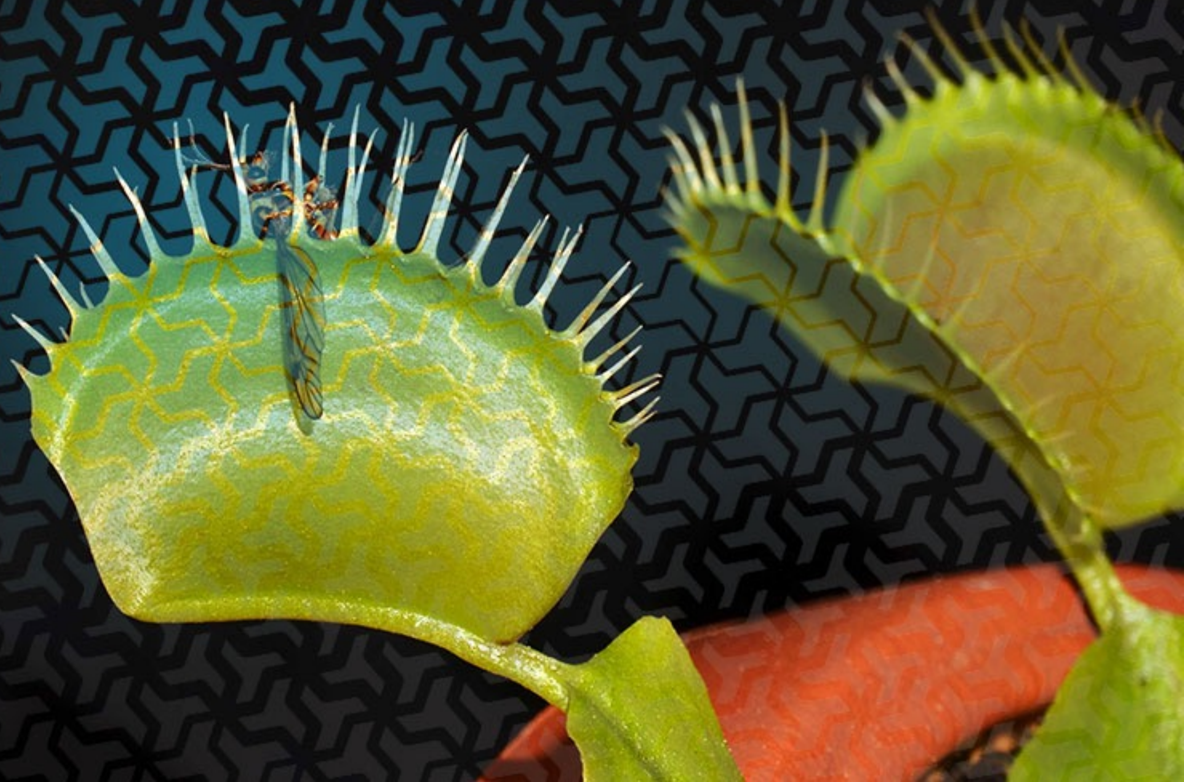
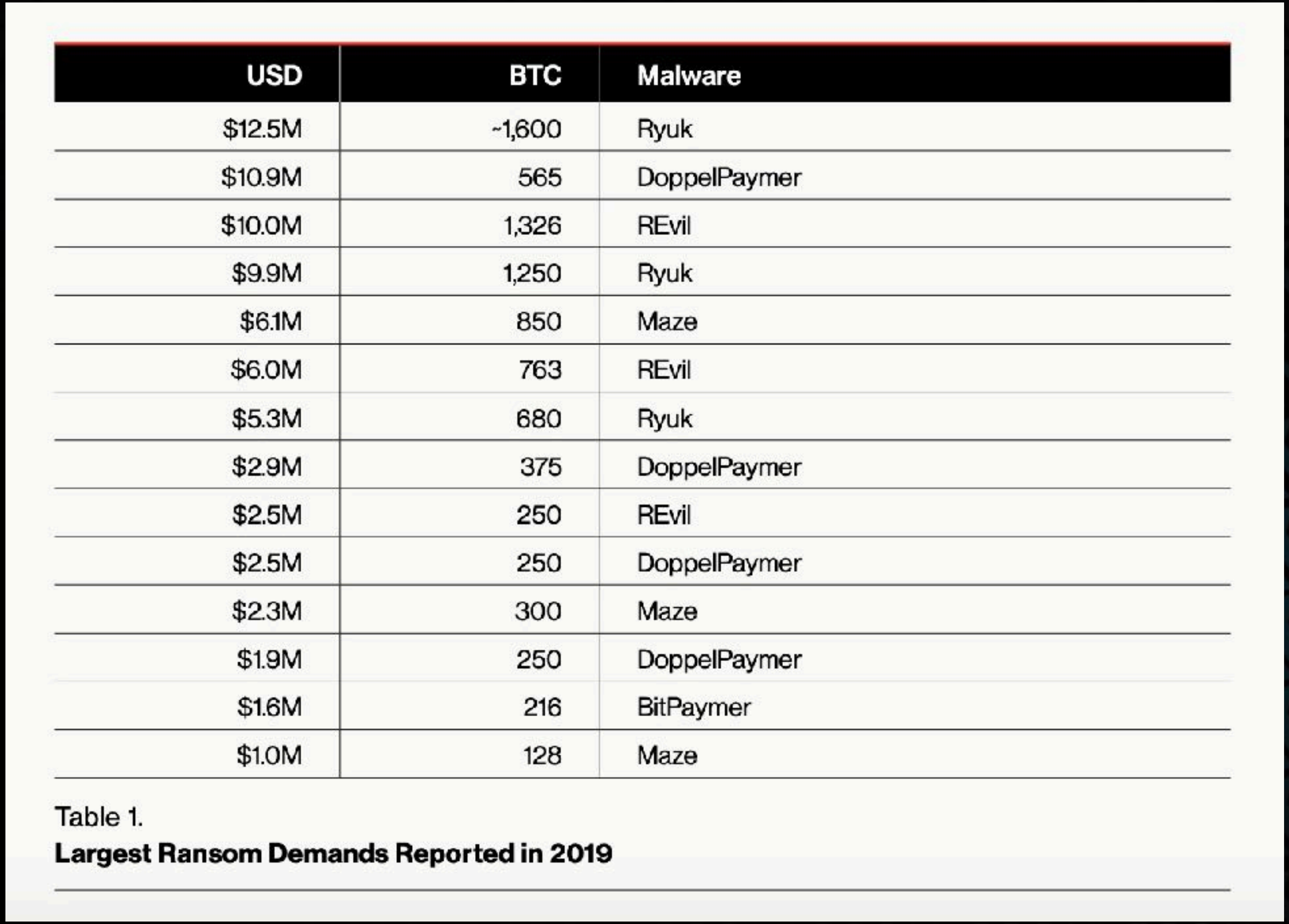
Nullcon 2020

InfoSec Deep Learning in Action

Satnam Singh, PhD
Chief Data Scientist
Acalvio Technologies



It is all about Money !!



USD	BTC	Malware
$12.5M	~1,600	Ryuk
$10.9M	565	DoppelPaymer
$10.0M	1,326	REvil
$9.9M	1,250	Ryuk
$6.1M	850	Maze
$6.0M	763	REvil
$5.3M	680	Ryuk
$2.9M	375	DoppelPaymer
$2.5M	250	REvil
$2.5M	250	DoppelPaymer
$2.3M	300	Maze
$1.9M	250	DoppelPaymer
$1.6M	216	BitPaymer
$1.0M	128	Maze

Table 1.
Largest Ransom Demands Reported in 2019

CrowdStrike Global Threat Report 2020

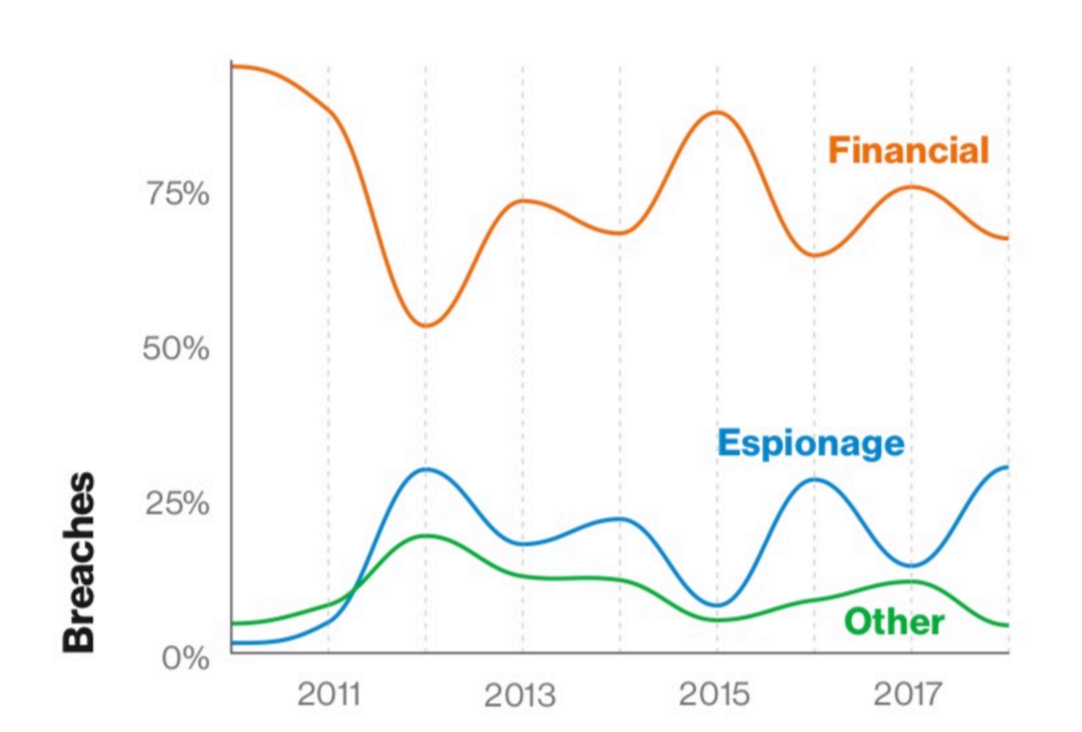
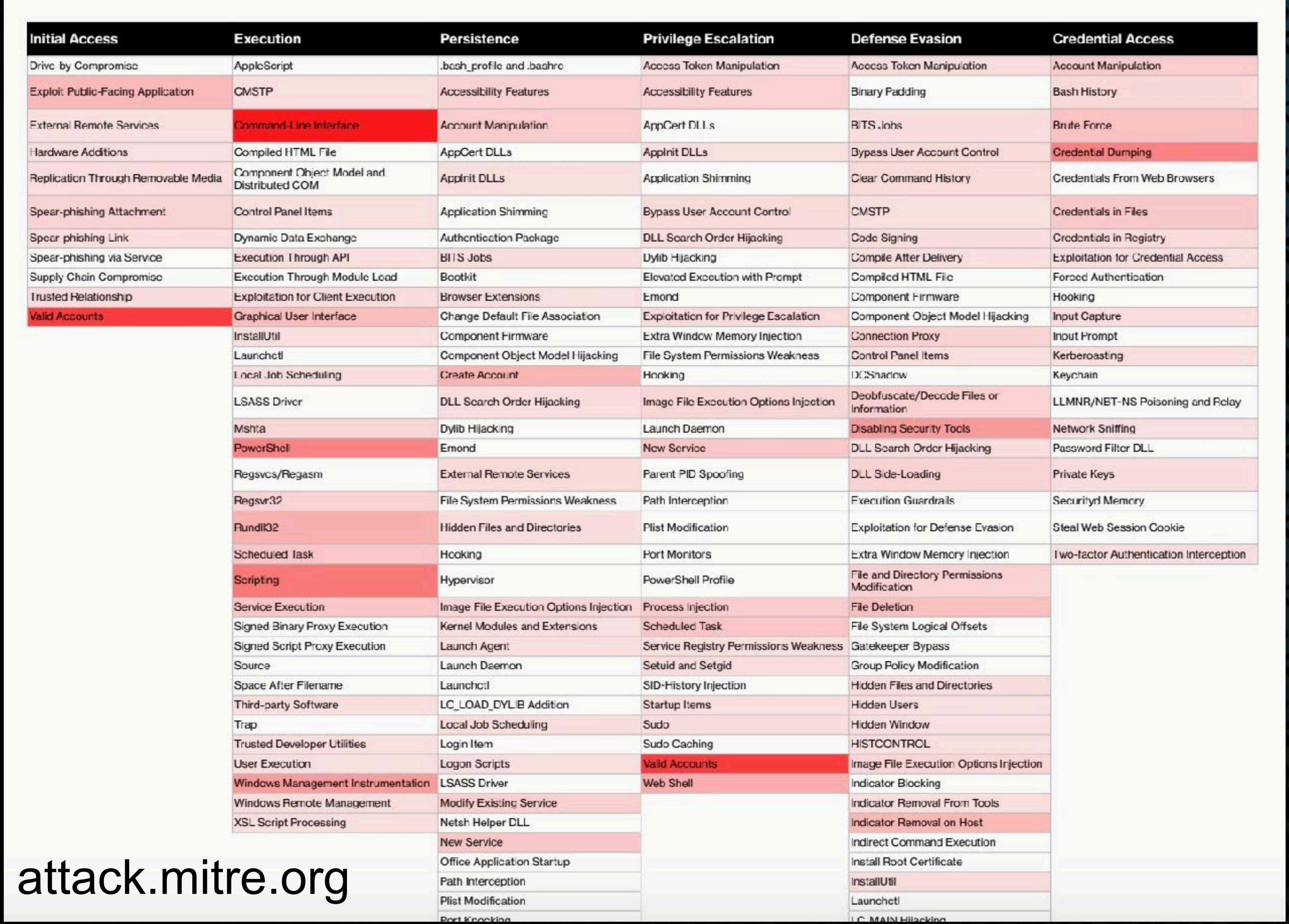


Figure 7. Threat actor motives in breaches over time

Verizon Data Breach Report - 2019

ATT&CK Heatmap by OverWatch- CrowdStrike



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials From Web Browsers
Spear-phishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files
Spear phishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry
Spear-phishing via Service	Execution Through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access
Supply Chain Compromise	Execution Through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie
	Scheduled Task	Hooking	Port Monitors	Extra Window Memory Injection	Two-factor Authentication Interception
	Scripting	Hypervisor	PowerShell Profile	File and Directory Permissions Modification	
	Service Execution	Image File Execution Options Injection	Process Injection	File Deletion	
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Scheduled Task	File System Logical Offsets	
	Signed Script Proxy Execution	Launch Agent	Service Registry Permissions Weakness	Gatekeeper Bypass	
	Source	Launch Daemon	Setuid and Setgid	Group Policy Modification	
	Space After Filename	Launchctl	SID-History Injection	Hidden Files and Directories	
	Third-party Software	LC_LOAD_DYLIB Addition	Startup Items	Hidden Users	
	Trap	Local Job Scheduling	Sudo	Hidden Window	
	Trusted Developer Utilities	Login Item	Sudo Caching	HISTCONTROL	
	User Execution	Logon Scripts	Valid Accounts	Image File Execution Options Injection	
	Windows Management Instrumentation	LSASS Driver	Web Shell	Indicator Blocking	
	Windows Remote Management	Modify Existing Service		Indicator Removal From Tools	
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host	
		New Service		Indirect Command Execution	
		Office Application Startup		Install Root Certificate	
		Path Interception		InstallUtil	
		Plist Modification		Launchctl	
		Port Knocking		LC_MAIN Hijacking	

