى اتكلمنا عليه فوق ونفهم الأول ال **Attacks** اللى هندور عليها أو هنعملها **Detection** .

- دا ممكن نشوفه من خلال ال **MITRE & Attack** ... ودا من خلاله
 هنشوف ال **Vendor Reports** التقارير اللى بتطلعها الشركات كل
 فتره عن آخر ال **Attacks** وال **Individual Researchers**
 هتلاقيهم برضه بيطلعوا آخر ال **Threats** ف **reports** كل دا هنشوفه
 من ال **MITRE & Attacks** وهنعرف ازاي نستفيد منه ... وبأختصار
 ال **MITRE & Attacks** دي بأختصار عباره عن منصه بتوضحك آخر
 ال **Attacks** وازاي يتم وبتشرحك ال **Steps** اللى تم بيه ال **Attack**
 وازاي تعمل **Detect** وكمان بتعرفك ال **Adversary Groups**
 المشهورين مين فال **Attacks** وال **Behavior** بتعمهم وكمان ال
Phases اللى ال **Adversary** بيعملها أثناء عمل ال **Attack** عال
Target بتاعه ... فلو انت ك **Threat Hunter** معرفتش تعمل
Detect لل **Attacker** فالأول فال **MITRE & Attack** بيمكنك كمان
 انك تعمل **Detect** لل **Attacker** في مراحلها ما بعد ال **Post**
Exploitation زي كدا بالضبط .



- ودي ال **Matrix** أو النمطيه اللى بيشتغل ومبني عليها ال **MITRE & Attack Model** .

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact

- فال **MITRE & Attack** دي بمثابة ال **Steps** اللى ال **Attacker** بينفذها عندنا فعليه الاختراق فأحنا حصل عندنا **Attack** ما ومش فاهمين ايه اللى حصل أو ازاي اتنفذ وتم عندنا فانت تروح لل **MITRE Attack &** تفهم منه ازاي ال **Attack** تم عليك والخطوات اللى اتنفذ بيه واللى مشي عليها ال **Attacker** عشان تعرف تعمل ال **Detection** وكمان تمنعها تعملها **Mitigation** ... فهي برضه بتوضحك ال **TTPs** بتاعت ال **Adversary** اللى كنا اتكلمنا عليها قبل كدا ... فال **MITRE & Attacks** بحتوي على أكثر من 400 **Technique** لسيناريوهات مختلفه من ال **TTPs** لل **Attacks** تقدر تستفيد من خلالهم وكل شويه بيتعملهم **Update** فخليك متابع ال **MITRE & Attack** هتفيدك جدا .

- تعالى ناخذ مثال من ال **Post Exploitation** من ال **MITRE & Attack** يعني لو ال **Attacker** عمل كل الخطوات اللى ذكرناها قبل كدا زي ال **Recon** وال **Weaponize** لحد منفذ ال **Exploit** ودلوقتي عاوز يعمل ترقية للصلاحيات بتعته ويعمل **Privileged Escalation** بس انت ك **Threat Hunter** عرفت انه نفذ عليك ال **Attack** ووصل لل **Exploit** ومكمل فطريقه تتعامل معاه ازاي عشان توقف أو تعمل **Mitigate** لل **Attack** ! فتعالى نشوف المثال على ال **Kerberoasting** ودا **Technique** من ال **Post Exploitation**

Kerberoasting

Service principal names (SPNs) are used to uniquely identify each instance of a Windows service. To enable authentication, Kerberos requires that SPNs be associated with at least one service logon account (an account specifically tasked with running a service [1], [2] [3] [4] [5]).

Adversaries possessing a valid Kerberos ticket-granting ticket (TGT) may request one or more Kerberos ticket-granting service (TGS) service tickets for any SPN from a domain controller (DC). [6] [7] Portions of these tickets may be encrypted with the RC4 algorithm, meaning the Kerberos 5 TGS-REP etype 23 hash of the service account associated with the SPN is used as the private key and is thus vulnerable to offline Brute Force attacks that may expose plaintext credentials. [7] [6] [5]

This same attack could be executed using service tickets captured from network traffic. [7]

Cracked hashes may enable Persistence, Privilege Escalation, and Lateral Movement via access to Valid Accounts. [4]

ID: T1208

Tactic: Credential Access

Platform: Windows

System Requirements: Valid domain account or the ability to sniff traffic within a domain.

