ENDPOINT SECURITY: A STEALTHY APPROACH TO CYBER DEFENCE

Author:

Nathaniel ADEWOLE

Threat Researcher

(B.Tech, CEH, Sec+)

Methodology Used

- Review of popular Endpoint solution used in the security operation centers(SOC).
- Review of related works (50) -publications, patents, articles, whitepapers, conferences/workshops; from 2000 to July 2021
- Survey and Questionnaire from security analyst,

Objectives

- To practically review challenges of endpoint security base on: the people, process and technology
- Outline expectations to maintain balance between effectiveness of endpoint security and productivity
- To guide decision makers on the minimum yardstick for a better endpoint security, instead of vendor bias approach or random selection

Internet Usage Category	
Student/Tutor	MOOC, YouTube, reading sites, streaming
Internet Addict	Use more applications, check almost everything
Socializers	Instant messengers, forum, dating sites
Basic	Search engines, emails, IM
Presenter	Write blogs, articles or topics in forum
Businessmen	e-commerce site, stocks, travelling, news
Gamer	Plays online games

Endpoints

TRADITIONALLY:

Endpoint are internet connected hardware (workstations)

NOW:

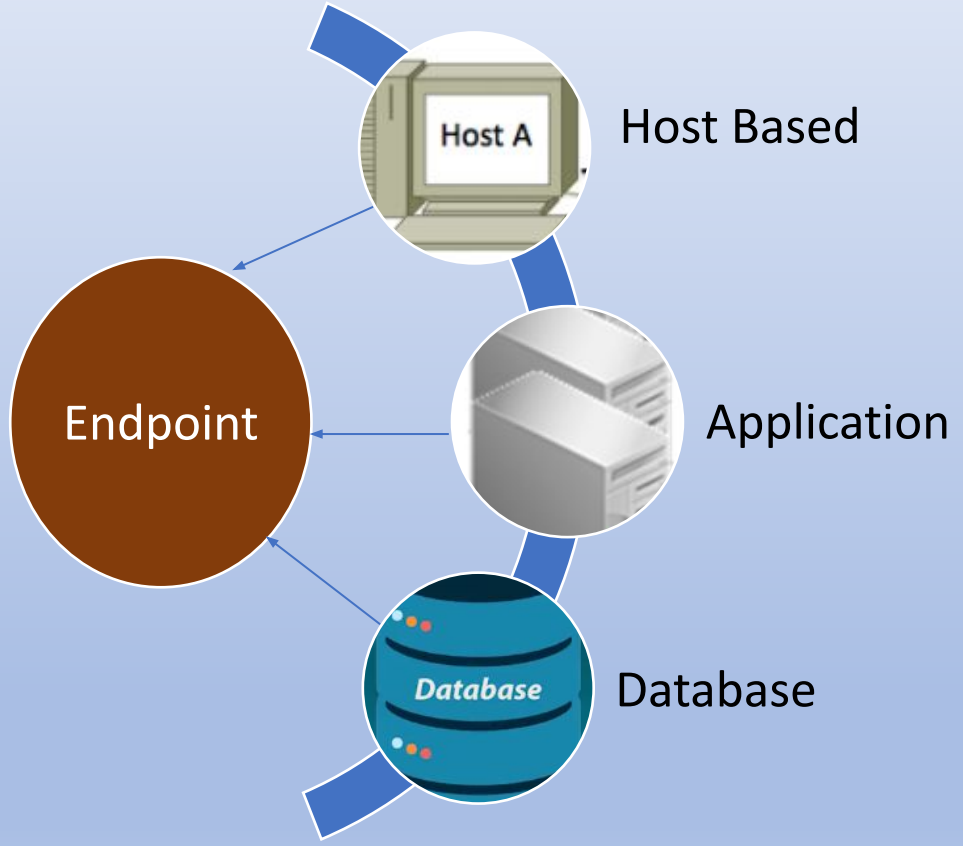
Servers, Tablets, Printers, Smart Devices, Internet of things(IOTs), point of sales terminal(POS), mobile phones.

…a URL in an API or EC2 instances is an endpoint that enable users to interact with server resources.

www.entrepreneurhandbook.co.uk/the-internet-of-things/

Why Endpoint ?