attack.mitre.org

Frequency of Observance	
	0-5% of intrusions
	5-20%
	20-50%
	50-70%
	>70%

TTPs Used by Adversaries in 2019- CrowdStrike

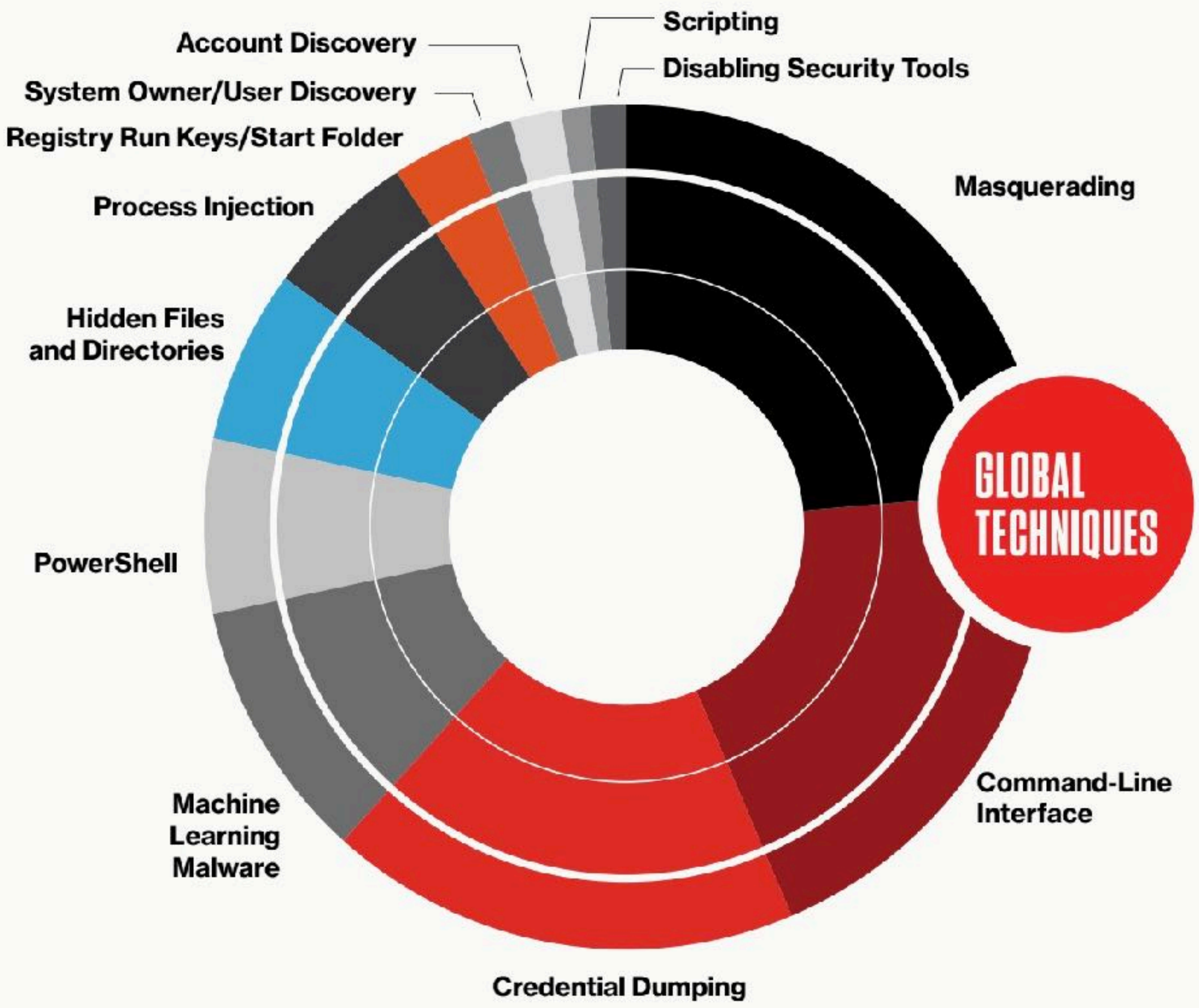
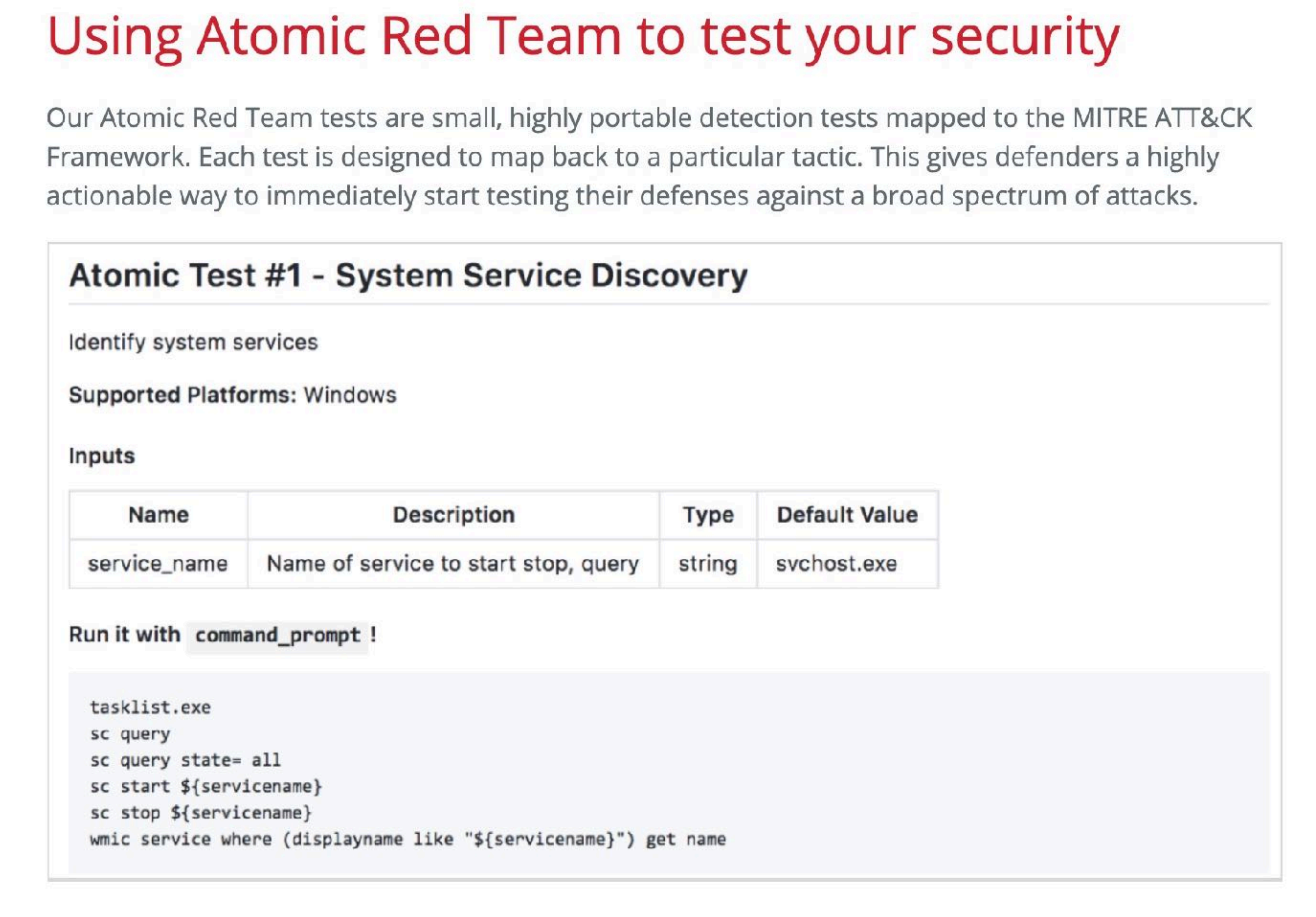


Figure 3.

TTPs Used by Attackers in 2019

atomicredteam.io



Using Atomic Red Team to test your security

Our Atomic Red Team tests are small, highly portable detection tests mapped to the MITRE ATT&CK Framework. Each test is designed to map back to a particular tactic. This gives defenders a highly actionable way to immediately start testing their defenses against a broad spectrum of attacks.

Atomic Test #1 - System Service Discovery

Identify system services

Supported Platforms: Windows

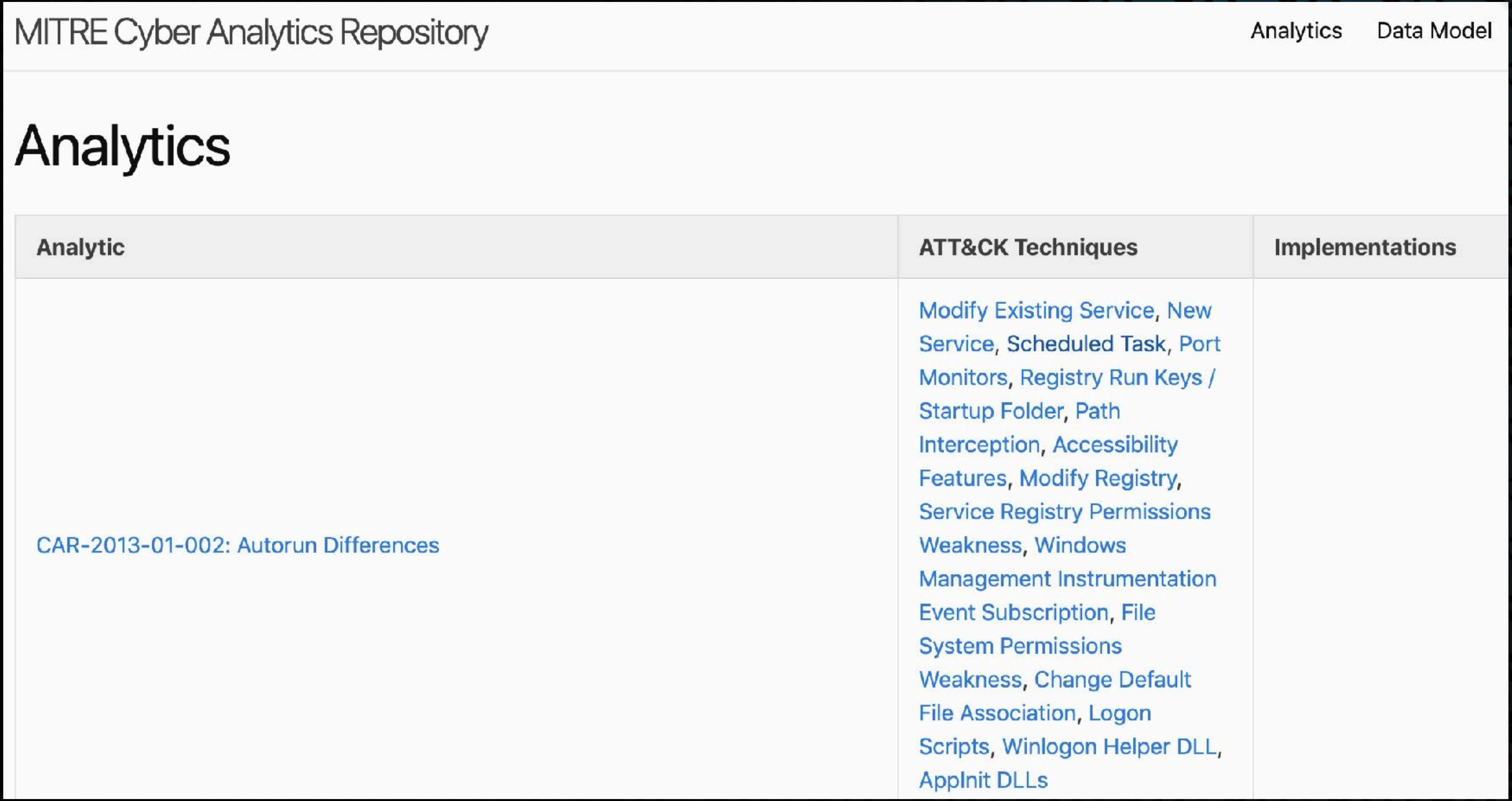
Inputs

Name	Description	Type	Default Value
service_name	Name of service to start stop, query	string	svchost.exe

Run it with `command_prompt` !

```
tasklist.exe
sc query
sc query state= all
sc start ${servicename}
sc stop ${servicename}
wmic service where (displayname like "${servicename}") get name
```

car.mitre.org

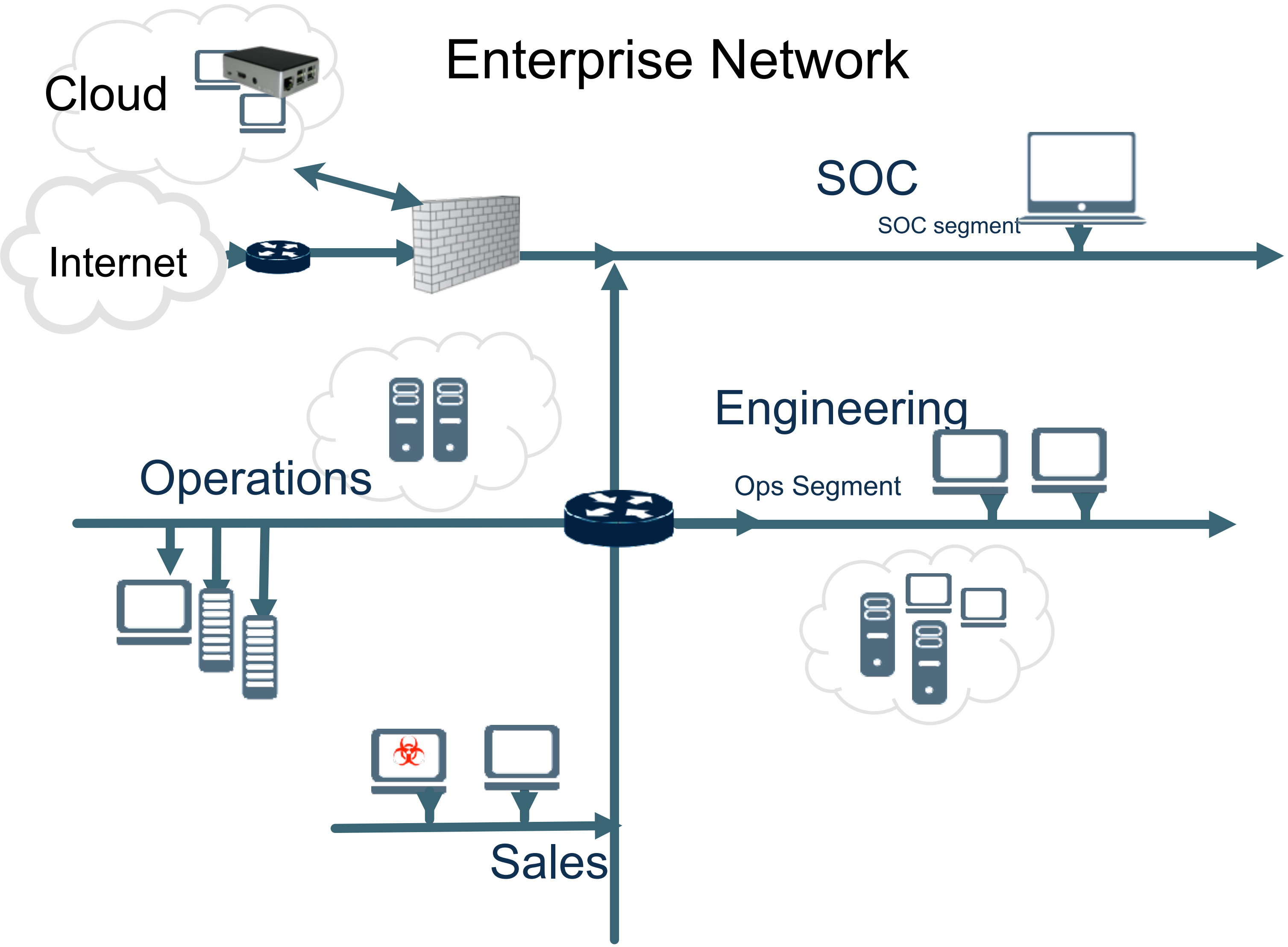


MITRE Cyber Analytics Repository

Analytics

Analytic	ATT&CK Techniques	Implementations
CAR-2013-01-002: Autorun Differences	Modify Existing Service, New Service, Scheduled Task, Port Monitors, Registry Run Keys / Startup Folder, Path Interception, Accessibility Features, Modify Registry, Service Registry Permissions Weakness, Windows Management Instrumentation Event Subscription, File System Permissions Weakness, Change Default File Association, Logon Scripts, Winlogon Helper DLL, AppInit DLLs	

