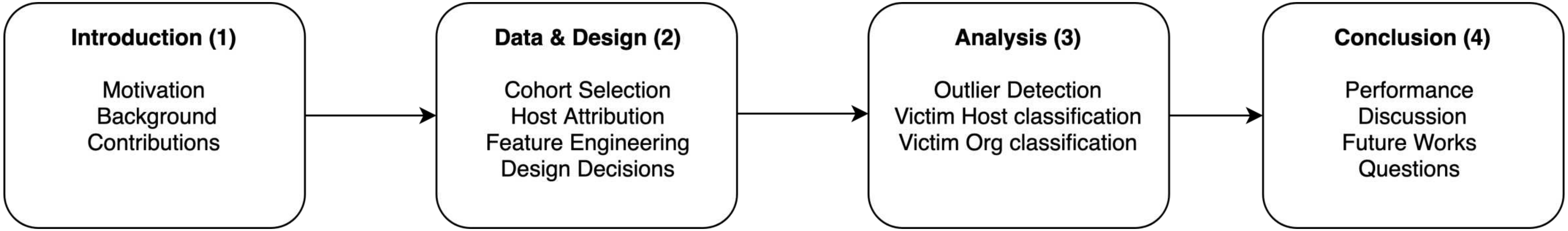
DREXEL UNIVERSITY
College of
Engineering

Security Posture Based Incident Forecasting

Master’s Thesis
Dagmawi Mulugeta
Advisors : Dr. Steven Weber & Ben Goodman
Electrical & Computer Engineering Dep’t
June 05 2019



Introduction (1)

Motivation
Background
Contributions

Data & Design (2)

Cohort Selection
Host Attribution
Feature Engineering
Design Decisions

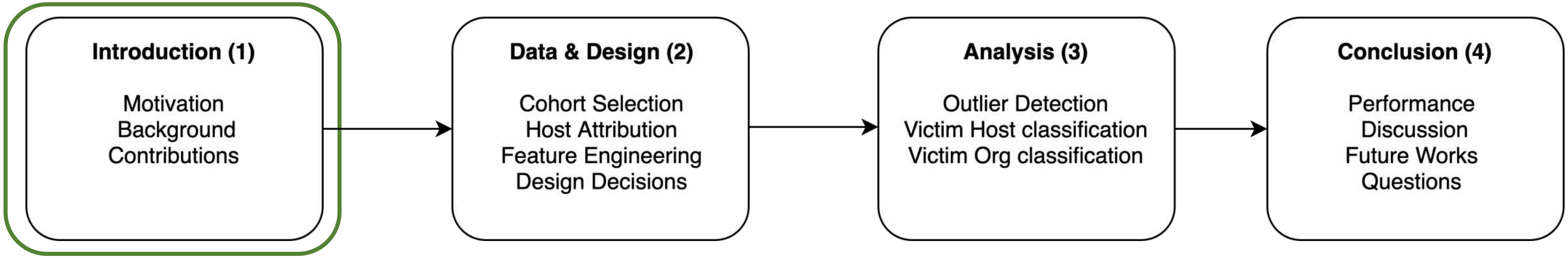
Analysis (3)

Outlier Detection
Victim Host classification
Victim Org classification

Conclusion (4)

Performance
Discussion
Future Works
Questions

Outline



Introduction (1)

Motivation
Background
Contributions

Data & Design (2)

Cohort Selection
Host Attribution
Feature Engineering
Design Decisions

Analysis (3)

Outlier Detection
Victim Host classification
Victim Org classification

Conclusion (4)

Performance
Discussion
Future Works
Questions

Introduction (1)

Motivation

- Privacy Rights Clearinghouse shows 614 hacking or malware incidents that are suspected to have disclosed 914,388,535 sensitive records in 2017-2018 [1]

- Edwards et al. projected that in the 2016-19 time span, breaches could cost north of $179 billion USD [2]

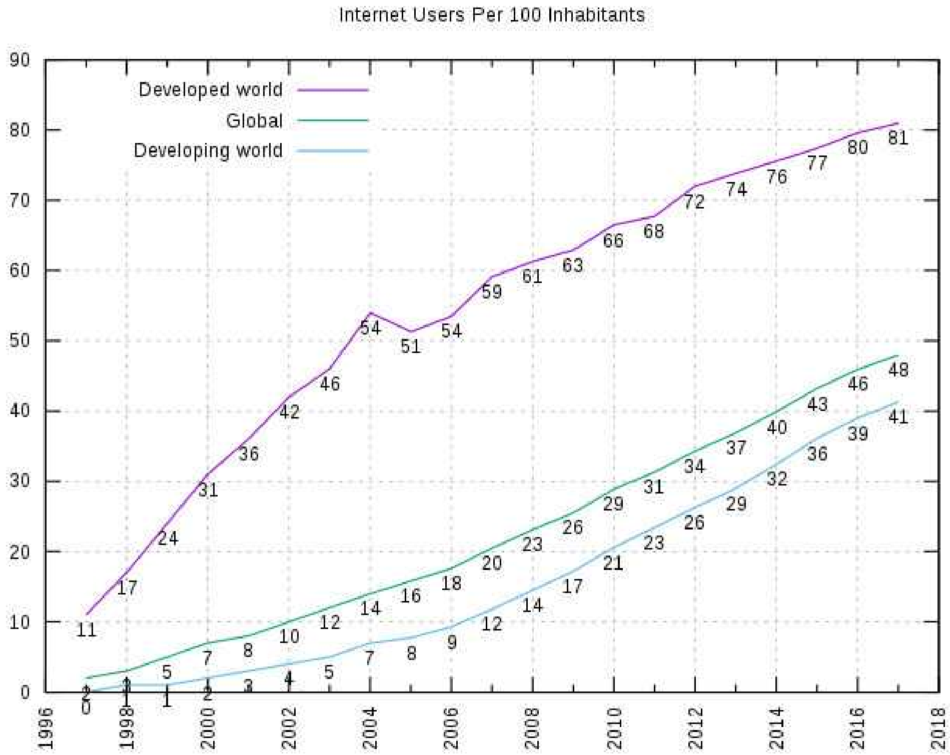
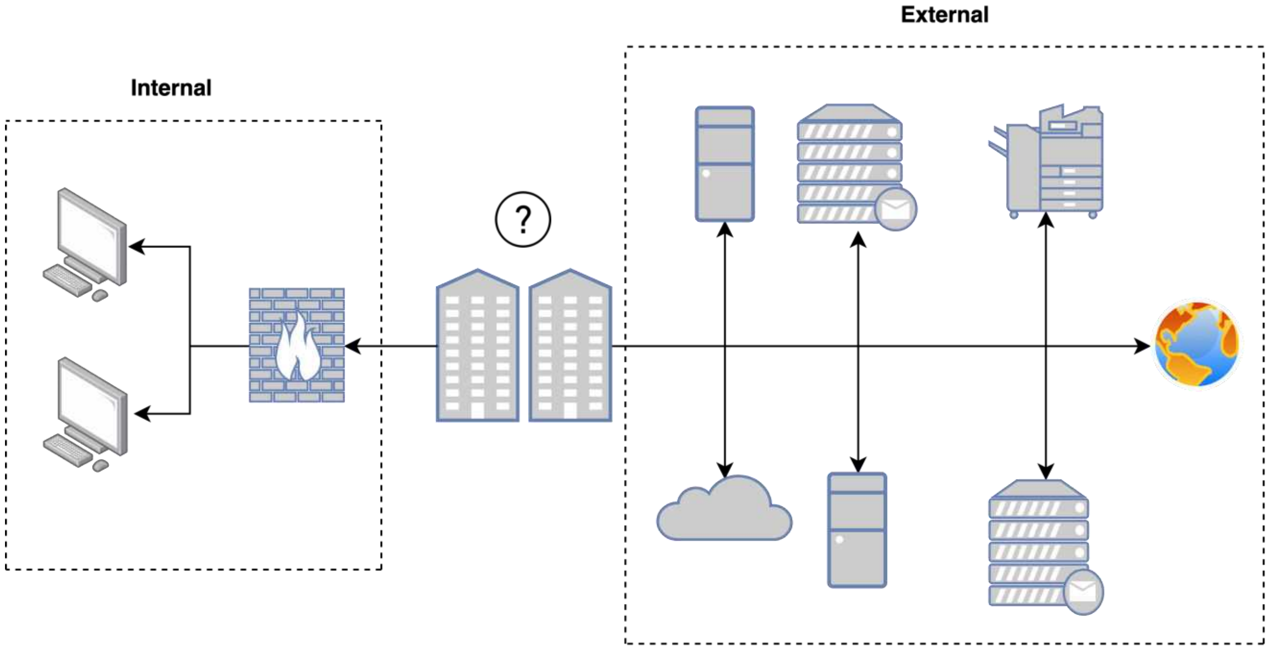


Image Source : [4, 5]

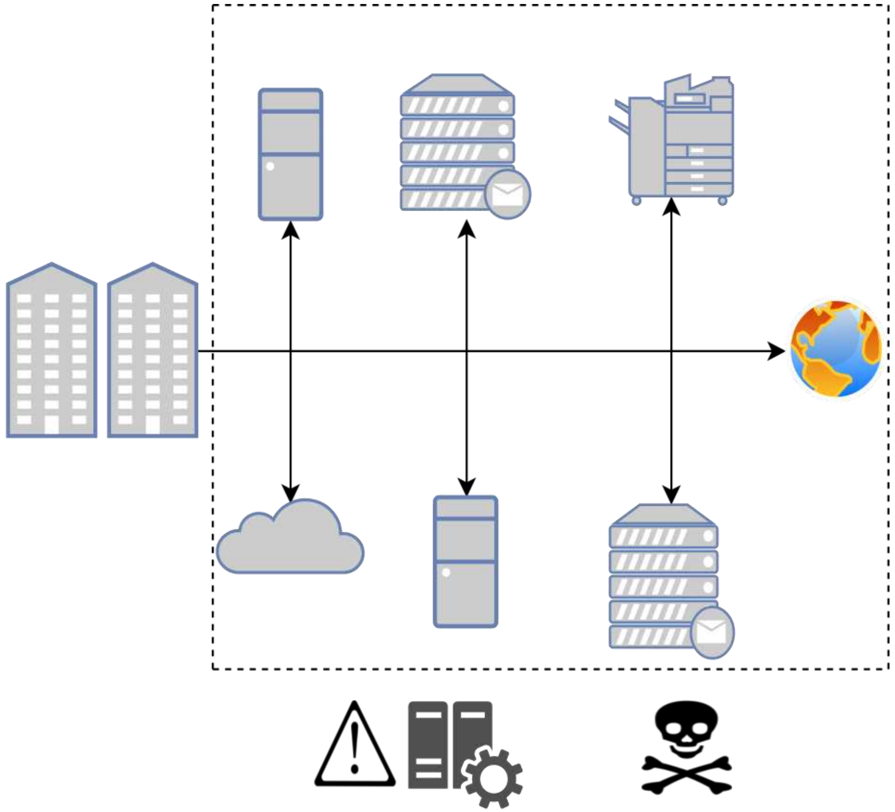
Overview of problem

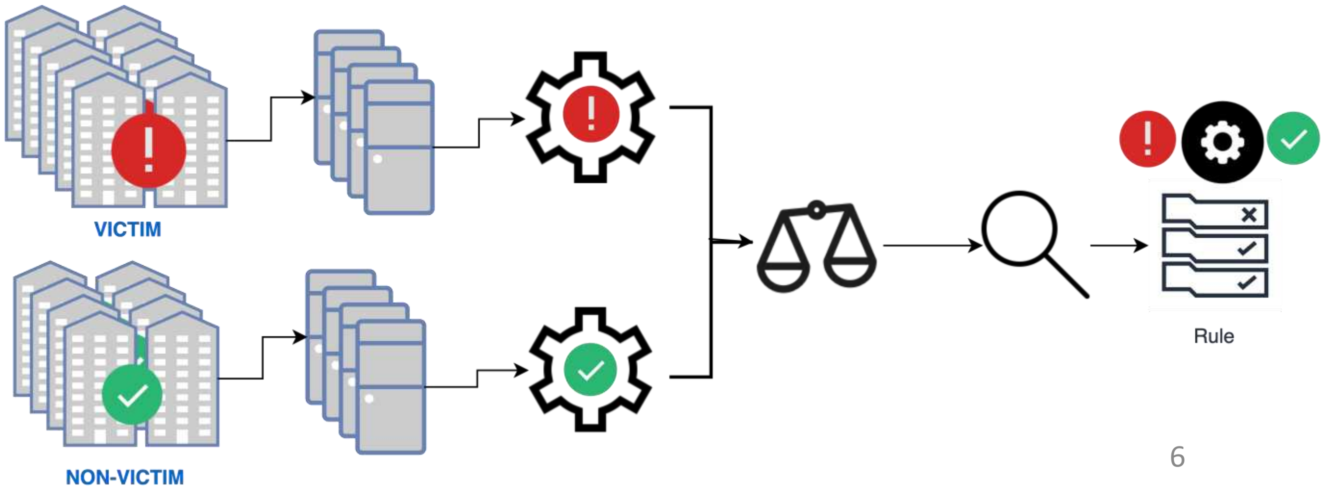
- How to assess the likelihood of security incident? e.g. data breach
- Internal
  - Telemetry, Logs, Network packet captures
- External
  - Web and Mail Server Configurations
- “Similar to rating the fire risk of a building based on a photograph from across the street.”[3]