Permissions Required: User

Data Sources: Windows event logs

Contributors: Praetorian

Version: 1.0

Created: 18 April 2018

Last Modified: 18 July 2019

- زي منتا شايف هتلاقية بيشركك ال **Attack** وال **Technique** بتاعه وازاي بيتم عال **Target** بشكل تفصيلي وكمان ال **Detection** **Technique** لل **Attack** دا زي كدا .

Detection

Enable Audit Kerberos Service Ticket Operations to log Kerberos TGS service ticket requests. Particularly investigate irregular patterns of activity (ex: accounts making numerous requests, Event ID 4769, within a small time frame, especially if they also request RC4 encryption [Type 0x17]).^{[1] [7]}

- هتلاقية بيقولك تشوف وتعمل **Search** عال **Event ID Number** اللى قدامك من خلال ال **Event Viewer** اللى عندك عال **Windows Machine** ولو ظهرك ان فيه **Event** شغال عندك عال **System** بالرقم دا تعرف علطول ان فيه ال **Attack** اللى هو **Kerberoasting** شغال عندك عال **Machine** حاليا .

- بس خد بالك من نقطه وهي ان ال **MITRE & Attack** بتحتوي فقط على ال **Most Common Attacks** وطريقه التعامل معاها فانت ك **Threat Hunter** متقدرش تعتمد عليها لوحدها فقط كمصدر أساسي فلازم تزود ال **Resources** الخاصه بيك فال **Hunting** وتنوعها زي مثلا انك تقرأ **Write ups** كتير لل **Researchers** من موقع زي **Medium** لأخر الثغرات المكتشفه وال **Attacks** اللى هتستخدم فيها وخطورتها ايه وتشوف منتديات وجروبات ال **Hackers** من خلال ال **Dark Web** وتكون مأمّن نفسك كويس وحذر طبعا وتبحث عن آخر ال **Techniques** بتعتهم وهكذا تطور من نفسك من كذا **Resource** وتبقا **Updated** بال **Techniques** الجديده عشان تحمى نفسك منها قبل متحصل وتسبب ضرر عندك فالمؤسسه ... وهسبك لينك كأضافه ليك لفديو يوتيوب ك **Source** ل **Team Researchers** معروف اسمه **BSides Bristol** بيوضحوا فيه ازاي ممكن تستعين بال **MITRE & Attack** فال **Threat Hunting** .

<https://www.youtube.com/watch?v=tmW60vC0tHE>

4.2 Data Collection & Analysis:

- عرفنا فالجزء اللي فات من خلال ال **MITRE & Attack** عال **Attack** ازاي بيتم وازاي نتعرف عليه وشوفنا كمان ازاي نعمله **Detect** ... عاوزين دلوقتي نبني ال **Knowledge** بتعتنا عال **Data** اللي جمعناها دي ... لازم واحنا شغالين بنعمل **Hunting** نكون عارفين ازاي نعمل **Data Collection** و **Data Analysis** اللي هما موضوع ال **Topic** بتعتنا هنا ... تعالى نسأل نفسنا شويه أسئلة ونحاول نجاب عليها عشان نغطي من خلالها شرح ال **Topic** دا .