Information Security Problem



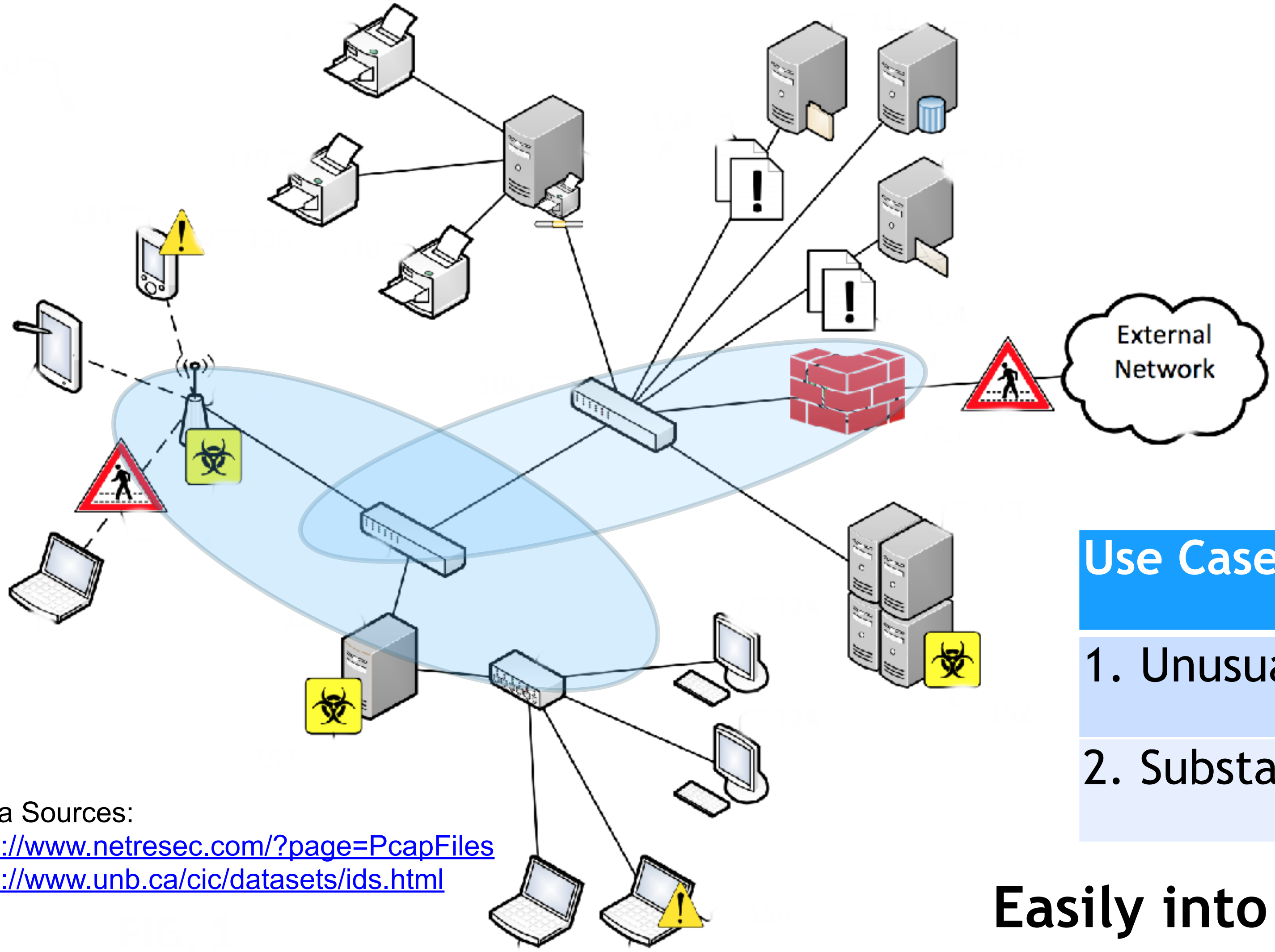
1. **Network Security**
2. **Endpoint Security**
3. **Application Security**
4. **Data Security**
5. **Cloud Security**
6. **Web Security**
7. **Mobile Security**
8. **IoT Security**
9. **Transaction Security**
10. **Messaging Security**

Basic Security Controls

- Boundary firewalls and internet gateways
- Malware protection
- Patch management
- Whitelisting and execution control
- Secure configuration
- Password policy
- User access control
- Incident management

Security Data Science

Security Data Sources: Network Logs



Network Logs
- Firewall
- IDS/IPS
- Network flow
- DNS
- Wi-fi

Use Cases
1. Unusual Volume of Network Activity
2. Substantial Increase in an Event/Port Activity

Easily into a few TBs of data per day

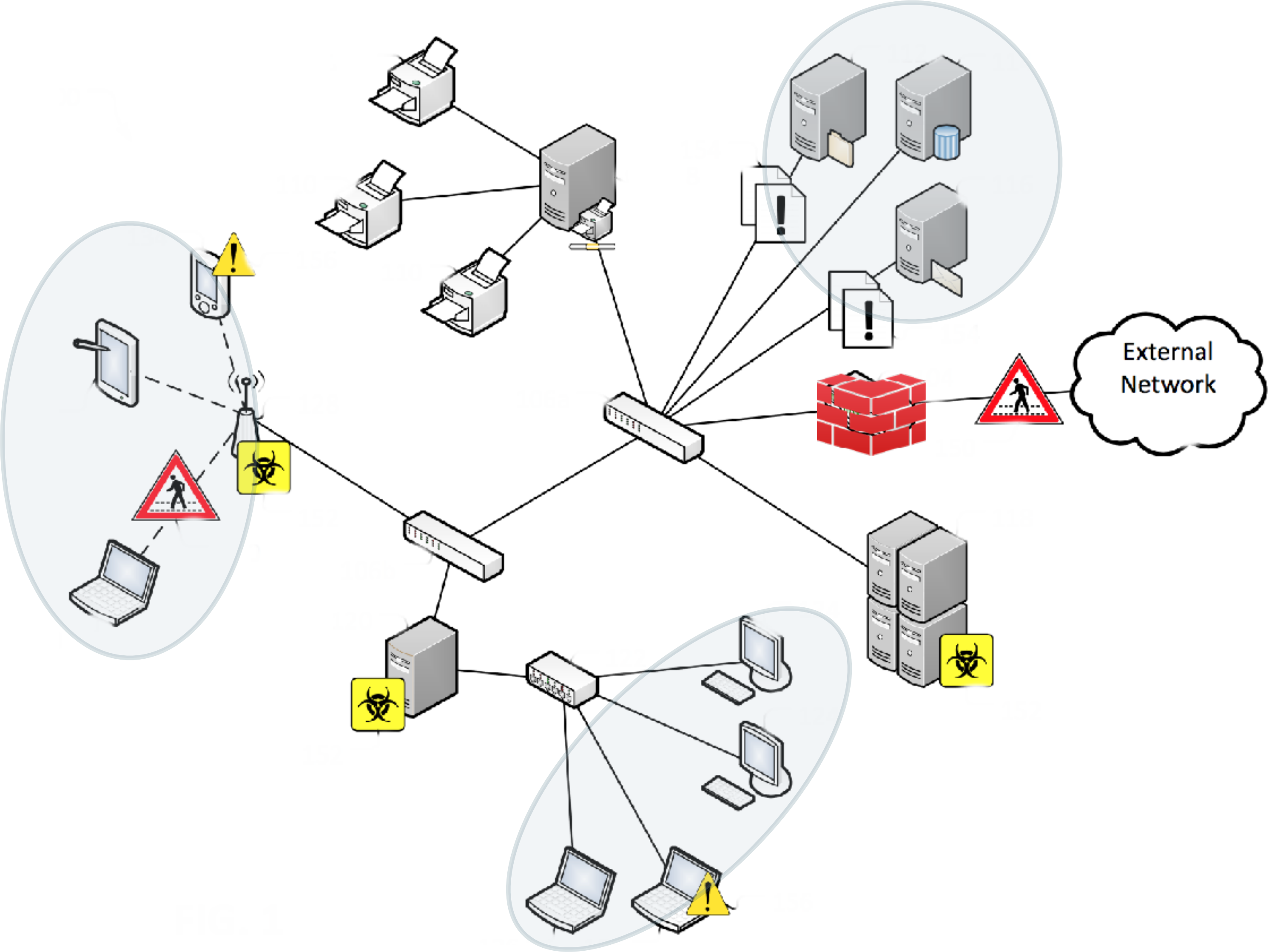
Data Sources:
http://www.netresec.com/?page=PcapFiles
http://www.unb.ca/cic/datasets/ids.html

Endpoint Logs and Use Cases

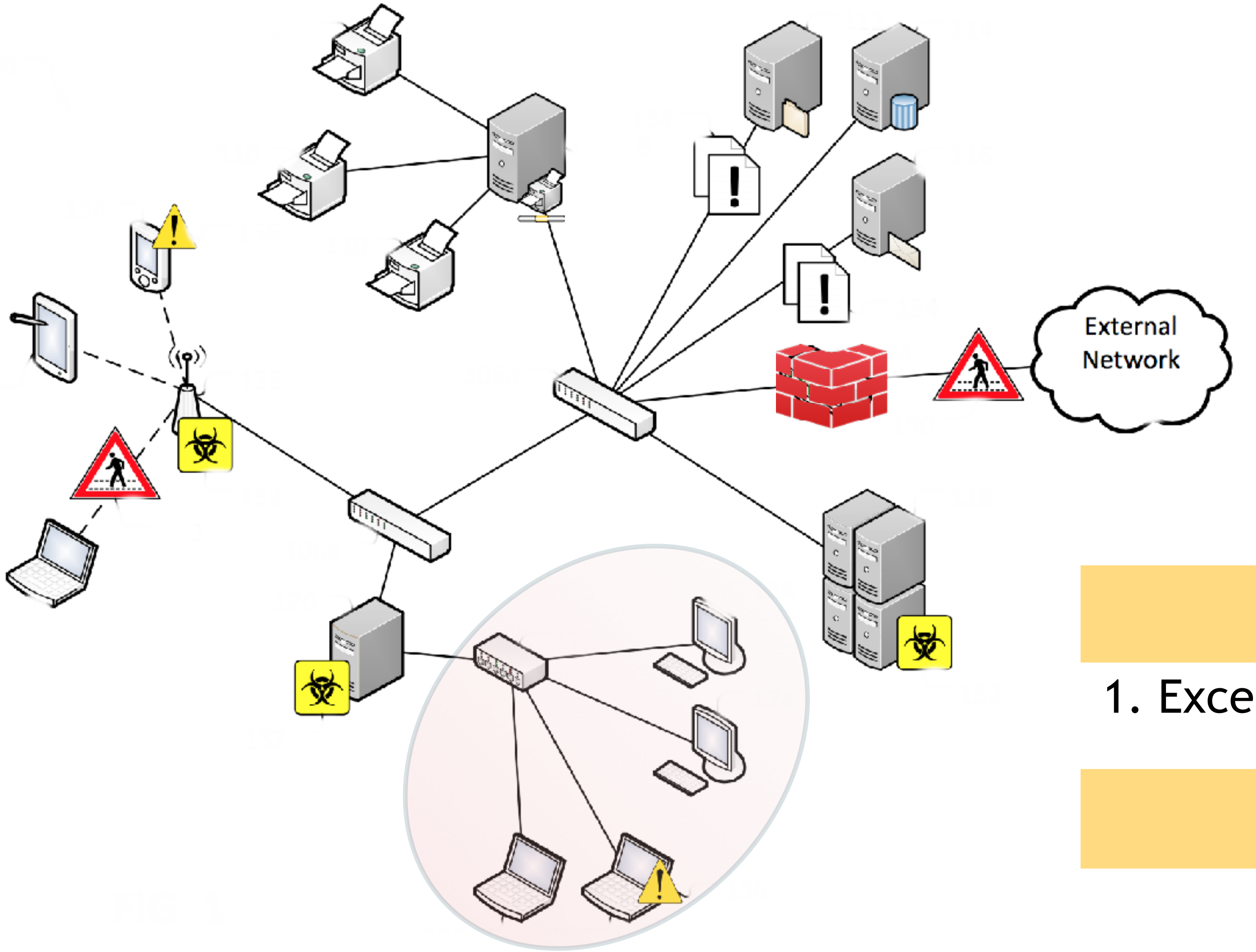
Endpoint Logs

- File System Changes
- Applications
- Process
- OS
- Antivirus Alerts

Use Cases
1. Anomalous New Listening Ports/ Services/Processes
2. Host with Excessive No. of Listening Ports/Services/Processes



Authentication Logs and Use Cases



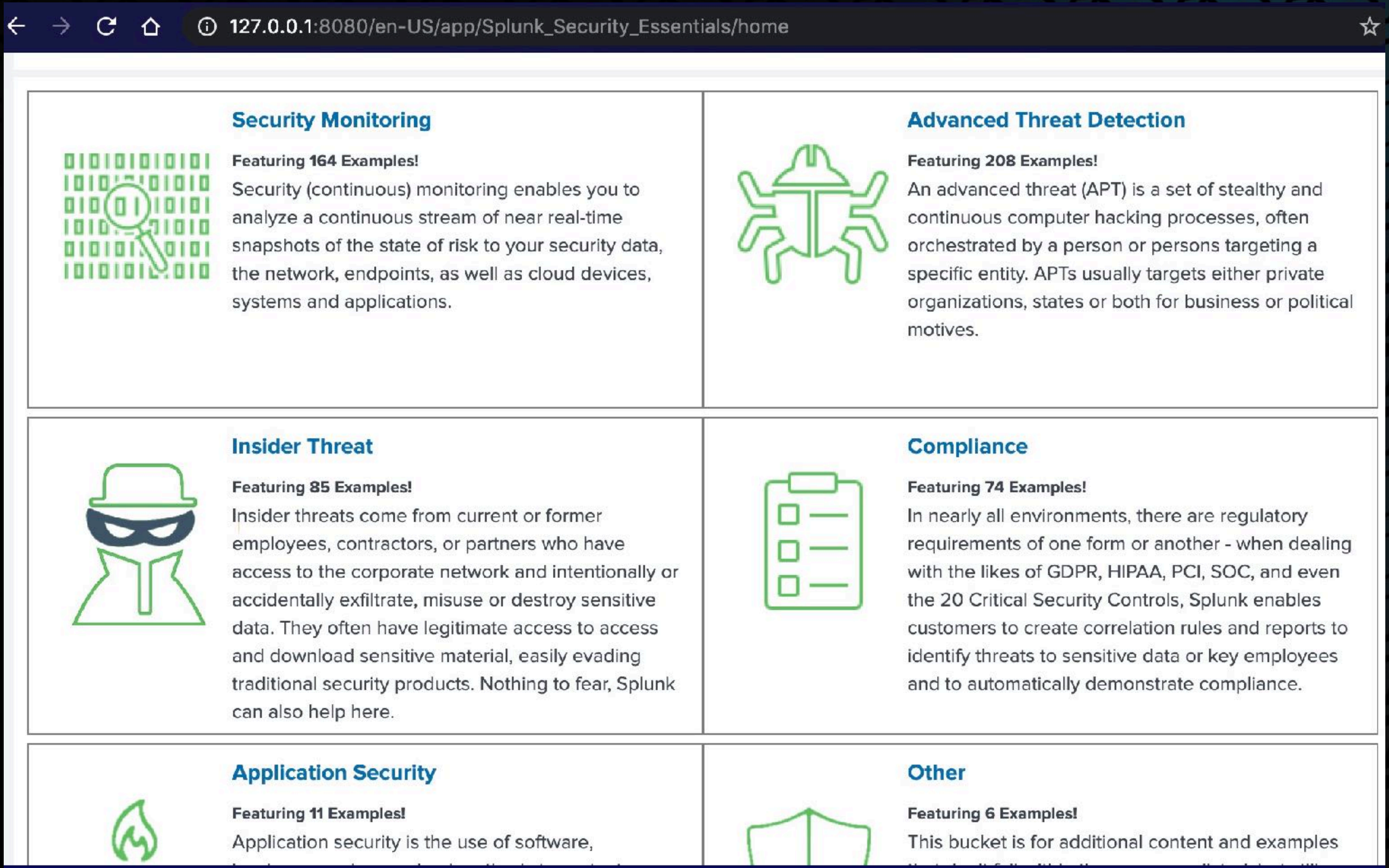
Authentication Logs
Windows Events
Active Directory User Logs
Privilege User

Use Cases

1. Excessive Failed Logins - Brute Force Attack

2. Default Account Usage

400+ Use Case.. Splunk Security Essentials App



127.0.0.1:8080/en-US/app/Splunk_Security_Essentials/home

Security Monitoring

Featuring 164 Examples!

Security (continuous) monitoring enables you to analyze a continuous stream of near real-time snapshots of the state of risk to your security data, the network, endpoints, as well as cloud devices, systems and applications.

Advanced Threat Detection

Featuring 208 Examples!

An advanced threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity. APTs usually targets either private organizations, states or both for business or political motives.

Insider Threat

Featuring 85 Examples!

Insider threats come from current or former employees, contractors, or partners who have access to the corporate network and intentionally or accidentally exfiltrate, misuse or destroy sensitive data. They often have legitimate access to access and download sensitive material, easily evading traditional security products. Nothing to fear, Splunk can also help here.

Compliance

Featuring 74 Examples!

In nearly all environments, there are regulatory requirements of one form or another - when dealing with the likes of GDPR, HIPAA, PCI, SOC, and even the 20 Critical Security Controls, Splunk enables customers to create correlation rules and reports to identify threats to sensitive data or key employees and to automatically demonstrate compliance.

