REDCORE

RDT&E Enterprise Defensive Cyber Operations Response Element

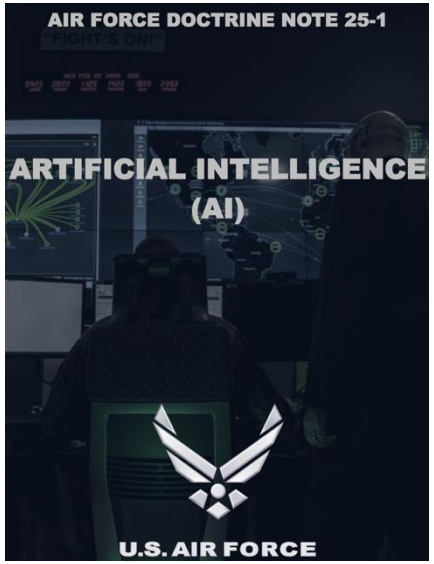
Operationalizing AI for Cybersecurity: Lessons Learned from Operation Unconquered Artemis

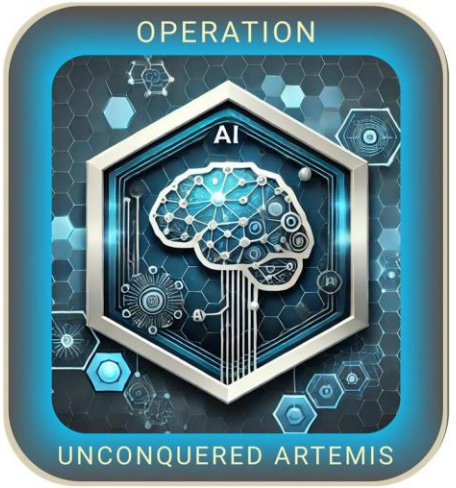
Agenda

- **Introduction**
  - RDT&E Defensive Cyber Operations Response Element (REDCORE)
  - Operation Unconquered Artemis (OUA)
- **Edwards AFB Cyberthreat Landscape**
- **Countering the Threat**
- **Network-based AI Models**
  - Artemis Aurora Delta – Identify Domain Generation Algorithms (DGAs)
  - Artemis Rose Bravo – DNS Exfiltration
- **Host-based Model**
  - Artemis Core Alpha – Detecting Server Log Anomalies
- **Closing Remarks**
- **Questions**

REDCORE - OPERATION UNCONQUERED ARTEMIS (OUA)

- **REDCORE Transformation**
  - Mission Defense Team → RDT&E Defensive Cyber Operations Response Element
- **Core Mission**
  - Execute and refine defensive countermeasures
  - Conduct targeted mapping & reconnaissance
- **Operation Unconquered Artemis (OUA)**
  - **Objective:** expand cyber monitoring through AI
  - **Framework:** aligned with Air Force Doctrine 25-1 Human-Machine Teaming (HMT)
  - **Outcome:** enable faster, superior operational decisions for Airmen