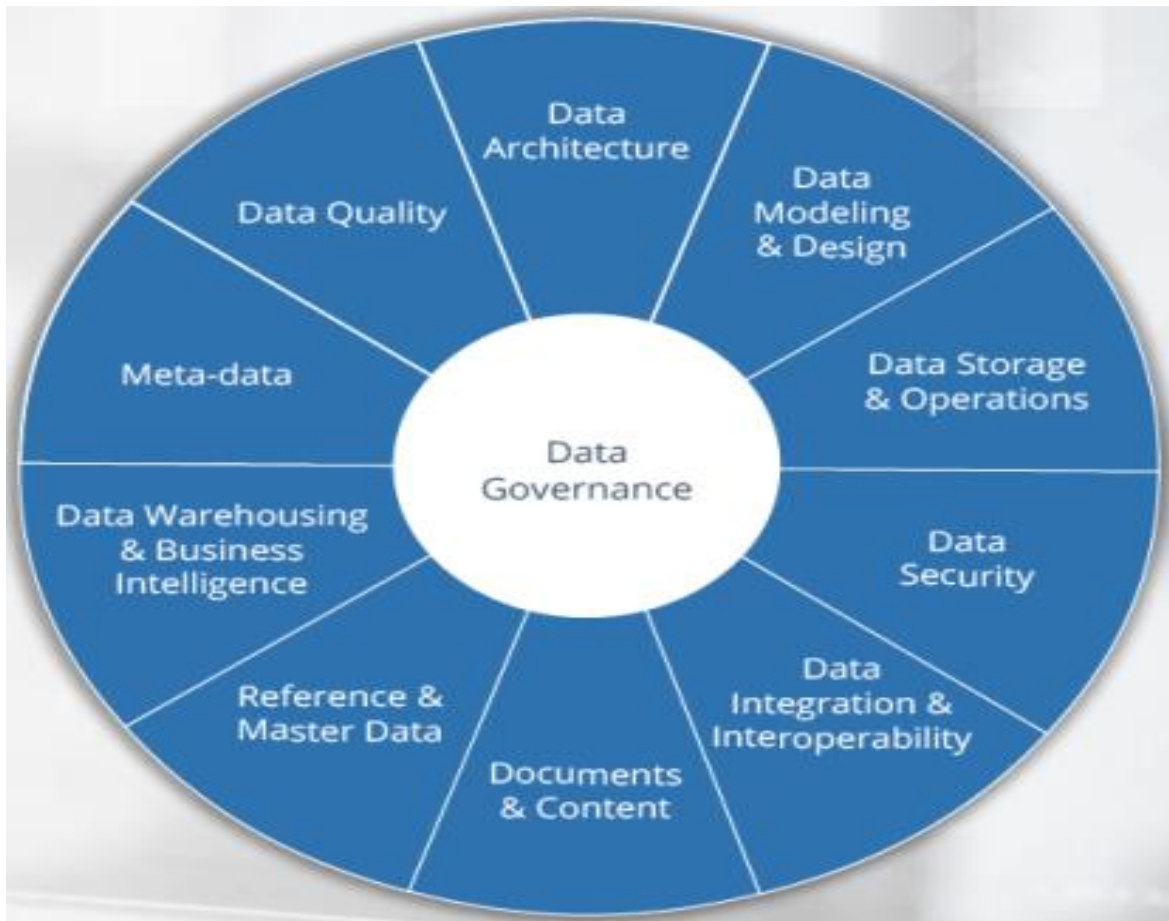
- أول حاجة ايه هي ال **Data** اللي عندي حاليا وهل ال **Data** دي كافيه عشان نكمل باقي ال **Steps** وايه هي نوع ال **Data** دي؟؟ وهل ال **Data** دي مرشحه انها تكون **Qualified** اني اشتغل عليها؟؟ وهل ال **Data** اللي موجوده معانا دي نقدر نعملها **Transform** ونحولها ل **Data** مفيده وللااء؟؟ .

- طبعا احنا عارفين عشان ننفذ ال **Hunt** بتعتنا لازم نعمل ال **Collect** لل **data** اللي هنعمل عليها **Hunt** دي الأول ... بس هنا فيه ملاحظه وهي وانت بتعمل **Collect** لل **Data** دي اعمل **Collect** لل **Data** الصح بالنسباك مش **Collect** وخلاص ... لاء احنا هنجمع ال **data** اللي هتخلينا نترجت نعمل عليها **Hunt** اللي بتخدم ال **Attack** اللي احنا ك **Threat Hunters** شاكين فيه وعاوزين نتأكد اذا كان دا حصل عندنا فعلا فالمؤسسه وللااء !! فهنروح نجيب ال **Data** اللي بالفعل بترجت ال **Attack** اللي عندي شك انه عندنا فالمؤسسه ... فأنت تعمل **Avoid** لل **Noise Populated Data** اللي هي ال **data** اللي ملهاش لازمه ومش هتفيدك فال **Attack** ال **Specific** اللي انت شاكك فيه وشغال عليه .