Reference	Statistics
IBM –Ponemon Institute May 28th, 2021	❑ $4.28million -Av. cost of a breach globally ❑ 78% Breaches
	❑ 64 % of Breaches -Confirmed by 3rd party
Dataprot	❑ 560 000/Day -New malwares Strains
IBM – 2020	❑ 228 days -Average time to detect ❑ 80 days -Average time to contain



Attack Trend

The Creeper Worm:

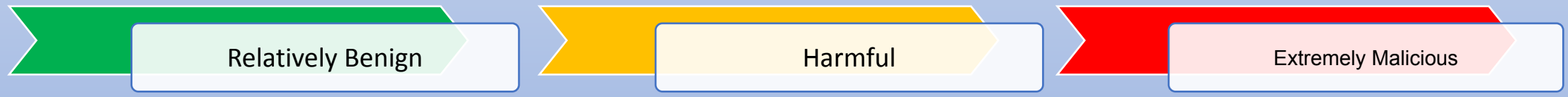
'*I am the creeper; catch me if you can*'

ELK Cloner:

'The program with a personality
It will get on all your disks
It will infiltrate your chips
Yes it's cloner!
It will stick to you like glue
It will modify ram too
Send in the Cloner! '

Melissa, Jerusalem, Morris Worm, CIH, ILoveYou, code red, slammer, mybloom, mpack, Asprox botnet, Gumblar, Stuxnet

Heartbleed, Duqu, ZeroAccess, flame, Crypto locker, Reveton, Locky, Mirai Botnet, WannaCry, Emotet, Petya, Trick Bot, Maze, Regassus, Ryuk, Kaseya …



Bob Thomas, 1971
(Experimental Work)
&
Richard Skrenta, 1982
(Practical Joke on Friends)

1980s – 2010

2011 – Till Date

Advanced Persistent Threat(APT) Groups

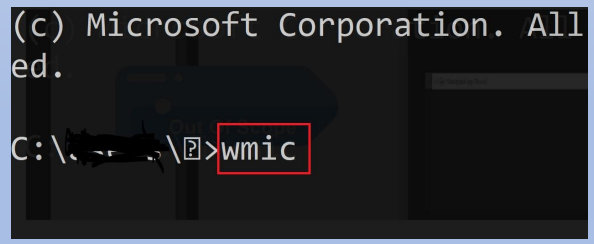
Attacks Are Smart

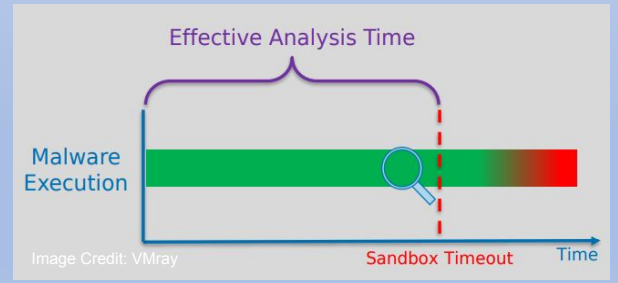
- Packers, polymorphic code and lateral movement attacks
- Signature bypass:
  Automated code permutation, register renaming, shrinking or expanding code, insertion of dump code
- Delayed Execution
  Logic bomb, stalling code, extended sleep
- User interaction, system properties, environmental awareness(e.g Carbanak, blacksquid malware)

```c
#include <stdio.h>

int main()
{
    int indicators = "Sandbox";

    if (indicators=="Sandbox")
        { // checking if in analysing environment
            printf("Suspend Action!\n");
        }
    else
        { // Real endpoints -VMs not detected
            printf("Execute Malicious Payloads\n");
        }

    return 0;
}
```

main.c — Run — Output

```
/tmp/CbAHcKgDzA.o
Suspend Action!
```





Evolution In Attacks

WHAT HAS CHANGED?

- Increasing Sophistication(the ‘A’ in APT)
- Increasing Scale(Count)
- Attack types (Malware to Fireless)
- More dangerous threat actors’ motivations
- Heavy Impact (Risk Analysis)

Malwares:
Backdoors, worms, virus, crypto miners, trojans, rootkits, ransomware.