Relevant Works

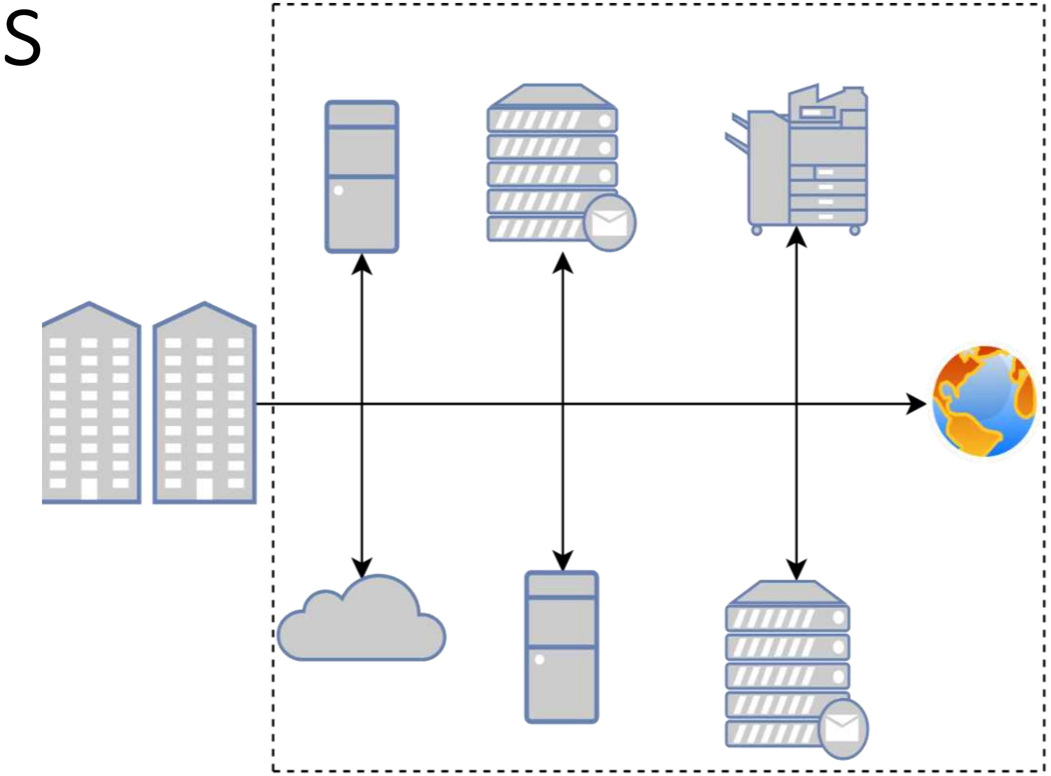
- *“On the Mismanagement and Maliciousness of Networks” 2014* [7]
  - Show correlation & causation between misconfiguration and maliciousness
- *“Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents” 2015* [8]
  - analyzed a data set of 1000 security incident reports (700 from VERIS, 300 from Hackmagedon, and 150 from WHID)
  - 90% accuracy and 10% FPR
- Industry
  - FICO ESS [23]
  - BitSight [24]
  - SecurityScorecard [25]
  - UpGuard [26]



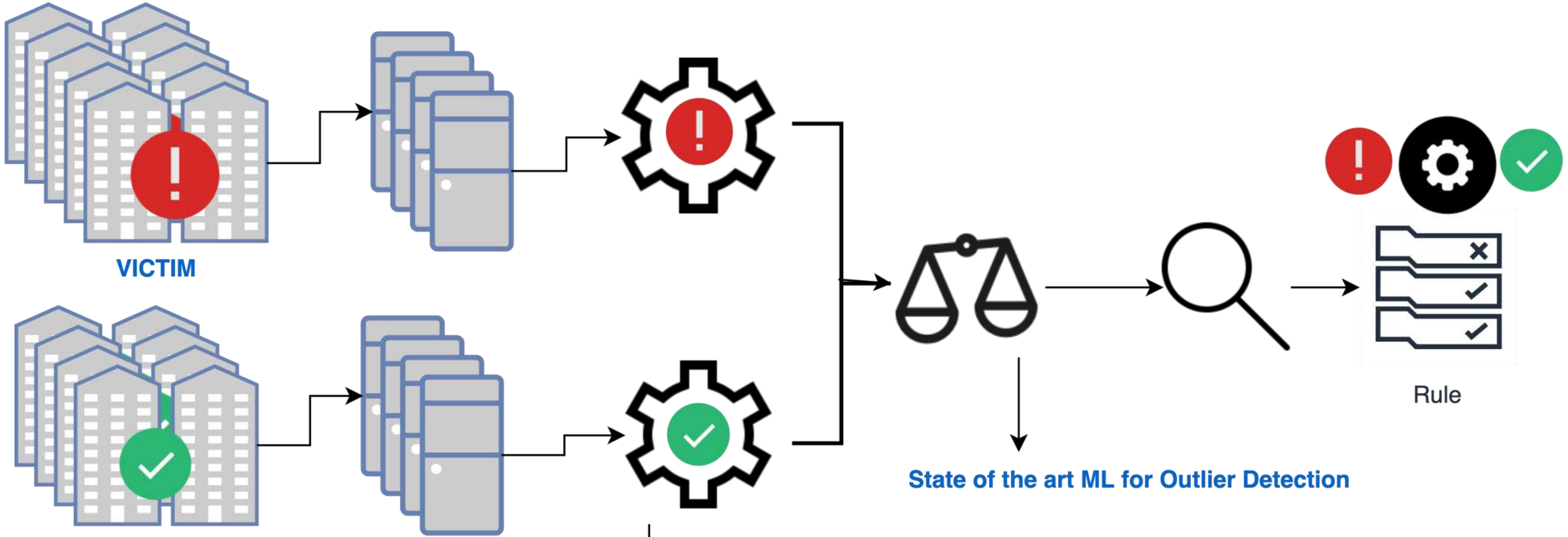


Proposed Solution : Censys

- Censys [9] is public search engine and data processing facility
  - Granted access to database
- ZMap [10] to scan the public IPv4 space in 45 minutes
- **Non-goals**
  - Vulnerability analysis
  - Intrusion Point Detection



Novel Contributions

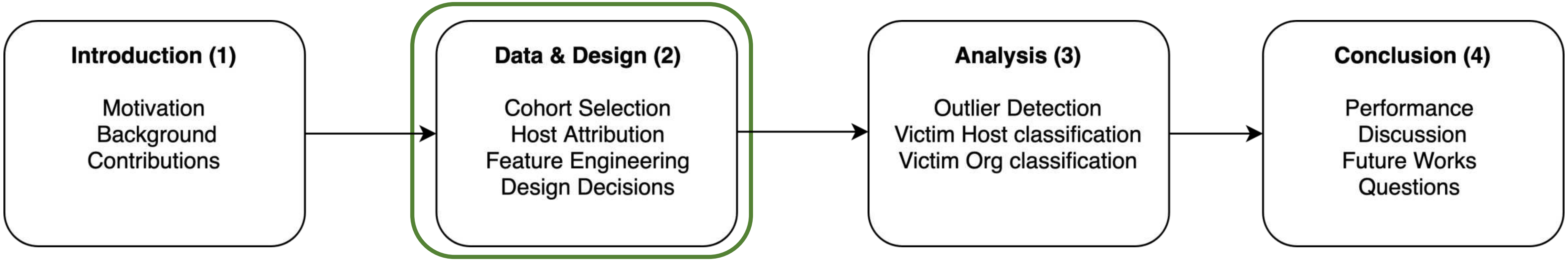


State of the art ML for Outlier Detection

More Holistic representation

Improved Attribution

Heterogenous Non-Victim Collection



Introduction (1)

Motivation
Background
Contributions

Data & Design (2)

Cohort Selection
Host Attribution
Feature Engineering
Design Decisions

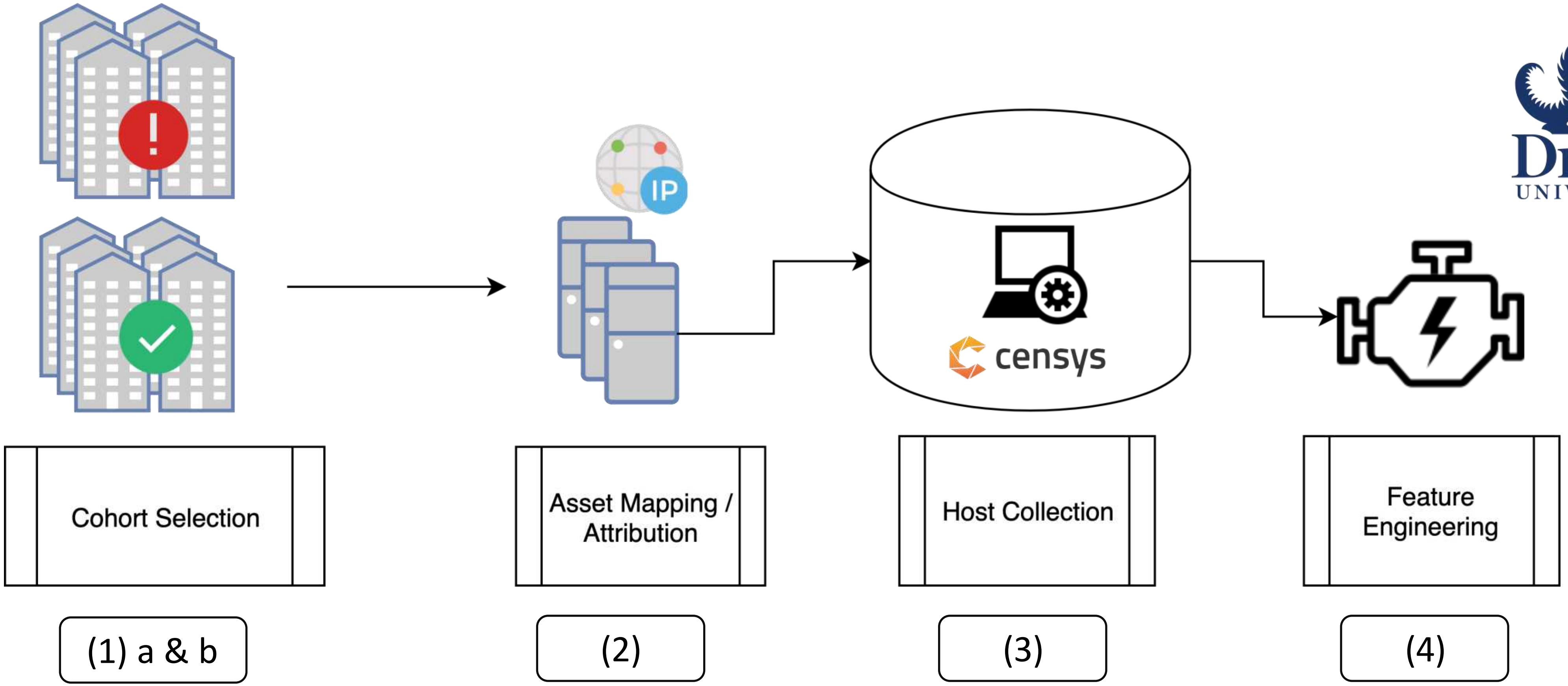
Analysis (3)

Outlier Detection
Victim Host classification
Victim Org classification

Conclusion (4)