- ال **Main Data** الى هنعملها **Collect** عشان نشغل عليها هي ال **Primary Data Types** زي ال **Data** الى تخص ال **Host** أو ال **Network** وهما دول الى قدام باعذن الله هنعمل عليهم ال **Hunt** فأخر **Section** فالكورس الخاص بال **Hunting Endpoint** ... فأحنا بنجمع **Data** على ال **Host** الموجود ف **Endpoint** معينه عندنا فالمؤسسه ونعمل لل **Data** دي **Hunt** أو نفس الكلام دا بس هنعمله على ال **Network Traffic** .

- تعالى فالأول نشوف الطريقه الى هناخد بيها ال **Data** دي أو نعملها **Export** من على ال **Host** بتعنا الموجود فال **Endpoint** ... **أول** **طريقه** معانا وهي اننا نخلي ال **Host** الى هو مجازا ال **PC 1** يعمل **Push** أو يدفع ال **Data** بتعته دي أو ال **Logs** لل **SIEM** الموجود عندنا فالمؤسسه واحنا نعمل ال **Collect** بتعنا من ال **SIEM** بشكل مباشر ... **الطريقه الثانيه** معانا هي اننا نعمل **Pull** الى هو سحب لل **Data** عن طريق ال **SIEM** بتعنا من ال **Host** الى هو **PC 1** الموجود فال **End point** ... هنسحبوا ال **Data** من ال **Host** عن طريق ال **SIEM** ونروح احنا ك **Hunters** نعملوا **Collect** لل **Data** دي من ال **SIEM** بدل مكننا بنروح نعمل **Collect** من ال **Host** فالمره الى فانت لاء هنا العكس هنروح نعمل ال **Collect** من ال **SIEM** ... **الطريقه الثالثه** معانا هي ال **Mix** مابينهم اننا نعمل **Collect** لل **Data** بتعنا الى هنشغل عليها شويه من ال **SIEM** وشويه من ال **Host** ... وطبعاً لاتنسى انك تعمل **Check** زي مقولنا عال **Data** الى بتعملها **Collection** وتشوف ال **Quality** بتعتها وتشوف الى انت عاوزه من الاول من قبل متشتغل عشان متضيعش وقت ومجهود فالفاضي واحنا اتكلمنا كتير عن أهميه عامل الوقت بالنسبالك ك **Threat Hunter** وانك لازم تبقى حريص عليه وعلى توفيره بأقصى درجه ... كمان نقطه فغايه الأهميه لازم تكون عارفها قبل منعمل **Collect** لل **Data** وهي اننا ازاى نعمل **Govern** لل **data** !

- اللى هو ازاي نراقب ال **Data** اللى عملناها **Collection** دي ...
تعالى نشوف ال **Data Governance** الأول ازاي نعملها !