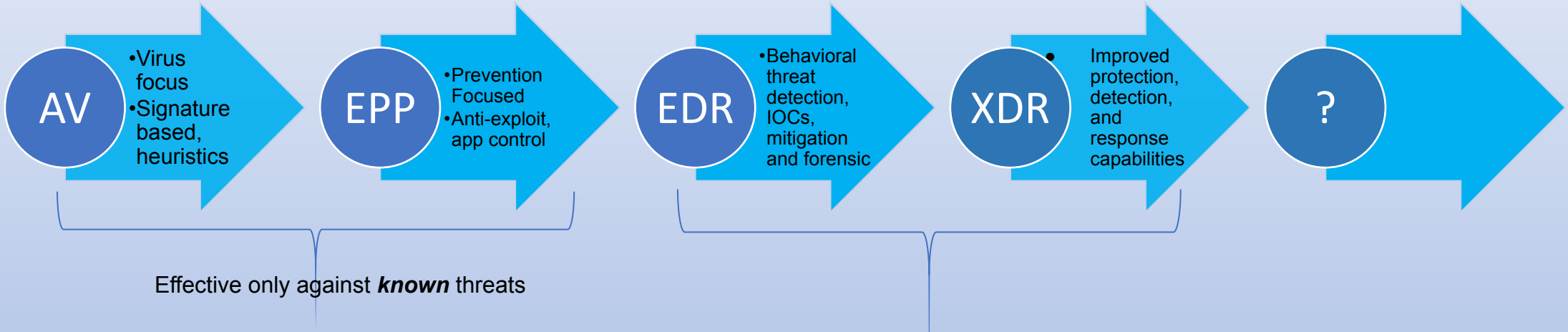
Exploiting legitimate files For Malicious Use:
Fireless Attacks: Malicious scripts(PowerShell, WMI), dll, macros.

Digitally signed or OS whitelisted malwares, Living Off the Land Binaries/LOLBAS projects(LOLBins, LOLScript, LOLLib)

Threat actors:
Researchers, hackers, Advanced persistent threat(APT) groups

Lazarus Group, Lazarus Group, Fancy Bear, Cobalt Group, FIN7, Mirage, Magecart, Equation Group, OilRig, Comment Crew, Syrian Electronic Army, PLATINUM, Anonymous, Numbered Panda, Dynamite Panda, Cozy Bear, Elfin, Charming Kitten, Ricochet Chollima, Mythic Leopard, Sodinokibi, Muddy Water, Patchwork, Energetic Bear, Sandworm Team, OceanLotus, APT39, APT35, APT34, APT33, APT41 etc.