Application Security

Featuring 11 Examples!

Application security is the use of software,

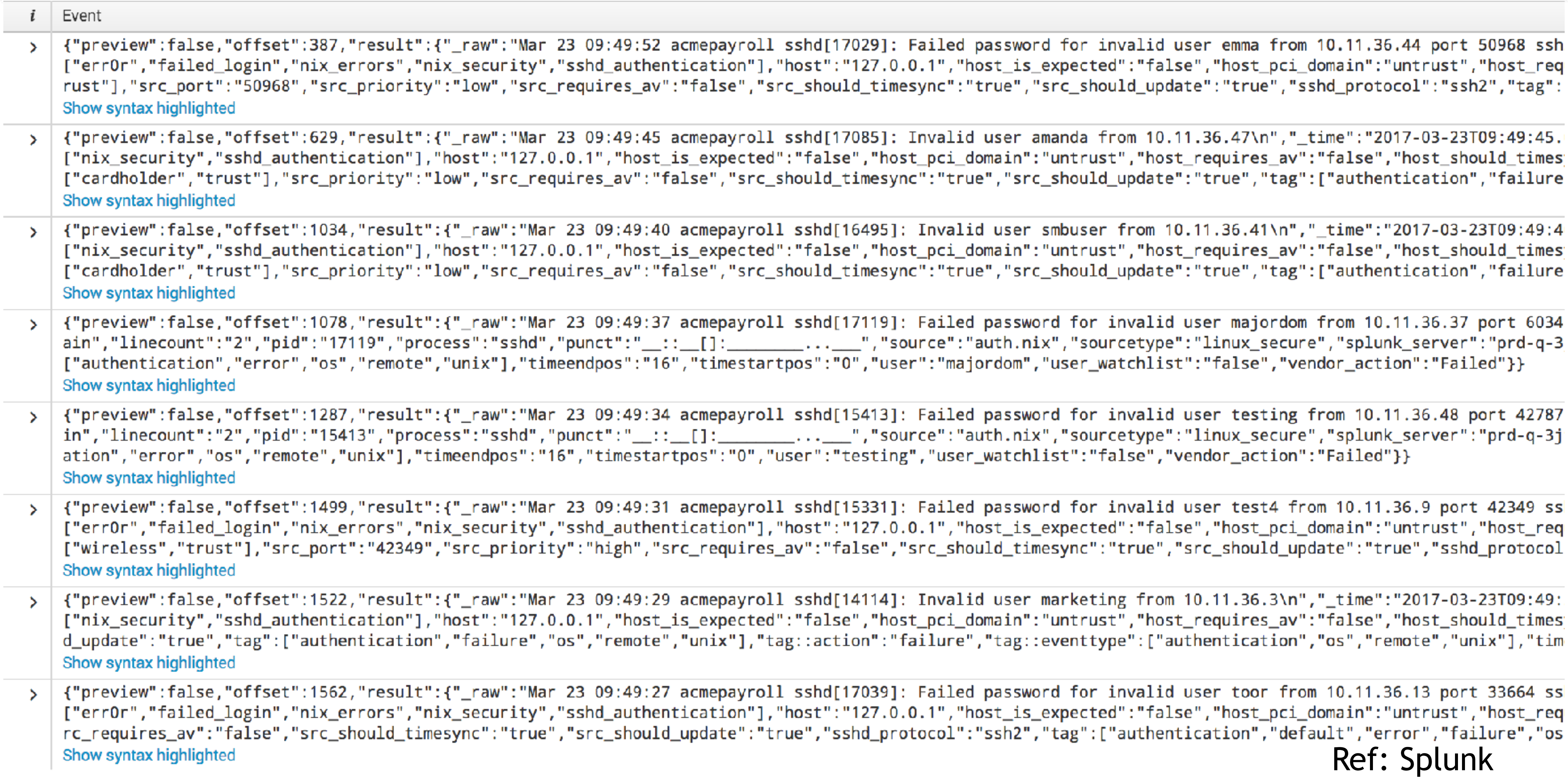
Other

Featuring 6 Examples!

This bucket is for additional content and examples

Data Processing Pipeline

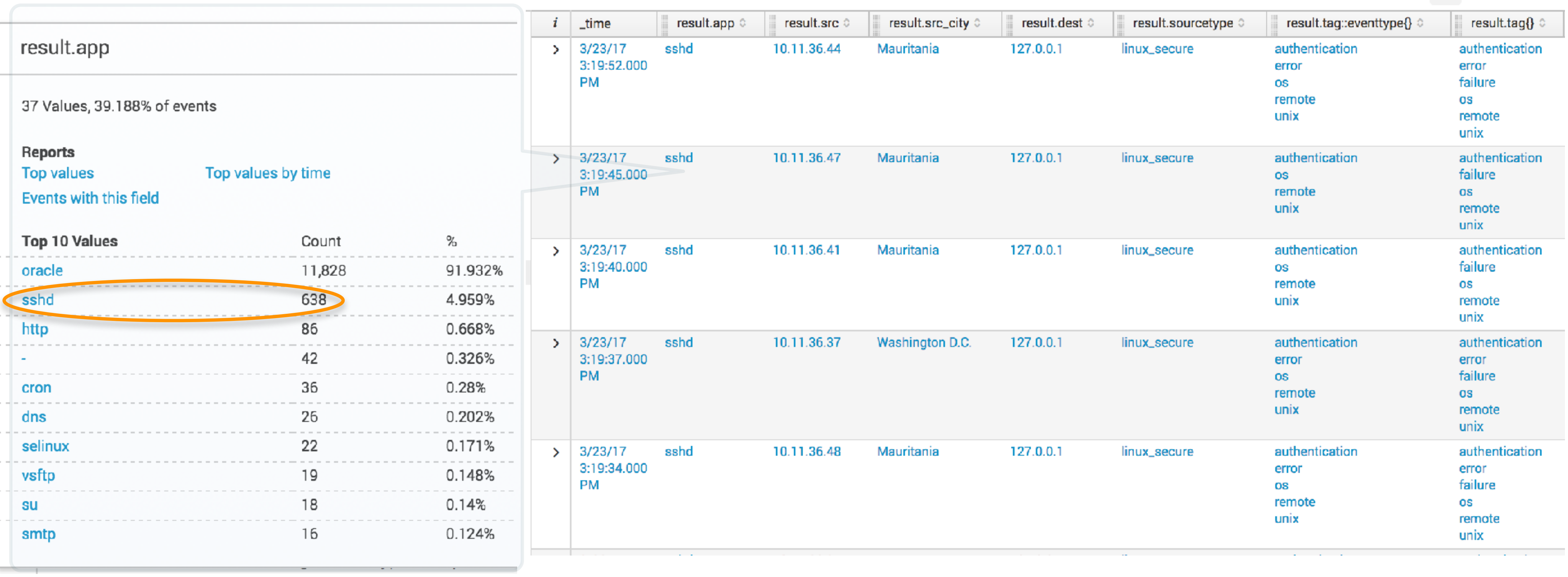
Simplified Pipeline- Step 1: Log Processing



```
i   Event
>   {"preview":false,"offset":387,"result":{"_raw":"Mar 23 09:49:52 acmepayroll sshd[17029]: Failed password for invalid user emma from 10.11.36.44 port 50968 ssh
    ["err0r","failed_login","nix_errors","nix_security","sshd_authentication"],"host":"127.0.0.1","host_is_expected":"false","host_pci_domain":"untrust","host_req
    rust"],"src_port":"50968","src_priority":"low","src_requires_av":"false","src_should_timesync":"true","src_should_update":"true","sshd_protocol":"ssh2","tag":
    Show syntax highlighted
>   {"preview":false,"offset":629,"result":{"_raw":"Mar 23 09:49:45 acmepayroll sshd[17085]: Invalid user amanda from 10.11.36.47\n","_time":"2017-03-23T09:49:45.
    ["nix_security","sshd_authentication"],"host":"127.0.0.1","host_is_expected":"false","host_pci_domain":"untrust","host_requires_av":"false","host_should_times
    ["cardholder","trust"],"src_priority":"low","src_requires_av":"false","src_should_timesync":"true","src_should_update":"true","tag":["authentication","failure
    Show syntax highlighted
>   {"preview":false,"offset":1034,"result":{"_raw":"Mar 23 09:49:40 acmepayroll sshd[16495]: Invalid user smbuser from 10.11.36.41\n","_time":"2017-03-23T09:49:4
    ["nix_security","sshd_authentication"],"host":"127.0.0.1","host_is_expected":"false","host_pci_domain":"untrust","host_requires_av":"false","host_should_times
    ["cardholder","trust"],"src_priority":"low","src_requires_av":"false","src_should_timesync":"true","src_should_update":"true","tag":["authentication","failure
    Show syntax highlighted
>   {"preview":false,"offset":1078,"result":{"_raw":"Mar 23 09:49:37 acmepayroll sshd[17119]: Failed password for invalid user majordom from 10.11.36.37 port 6034
    ain","linecount":"2","pid":"17119","process":"sshd","punct":"__::__[]:_________...___","source":"auth.nix","sourcetype":"linux_secure","splunk_server":"prd-q-3
    ["authentication","error","os","remote","unix"],"timeendpos":"16","timestartpos":"0","user":"majordom","user_watchlist":"false","vendor_action":"Failed"}}
    Show syntax highlighted
>   {"preview":false,"offset":1287,"result":{"_raw":"Mar 23 09:49:34 acmepayroll sshd[15413]: Failed password for invalid user testing from 10.11.36.48 port 42787
    in","linecount":"2","pid":"15413","process":"sshd","punct":"__::__[]:_________...___","source":"auth.nix","sourcetype":"linux_secure","splunk_server":"prd-q-3j
    ation","error","os","remote","unix"],"timeendpos":"16","timestartpos":"0","user":"testing","user_watchlist":"false","vendor_action":"Failed"}}
    Show syntax highlighted
>   {"preview":false,"offset":1499,"result":{"_raw":"Mar 23 09:49:31 acmepayroll sshd[15331]: Failed password for invalid user test4 from 10.11.36.9 port 42349 ss
    ["err0r","failed_login","nix_errors","nix_security","sshd_authentication"],"host":"127.0.0.1","host_is_expected":"false","host_pci_domain":"untrust","host_req
    ["wireless","trust"],"src_port":"42349","src_priority":"high","src_requires_av":"false","src_should_timesync":"true","src_should_update":"true","sshd_protocol
    Show syntax highlighted
>   {"preview":false,"offset":1522,"result":{"_raw":"Mar 23 09:49:29 acmepayroll sshd[14114]: Invalid user marketing from 10.11.36.3\n","_time":"2017-03-23T09:49:
    ["nix_security","sshd_authentication"],"host":"127.0.0.1","host_is_expected":"false","host_pci_domain":"untrust","host_requires_av":"false","host_should_times
    d_update":"true","tag":["authentication","failure","os","remote","unix"],"tag::action":"failure","tag::eventtype":["authentication","os","remote","unix"],"tim
    Show syntax highlighted
>   {"preview":false,"offset":1562,"result":{"_raw":"Mar 23 09:49:27 acmepayroll sshd[17039]: Failed password for invalid user toor from 10.11.36.13 port 33664 ss
    ["err0r","failed_login","nix_errors","nix_security","sshd_authentication"],"host":"127.0.0.1","host_is_expected":"false","host_pci_domain":"untrust","host_req
    rc_requires_av":"false","src_should_timesync":"true","src_should_update":"true","sshd_protocol":"ssh2","tag":["authentication","default","error","failure","os
    Show syntax highlighted
```

Ref: Splunk

Step 2: Compute Statistics



result.app

37 Values, 39.188% of events

Reports

Top values Top values by time

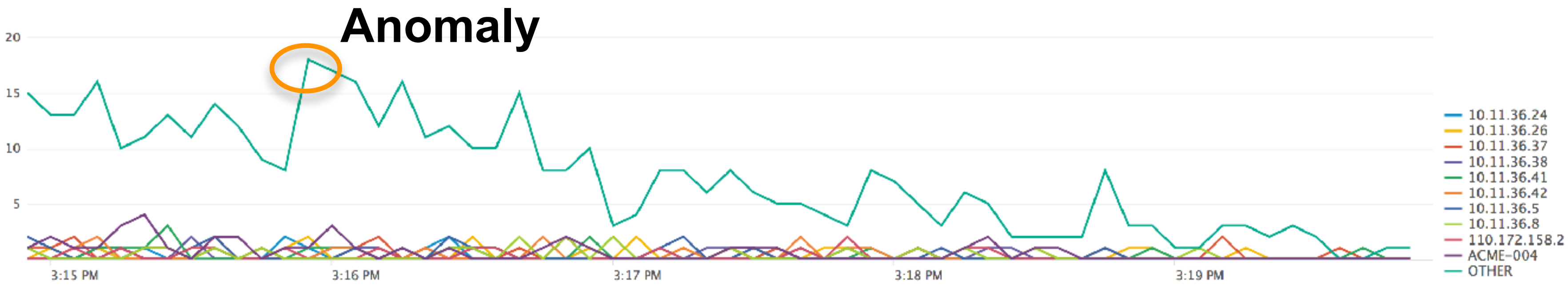
Events with this field

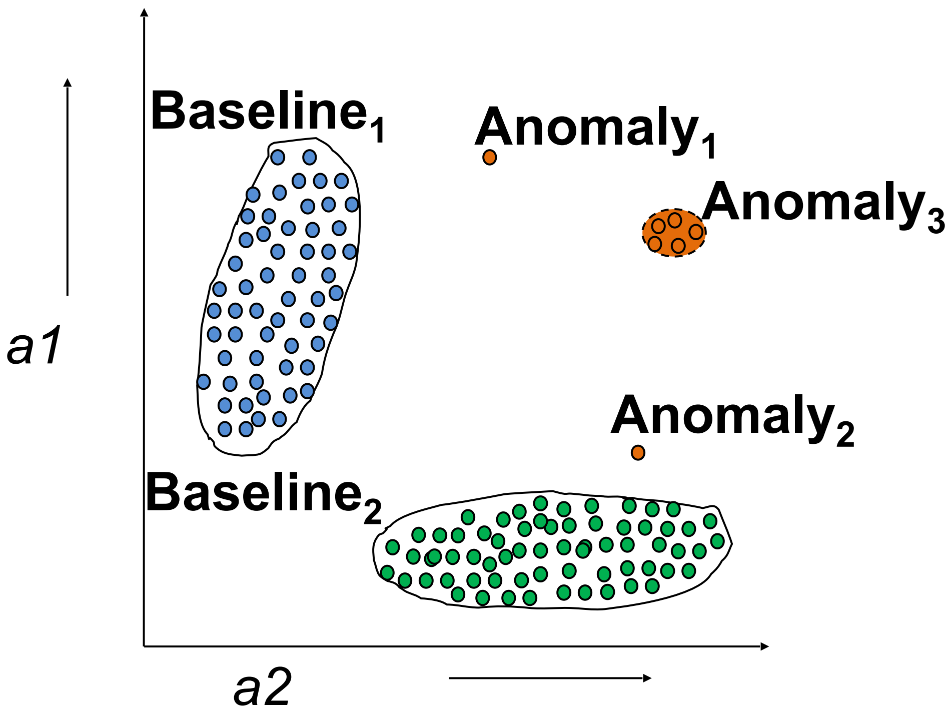
Top 10 Values	Count	%
oracle	11,828	91.932%
sshd	638	4.959%
http	86	0.668%
-	42	0.326%
cron	36	0.28%
dns	26	0.202%
selinux	22	0.171%
vsftp	19	0.148%
su	18	0.14%
smtp	16	0.124%

i	_time	result.app	result.src	result.src_city	result.dest	result.sourcetype	result.tag::eventtype{}	result.tag{}
>	3/23/17 3:19:52.000 PM	sshd	10.11.36.44	Mauritania	127.0.0.1	linux_secure	authentication error os remote unix	authentication error failure os remote unix
>	3/23/17 3:19:45.000 PM	sshd	10.11.36.47	Mauritania	127.0.0.1	linux_secure	authentication os remote unix	authentication failure os remote unix
>	3/23/17 3:19:40.000 PM	sshd	10.11.36.41	Mauritania	127.0.0.1	linux_secure	authentication os remote unix	authentication failure os remote unix
>	3/23/17 3:19:37.000 PM	sshd	10.11.36.37	Washington D.C.	127.0.0.1	linux_secure	authentication error os remote unix	authentication error failure os remote unix
>	3/23/17 3:19:34.000 PM	sshd	10.11.36.48	Mauritania	127.0.0.1	linux_secure	authentication error os remote unix	authentication error failure os remote unix