- نتأكد الأول من ال **Source** اللى جيانا منه ال **Data** دي مش أي **Data** تجيلك وخلاص تقوم عملها **Analysis** لاء بنتأكد الأول هل ال **Data** دي بت **Match** الشغل اللى شغال عليه وال **Cases** اللى شاكك فيها وشغال عليها دلوقتي ! وكمان تتأكد من ال **Integrity** الخاصه بال **data** دي بالأضافه هل ال **Data** دي مهمه وتستحق انها تاخد مني الوقت اللى هتاخده دا كله ولا لاء ولا هتطلع **Data** مش بالأهميه اللى مستنيها انت وهكذا ... عشان نعمل ال **Data Governance** بشكل مضبوط لازم ندور الأول على ال **Data Completeness** اللى هو ال **Data** اللى انا عاوزها فعلا **Available** وفتره وجودها هي ايه ؟ بالأضافه اننا هندور على ال **Data Consistency** اللى هو دقه ال **data** اللى عملتها **Collect** هل جايلك من **Source** موثوق فيه وهل جايلك من **Different Resources** ولا لاء ... كمان لازم نتأكد من ال **Data Timeliness** اللى هو ال **Data** اللى هنعملها **Collect** يكون عليها **Time Stamp** دي بتحددك ال **Creation Time** لل **Files** مثلا وليكن هتلاقي عندك **File** معموله **Create** فتوقيت ما لازم تتأكد من التوقيتات الخاصه بال **Data** اللى مجمعتها عشان هتحتاجها قدام لما تيجي تعمل **Investigation** لل **Events** .

- طب ايه اللى هستفيدة أنا ك **Threat Hunter** لما أعمل **Data Governance** !! هتفيدنا بأيه مراقبه ال **Data** دي ؟!

- احنا عندنا فالطبيعي نوعين من ال **Data** اللى هتجيلنا وهما ال **Normal** وال **Abnormal** الحاجات الطبيعیه اللى متعودين عليها والحاجات الشاذة واللى مشكوك فيها فطول محنا بنراقب ال **Data** دي هنعرف من خلال خبرتنا وال **Cases** اللى اتعرضناها كتير فشغلنا ان ال **Data** دي طبيعیه ولا لاء وعلى اساس الاستنتاج دا هنعرف نعمل ال **Hunting** لل **Data** اللى شاكين فيها فمثلا **Traffic** جاي من ال **WAN** لل **LAN** شكله **Abnormal** فدا يثير الشكوك حوله اننا نعمله **Investigation** لول فيه حاجه **malicious** نعملها **Hunt** ... وهكذا على اي **Case** تقابلنا من **Abnormal Data** ... وطبعاً انت ك **Threat Hunter** مش هتعرف ال **Abnormal** الا اما تكون عارف ال **Normal** من ال **data** عامل ازاي عشان اي حاجه غيرها تعرف تميزها وتقول عليها **Abnormal** .

- على سبيل المثال انت مؤسستك كل يوم بتعمل **Download** من ال **Internet** بمعدل **100** جيجا دا ال **Bandwidth** بتاع مؤسستك وانت عارفه ك **Threat Hunter** يبقا دا بالنسبانا هنا ال **Base line** بتاع ال **Normal** تمام ... جينا فيوم ما واحنا بنراقب ال **Data** بتعتنا لقينا ال **Download** مره واحده زاد ل **200** جيجا واحنا معملناش جديد اللى هو كل يوم بنعمل نفس ال **Tasks** بتعتنا ومع ذلك في حاجه غريبه بتحصل !! هنا بقا دا يتصنف **Abnormal** وهتبدء تعمل **Investigation** ليه وت **Hunt** عالحاجه المشكوك فيها ... قولي بقا هتعرف ازاي ال **Normal** من ال **Abnormal** لو انت مش بتراقب ال **Data** بتعتك ؟!.

- الحاجات ال Normal اللى انت ك Threat Hunter لازم تكون عارفها هي كالتالي ...

- أول حاجة هي ال Running Processes اللى شغاله عندك عال System عشان أي حاجة غيرها هتكون Abnormal ... ال User Login وكمات تعرف كام نقطه عنه زي التوقيت اللى بيعمل فيه Login والمكان اللى عمل منه ال Login وايه نوع ال Login دا وهل مسمحوه بيه وللااء ... ال Network Connections اللى هو المفروض نفتح Connection مع مين ومسمحولنا نفتح أصلا مع مين وال Bandwidth بتعتنا كام اللى هنمشي عليها ... كمان ال Services وال Scheduled Tasks اللى شغالين عال End points Devices ... بالأضافه لل Software's اللى مسموح انها يتعملها Execute وتشتغل عندنا عالأجهزة ... وبكدا نكون عرفنا ازاى هنعمل Collection لل Data بتعتنا وعلنالها ال Data Governance عشان نفلترها كمان ودلوقتي جه دور اننا نعمل لل Data دي عمليه ال Analysis .