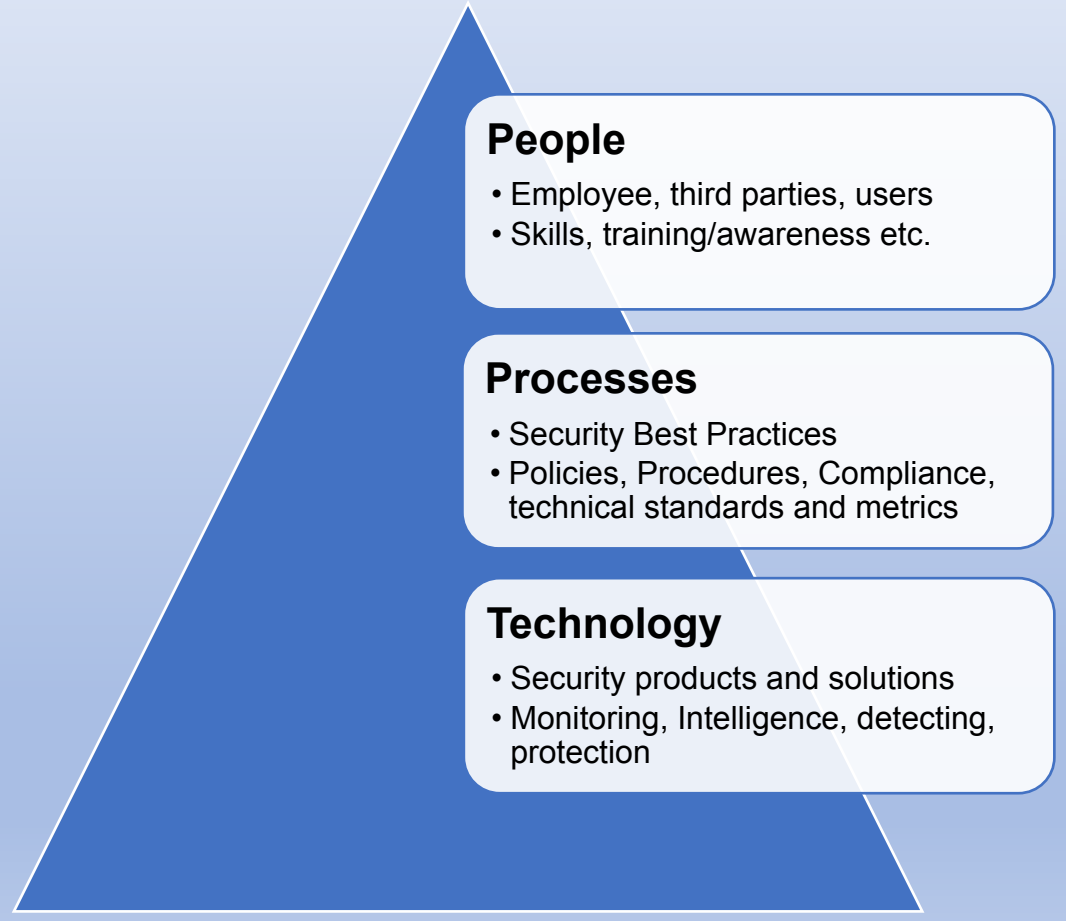
Trend in Anti-Malware Products



Malware author easily bypass Antivirus by altering the signature of their malicious codes	Known* Known to vendors, Updated to the agent/sensors	Focus on detection, little or no prevention	EDR, NTA, Wider visibility

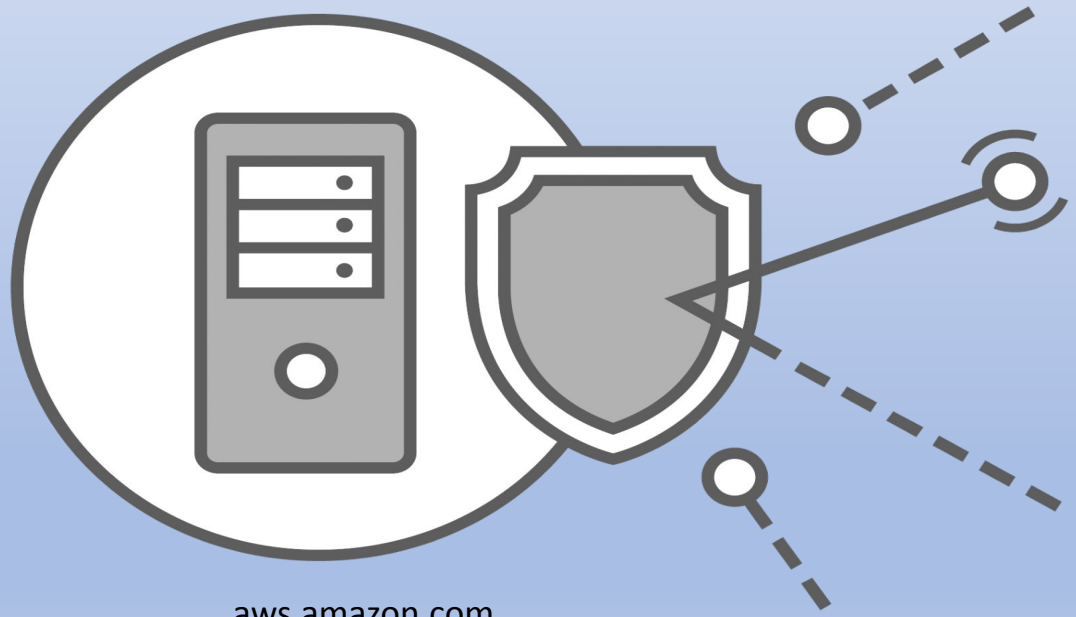
Endpoint Security Overview

3 PILLAR OF CYBER ATTACK & DEFENSE



CHECKBOX FOR ENDPOINT SECURITY SOLUTION

- *Products and solutions to protect systems and data*



aws.amazon.com

Deployment/Asset Coverage

Expectations

- Compatibility with existing tools/controls e.g AV, agents
- Ease of deployment e.g large environment, diverse OS and architectures, environment(cloud/ on premise)
- Installation requirement should not be too resource intensive
- Offline protection for agent-based

Situations

- Complexity in deployment process.
- Failure of solution to integrate with existing controls: no aggregated threat view
- Analyst navigates several management console to investigate suspicious behaviours
- Adversaries target workloads in the cloud