Performance
Discussion
Future Works
Questions

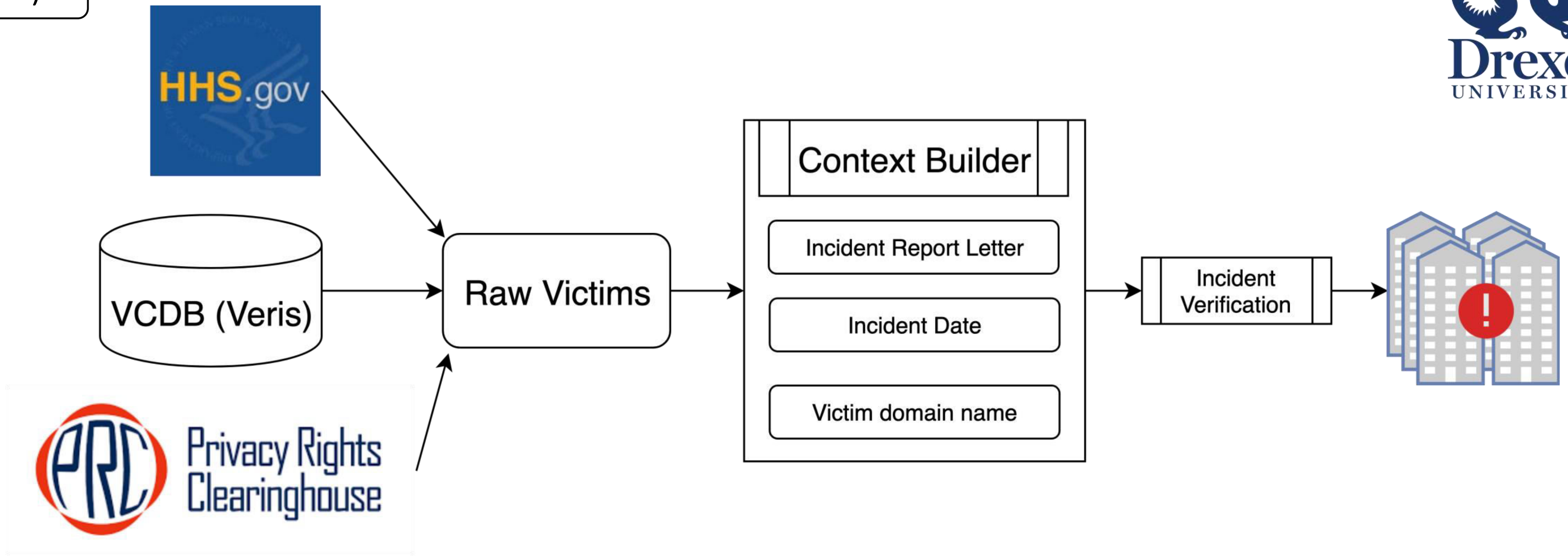
Data & Design (2)



Data Pipeline

- Cohort refers to a collection of organizations (both victim and non-victim)
- Time span : Jan/01/2017 - Jan/01/2019
- Digital asset could be IPv4 address or domain name

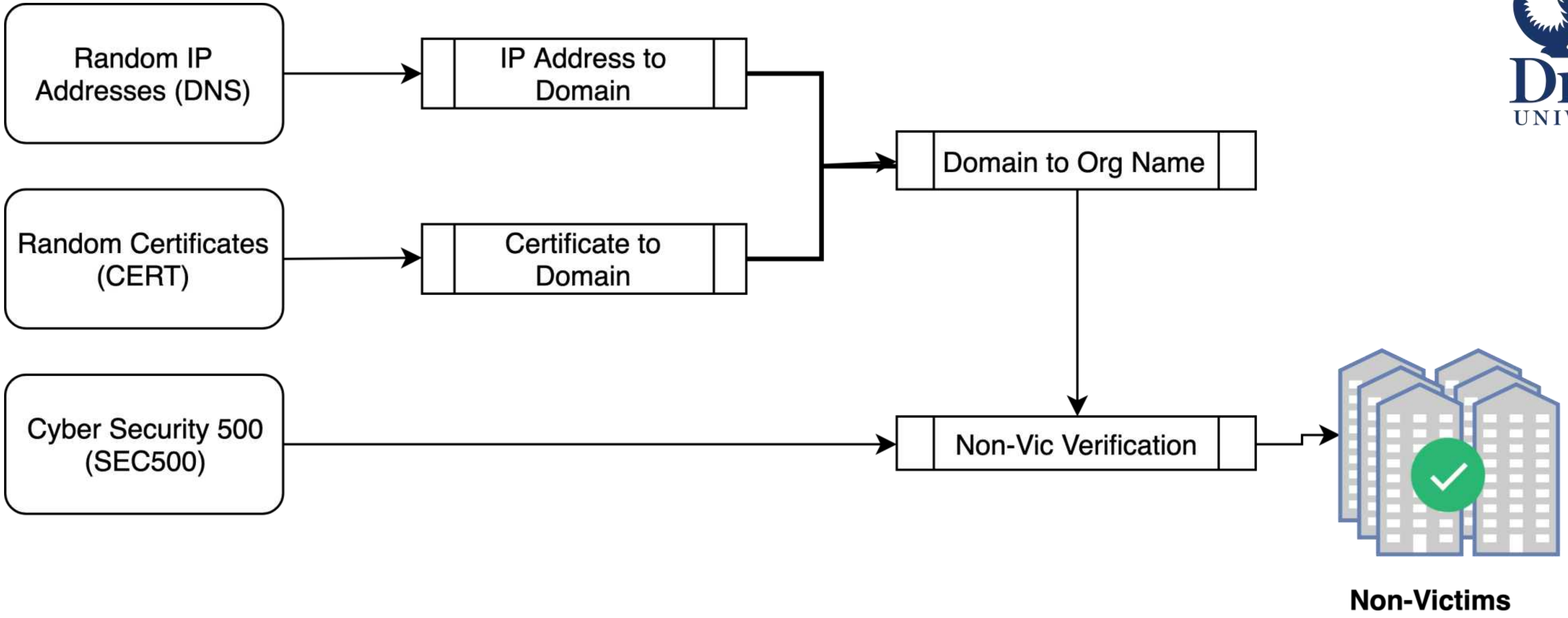
(1 of 4) a



Victim Selection

- Final count was 263 orgs, of which we randomly selected 200

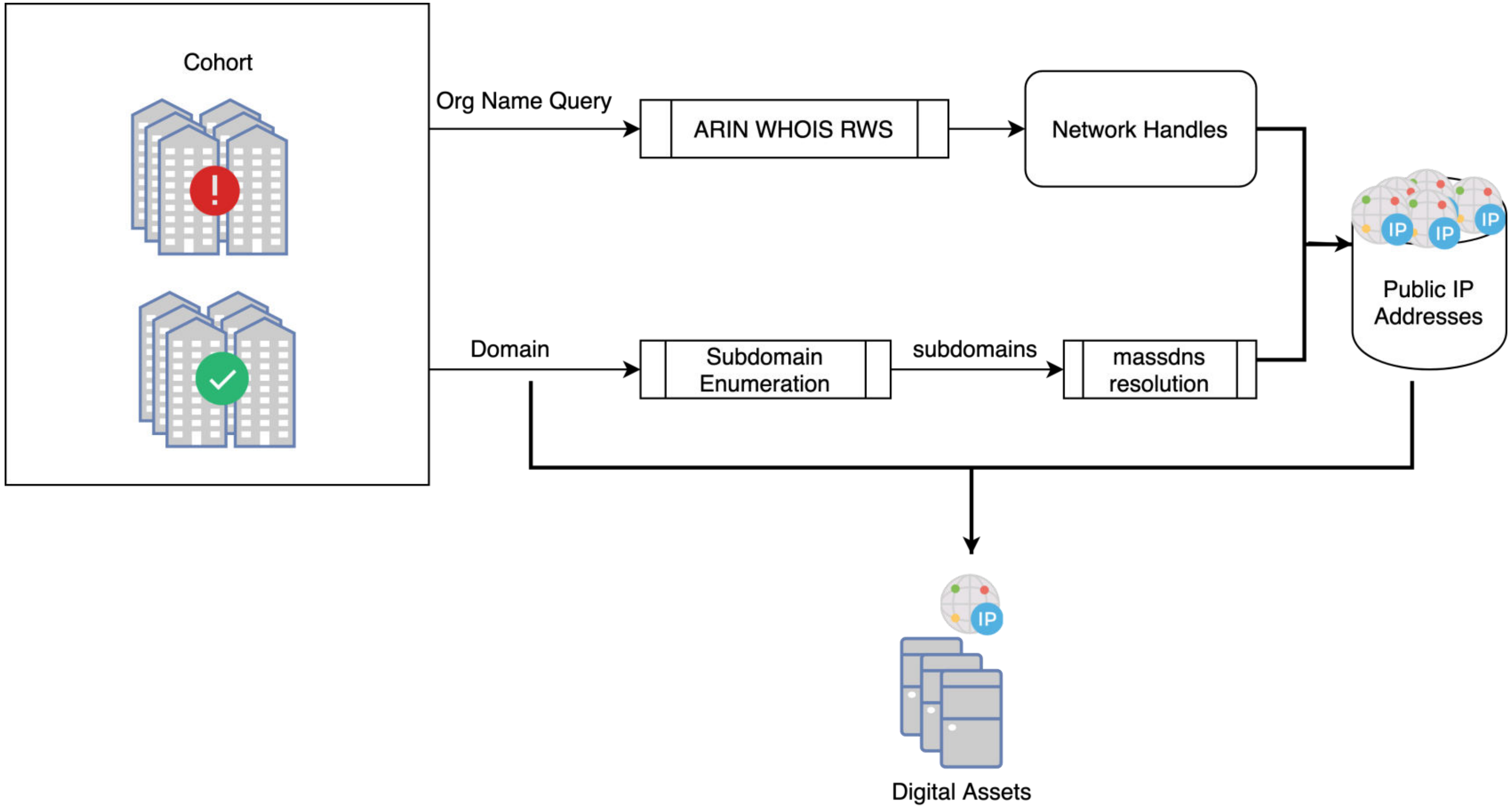
(1 of 4) b



Non-Victim Selection

- Selected 200 non-victims per selection method
- Randomly assigned lookup date within time span
- Collected 800 total (785 unique) organizations

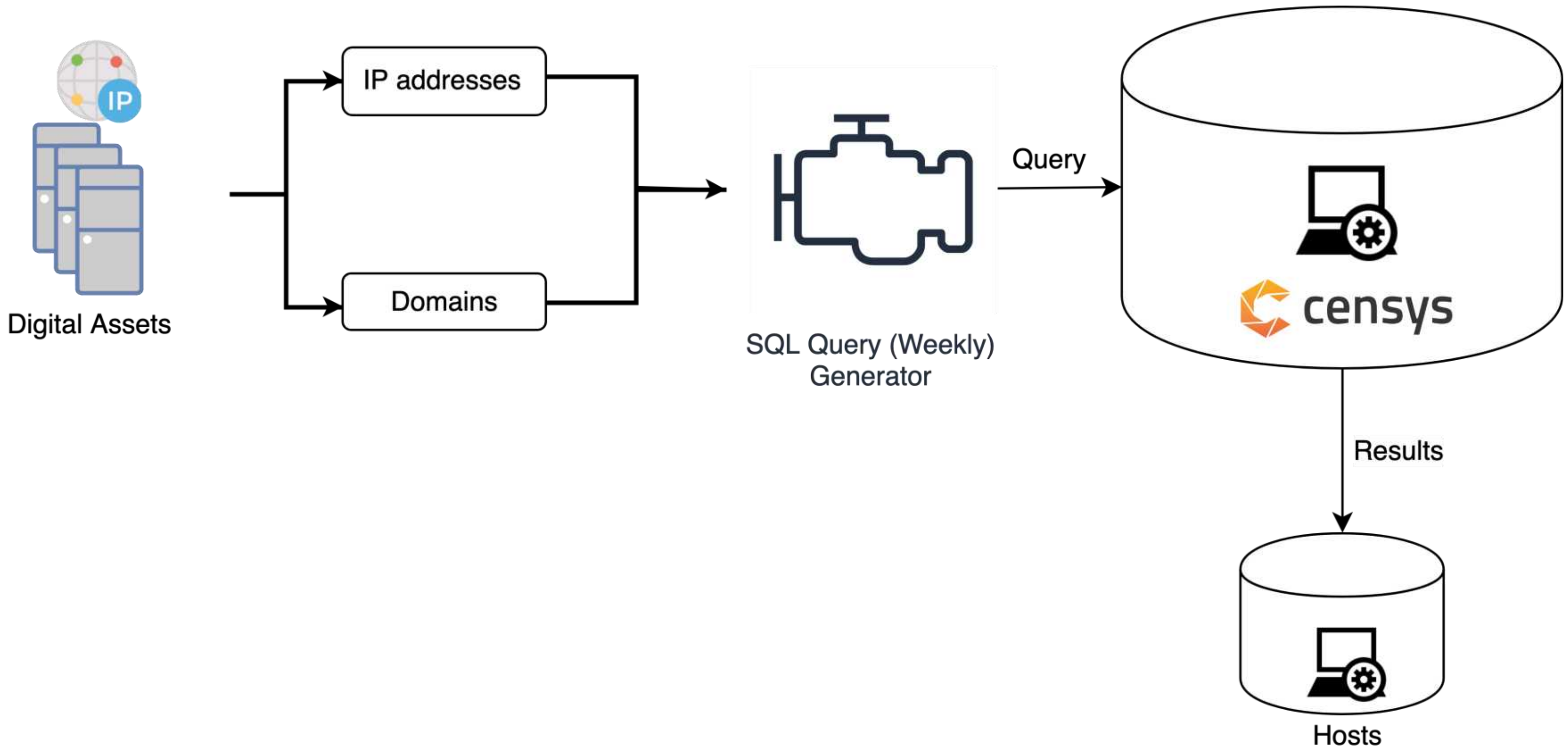
(2 of 4)