- أسهل طريقه عندنا هي اننا نروح لل SIEM يحلل ال Data اللى هو برضه عنصر معانا من العناصر اللى عملت Collect فيحلل ال Data اللى عملها Collect ويصنفها وال SIEM دا بقا على حسب مؤسستك بتشتغل بأيه ممكن Splunk وممكن ELK وممكن Gray log على حسب المؤسسة شغاله بأنهو SIEM ... وال Analyzing دا معناه اننا نعرف نعمل Manipulation لل Data اللى عملنالها Collect اللى هو نعرف نعدل عليها ونشتغل عليها ونعرف نعمل عليها ال Search بتعنا وكمات نعملها Filtration ونعملها Join مع Data تانيه وكمات نعملها Aggregation اللى هو التجميع لل Data دي واهم حاجة بالنسبالنا هما ال Search وال Aggregate .

- ال **Search** بالنسبه لينا اننا عندنا بعض ال **Questions** والمفروض اننا عن طريق ال **Search** جوا ال **data** بتعتنا نطلع ال **Answers** بتعتهم ... الغرض من ال **Search** اننا نضيق ال **Gap** ونرد عال **Questions** اللى عندنا مش نفتح **Questions** جديده !!
خد بالك من النقطه دي احنا من الأول غرضنا اننا نعمل **Analysis** يعني تحليل وفلتره لل **Data** اللى جمعناها عشان نطلع منها المهم بالنسبه لينا اللى هنفذ ال **Hunt** عليها وانت عارف ال **Normal** من ال **data** وبالتالي هتشوف ايه ال **Abnormal** وتطلعاه .

- نيجي لل **Aggregation** اللى هو عمليه تجميع ال **Data** ... اللى هو عاوز تطلع نتيجته لسؤال عندك بكذا حاجه مع بعض مش مجرد حاجه واحده فقط !! يعني مثلا عاوز تطلع ال **Processes** ال **Specific** دي وليكن زي **Calc.exe** وكمان اشتغلت كام مره عال **End point** .

Process name	Occurrences
Svchost.exe	13
Winword.exe	9
Calc.exe	1

- فهنا أحنا جمعنا كذا **Field** مع بعض وهما ال **Process name** وال **Occurrences** عن طريق ال **Aggregation** ... خد مثال تاني عال **Aggregation** ... عندك **Command** معين عاوز أعرف مين عمله **Executed** وكتبه على أنهو **PC** وكتبه كام مره فدا كذا نوع من ال **Aggregation** اللى هو بنجمع كذا نقطه مع بعضهم عشان نطلعهم قدامنا ف **Result** واحده ... وفالنهايه احنا بنعمل ال **Data analysis** بال **Search** وال **Aggregation** عشان نتأكد من حاجه احنا شاكين فيها انها ممكن تكون **Suspicious** ... تعالى ناخد مثال ... عندنا واحد فالمؤسسه شغال معانا بيحاول يعمل **Connect** بال **Suspicious IP** احنا مصنفينه كذا أو معروف عندنا .

- هنا احنا عاوزين نعرف ليه الشخص دا بيعمل كدا؟! هنروح عن طريق ال **PCAP** أو **NetFlow** عشان نعرف نحلل ال **Traffic** دا ونشوف اذا كان دا **Malicious Event** ولا دا **False Positive** يعني طلعت الدنيا عادي والشك بتعنا مش فمكانه الصحيح والدنيا **Normal** ... فأحنا مش مجرد بنعمل **Search** وخلص ونطلع المعلومه لاء احنا بنربطها بمعلومه تانيه نحاول نوصل بيها لمعلومات أكثر توصلنا فالآخر لتفسير منطقي نعرف نوظف المعلومه فالمكان اللي تفدنا بيه فال **Threat Hunting Process** .