Ref: Splunk

Step 3: Anomaly Detection

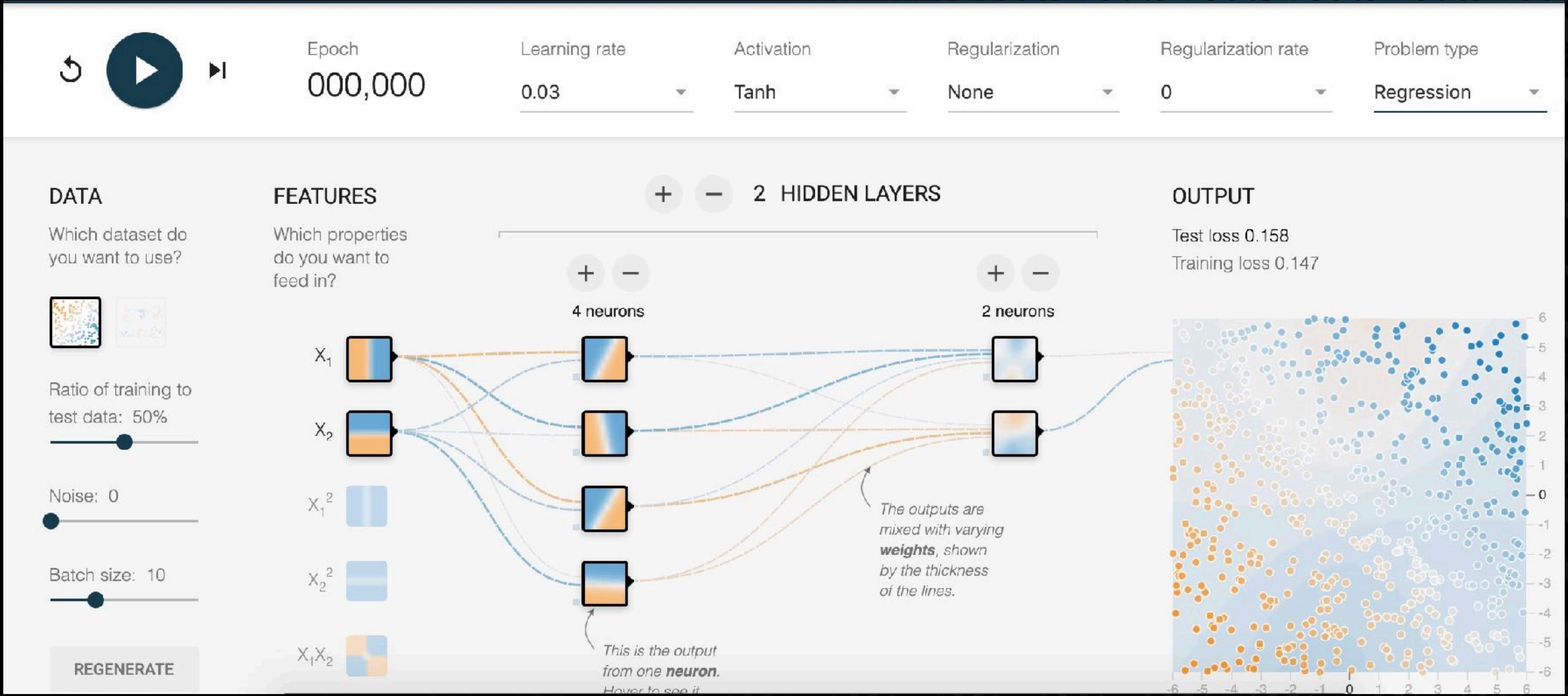

Anomaly



Ref: Splunk

Deep Learning

playground.tensorflow.org



Epoch 000,000

Learning rate 0.03

Activation Tanh

Regularization None

Regularization rate 0

Problem type Regression

DATA

Which dataset do you want to use?

Ratio of training to test data: 50%

Noise: 0

Batch size: 10

REGENERATE

FEATURES

Which properties do you want to feed in?

2 HIDDEN LAYERS

4 neurons

2 neurons

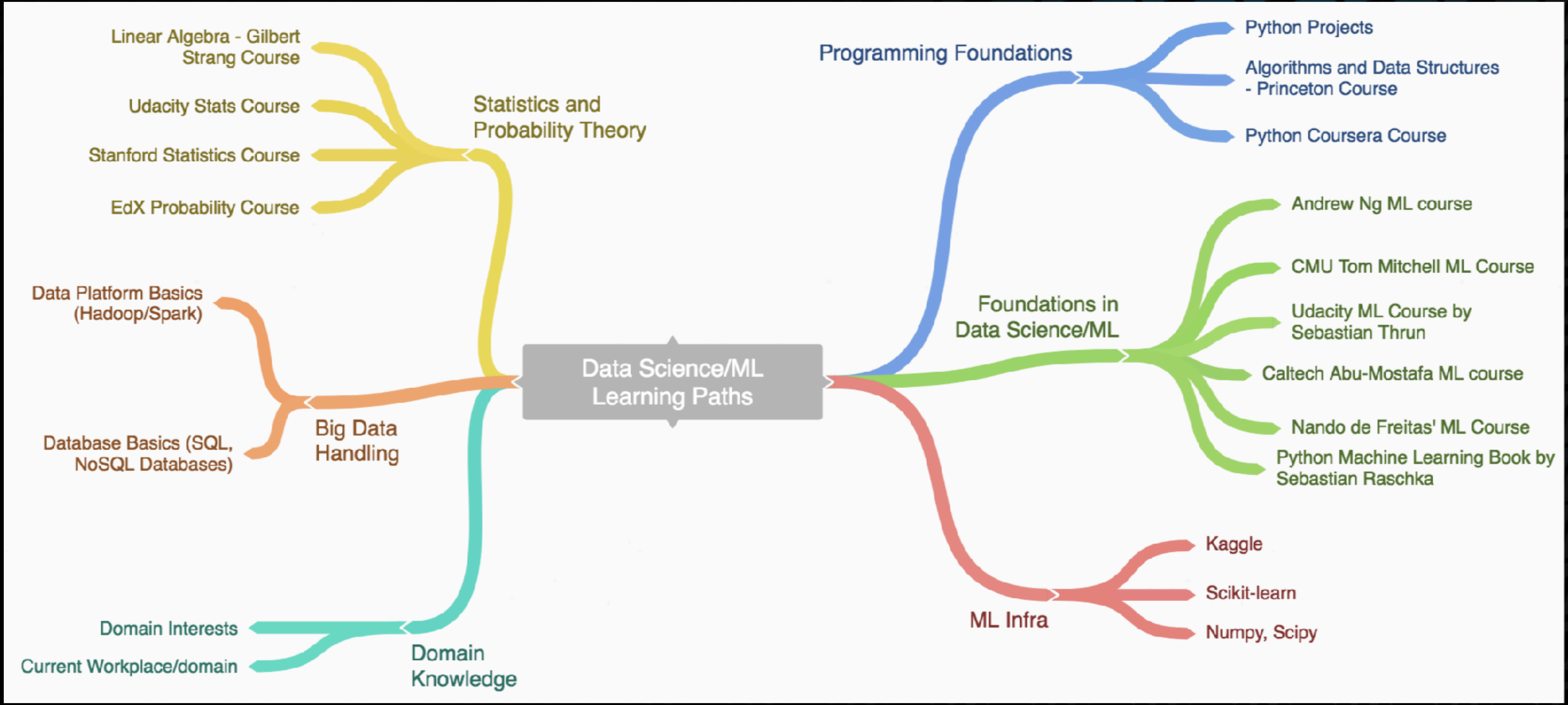
OUTPUT

Test loss 0.158

Training loss 0.147

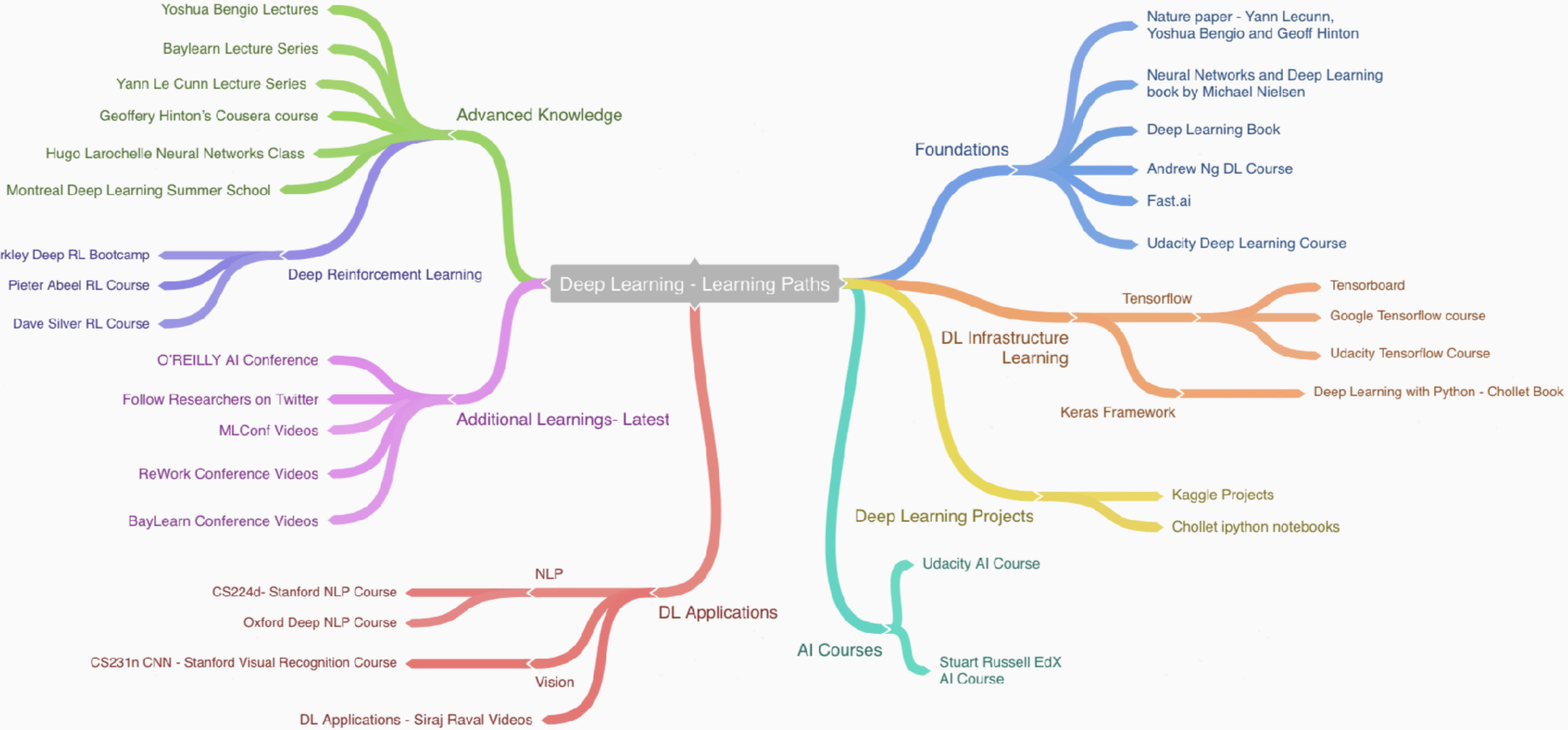
*The outputs are mixed with varying **weights**, shown by the thickness of the lines.*

*This is the output from one **neuron**. Hover to see it*



Data Science/ML Learning Paths

- Statistics and Probability Theory
  - Linear Algebra - Gilbert Strang Course
  - Udacity Stats Course
  - Stanford Statistics Course
  - EdX Probability Course
- Big Data Handling
  - Data Platform Basics (Hadoop/Spark)
  - Database Basics (SQL, NoSQL Databases)
- Domain Knowledge
  - Domain Interests
  - Current Workplace/domain
- Programming Foundations
  - Python Projects
  - Algorithms and Data Structures - Princeton Course
  - Python Coursera Course
- Foundations in Data Science/ML
  - Andrew Ng ML course
  - CMU Tom Mitchell ML Course
  - Udacity ML Course by Sebastian Thrun
  - Caltech Abu-Mostafa ML course
  - Nando de Freitas' ML Course
  - Python Machine Learning Book by Sebastian Raschka
- ML Infra
  - Kaggle
  - Scikit-learn
  - Numpy, Scipy



Deep Learning - Learning Paths

- Advanced Knowledge
  - Yoshua Bengio Lectures
  - Baylearn Lecture Series
  - Yann Le Cunn Lecture Series
  - Geoffery Hinton's Cousera course
  - Hugo Larochelle Neural Networks Class
  - Montreal Deep Learning Summer School
- Deep Reinforcement Learning
  - Berkley Deep RL Bootcamp
  - Pieter Abeel RL Course
  - Dave Silver RL Course
- Additional Learnings- Latest
  - O'REILLY AI Conference
  - Follow Researchers on Twitter
  - MLConf Videos
  - ReWork Conference Videos
  - BayLearn Conference Videos
- DL Applications
  - NLP
    - CS224d- Stanford NLP Course
    - Oxford Deep NLP Course
  - Vision
    - CS231n CNN - Stanford Visual Recognition Course
  - DL Applications - Siraj Raval Videos
- Foundations
  - Nature paper - Yann Lecunn, Yoshua Bengio and Geoff Hinton
  - Neural Networks and Deep Learning book by Michael Nielsen
  - Deep Learning Book
  - Andrew Ng DL Course
  - Fast.ai
  - Udacity Deep Learning Course
- DL Infrastructure Learning
  - Tensorflow
    - Tensorboard
    - Google Tensorflow course
    - Udacity Tensorflow Course
  - Keras Framework
    - Deep Learning with Python - Chollet Book
- Deep Learning Projects
  - Kaggle Projects
  - Chollet ipython notebooks
- AI Courses
  - Udacity AI Course
  - Stuart Russell EdX AI Course

InfoSec DL Use Cases

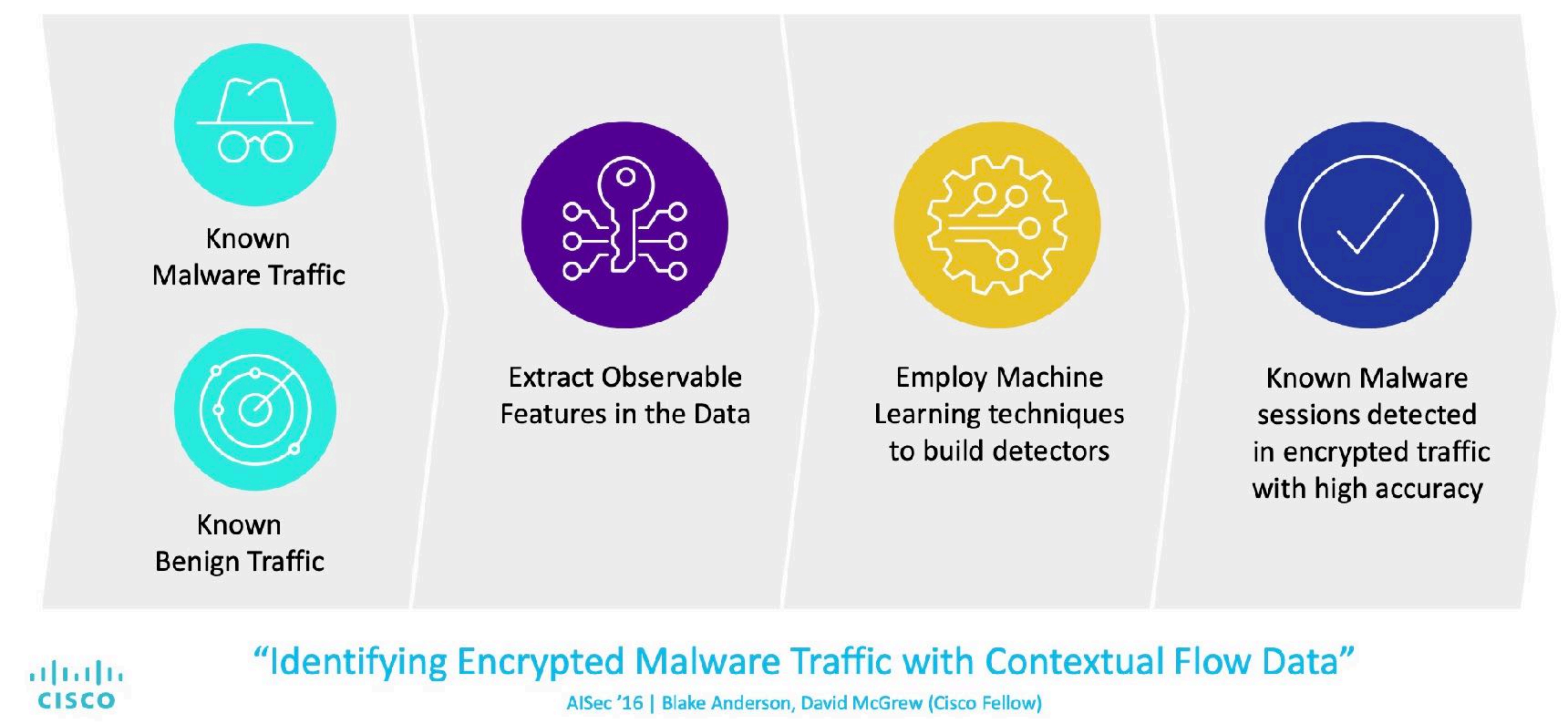
Use Cases

Network Security
1. Network intrusion detection (scanning, spoofing, etc.)
2. Application attack detection (OWASP-Top 10 attacks)
3. Phishing attack malicious URL detection