Cyberthreat Landscape - Edwards AFB

Weekly DNS Records To Be Analyzed: **1,401,610,723**

14 SOC Analysts

NIPRNET

KTR Networks

Mission Partners

DREN

Test Planning and Reporting

Distributed Test Ops

Ground Systems

Platform

Post-Test Data

Test Sq

SAP Systems

Control Room

Control Room

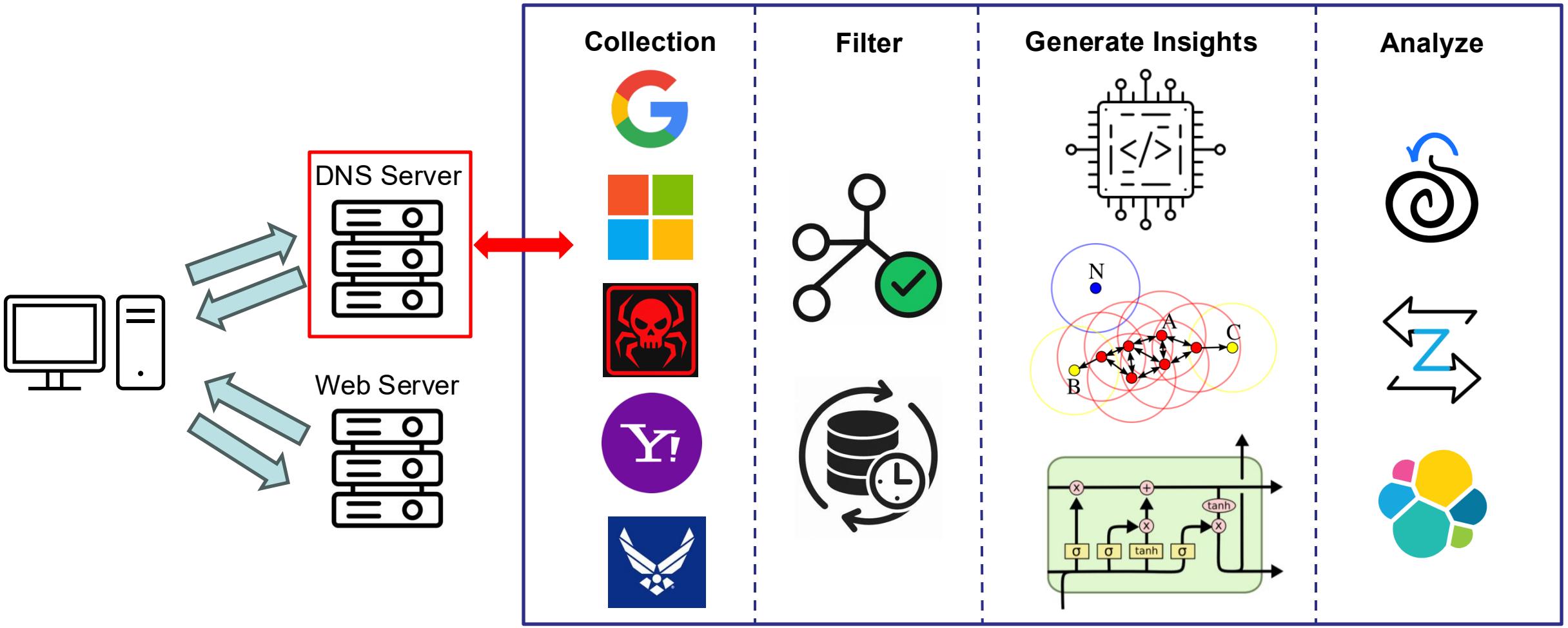
Control Room

Range Network

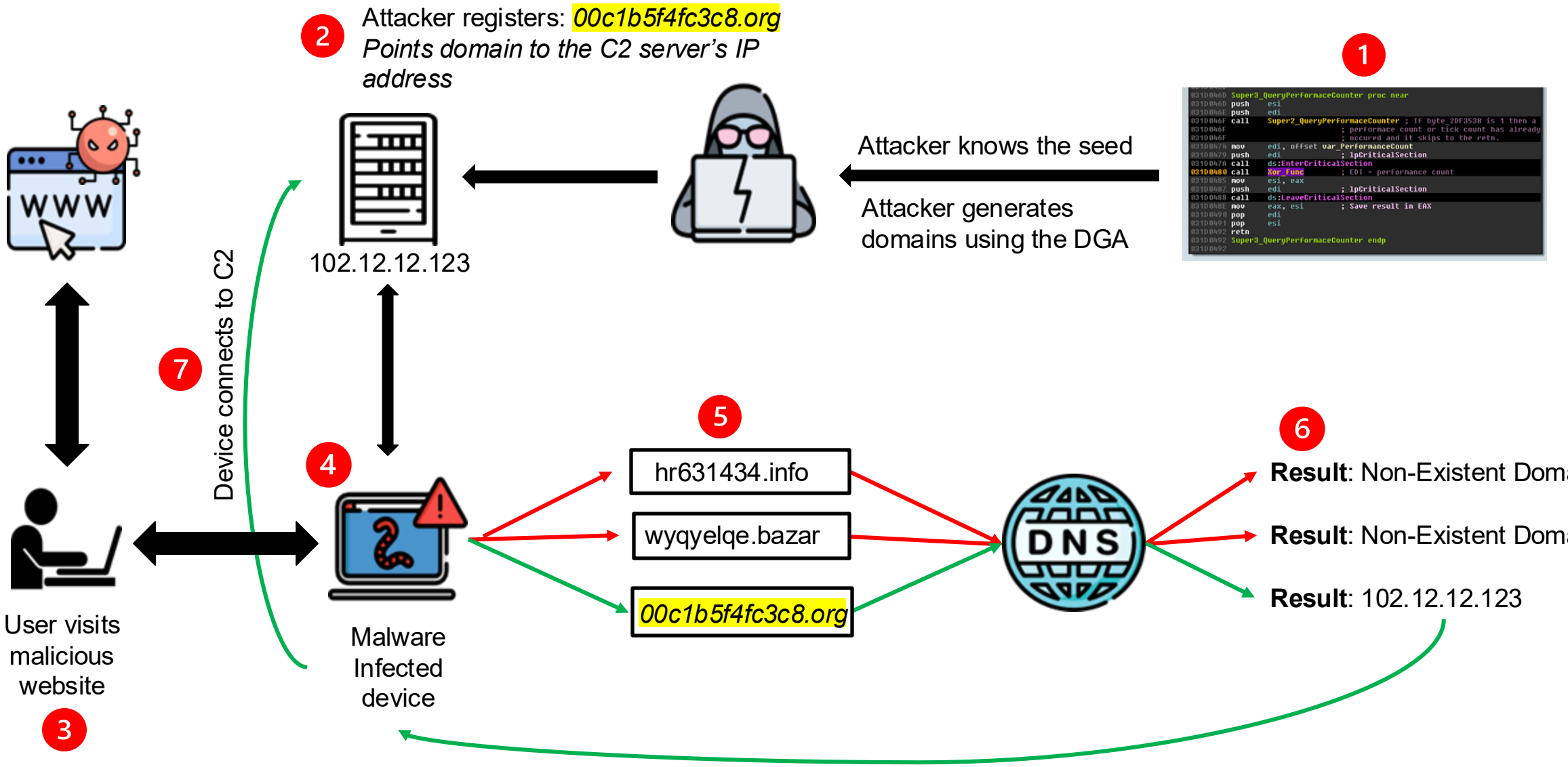
External Ranges

Countering the Threat

The **Domain Name System (DNS)** translates human-friendly domain names (*google.com*) into machine-readable IP addresses (*8.8.8.8*)

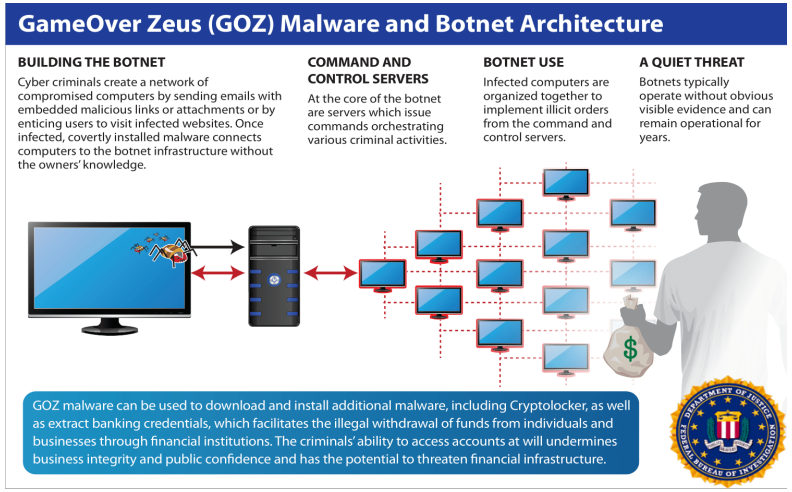


Artemis Aurora Delta – Domain Generation Algorithms (DGAs)



Artemis Aurora Delta - DGA Types

Arithmetic-based DGAs



Definition: Create domain names using predictable numeric formulas that map to characters or positions in a predefined list.