Asset Attribution

- **Foot printing** or **Host (Asset) attribution** is process of finding digital assets associated with a certain organization
- Subdomain Enumeration (*identifies all the subdomain for a specific domain*)
  - Tools : Amass, dnsrecon, Sublist3r, SubFinder, etc…
- Research Access : RiskIQ [11], Binary Edge [12], Security Trails [13], VirusTotal [14]

(3 of 4)



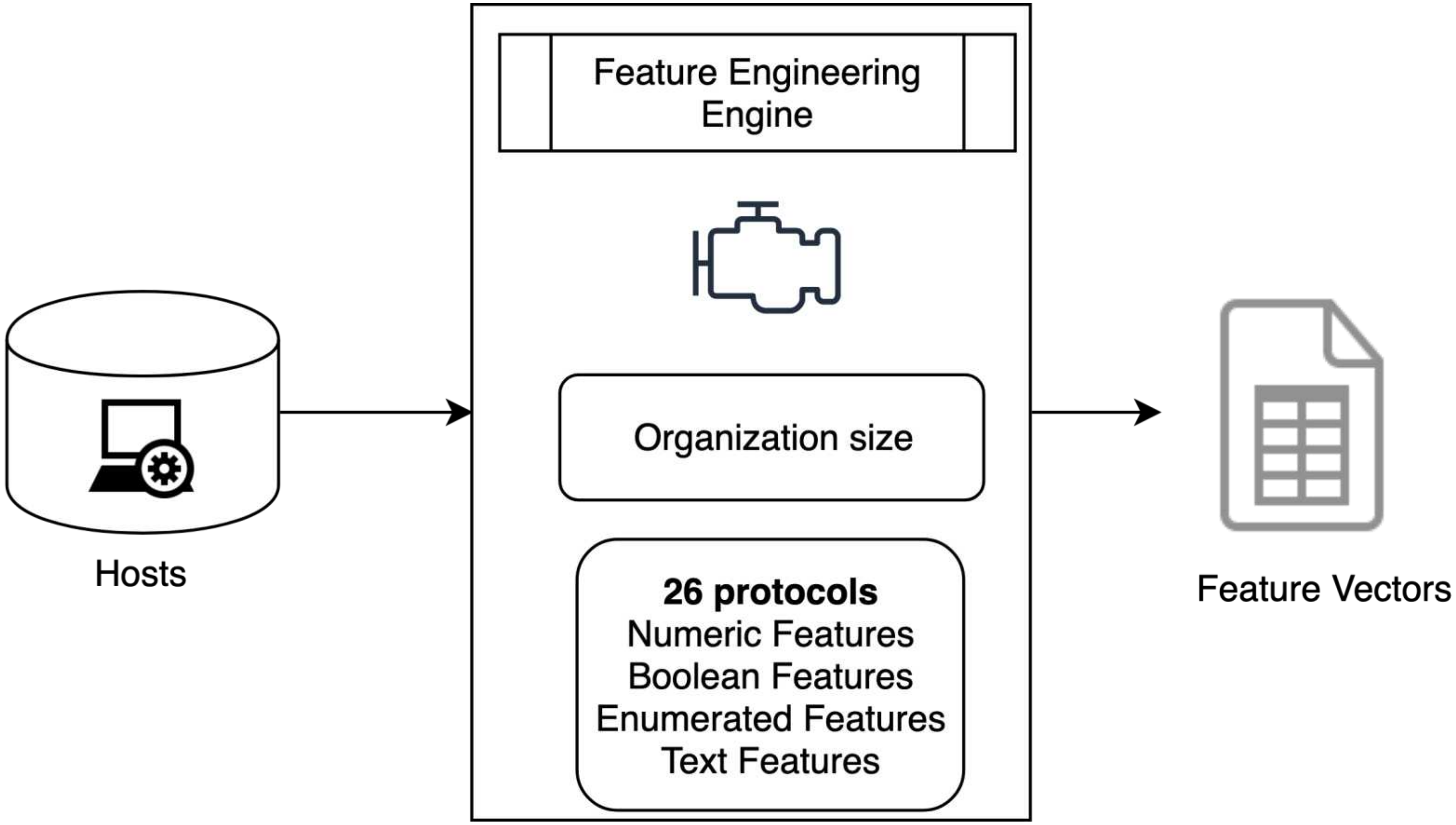
Host collection

- Censys
  - Scan result accessed through Big Query API
- Aggregated lookup and split for organizations in the same week
  - Fiscal Constraints
  - Assumption that posture on Monday is similar to one on Friday

Host Collection (Cont’d)

Cohort Subset	Organizations	Hosts	Avg host / org
VICTIM (BREACH)	199	48017	241.3
CERT	198	388552	1962.4
DNS	194	271844	1401.3
SEC500	200	55372	276.9
All	**791**	**763785**	**965.6**
All (Unique)	**776**	**714244**	**920.4**

(4 of 4)

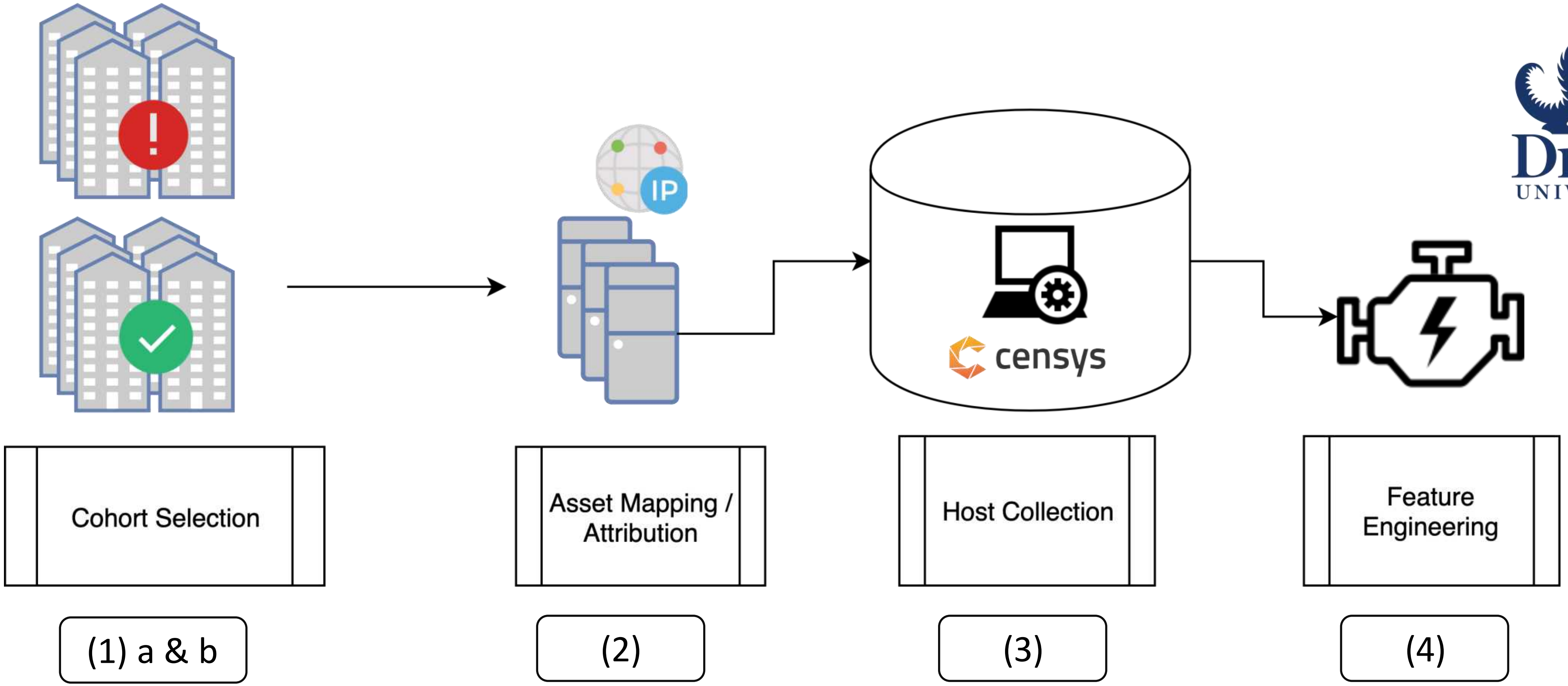


Feature Engineering

- Numeric: e.g. Validity Length in seconds for HTTPS certificate
- Boolean: e.g. Is HTTPS running on a host
- Enumerated: **One hot encoded into list of Boolean fields**
  - e.g. Is HTTPS TLS version 1.0, 1.1, or 1.2? Results in 3 Boolean features
- Text:
  - Used Censys reporter to collect top 10 - 20 values for field
  - Then treated like enumerated field
  - e.g. Operating System of a host

Feature Engineering - Total 1,386 features

Feature	Count	Feature	Count
P995_POP3S	77	P993_IMAPS	74
P8888_HTTP	43	P80_HTTP	96
P8080_HTTP	74	P7547_CWMP	22
P631_IPP	20	P587_SMTP	53
P5432_POSTGRES	32	P53_DNS	5
P502_MODBUS	5	P47808_BACNET	64
P445_SMB	1	P443_HTTPS	112
P3306_MYSQL	69	P25_SMTP	99
P23_TELNET	3	P2323_TELNET	2
P22_SSH	204	P21_FTP	26
P1911_FOX	54	P1900_UPNP	2
P1521_ORACLE	5	P143_IMAP	87
P1433_MSSQL	33	P110_POP3	77
P102_S7	2	ORG_SIZE	1
NUM_PORTS	1	METADATA_DESCRIPTION	17
COMPANY_NAME_IN_ASN	1	AUTONOMOUS_SYSTEM	15



Cohort Selection

(1) a & b

Asset Mapping / Attribution

(2)