Endpoint Security
1. Malware detection and classification
2. Spyware, Ransomware detection

User Security
1. User behaviour Analytics
2. Detection of suspicious sign-in activities, brute force attacks and infected devices

Example 1: Cisco Encrypted Traffic Analysis



Known
Malware Traffic

Known
Benign Traffic

Extract Observable
Features in the Data

Employ Machine
Learning techniques
to build detectors

Known Malware
sessions detected
in encrypted traffic
with high accuracy

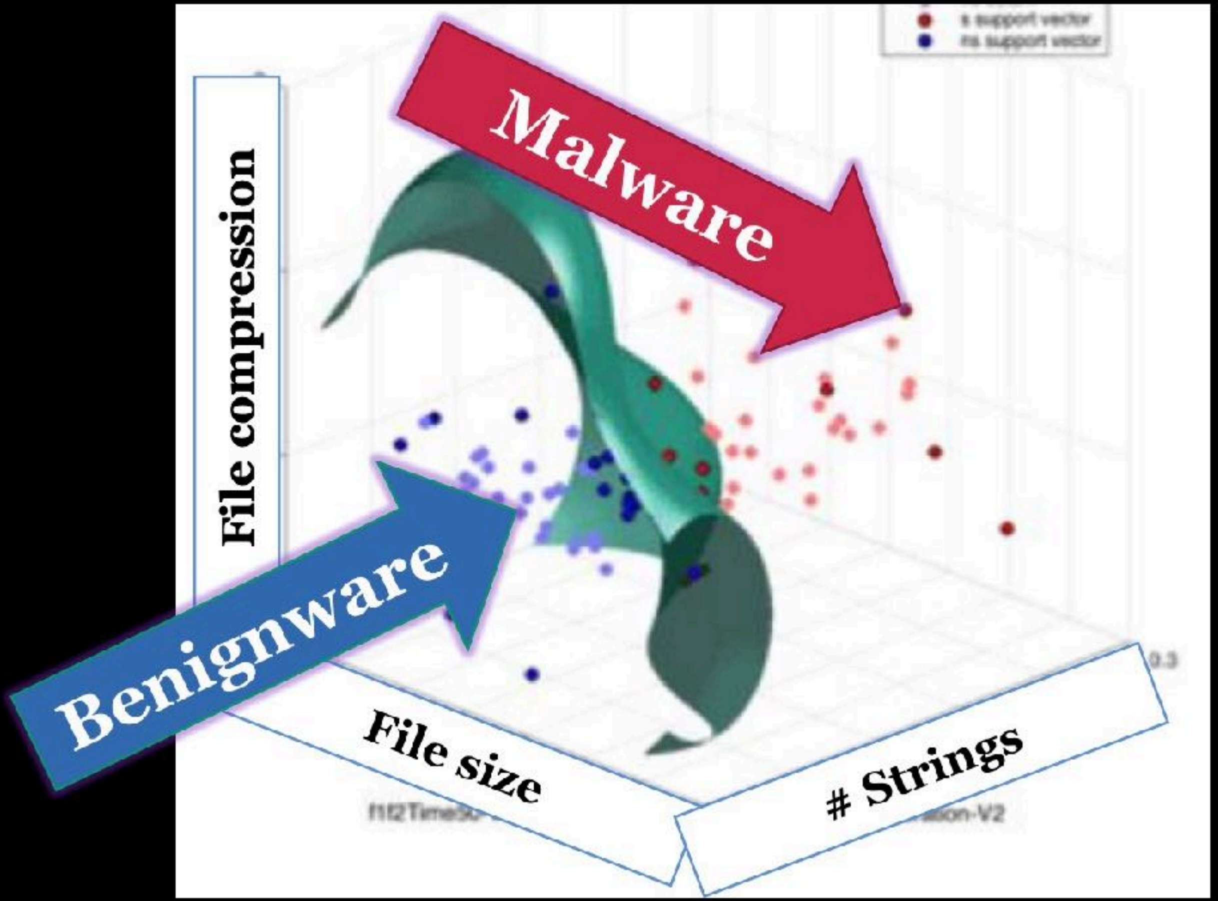
CISCO

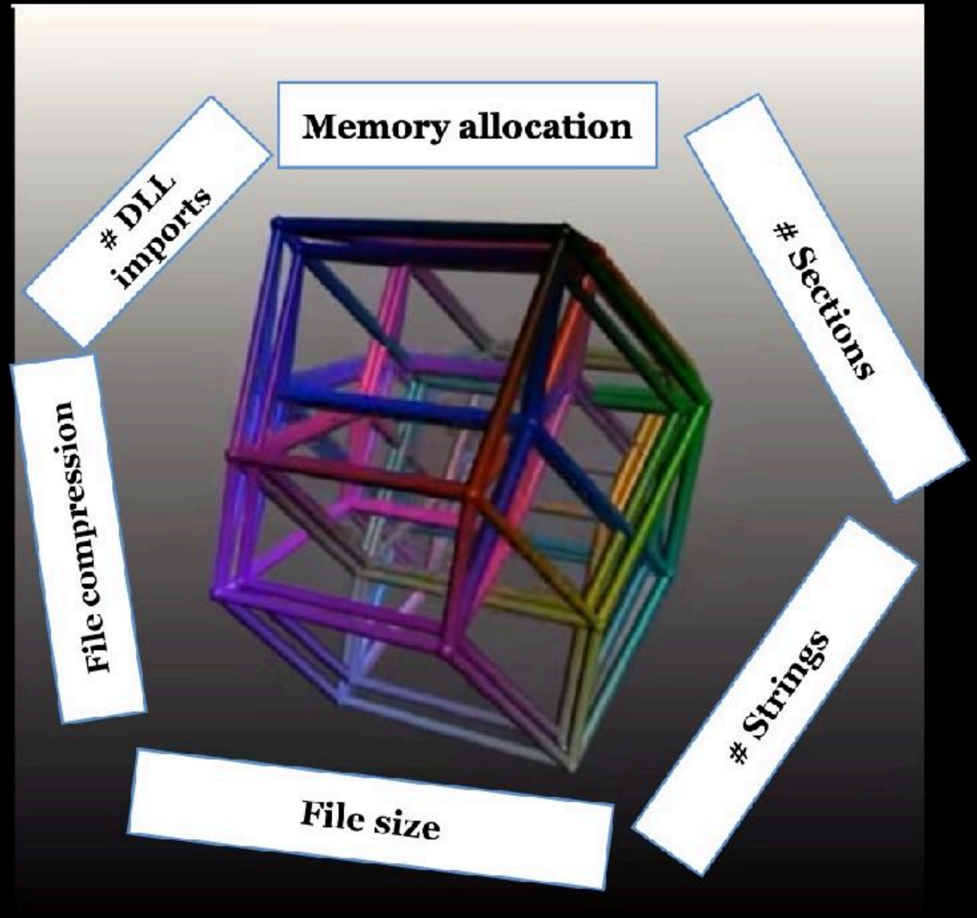
“Identifying Encrypted Malware Traffic with Contextual Flow Data”

AISec ’16 | Blake Anderson, David McGrew (Cisco Fellow)

TK Keanini, “Machine Learning: The What and Why of AI,” RSA Conf’19

Example 2: Malware Detection

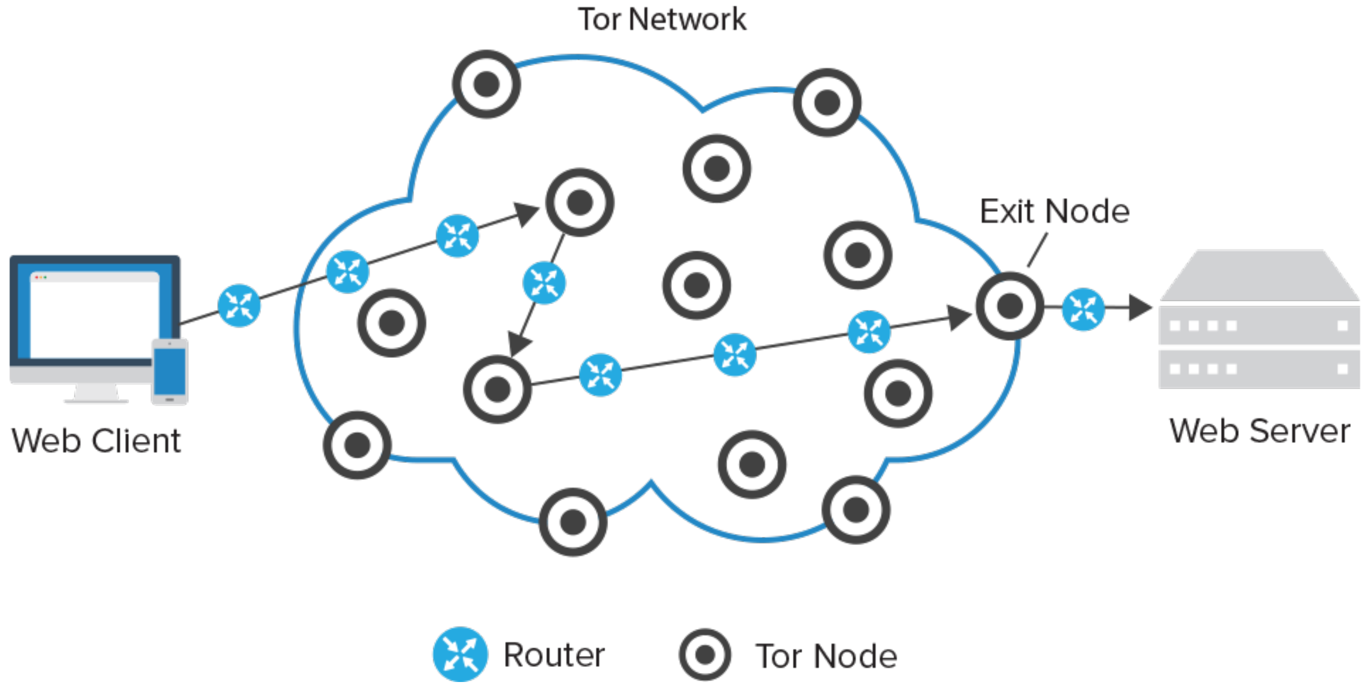


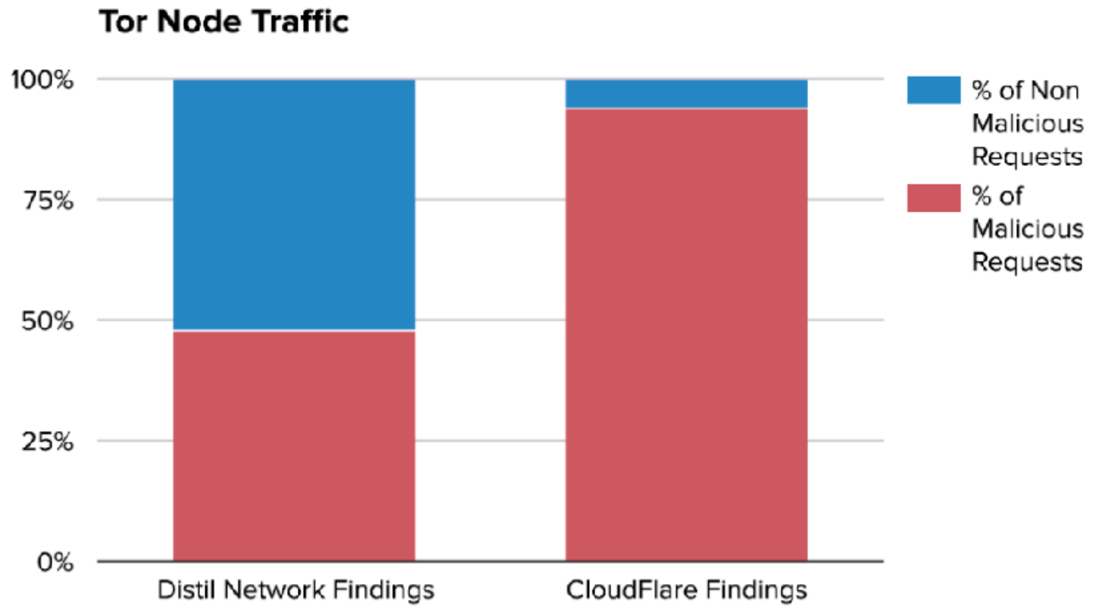


Joshua Saxe, Sophos, "Deep Neural Networks for Hackers: Methods, Applications, and Open Source Tools," BlackHat Conf'18

Case Study 1:
Tor Traffic Detection

Tor Network

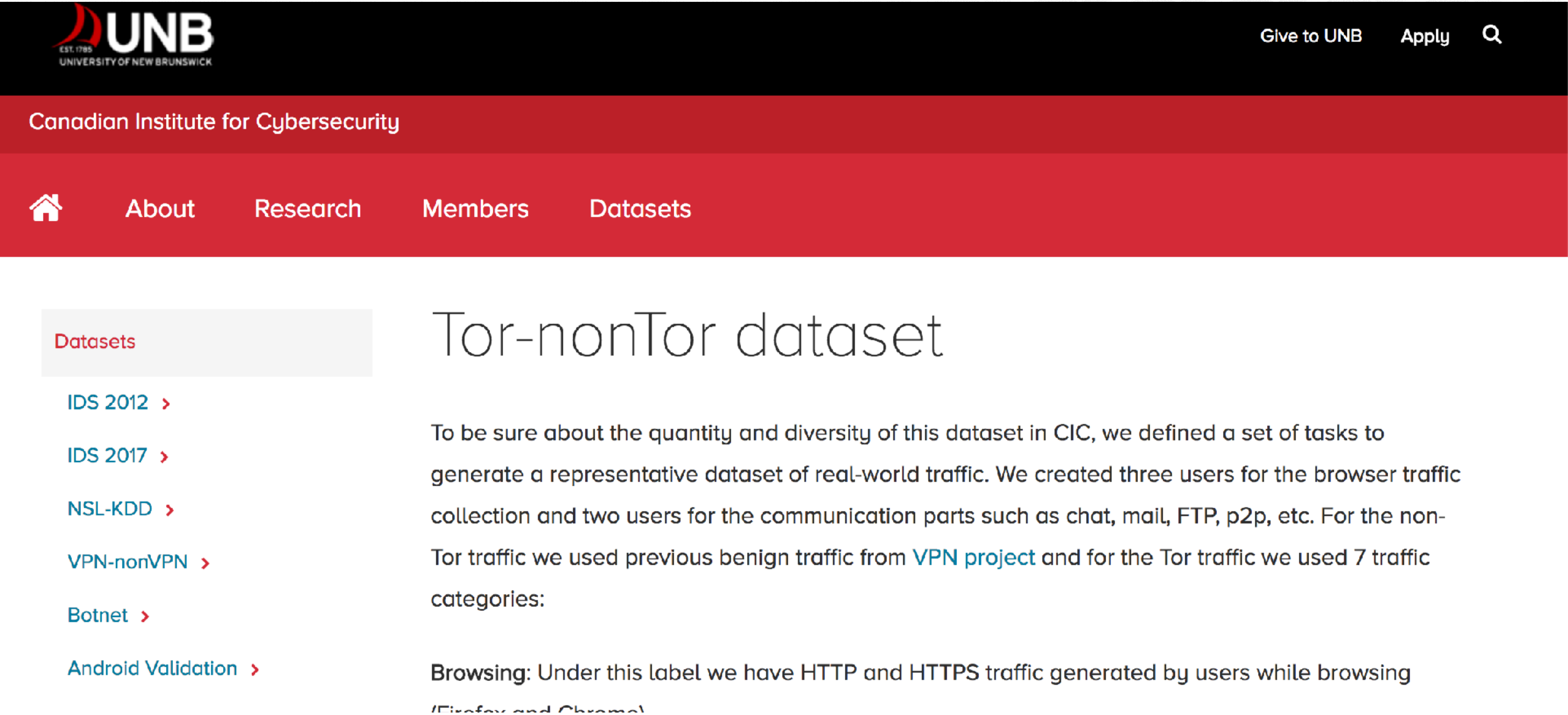




Adversaries use tor traffic for port scans, dark web purchases, extortion and data exfiltration