Example: isx5gq2h27k77pc7ph17rsudo.com

Dictionary-based DGAs

Definition: Dictionary-based DGAs form domains by selecting and concatenating words from one or more wordlists.

Example: degreemagnitude.com

Artemis Aurora Delta – Domain Generation Algorithms (DGAs)

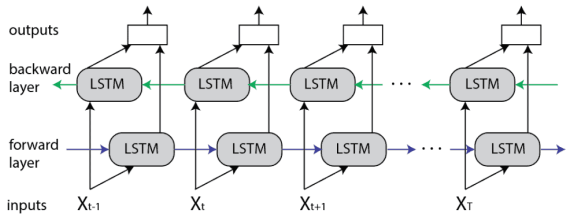
Collection

DGA ARCHIVE

Model Architecture

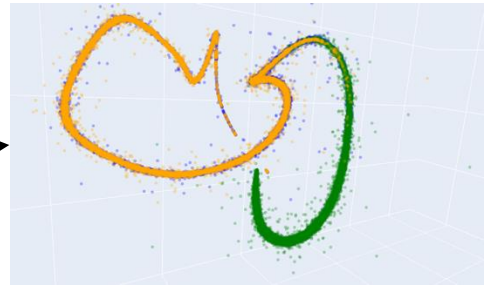
1. fastText

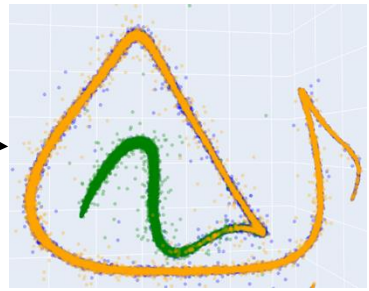
Semantic Embedding Layer

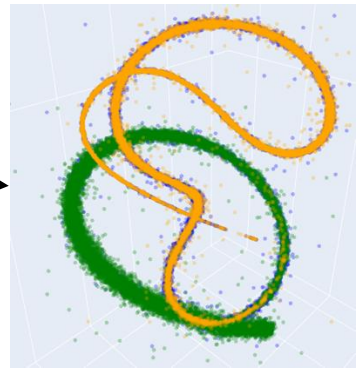
2. 