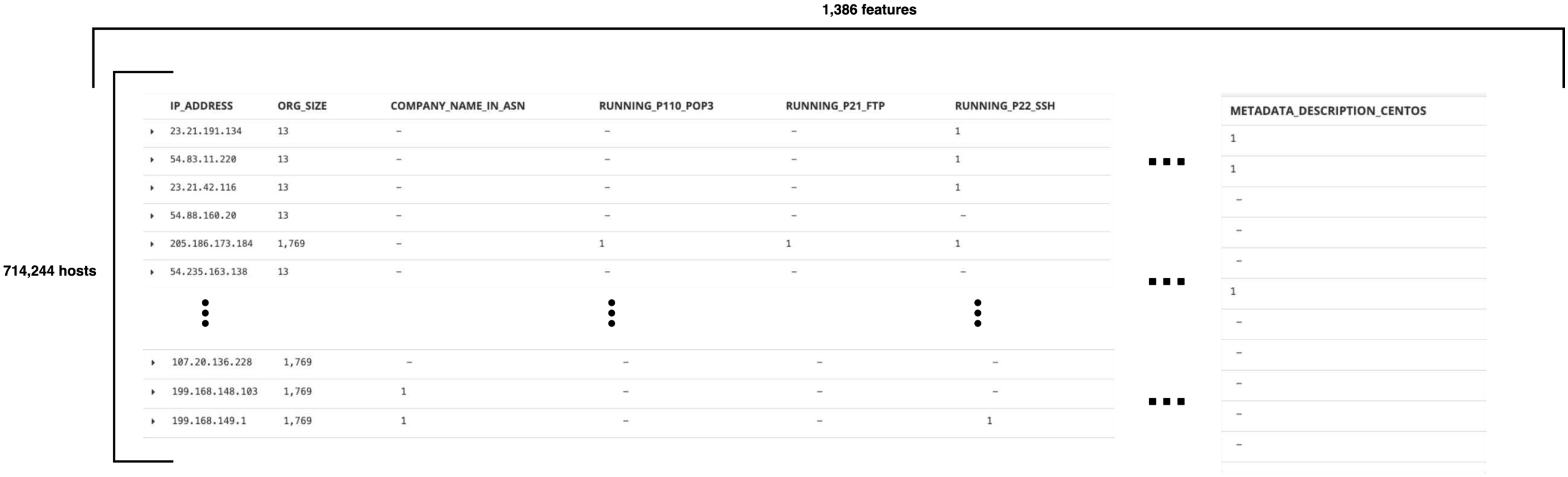
Host Collection

(3)

Feature Engineering

(4)

Data Pipeline Recap



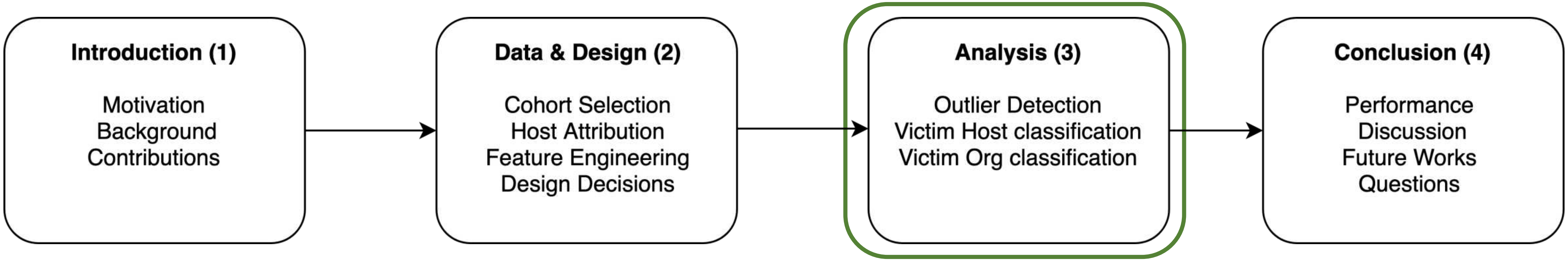
	IP_ADDRESS	ORG_SIZE	COMPANY_NAME_IN_ASN	RUNNING_P110_POP3	RUNNING_P21_FTP	RUNNING_P22_SSH
▸	23.21.191.134	13	–	–	–	1
▸	54.83.11.220	13	–	–	–	1
▸	23.21.42.116	13	–	–	–	1
▸	54.88.160.20	13	–	–	–	–
▸	205.186.173.184	1,769	–	1	1	1
▸	54.235.163.138	13	–	–	–	–
	⋮			⋮		⋮
▸	107.20.136.228	1,769	–	–	–	–
▸	199.168.148.103	1,769	1	–	–	–
▸	199.168.149.1	1,769	1	–	–	1

METADATA_DESCRIPTION_CENTOS
1
1
–
–
–
1
–
–
–
–
–

Total data collected
(714,244 hosts x 1,386 features)

Design Decisions

- Cohort Selection
  - Assumed non-victims have not had a security incident
  - Assigned random dates to the non-victim organizations
  - Analyzed hacking / malware incidents only
  - Did not double sample organizations
- Host Attribution
  - Attributed only one sample domain for an organization
  - Collected maximum 256 ARIN network handles
- Host Collection
  - Assumed all organizations have hosts in Censys
- Feature Engineering
  - Assume that feature count imbalance among protocols is not an issue
  - Extracted no inter host information (except ORG_SIZE).
    - e.g. Number of HTTPS servers



Introduction (1)

Motivation
Background
Contributions

Data & Design (2)

Cohort Selection
Host Attribution
Feature Engineering
Design Decisions

Analysis (3)

Outlier Detection
Victim Host classification
Victim Org classification

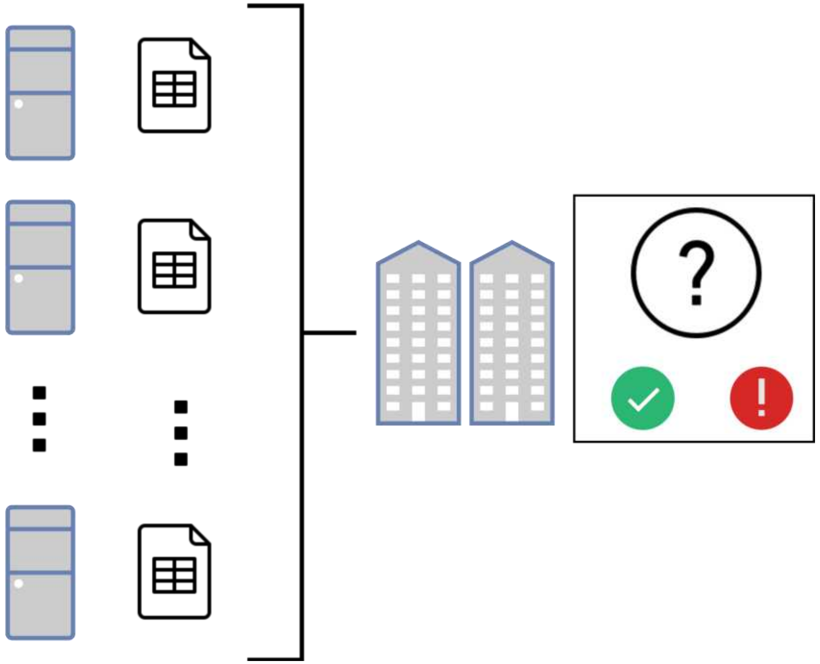
Conclusion (4)

Performance
Discussion
Future Works
Questions

Analysis (3)

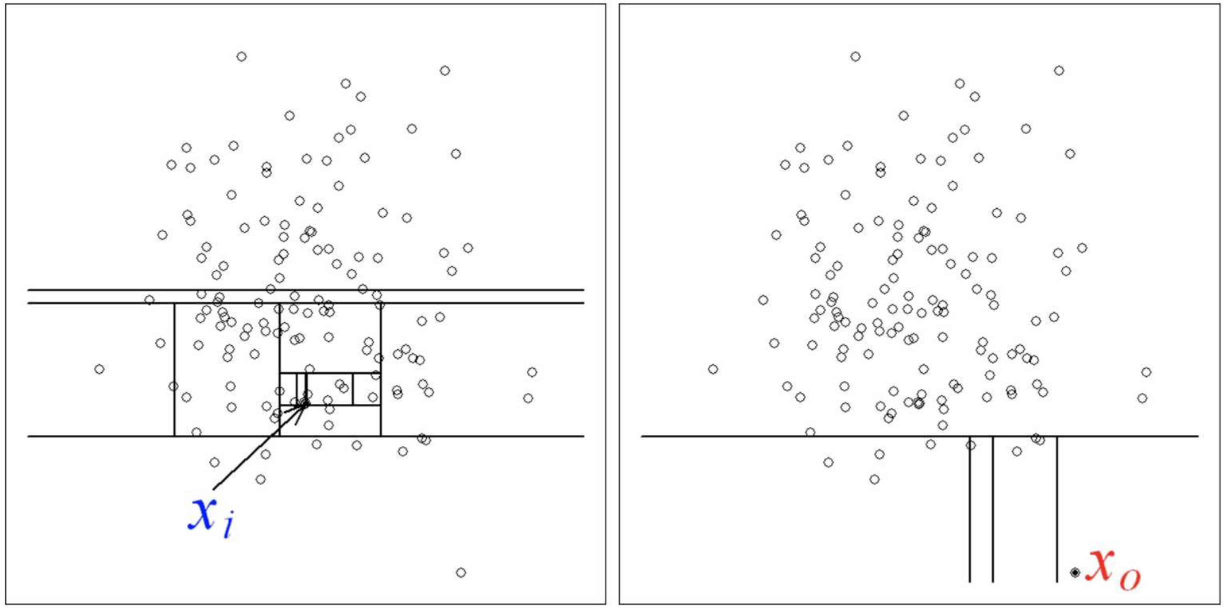
Experimental Setup

- **Issue** : Features vectors at different resolution than target label
- Possible approaches
  - Average features from all the hosts
  - Assign label to every host in an organization
  - Graphical approach, where nodes are host machines
  - Sampling to locate “interesting” hosts (outlier detection)

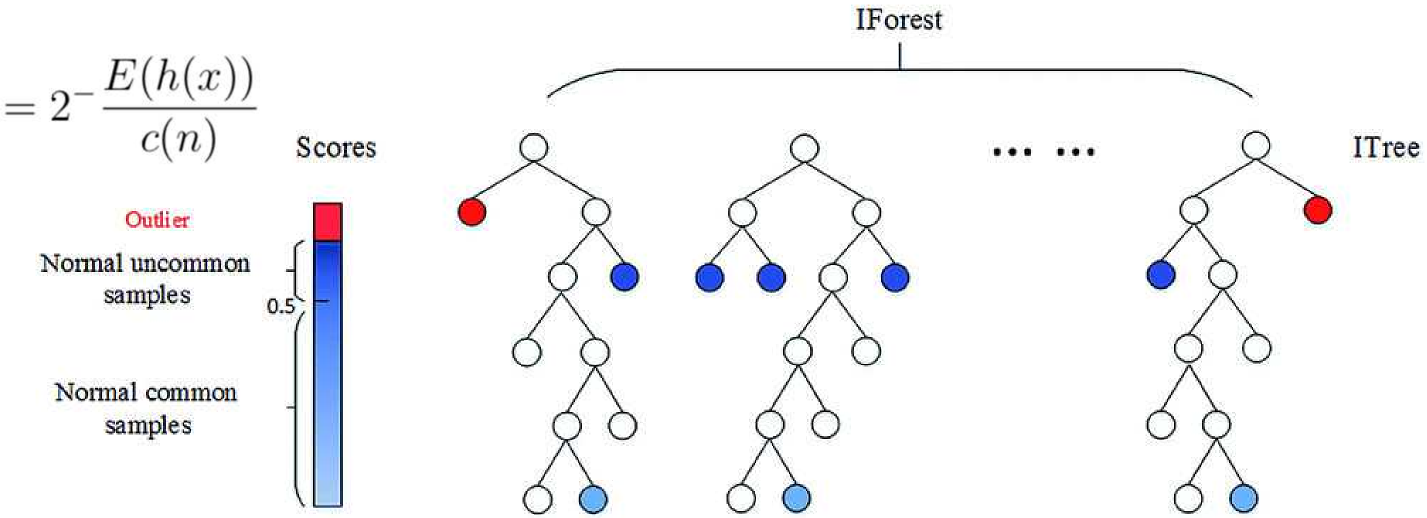


Outlier detection

- Incorrect and weak configurations stand out compared to peer hosts
- Do not needlessly analyze similar hosts
- Reduce the data space to improve run time



$$s(x,n) = 2^{-\frac{E(h(x))}{c(n)}}$$

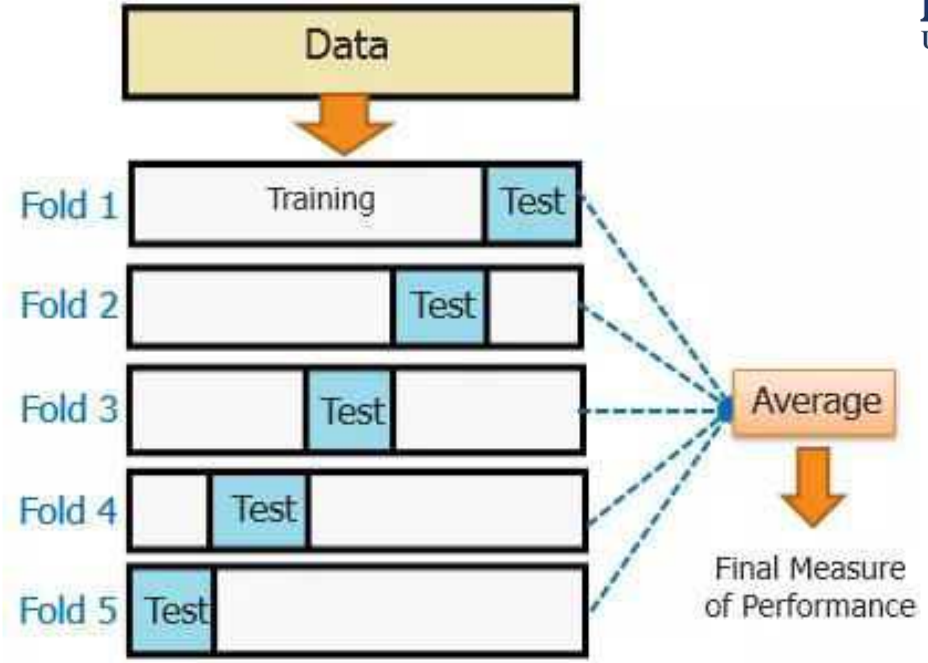


- Isolation Forest Algorithm[15]
- Collected 45,329 outliers (6%)