Use Case Implementation

Expectations

- Need to localize policy, update watchlist
- Capable/Flexible of assigning reputations: blacklist and whitelist
- Interactive API design(excellent documentation, support)

Situations

- Organization face different threats
- Variation in Client's Architecture, Infrastructural Setup
- Rigid solution: unable to meetup with customizations required by blue teams

Security Activities on System Resources

Expectations

- Security activities of EDR should not be resource intensive
- Lightweight agents/sensor

Situations

- Periodic scanning of enormous event artifacts by endpoint security solutions and analyst queries
- Devices are slow/hang; denial of service due to excessive system resource utilisation
- End-users often forced to disable security solution

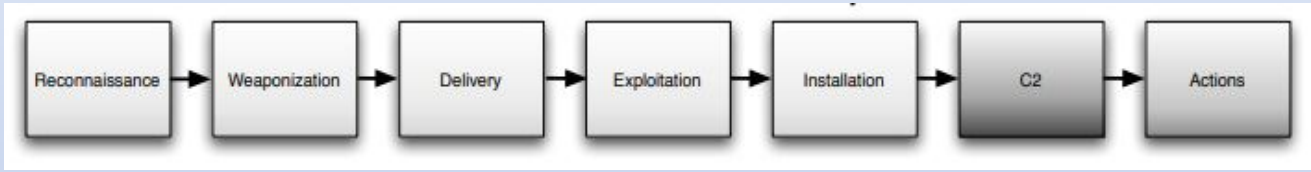
Useful Frameworks/Knowledge Base

Challenges:

- Questions, justification for each investigations/conclusion : why, how, … ?
- Emphasis on attack stages instead of the in depth overview of threats

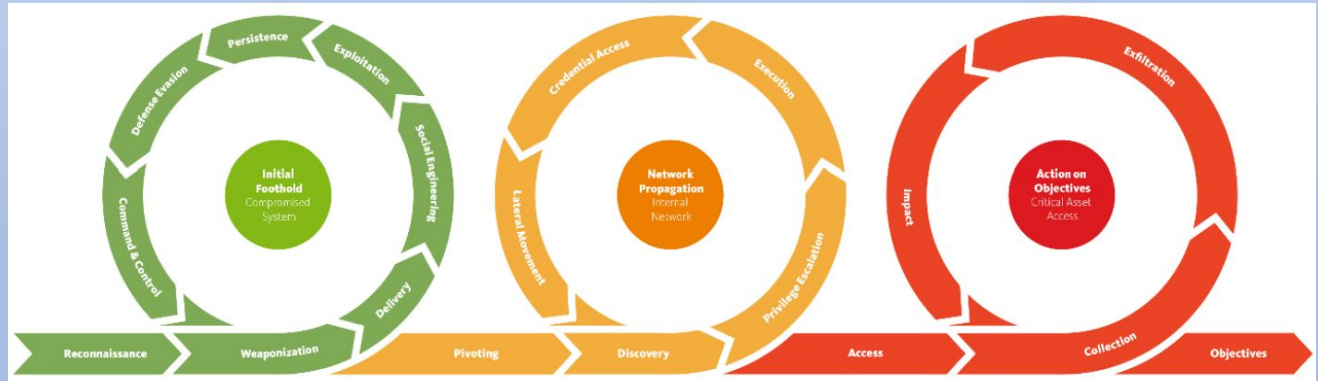
Expectations

- Must be simple, interpretable model, plugins
- Knowledge bases optimized for reference



www.lockheedmartin.com

https://attack.mitre.org/



The Unified Kill Chain

Integrated Threat Intelligence

Expectations

- Combination of threat intelligence, inbuilt correlation rule enables an optimized and real time detections
- Facilitates automated response actions
- Scan endpoint traffic for IOCs of known threats.

Situations

- Numerous malware released every 24 hrs, globally not in sync into the endpoint solution
- Vendors taking long to release new signature
- False negatives/positives (accuracy, fidelity)

Automation Capability

Expectations

- Scheduled agent/updates push, scans e.g off-peak period; spool/send reports
- Auto prevention of malwares, scripts, exploits, macros; remediation actions. (consolidated playbooks)

Situations

- Analysts complained of alerts fatigue -overwhelming low level activities
- End-user often hesitate to roll updates
- Diverse data with unique properties; hence require separate interpretations (user, host, file/documents

Consolidated Process Visualization

Expectations

- Contextual view, quick holistic view

…IOCs: extent/duration, attack stage/path/vector, breach status, C2, data accessed/Exfiltration etc.