BiLSTM

Analyze





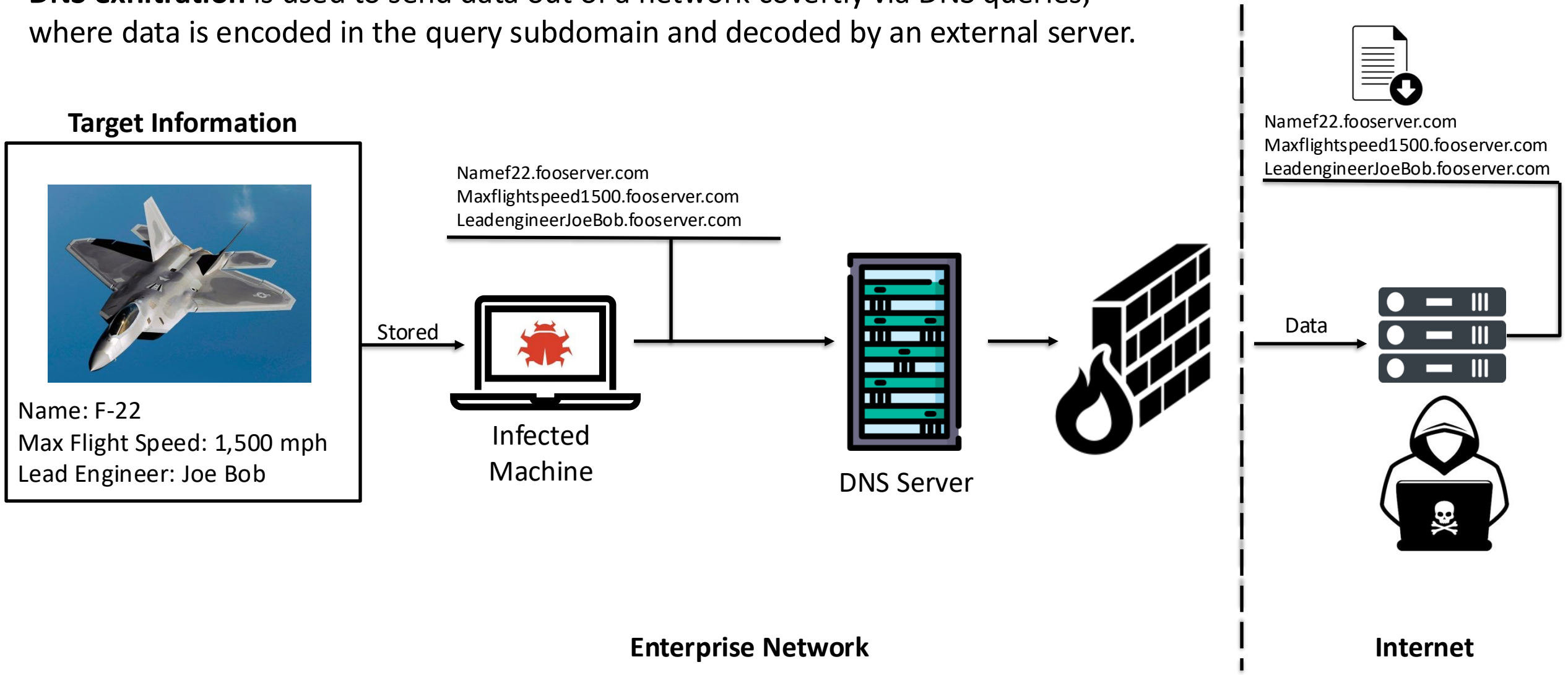


Legend		
A	Emotet	
A	Qadars	
A	Conficker	
B	Tranco	
D	Matsnu	
D	Suppobox	

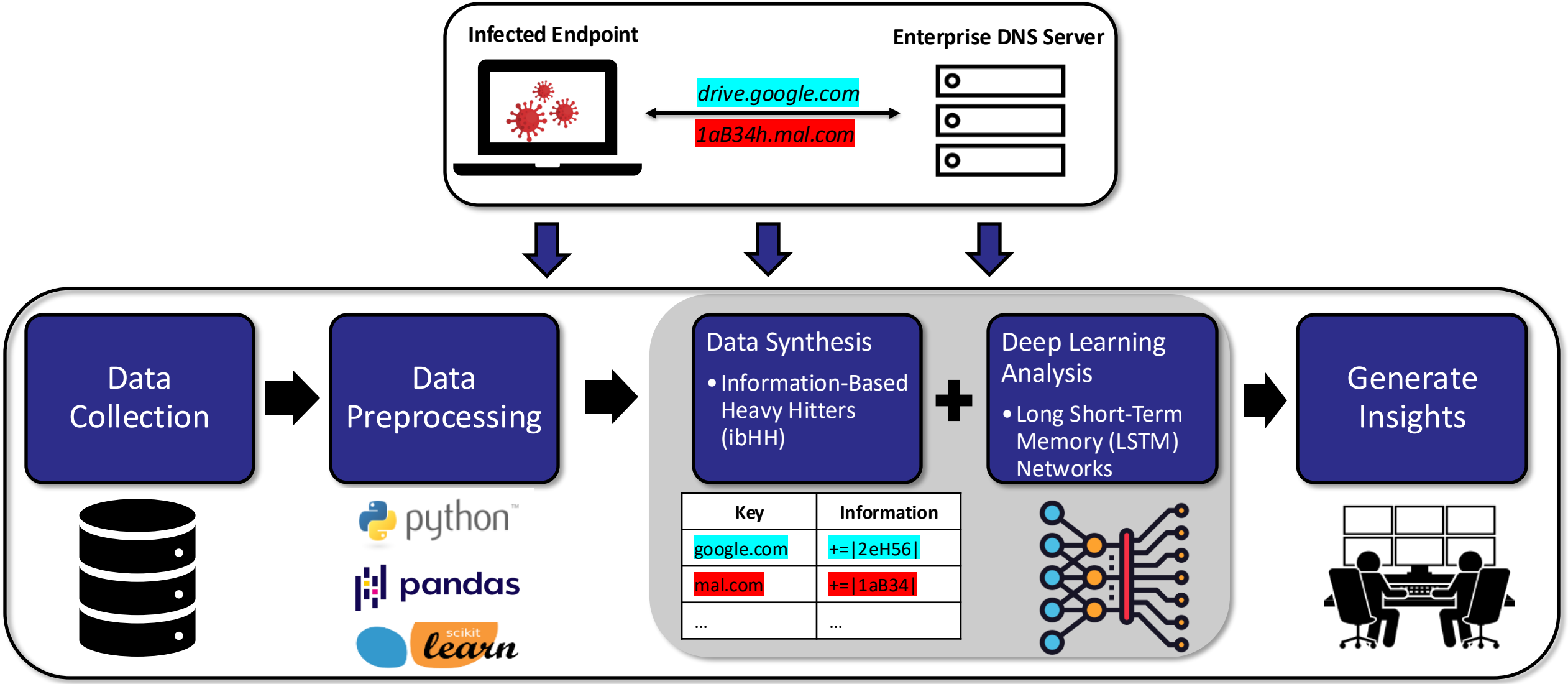
A - Arithmetic-based DGAs
B - Benign domain names
D - Dictionary-based DGAs

Artemis Rose Bravo – DNS Exfiltration

DNS exfiltration is used to send data out of a network covertly via DNS queries, where data is encoded in the query subdomain and decoded by an external server.