4.3 Hunting Hypothesis & Methodology:

- هنا هنعرف ازاي نمشي عال **Methods** اللي هنعمل من خلالها ال **Hunt** ... فأحنا محتاجين الأول قبل أي حاجه نحدد ال **Behavior** بتاع ال **Data** اللي هنعمل عليها **Hunt** فهي **Data** تخص ال **DOS Attack** ولا ال **Privileged Escalation Attacks** ولا ال **Attackers** اللي بيزرعوا **Back Doors** ولا ايه بالضبط محنا مش هنشتغل بشكل عشوائي أكيد !! ... ومحتاج تفهم ال **Attack Technique** بيتم ازاي ودا كنا ذكرناه انك تقدر تجيبه من خلال ال **MITRE & ATTACK** ... بالإضافة انك تكون عارف ال **Data Source** اللي هتعمل منه ال **Detection** ... وبعد كدا هنمشي على ال **Methodology** الخاصه بال **Hunting** اللي هي **5 Steps** .

- وهما كالتالي ... هنختار ال **Technique** وال **Tactic** اللي هنشتغل عليهم وبعد كدا نشوف ال **Procedures** اللي هي الإجراءات اللي شغال بيها اللي هما تقدر تلمهم فال **TTPs** اللي اتكلمنا عليهم قبل كدا ...

بعد كدا تعمل ال **Attack Stimulation** تشوف السيناريو دا حقيقي بالتجربه وشغال ولا لاء عشان تأكد الافتراضيه بتعتك بحدوث ال **Attack** دا فعلا ... بعد كدا تجمع **Evidence** من ال **Stimulation Process** اللى علمتها وبعد كدا تحدد ال **Scope** اللى هتشتغل عليه ... وتعالى نشوف **Step Step** كدا بالراحه .

- ال **Step الأولي** معانا وهي ال **Pick technique & Tactic** ودا احنا كنا شوفناه من خلال ال **MITRE & ATTACK** فالجزء اللى فات اللى هو كان عندنا أكثر من **Tactic** وكل **Tactic** جواه بيحتوى على أكثر من **Technique** ... تعالى ناخذ مثال على ال **Technique** اللى هو **Privileged Escalation** اللى ال **Tactic** بتاعه رقمه **T1502** فلو دخلت عليه من خلال ال **MITRE & ATTACK** هتلاقيه بيشرحها لك بالتفصيل وتفهمه بيشتغل ازاي ... ال **Step الثانيه** اللى بعدها محتاج تعرف ال **Procedure** بتاع ال **Attack** اللى هو ازاي بيشتغل عال **End Point** لما بيصيبها ... زي كدا بالضبط .

Procedure Examples	
Name	Description
Cobalt Strike	Cobalt Strike can spawn processes with alternate PIDs. ^[6]

- فممكن تلاقي ال **MITRE & ATTACK** مش مدياك معلومات كافيه وال **Details** مش كافيه ... فانت تعمل **Search** بطريقه **Manual** عن طريق انك تشوف **Report** وتقرؤه وتطلع منه ال **Details** اللى تفيدك وهكذا بقا من **Blogs** و **Reports** هتمدك بالتفاصيل اللى هتحتاجها .

- ال **Step الثالثه** بعد أما عرفنا معلومات عن ال **Attack** وطريقه شغله ايه هي ال **Perform Attack Stimulation** ... عاوزين نعمل محاكاة لل **Attack** دا فمكان عمل خاصه بيه .