IMAGE SOURCE : [15]

Classification(1 of 2)

- Cross Validation



- RFE

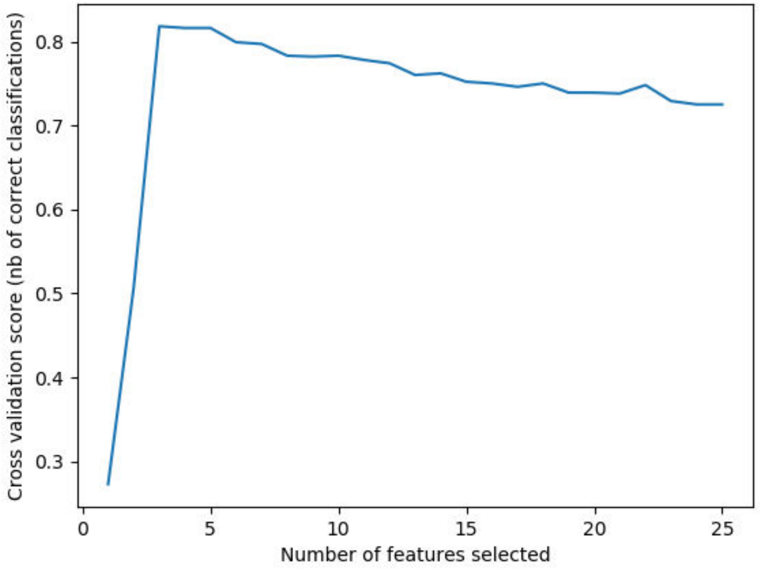
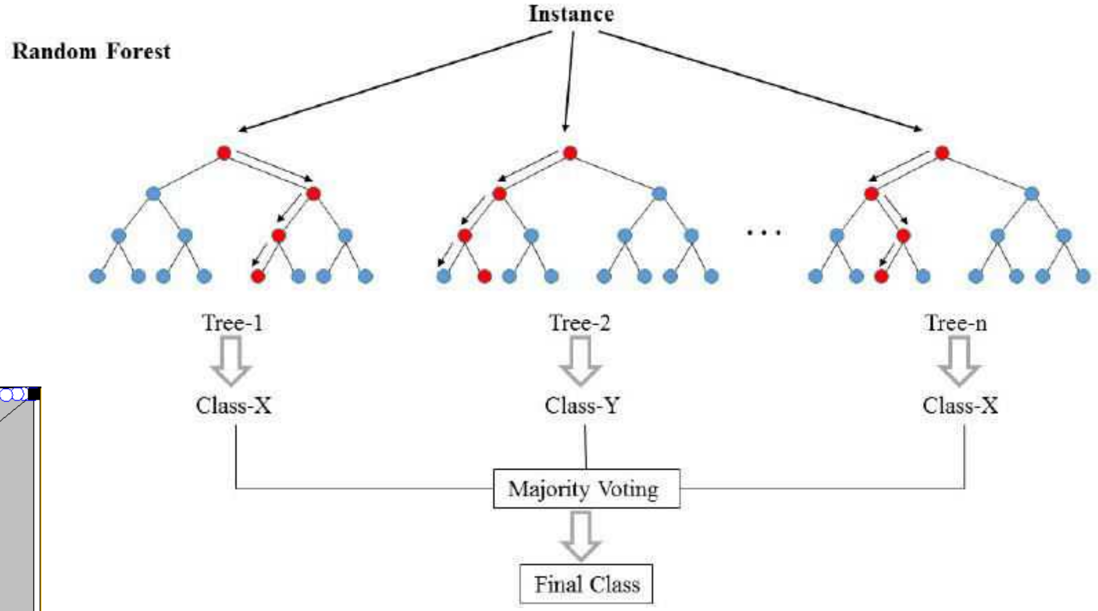


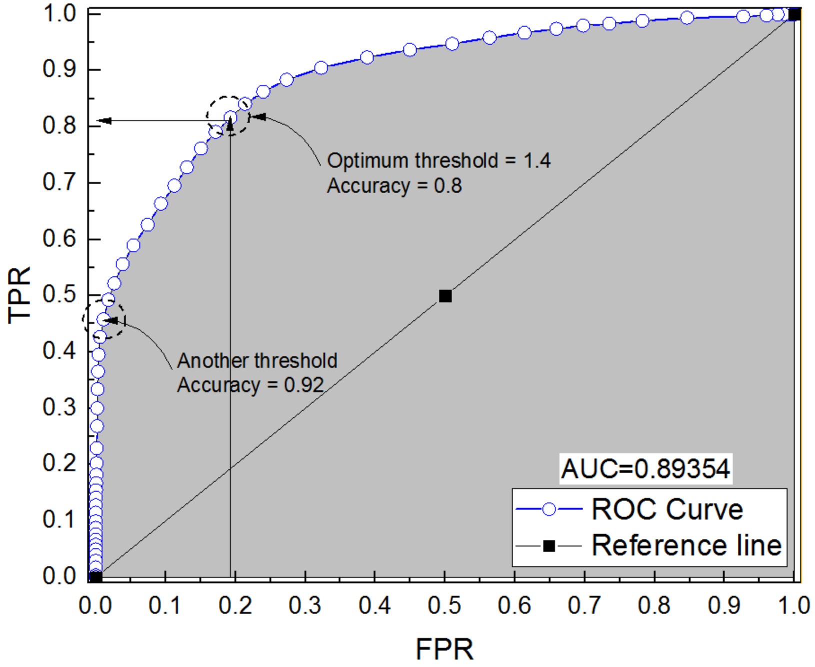
Image Source:[16,17,18,19]

Classification(2 of 2)

- Random Forest



- ROC Curve

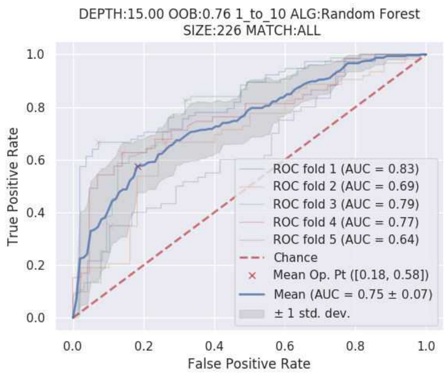


Outlier Detection: Easier for larger organizations

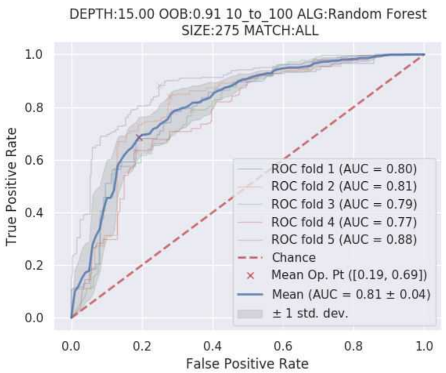
- **Interesting Question** : Are there general rules that make a host an outlier?

- Analyzed 7,208 inliers and 7,312 outliers (20 per org)

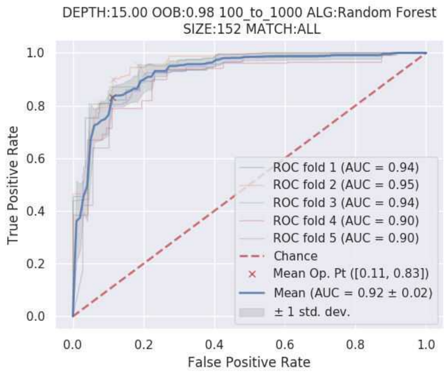
- Inlier has target label 0
- Outlier has target label 1
- Separated based on organization size