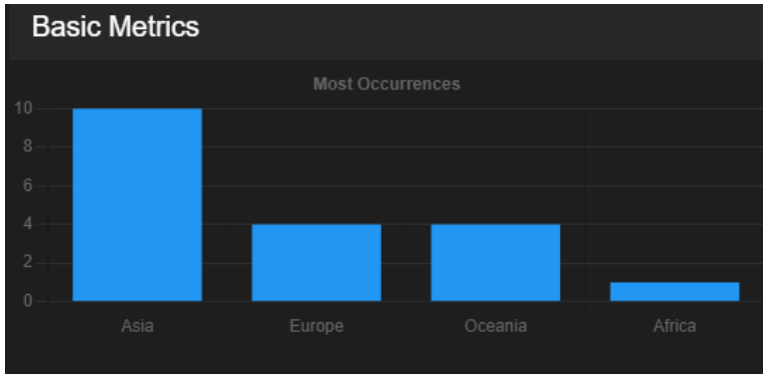
Artemis Rose Bravo – DNS Exfiltration

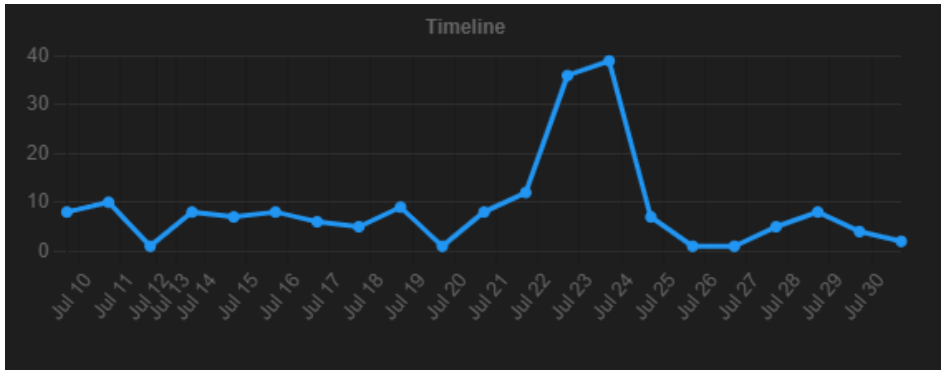


Case Study: Artemis Rose Bravo (Part 1)

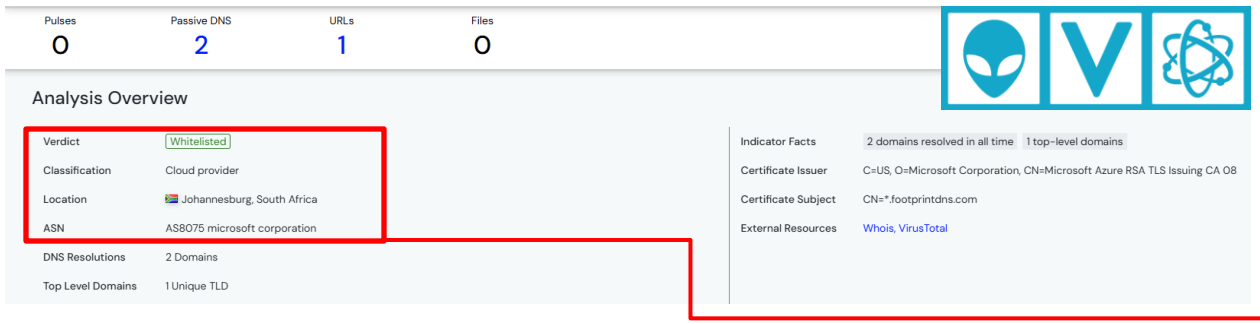
Network traffic is flagged as DNS exfiltration

- ca9583bf91bdf0ca7a366b8c15766c6d.azr.footprintdns.com
- 9893e3410df2071ed7900969e66c6233.nrb.footprintdns.com
- ccb57371ac4a124517c52f3fecd6fad8.azr.footprintdns.com





High-frequency traffic to foreign IP addresses triggered further investigation



Open-source intelligence confirmed IP was based in South Africa. It was Microsoft-owned and whitelisted

Case Study: Artemis Rose Bravo (Part 2)

Jan 07, 2019

The domain nrb.footprintdns.com is owned by Microsoft and represents servers in Microsoft datacenters. It is used for telemetry purposes that comply with Microsoft privacy commitments that you can read about at: https://products.office.com/en-us/business/office-365-trust-center-privacy. Data sent to this domain is used to identify network connectivity and performance issues and to support improvements to the service. We have plans to rename it to be more descriptive, and to publish it at the Office 365 IP Address and URL publishing site at http://aka.ms/o365ip. If you have any problems using

Research uncovered a 2019 Microsoft forum post explaining legitimate purpose:

- Traffic used for "network connectivity and performance improvements"

2024 forum post confirm ongoing user reports of this Windows Search behavior

May 21, 2024

It's been 5 years and there is nothing about this domain on official microsoft documentation websites. Better yet, I've started seeing this coming not from office, but from Windows Search. Here's a screenshot from ESET Protect report from one of our computers.

More details

Hash	2FA25AE5101F3D2EE02AA5A96724C33E83BE403A
Uniform Resource Identifier (URI)	https://6d224a8d6cc7d632d8cdfc5f34d705ae.azr.footprintdns.com
Process name	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe

Key Takeaway: Artemis Rose Bravo enabled analysts to efficiently investigate potential DNS exfiltration while dealing with 1.4 billion DNS queries per week, further establishing network behavior baselines that would otherwise be unmanageable.

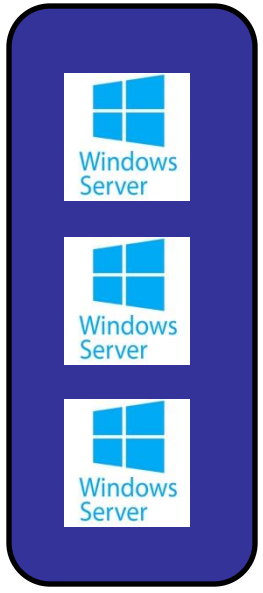
Expanding the Detection Surface

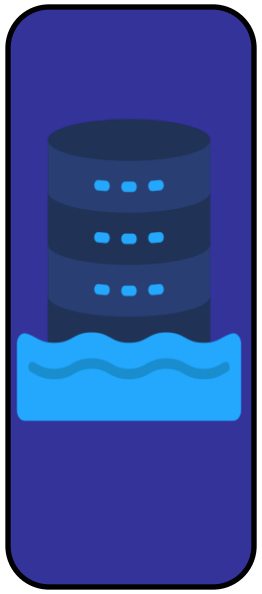
Shifting the Lens:

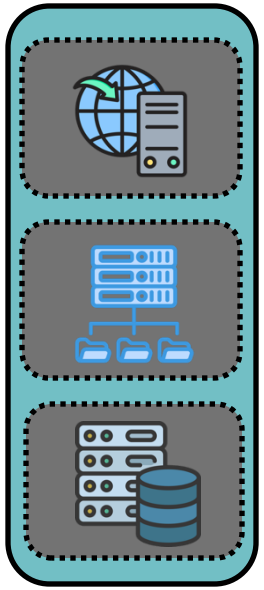
Moving from monitoring network traffic to analyzing behavior using AI at the endpoint level

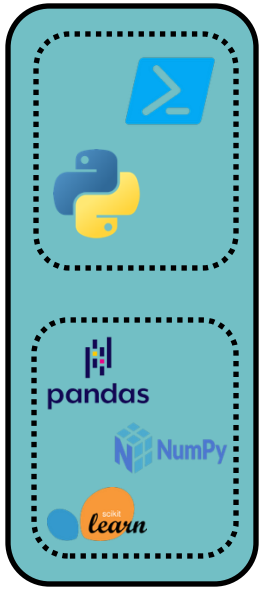
Artemis Core Alpha – Detecting Server Log Anomalies

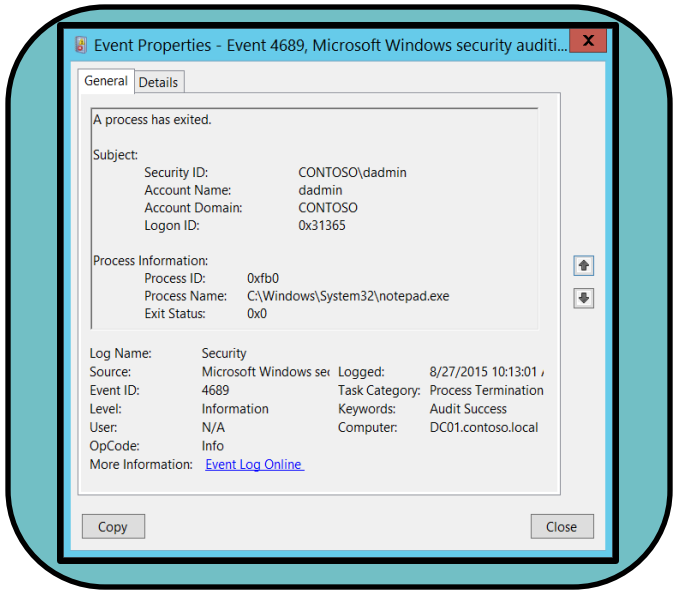
Collection | Storage | Segmentation | Normalization | Event ID Selection | Evaluate | Alert











Data Collection | Data Preprocessing | Generate Insights

Artemis Core Alpha – Detecting Server Log Anomalies

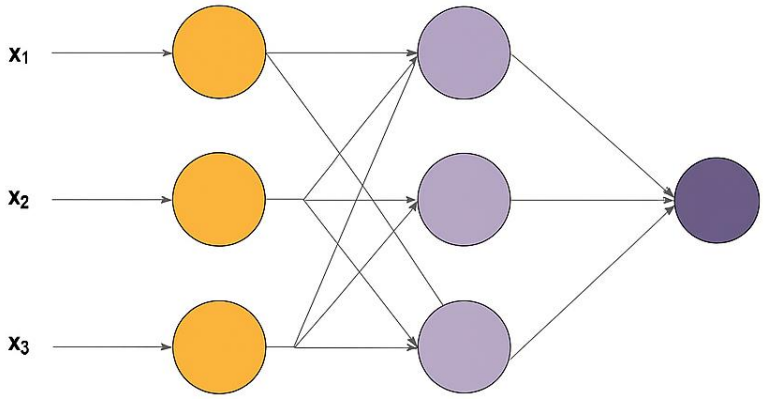
Neural Network

$$\hat{Y} = \sigma(wX + b)$$

Goal: design a network with the goal of classifying or fitting input data (x) to an expected output (y)

Problem:

- Do not have labeled data
- Hard to determine what 'normal' looks like



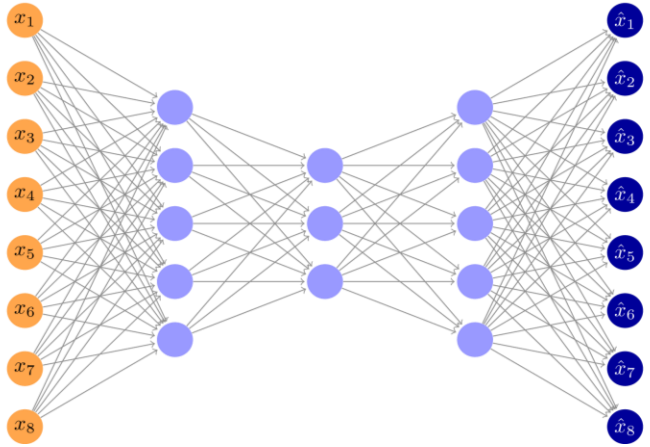
Autoencoder

$$\hat{\mathbf{x}} = \sigma_{\text{dec}}\left(W_{\text{dec}}\,\sigma_{\text{enc}}(W_{\text{enc}}\mathbf{x} + \mathbf{b}_{\text{enc}}) + \mathbf{b}_{\text{dec}}\right)$$

Goal: accept data as an input, perform some type of transformation, and produce an output that matches the input

Benefit:

- Does not require labeled data
- Help us understand what 'normal' looks like



Research Testbed

Network Traffic	Title	Source	OS	Collection Period	Description
Benign	Unified Host and Network Dataset	Los Alamos NATIONAL LABORATORY	Windows, Linux	90 days	Network and computer host events collected from Los Alamos National Lab
Malicious	EVTX-Attack-Samples	GitHub	Windows	-	Windows event samples associated with specific tactics, techniques, and procedures represented in MITRE ATT&CK

Tactic	ID	Method
Command and Control (C2)	TA0011	RDP Tunnel
Lateral Movement	TA0008	Mimikatz malware
Privilege Escalation	TA0004	Token Manipulation

Model Training

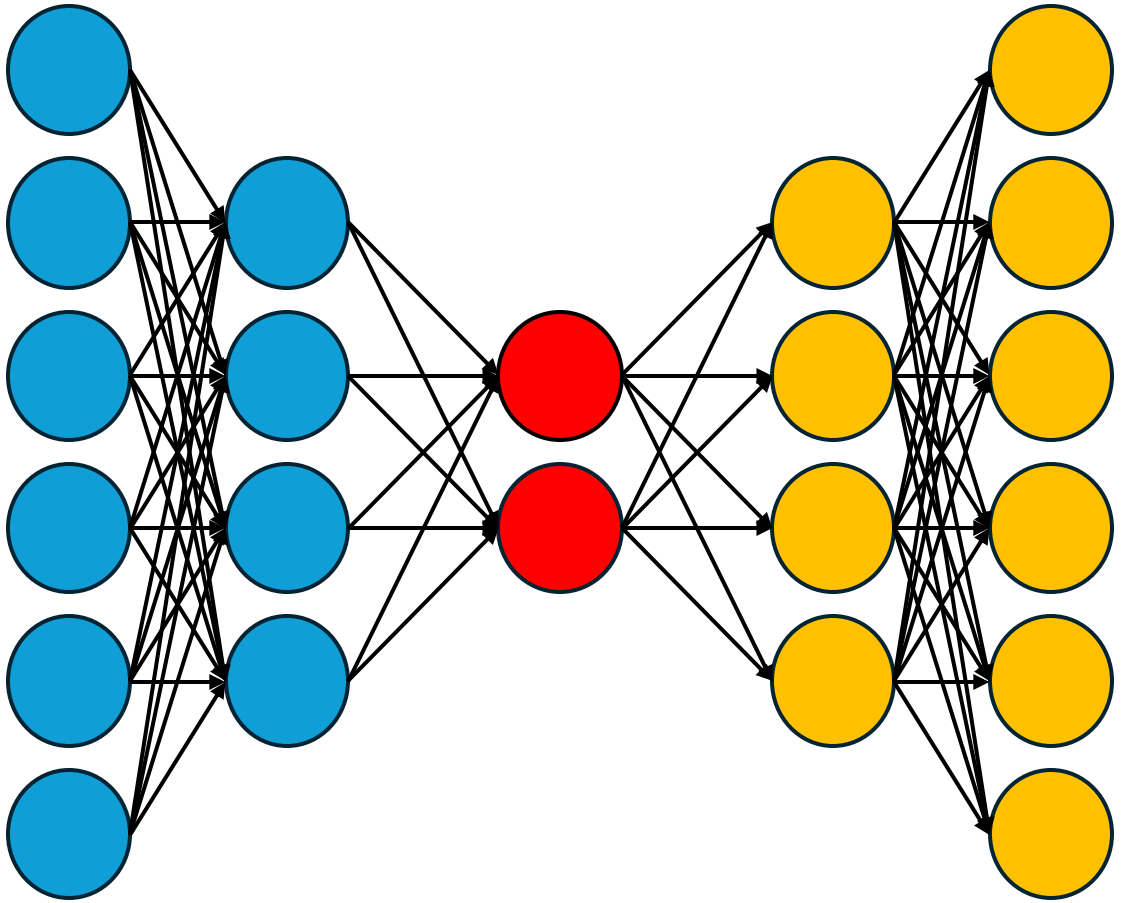
Benign Network Traffic

Inputs

Domain001 svchost dllhost.exe
Domain001 svchost taskeng.exe
Domain001 taskeng Proc857443.exe
Domain002 csrss conhost.exe
Domain001 Proc443607 searchprotocolh

nt authority taskeng Proc789201.exe
nt authority svchost Proc639466.exe
nt authority Proc639466 conhost.exe
nt authority svchost Proc639466.exe
nt authority Proc639466 conhost.exe

Comp241588 Proc625867 Proc461749.exe
Comp672296 svchost wmiprvse.exe
Comp068157 taskeng Proc619800.exe



Outputs

Domain001 svchost dllhost.exe
Domain001 svchost taskeng.exd
Domain001 taskeng Qroc857443.ewd
Domain002 csrss conhost.exe
Domain001 Proc443607 searchprotocolh

nt authprity taskfng Proc789211.f|i
nt authority svchpst Proc639476.fzg
nt authority Proc639467 donhpuv/i~j
nt authority svchpst Proc639476.fzg
nt authority Proc639467 donhpuv/i~

Comp725657 Proc525866 Prod46163:-_wh
Comp773343 olcgnrt vlhoqvrc-cwb
Comp535556 tbtndlh#Osoe608<..)a{\