Source: Distill networks

Tor-nonTor Traffic - Dataset



Tor-nonTor dataset

To be sure about the quantity and diversity of this dataset in CIC, we defined a set of tasks to generate a representative dataset of real-world traffic. We created three users for the browser traffic collection and two users for the communication parts such as chat, mail, FTP, p2p, etc. For the non-Tor traffic we used previous benign traffic from VPN project and for the Tor traffic we used 7 traffic categories:

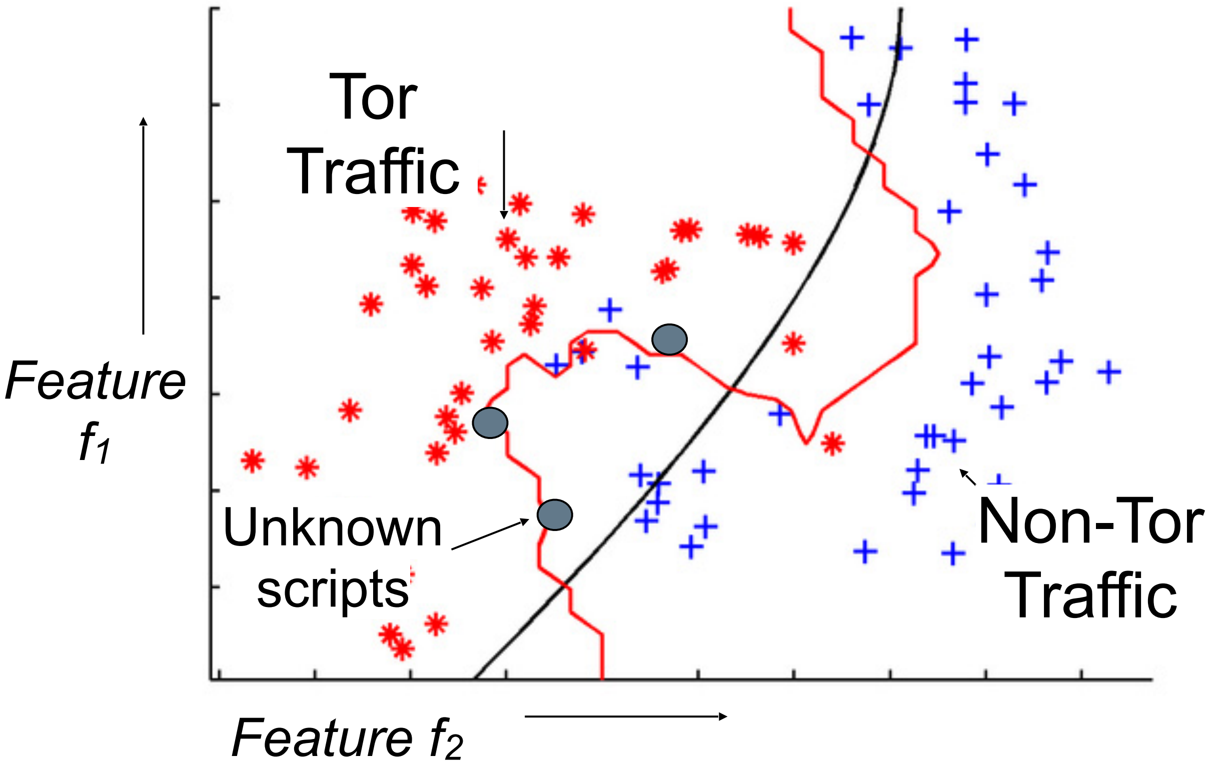
Browsing: Under this label we have HTTP and HTTPS traffic generated by users while browsing (Firefox and Chrome)

Tor-nonTor Traffic - Dataset

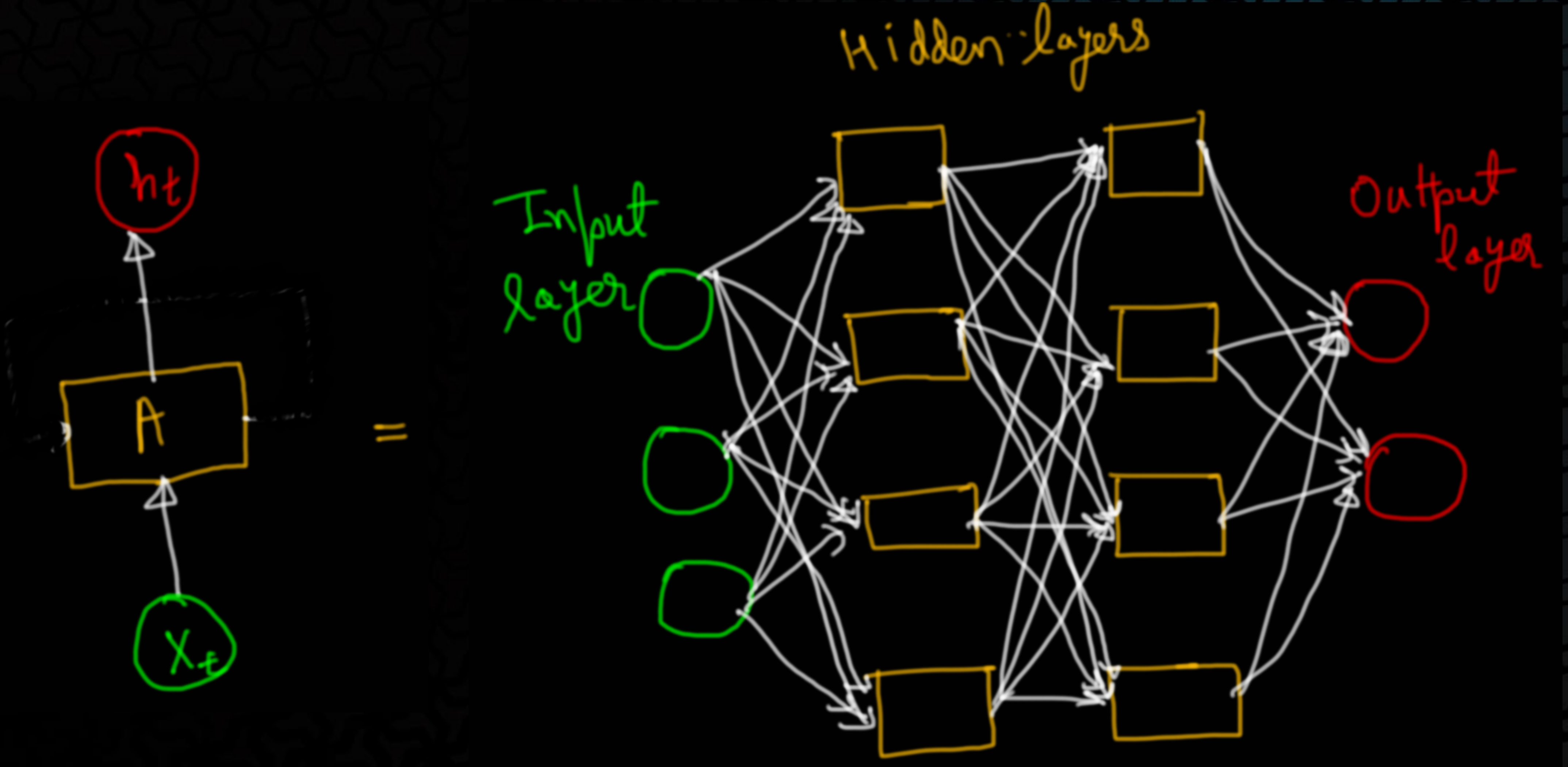
Activity	Details
Browsing	HTTP, HTTPS traffic using Chrome and Firefox
Email	Mails delivered via SMTP/S and received via POP3/SSL and IMAP/SSL, Thunderbird client
Chat	Facebook, Hangout, ICQ and IAM chat activities
Audio-streaming	Spotify audio streaming
Video-streaming	Youtube and Vimeo services over Chrome and Firefox
File transfer	Skype file transfers, FTP over SSH, FTP over SSL traffic sessions
VoIP	Facebook, Hangout and Skype

Demo Using Tensorflow and Keras

Classification



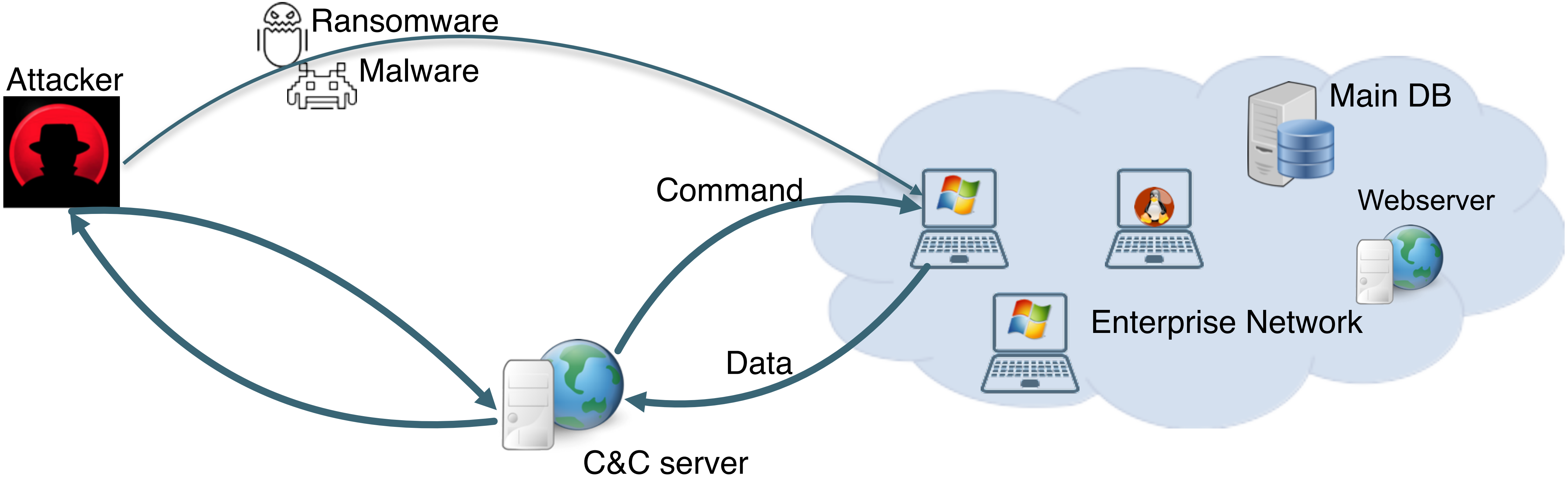
Feed Forward Neural Network



Input and output are independent

Case Study 2:
C&C Detection

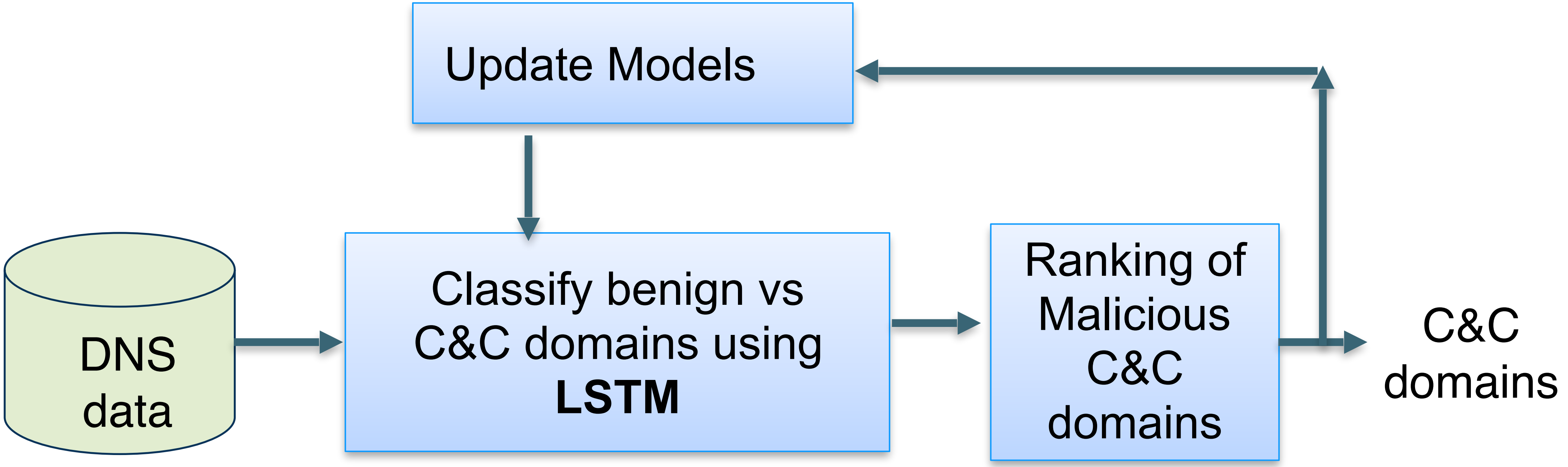
Command and Control Detection



C&C domain examples:

- DGA based: gvludcvhcrjwmgq.in, uqvwxfrhhwreddf.yt
- non DGA based: thisisyourchangeqq.com, homejobsinstitute.biz