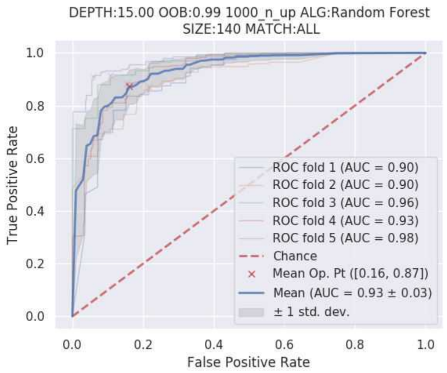
Size: <= 10



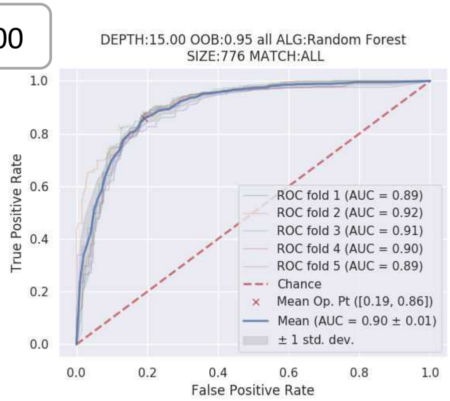
Size: 10 to 100



Size: 100 to 1000

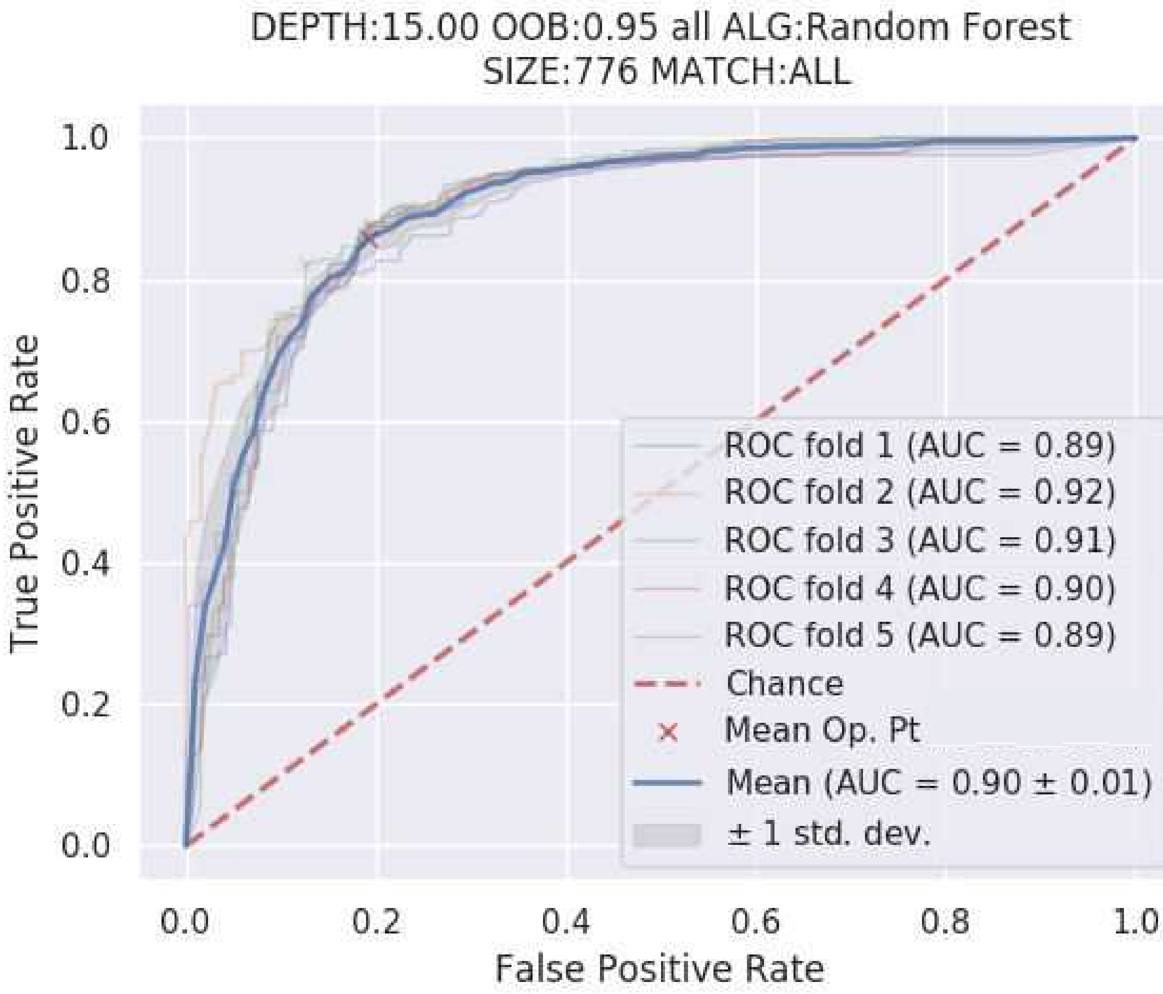


Size: >= 1000



Size: all

Outlier classification – all sizes

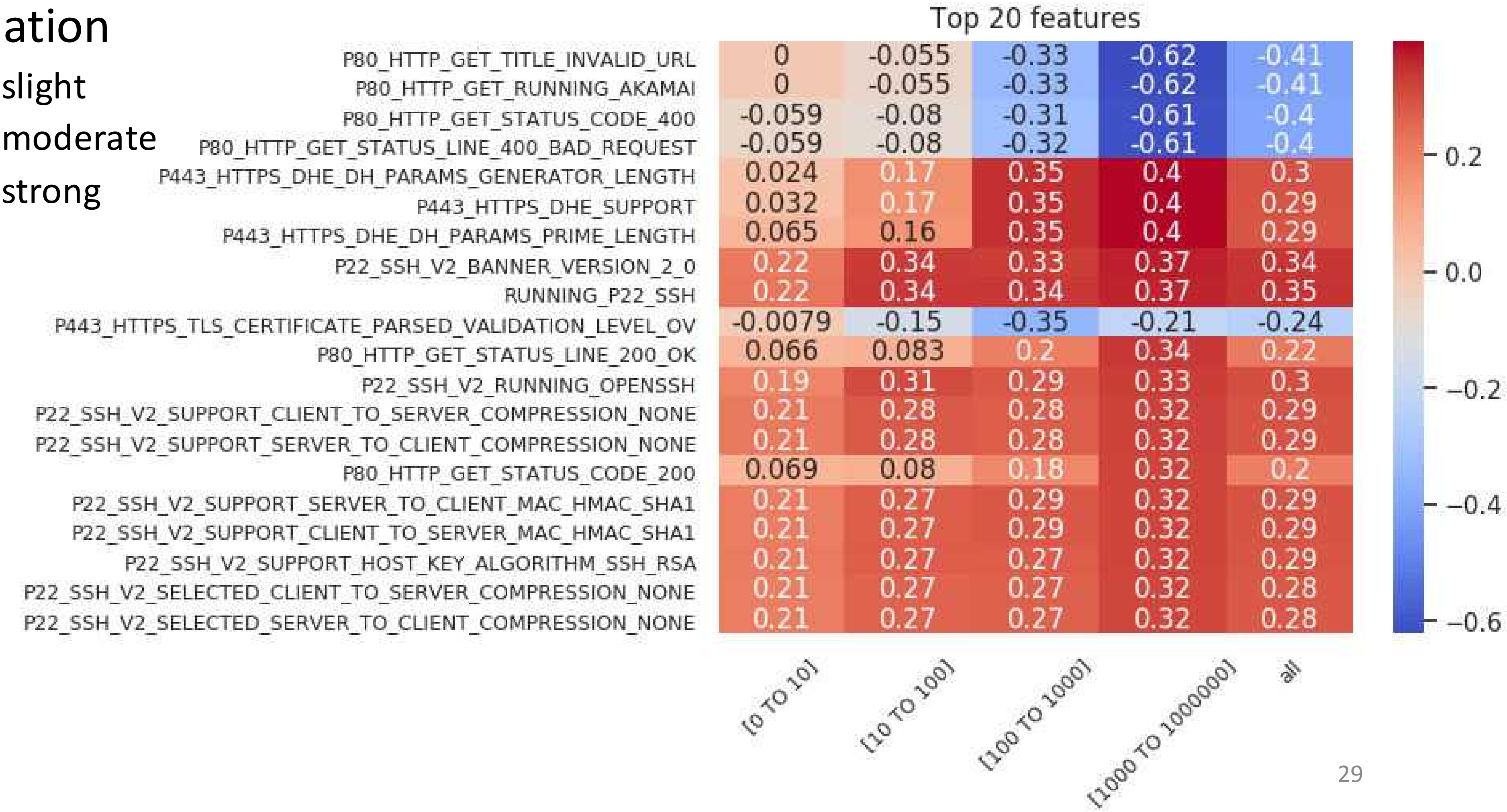


Outlier Classification(cont’d)

	f1-score	accuracy	fpr	supp0	supp1	no feats
≤ 10	0.70 ± 0.07	0.71 ± 0.06	0.18 ± 0.09	259	335	231
10 - 100	0.76 ± 0.04	0.76 ± 0.04	0.27 ± 0.05	1788	1816	71
100 - 1000	0.87 ± 0.02	0.87 ± 0.02	0.14 ± 0.05	2423	2423	61
≥ 1000	0.87 ± 0.04	0.87 ± 0.04	0.14 ± 0.05	2798	2798	40
all sizes	0.84 ± 0.01	0.84 ± 0.01	0.18 ± 0.04	7208	7312	41

Outlier Classification (cont'd)

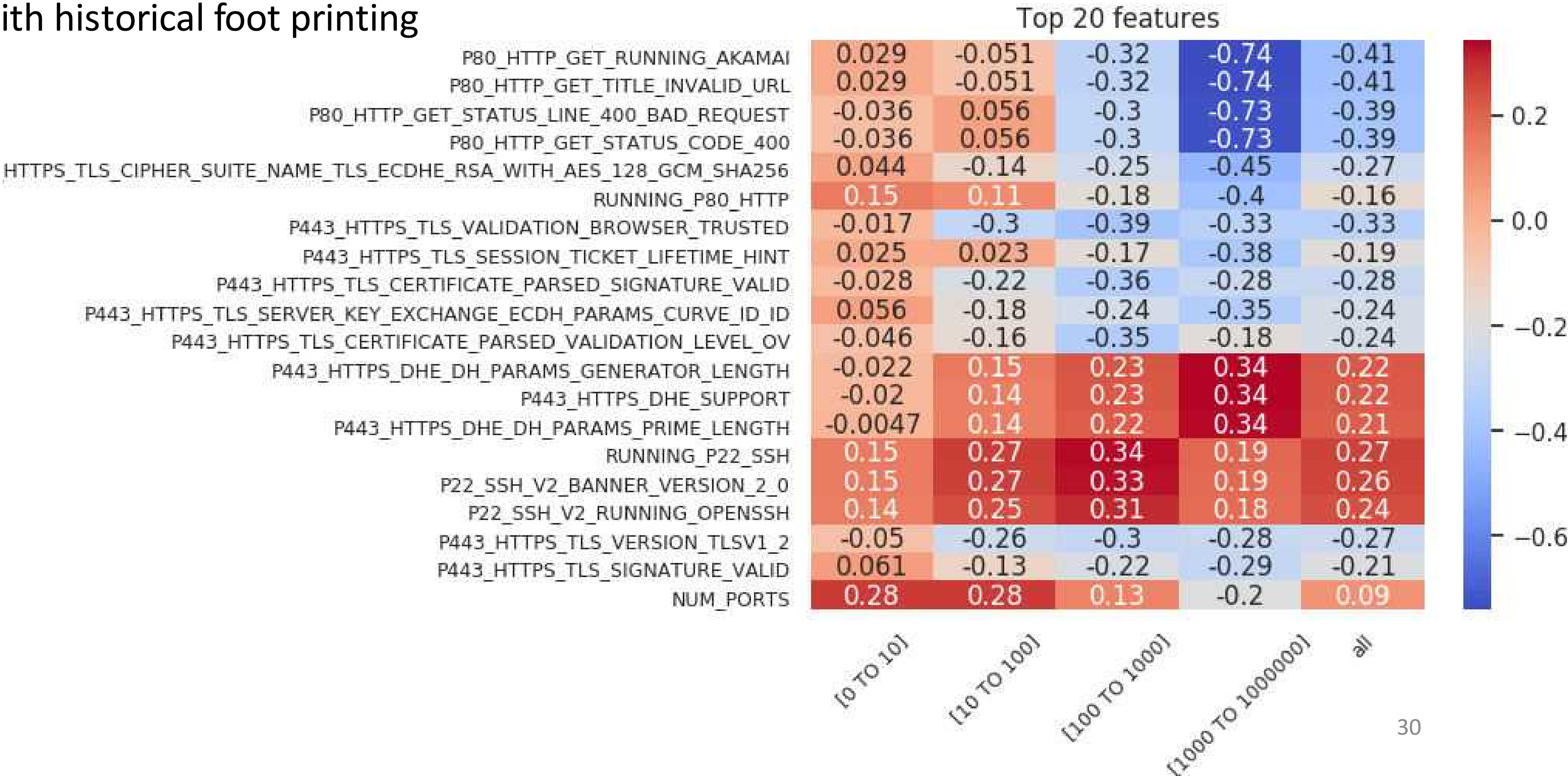
- Feature Importance
- Spearman correlation
  - 0.1 to 0.3 is slight
  - 0.3 to 0.5 is moderate
  - 0.5 to 1.0 is strong


Top 20 features

	[0 TO 10]	[10 TO 100]	[100 TO 1000]	[1000 TO 1000000]	all
P80_HTTP_GET_TITLE_INVALID_URL	0	-0.055	-0.33	-0.62	-0.41
P80_HTTP_GET_RUNNING_AKAMAI	0	-0.055	-0.33	-0.62	-0.41
P80_HTTP_GET_STATUS_CODE_400	-0.059	-0.08	-0.31	-0.61	-0.4
P80_HTTP_GET_STATUS_LINE_400_BAD_REQUEST	-0.059	-0.08	-0.32	-0.61	-0.4
P443_HTTPS_DHE_DH_PARAMS_GENERATOR_LENGTH	0.024	0.17	0.35	0.4	0.3
P443_HTTPS_DHE_SUPPORT	0.032	0.17	0.35	0.4	0.29
P443_HTTPS_DHE_DH_PARAMS_PRIME_LENGTH	0.065	0.16	0.35	0.4	0.29
P22_SSH_V2_BANNER_VERSION_2_0	0.22	0.34	0.33	0.37	0.34
RUNNING_P22_SSH	0.22	0.34	0.34	0.37	0.35
P443_HTTPS_TLS_CERTIFICATE_PARSED_VALIDATION_LEVEL_OV	-0.0079	-0.15	-0.35	-0.21	-0.24
P80_HTTP_GET_STATUS_LINE_200_OK	0.066	0.083	0.2	0.34	0.22
P22_SSH_V2_RUNNING_OPENSSH	0.19	0.31	0.29	0.33	0.3
P22_SSH_V2_SUPPORT_CLIENT_TO_SERVER_COMPRESSION_NONE	0.21	0.28	0.28	0.32	0.29
P22_SSH_V2_SUPPORT_SERVER_TO_CLIENT_COMPRESSION_NONE	0.21	0.28	0.28	0.32	0.29
P80_HTTP_GET_STATUS_CODE_200	0.069	0.08	0.18	0.32	0.2
P22_SSH_V2_SUPPORT_SERVER_TO_CLIENT_MAC_HMAC_SHA1	0.21	0.27	0.29	0.32	0.29
P22_SSH_V2_SUPPORT_CLIENT_TO_SERVER_MAC_HMAC_SHA1	0.21	0.27	0.29	0.32	0.29
P22_SSH_V2_SUPPORT_HOST_KEY_ALGORITHM_SSH_RSA	0.21	0.27	0.27	0.32	0.29
P22_SSH_V2_SELECTED_CLIENT_TO_SERVER_COMPRESSION_NONE	0.21	0.27	0.27	0.32	0.28
P22_SSH_V2_SELECTED_SERVER_TO_CLIENT_COMPRESSION_NONE	0.21	0.27	0.27	0.32	0.28