- الخطوة التي فاتت دي اننا نعمل محاكاة لل **Attack** ونحاول ننفذه ونشوف فالواقع دا هيحصل وللااء دا هيفدنا فال **Step** الرابعه معانا وهي ال **Identify Evidence to Collect** بمعنى ... التي انت طبقته دا بقا عندك معلومات منه تعرف تعملها **Collect** بعد كدا وتضيفها لل **Report** بتاعك ومنها هتعرف تعمل **Identify** لل **Behavior** بتاع ال **Attack** دا عشان فالمستقبل دا هنستخدمه عشان نعرف نعمل **Detect** لل **Malicious Activity** دي ... طب لما تنفذ ال **Attack** تعمل **Collect** لأيه بالضبط ؟ أول حاجه الحاجات المختلفه عن ال **Baselines** التي انت حاططها وشوف هل حاجه عندك عال **System** اتعملها **Encryption** وهل فيه حاجه اتعلمها **Occurrence** لأكثر من مره **Process** مثلا أشتغلت بنفس الاسم مرتين أو اكتر وهكذا تبدء تشوف الحاجات ال **Abnormal** عشان دي التي تهمننا فالتعرف عال **Attack** دا والحاجات التي بينفذها علينا دا لو أصابنا فالمستقبل .

- ال **Step** الخامسه والأخير معانا فال **Methodology** هي اننا ن **Set** ال **Scope** بتعنا ... هنا بقا هنعمل للأفترضيه بتعتنا التي تخص ال **Attack** التي احنا قولنا ان المؤسسه بتعتنا ممكن الأجهزة التي فيها تكون مصابه ب **Attack** زي مثلا **Privileged Escalation** هنا بقا هنشوف ال **Proving** أو ال **Disproving** التي هو هنثبت فعلا صحتها من خطأها ... هنحتاج فال **Step** دي نحدد هنعمل **Hunt** قد ايه يعني الوقت التي هتأخده عمليه ال **Hunting** وكمان ال **Data** التي التي هنشتغل عليها ايه هي التي اتعملها **Collection** ... وكمان ملحوظه مهمه عالأقل تفضل مستمر في عمليه ال **Hunt** دي لمدى أسبوع دا أقل حاجه حتى وانت بتعمل **Collect** لل **Data** عالأقل تاخذ منك ال **Process** دي أسبوع دا عالأقل خالص ... ودا علشان بعض ال **Attacks** مبتظهرش علطول عال **End points** التي بتعملها **Infection** وبتأخذ شويه وقت ممكن يوم ممكن اتنين .

- ملحوظة تانيه ... تركيزنا فال **Collection** الخاص بال **Data** يكون على المناطق الحساسه عندنا فالمؤسسه مش كل ال **Devices** وكل ال **Departments** لاء !! الأماكن اللى محتاجه تأمين كويس وأغلب ال **Attacks** اللى عندنا بتحصل عليها ... وطبعاً متنساش تاخذ **Notes** أثناء ال **Threat Hunting Process** لأي حاجه **Activity** أو انت شايفها مهمه وكمان تستخدم ال **Tools** اللى انت شايفها مناسبه لل **Task** اللى هتفعلها .

4.4 Hunting Metric's:

- هنا بقا فالنهايه عاوزين نعرف ونقيس ال **Threat Hunting Process** اللى عملناها دي هل فعلاً ناجحه ولا هحتاج نعمل ال **Process** تاني من أول وجديد !! هنا بنقيس مدي نجاح ال **Process** بتعتنا وتأثيرها ... تشوف أول حاجه احنا بنعمل **Hunt** أمّا ولمده من الوقت ايه هي تعرفها برضه .. شوف احنا غطينا وجاوبنا على كل ال **Questions** بتاعت ال **Attack** اللى كنا مفترضين انه عندنا عال **Endpoints** ولالاء ... هل غطينا كل ال **Critical Points** الموجوده فالمؤسسه بتعتنا وليكن أهم ال **Business Point** عملنا عليه ال **Hunt** وبقا **Secure** ... وهل عملنا **Hunt** عال **Network** ولالاء ... وهل عملنا **Historic Logging** للحاجات اللى عملناها **Hunt** ولالاء ... فدي زي **Questions** بنحاول نجاب عليها عشان نغطي ال **Threat Hunting Process** .

- وبكدا نكون أنهينا الحديث فال **Module** دا وال **Section** كمان انهيناه الخاص بال **Threat Hunting** وحطينا كل ال **Baselines** بتعتنا وال **Steps** اللى هنمشي عليها قدام فالكورس بشكل عملي أكثر بآذن الله .