- Process workflows from initial foothold to data harvesting, showing attack paths
- Ease of Navigation
- Relationship between correlated events

Situations

- Enormous notifications;

  "short investigation : resolution" timeline

- Security incidents are aggregated from series of smaller events, not a single events

Log Retention Policy

Expectations

- Durable storage of low-level event artifacts e.g >= 1 years.
- Storage can be scalable based on subscription plan, instead of being the default.
- Logs should be easy to query/reference on need basis

Situations

- Logs of prolong attacks are often purged before investigation are completed.
- Threat actors lurks in the environment for months(years) before the actual attacks (the ‘P’ in APT group attacks)

Enhanced Threat Hunting

Expectations

- Access to large scale, unfiltered data lake
- Easy to use query syntax
- Excellent documentation, forums

Situations

- Evasive threats in the environment
- Data is rigidly structured by inbuilt analytics
- Query syntax are either too complex or not robust enough

Visibility Into Endpoints' Health

Expectations

- Insight into system resources for statistics related to memory, compute, storage
- Digital fingerprinting of properties like device type, battery details, user's informations
- Discovery of outdated programs, enhanced virtual patching, advisory reports

Situations

- Incomplete visibility into the health status of sensors, devices, associated files

Advanced Threat Detections

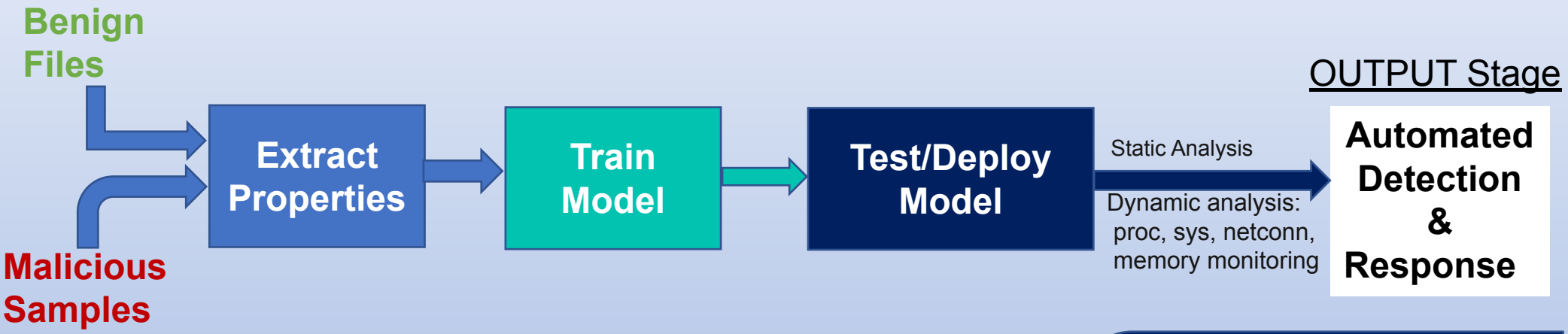
Expectations

- Early detection, accurate and precise classification engines i.e bad, suspicious, benign, failed or successful attempts
- Effective priority/severity/ or allocation of threat score
- Provision for analyst input: open, closed, resolved

Situations

- Inaccurate detections
- Large backlogged alarms heavily requires analyst validation

Integrated ML



INPUT Stage:
Data from problematic software, normal programs from forums, threat feeds etc.

OUTPUT Stage

Data Properties

Strings, imports/Exports, Opcodes, section entropy, code entropy, auto method call, callByNames, AutoExecMethod, XOR operator etc.