C&C Detection: Pipeline



Update Models

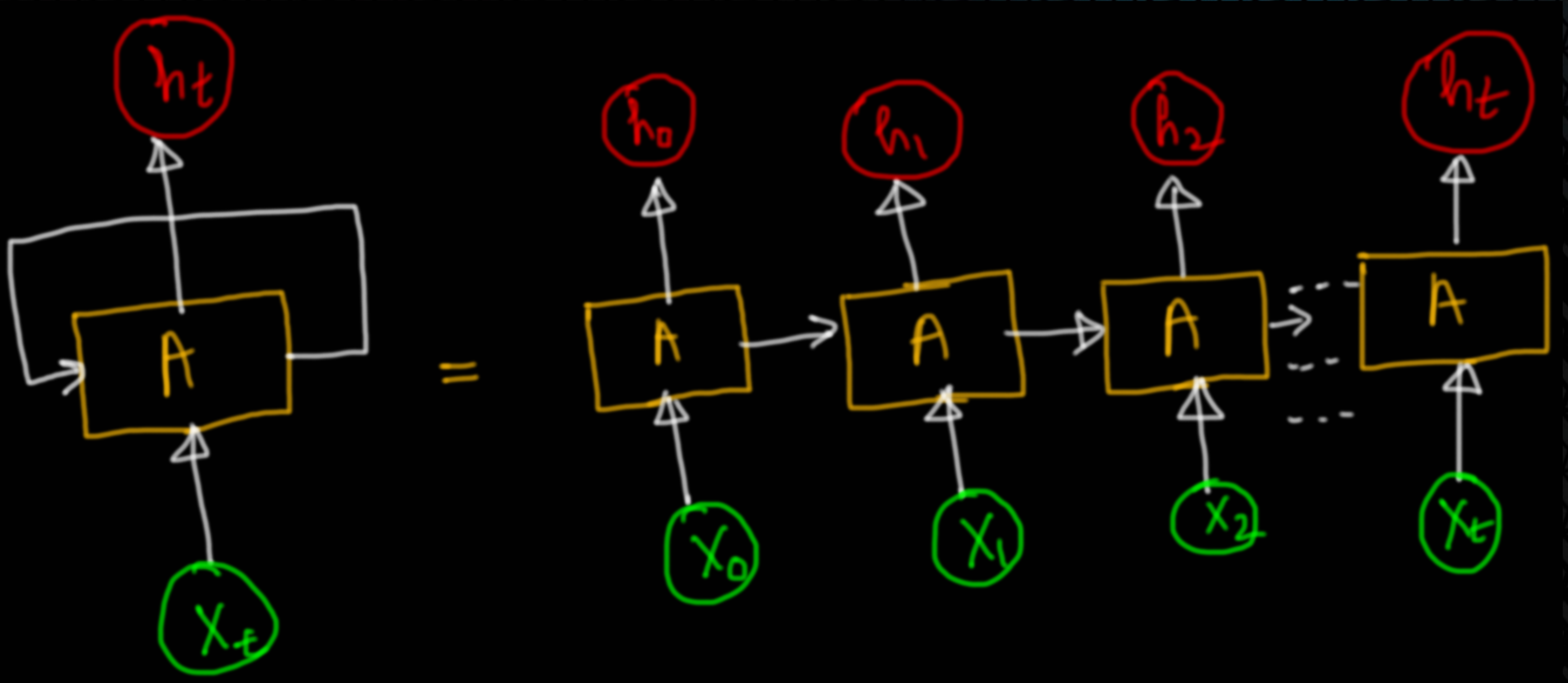
DNS data

Classify benign vs C&C domains using **LSTM**

Ranking of Malicious C&C domains

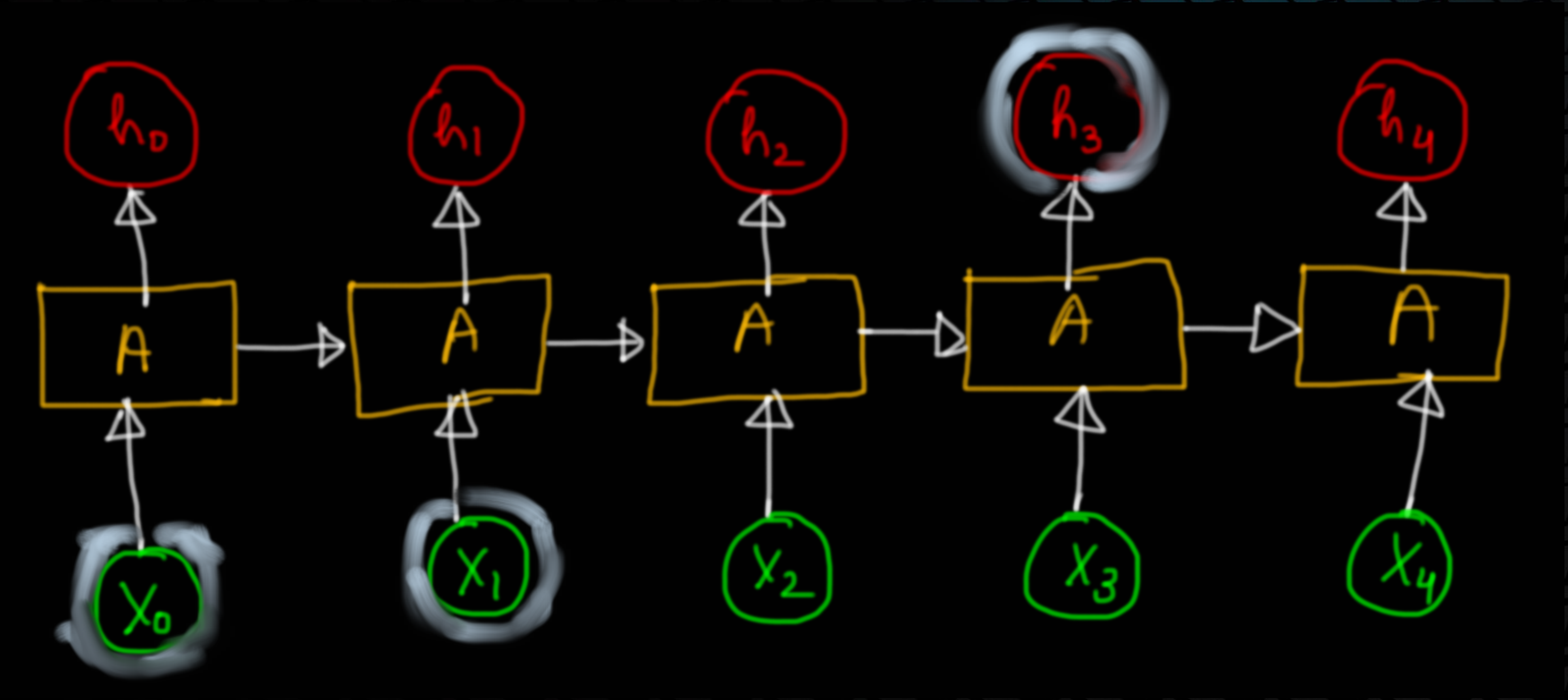
C&C domains

Recurrent Neural Network



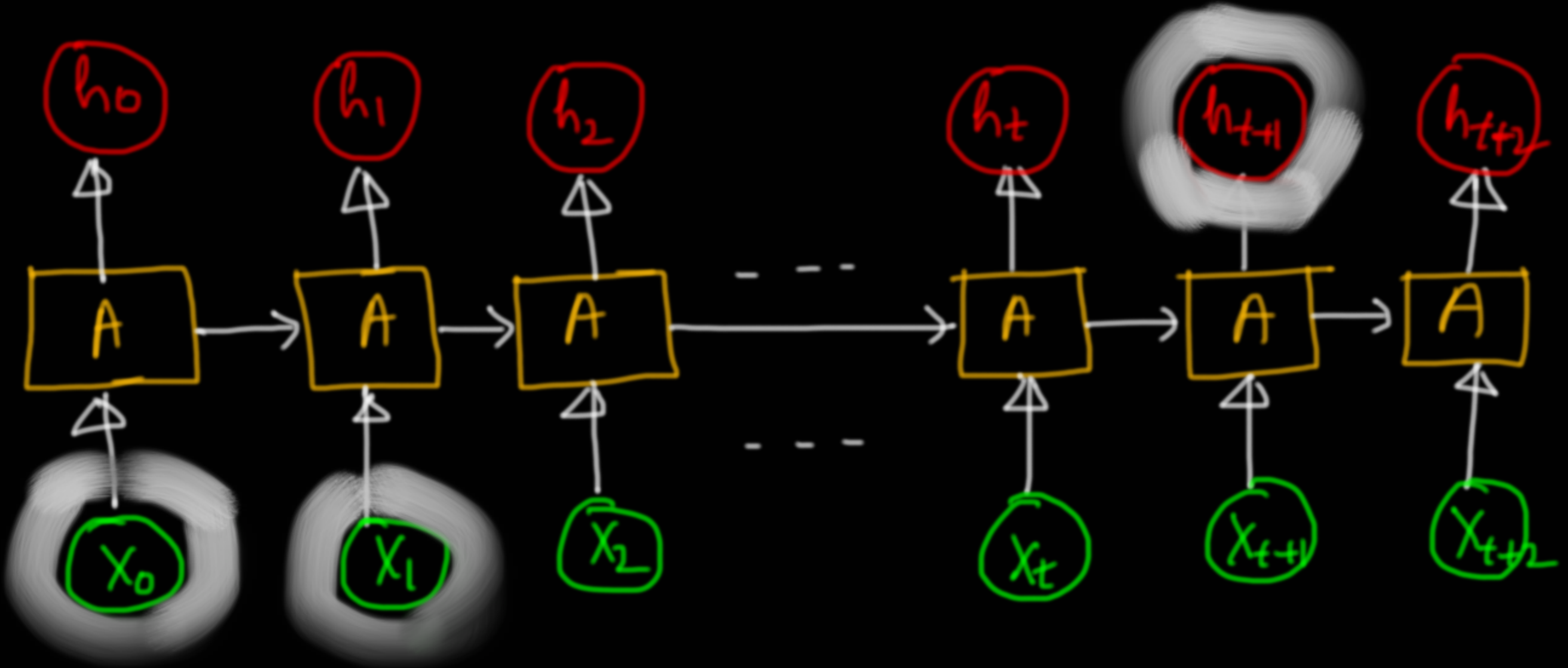
Output is dependent on Previous output

RNN - Memory



Source: Colah’s blog

RNN - Missing Long Term Memory



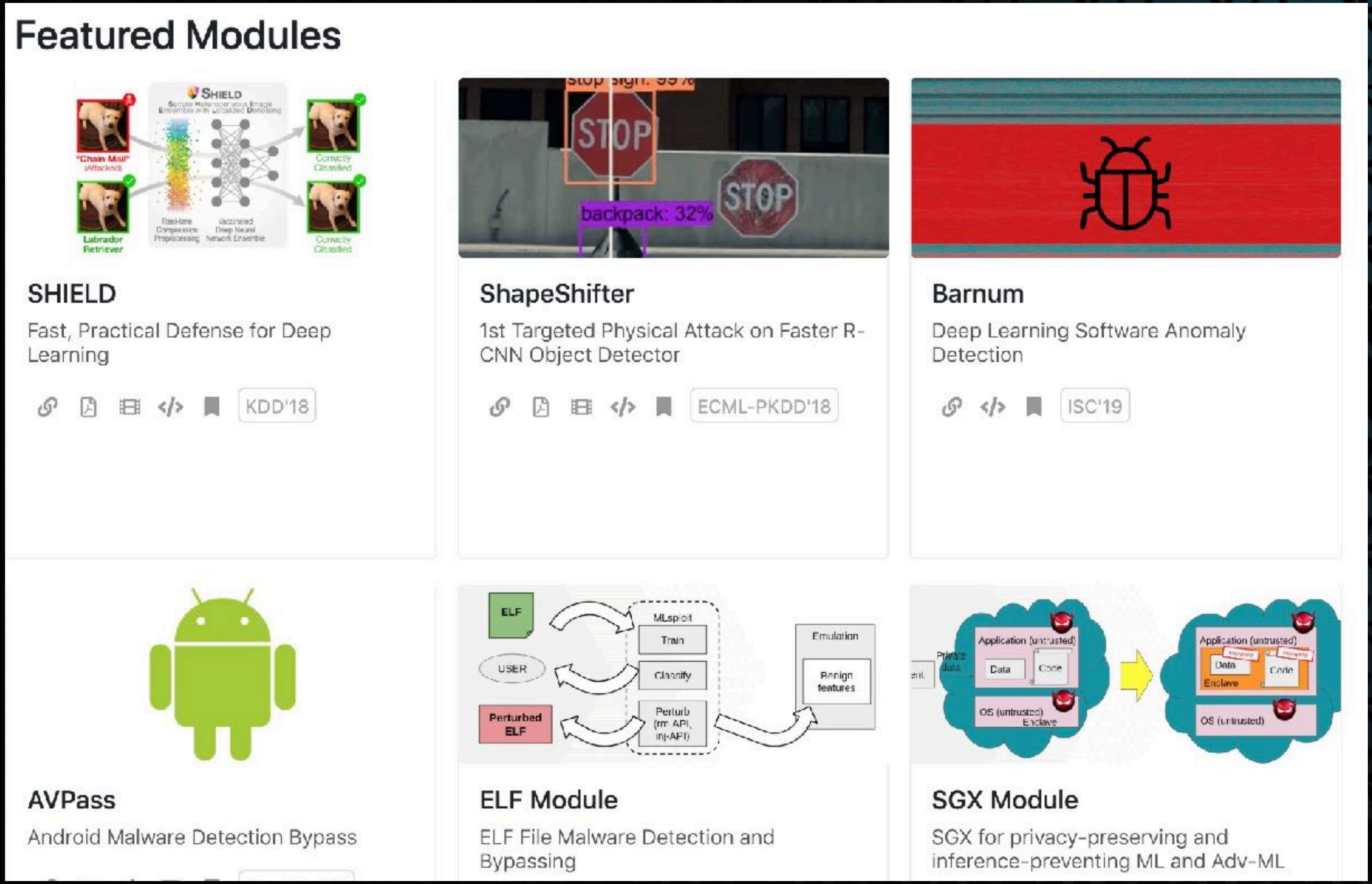
RNN has Vanishing Gradient Problem

How are Adversaries using ML/DL?

Adversarial ML Use-cases

- Discovery/Information gathering
  - By mining social data —>determine a group of people for phishing attack
  - Identify security controls, network flow rules
- Automated phishing
  - SNAP_R tool by John Seymour and Philip Tully
- Password Guessing
  - PassGAN by Briland Hitaj et al.

MLsploit- Adversarial ML



Featured Modules

SHIELD

Fast, Practical Defense for Deep Learning

KDD'18

ShapeShifter

1st Targeted Physical Attack on Faster R-CNN Object Detector

ECML-PKDD'18

Barnum

Deep Learning Software Anomaly Detection

ISC'19

AVPass

Android Malware Detection Bypass

ELF Module

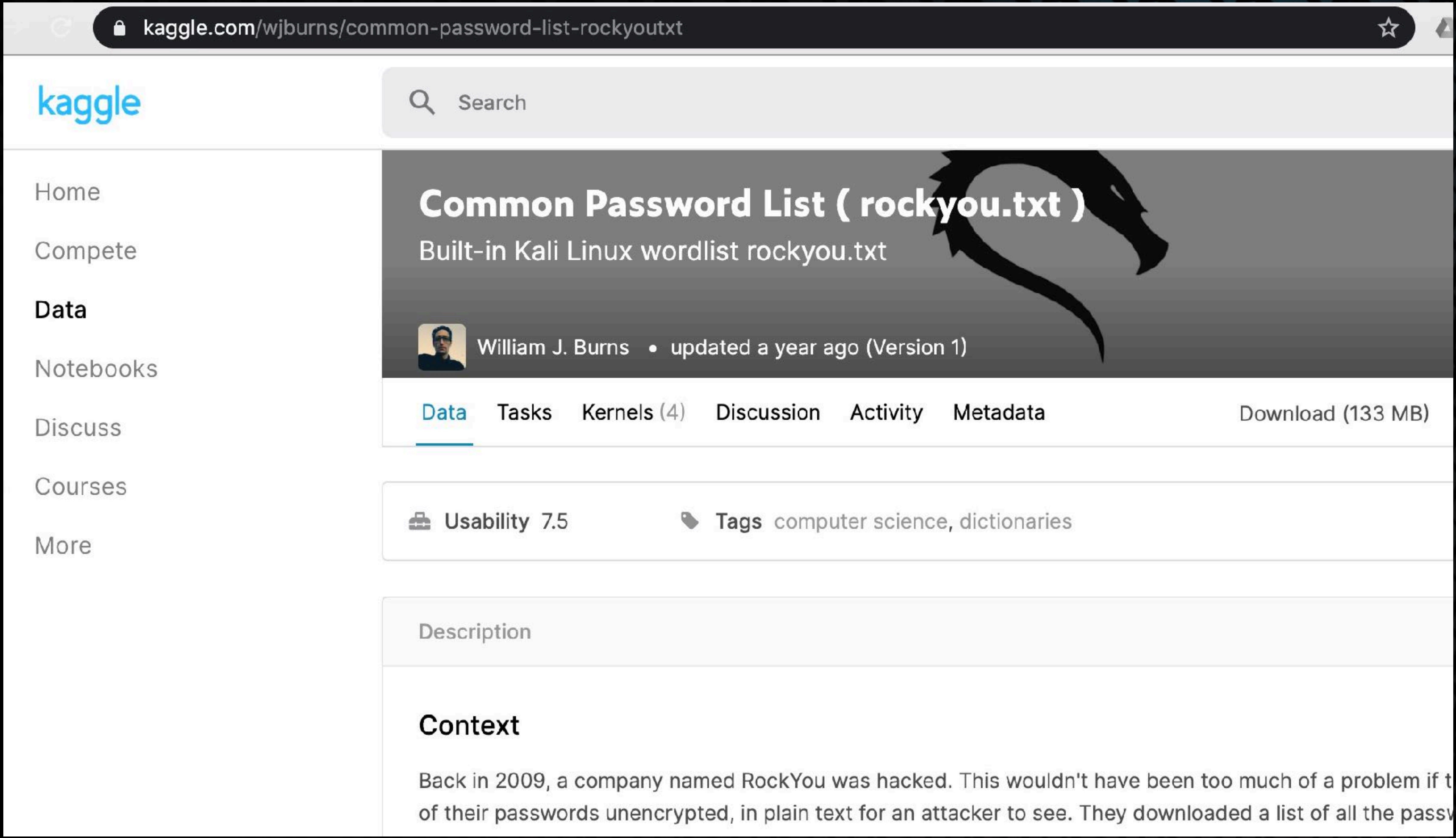
ELF File Malware Detection and Bypassing

SGX Module

SGX for privacy-preserving and inference-preventing ML and Adv-ML

GeorgiaTech & Intel https://mlsploit.github.io/

Case study: Password Generation



Common Password List (rockyou.txt)

Built-in Kali Linux wordlist rockyou.txt

William J. Burns • updated a year ago (Version 1)

Usability 7.5

Tags computer science, dictionaries

Description

Context

Back in 2009, a company named RockYou was hacked. This wouldn't have been too much of a problem if t
of their passwords unencrypted, in plain text for an attacker to see. They downloaded a list of all the passw

Prototype to Product

- How the data will be collected?
  - Data processing pipeline, data security in-transit
  - Access to Security data lake?
- Combining security knowledge along with deep learning model
  - What to combine? How to combine?
- DL Model Training, Storage and Orchestration
  - Logging and RESTful APIs

Team !!