Model Results

Benign	C2	Lateral Movement	Privilege Escalation

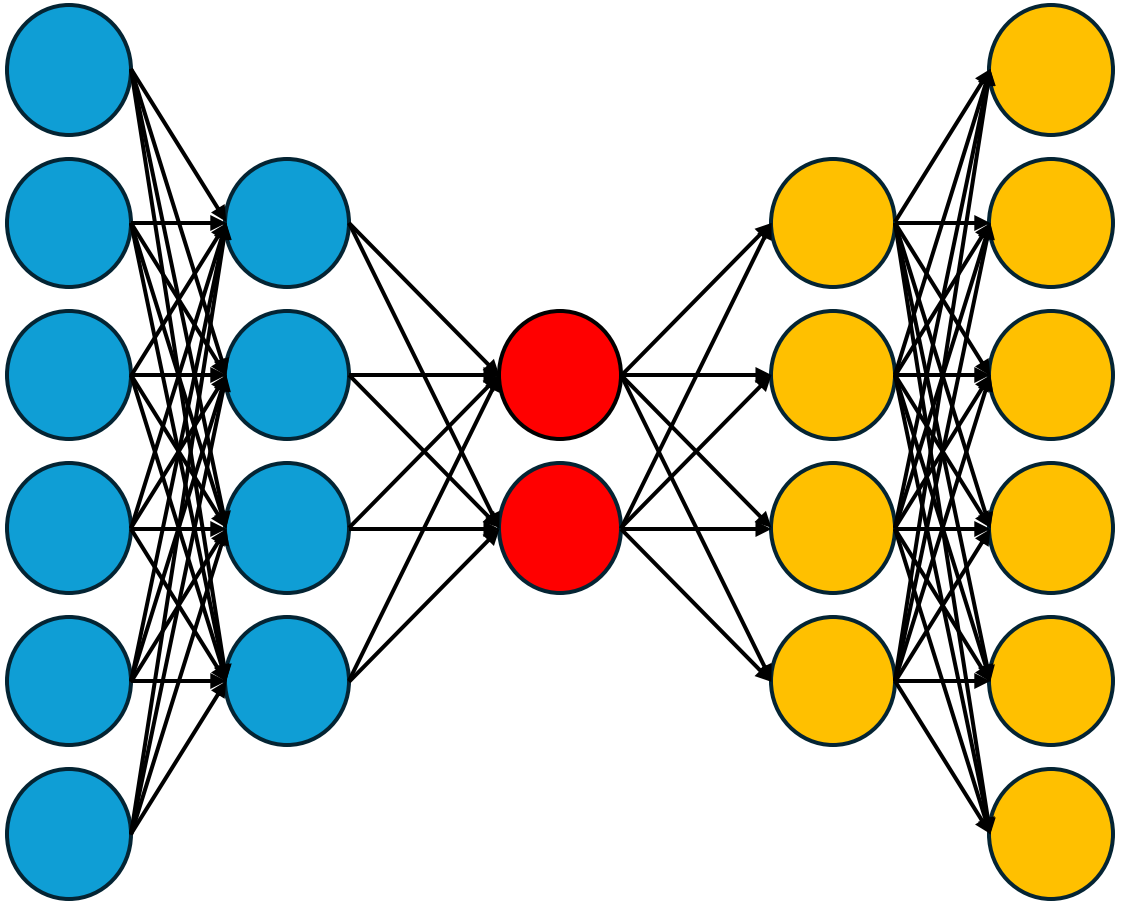
Inputs

Domain001 svchost dllhost.exe
Domain001 svchost taskeng.exe
Domain001 taskeng Proc857443.exe
Domain002 csrss conhost.exe
Domain001 Proc443607 searchprotocolh

Domain001 csrss plink.exe
Domain001 Proc443607 AtBroker.exe
Domain001 services rundlll32.exe
Domain002 services rdpclip.exe

nt authority Proc126308 WMIC.exe
Domain001 Proc247259 tasklist.exe
Domain002 csrss calc.exe
EnterpriseAppServer svchost tasklist
Comp032135 svchost WmiPrvSE.exe

nt authority Proc443607 python1.exe
Domain002 csrss wusa.exe
Domain001 svchost consent.exe
EnterpriseAppServer cmd conhost1.exe



Outputs

Domain001 svchost dllhost.exe
Domain001 svchost taskeng.exd
Domain001 taskeng Qroc857443.ewd
Domain002 csrss conhost.exe
Domain001 Proc443607 searchprotocolh

Copbhl0/0 ellVlPsJfcnBhp_
Boraim../Vqr^6928,9'Xv[eg]X^8Rvl
Bopain../pjnrh`gZ)jnv_Y_XCS@Va=
Eokajn112!terwmi]m%tkithj_'Utk

Ho`]oq56:&lvSbr/[NJHi^DYF
Gofako345#Rrkg627/19$r[jjvh`f5T|a
Gofajm457&]u]xKDU9gKB\P[
er-nhqh^\WAj_ZqqnLS4uWRW_gR+HUlh□□
Dorr2/566:!giVasmt&UpU]bl□0•|

is&attagi^vx'Srjd;=:?0@%_s□J=)'.>+
Gofajo456%cp`yNLiZcPUa@
Donain001 pudjmqt!finljpp0fwf
\r9jjrWQODKn^RVaa@A)A^ZKoW]n□À□¤□

Closing Remarks

Key Takeaways

- AI has proven extremely valuable to REDCORE by streamlining operational decisions and providing previously unavailable insights to cyber analysts

- Building production-ready classifiers involves expected challenges and iterations—learning from failures drives improvement

Collaboration Opportunity

- Interested in implementing similar AI-driven security solutions? We're happy to share our work, insights, and lessons learned

Contact Information & Questions

- **Contact Information**:
  - Payton Rudnick, Cyber Analyst, Special Missions Flight 412th CS SCPM
    - payton.rudnick@us.af.mil
  - Syria McCullough, Cyber Analyst, Special Missions Flight 412th CS SCPM
    - syria.mccullough@us.af.mil
  - Jason Schalow, Chief, Special Missions Flight 412th CS SCPM
    - jason.schalow@us.af.mil

Questions?