Machine Learning Model

Supervised learning(e.g. logistic regression, back propagation neural neural networks, using random forests, decision trees etc.), unsupervised learning(e.g. Apriori algorithm, K-means clustering), Semi-supervised learning, reinforcement learning(e.g. Q-learning algorithm, temporal difference learning). Regression algorithm(e.g. ordinary least squares, logistic regression, stepwise regression, multivariate adaptive regression splines, locally estimated scatterplot smoothing, etc.) an instance-based method (e.g. K-nearest neighbor, learning vector quantization, self-organising map, etc.), regularisation method(e.g. ridge regression, least absolute shrinkage and selection operator, elastic net, etc.), decision tree learning method(e.g. classification and regression tree, iterative dichotomiser 3, C4.5, chi-squared automatic interaction detection, decision stump, random forest, gradient boosting machines etc.), a Bayesian method (e.g. naive Bayes, averaged one-dependence estimators, Bayesian belief network, etc.), kernel method(e.g. support vector machine, radial basis function, linear discriminate analysis etc.), a clustering method(e.g. K-means clustering, expectation maximisation, etc.), associated rule learning algorithm(e.g. apriori algorithm, Eclat algorithm etc.), artificial neural network model(e.g. perception method, back propagation method, Hopfield network method, self organising map method, learning vector quantization method etc.), deep learning algorithm (e.g. restricted Boltzmann machine, deep belief network method, convolution network method, a stacked auto-encoder method etc.), a dimensionality reduction method(e.g. principal component analysis, partial lest squares regression, Sammon mapping, multidimensional scaling, projection pursuit etc.), ensemble method(e.g. boosting, bootstrapped aggregation, AdaBoost, stacked generalization, gradient boosting machine method, random forest method etc.). Others probabilistic, heuristic or deterministic module etc.

SOME MODEL USED IN EDR FROM YEAR 2000

SVM, RSVM, Threshold Random Walk(TRW), glyph-based visualisation, graph-based representation, dendric cell algorithm(DCA), Adaptive Neuro Fuzzy Inference System(ANFIS), Rate limiting(RL), maximum-Entropy(ME), Linear regression, Deep learning, multi-path exploration, MLP, KNN, Deep Learning, TW SVM, TW Logistic Regression, Cumulative Sum, Logistic Regression, Hierarchy clustering approach, Ant Colony based Graph Theory(ACGT), Heuristic approach, Markov chain algorithm, Clustering, Sequential Minimal Optimisation(SMO), Naive Bayes, Decision Tree(J48, etc.) Logistic Model Tree(LMT), Random Tree, Random Forest, Self organizing feature Map(SOFM), Malware Operational Plot Review(MOPR), Bayesian Network, Logit Boost, Bagging, AdaBoost Gradient Boosting, Ensemble, Hoeffding Tree, Principle Component Analysis(PCA), Modified Apriori, Ensemble Recurrent Neural Network, akNN Knowledge-assisted visual analytics(KAVAS), IDS & forensics tool

Response And Recovery

Expectations

- Other response actions: uniquely terminate malicious process, and or subprocesses
- IR/Forensic Capability
  - support live mode via remote connection to execute commands, launch tools etc.
  - collection of running process, established connection, memory dumps, fetch system and application logs
- Complete roll back to last clean snapshot: revert files/config modified, terminate active sessions etc.

Situations

- Security hardly goes beyond detection phase(... of what benefit is detection alone to ransomware, DOS attacks ?).
- Response action are mostly asset quarantine and malware removal; no recovery !

OTHERS

Expectations

- Offline protection of endpoints
- Ease of auditing user activities on the console
- Flexible role-based access on the management console
- Ease of spooling reports: executive view, technical, etc.

CHECKBOX FOR PEOPLE AND PROCESSES

- *Teams, best practices or established mechanism to achieve cybersecurity program objectives*

www.wgu.edu

Process

- Delayed management approval
- Refusal/reluctance to give required privilege for troubleshooting, deployment
- Sales engineering team often oversells/overshoot product capabilities

- Policies(e.g BYOD), procedures, compliance.
- IR & BCP Plan, SLA & performance metrics,
- Procedures for handling vendor/third parties.
- Drills and audits

Blueteams/End-users

- Maximise the capability of Endpoint solution

  NewYorkTimes breached vs Symantec 2013 (www.theregister.co.uk/2013/02/01/symantec_responds_nyt_apt/)

- Map configuration parameter impacting system resources; upgrade hardware, optimal testing
- Cross platform correlation during incidence investigations
- Routine user training and security awareness
- Enforce/Imbibe security best practices e.g EDR agents are some uninstalled, bypassed, for convenience

OUT OF SCOPE

- Cost implication to implement each of these checkboxes
- Review of agent/agentless deployment, centralised and decentralised management
- Recommendation on perfect machine learning model for anti-malware detection engines or suitable vendors

THANK YOU

email: adewolenath@yahoo.com
(Questions)