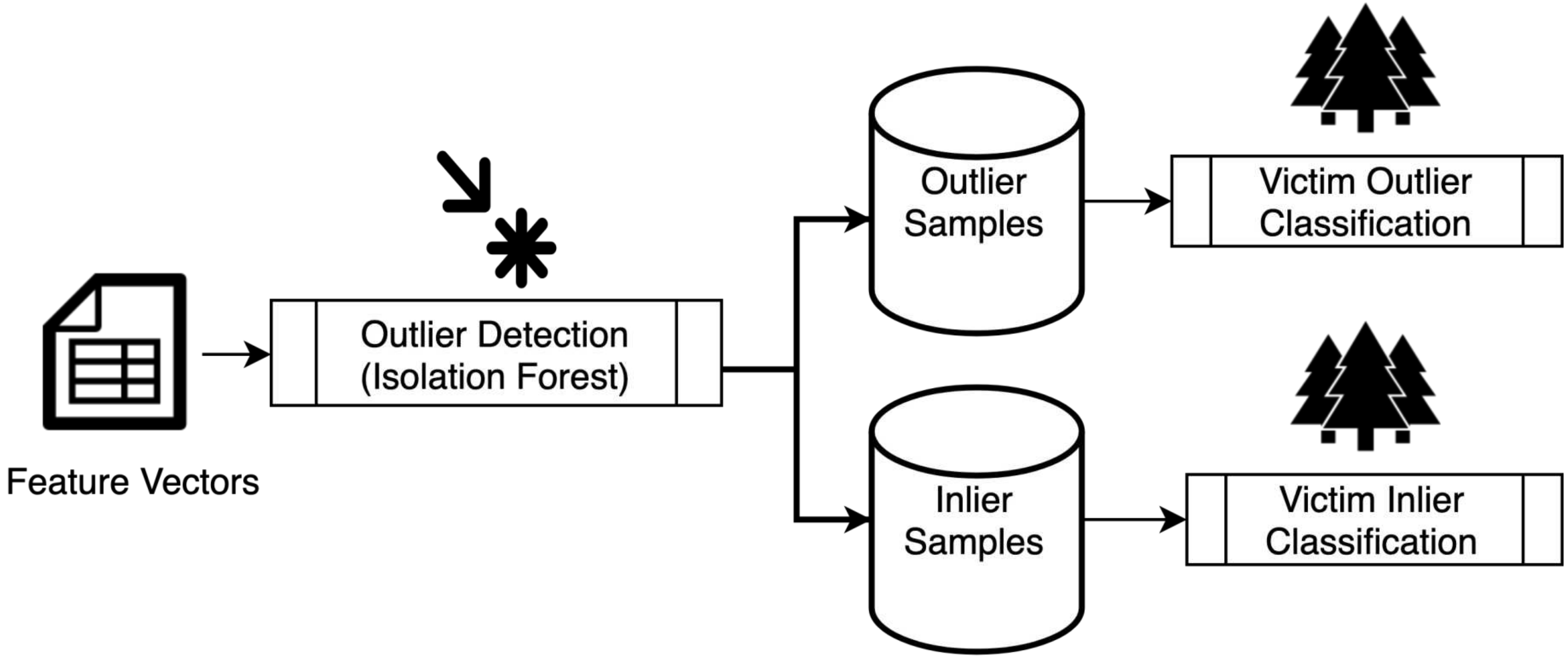
Outlier Classification (cont’d)

- Certificate attribution
  - Issue with historical foot printing



Top 20 features

	[0 TO 10)	[10 TO 100)	[100 TO 1000)	[1000 TO 1000000)	all
P80_HTTP_GET_RUNNING_AKAMAI	0.029	-0.051	-0.32	-0.74	-0.41
P80_HTTP_GET_TITLE_INVALID_URL	0.029	-0.051	-0.32	-0.74	-0.41
P80_HTTP_GET_STATUS_LINE_400_BAD_REQUEST	-0.036	0.056	-0.3	-0.73	-0.39
P80_HTTP_GET_STATUS_CODE_400	-0.036	0.056	-0.3	-0.73	-0.39
HTTPS_TLS_CIPHER_SUITE_NAME_TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0.044	-0.14	-0.25	-0.45	-0.27
RUNNING_P80_HTTP	0.15	0.11	-0.18	-0.4	-0.16
P443_HTTPS_TLS_VALIDATION_BROWSER_TRUSTED	-0.017	-0.3	-0.39	-0.33	-0.33
P443_HTTPS_TLS_SESSION_TICKET_LIFETIME_HINT	0.025	0.023	-0.17	-0.38	-0.19
P443_HTTPS_TLS_CERTIFICATE_PARSED_SIGNATURE_VALID	-0.028	-0.22	-0.36	-0.28	-0.28
P443_HTTPS_TLS_SERVER_KEY_EXCHANGE_ECDH_PARAMS_CURVE_ID_ID	0.056	-0.18	-0.24	-0.35	-0.24
P443_HTTPS_TLS_CERTIFICATE_PARSED_VALIDATION_LEVEL_OV	-0.046	-0.16	-0.35	-0.18	-0.24
P443_HTTPS_DHE_DH_PARAMS_GENERATOR_LENGTH	-0.022	0.15	0.23	0.34	0.22
P443_HTTPS_DHE_SUPPORT	-0.02	0.14	0.23	0.34	0.22
P443_HTTPS_DHE_DH_PARAMS_PRIME_LENGTH	-0.0047	0.14	0.22	0.34	0.21
RUNNING_P22_SSH	0.15	0.27	0.34	0.19	0.27
P22_SSH_V2_BANNER_VERSION_2_0	0.15	0.27	0.33	0.19	0.26
P22_SSH_V2_RUNNING_OPENSSH	0.14	0.25	0.31	0.18	0.24
P443_HTTPS_TLS_VERSION_TLSV1_2	-0.05	-0.26	-0.3	-0.28	-0.27
P443_HTTPS_TLS_SIGNATURE_VALID	0.061	-0.13	-0.22	-0.29	-0.21
NUM_PORTS	0.28	0.28	0.13	-0.2	0.09

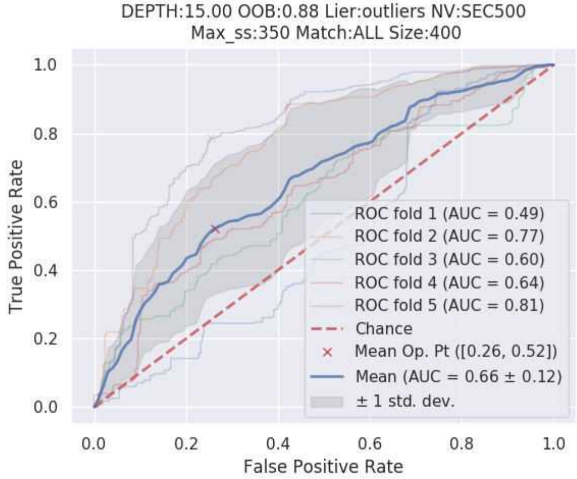

Feature Vectors
Outlier Detection (Isolation Forest)
Outlier Samples
Inlier Samples
Victim Outlier Classification
Victim Inlier Classification

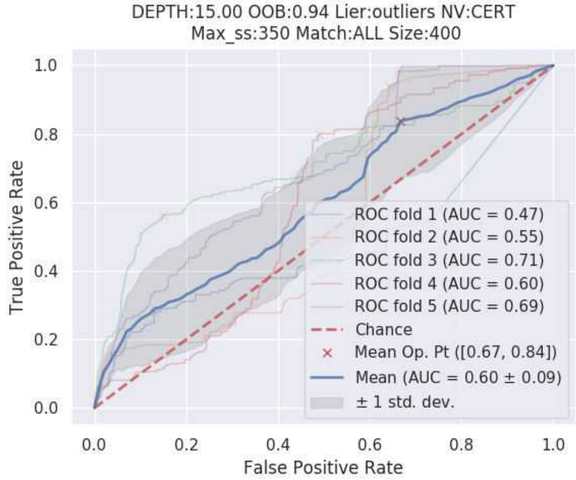
Victim Host Classification

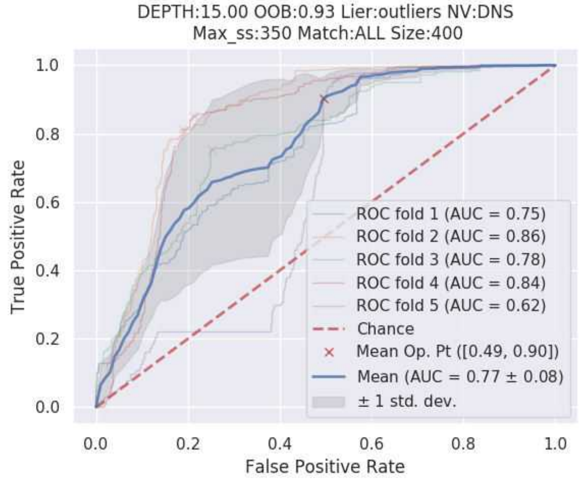
- Organization label are then be assigned to these liers
- Six classification problems
  - Two types of liers (outliers and inliers)
  - Three different methods of identifying non-victim organizations

Victim host classification (cont’d)

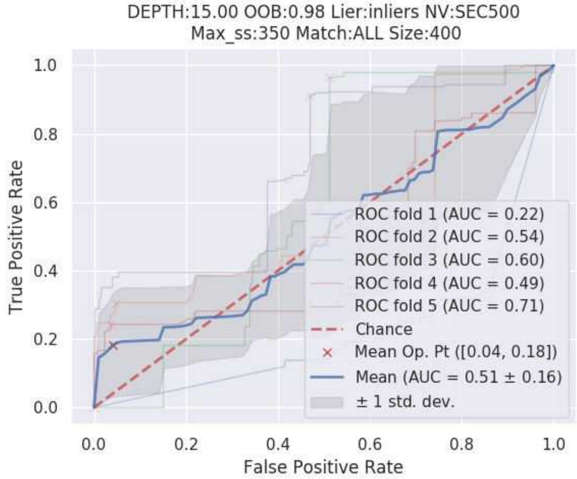
Outliers

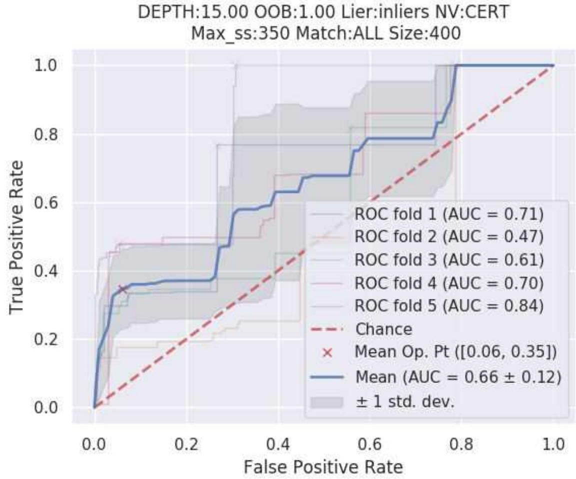


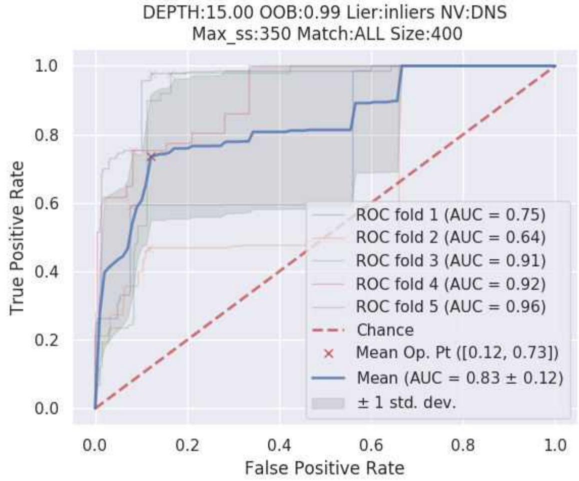




Inliers





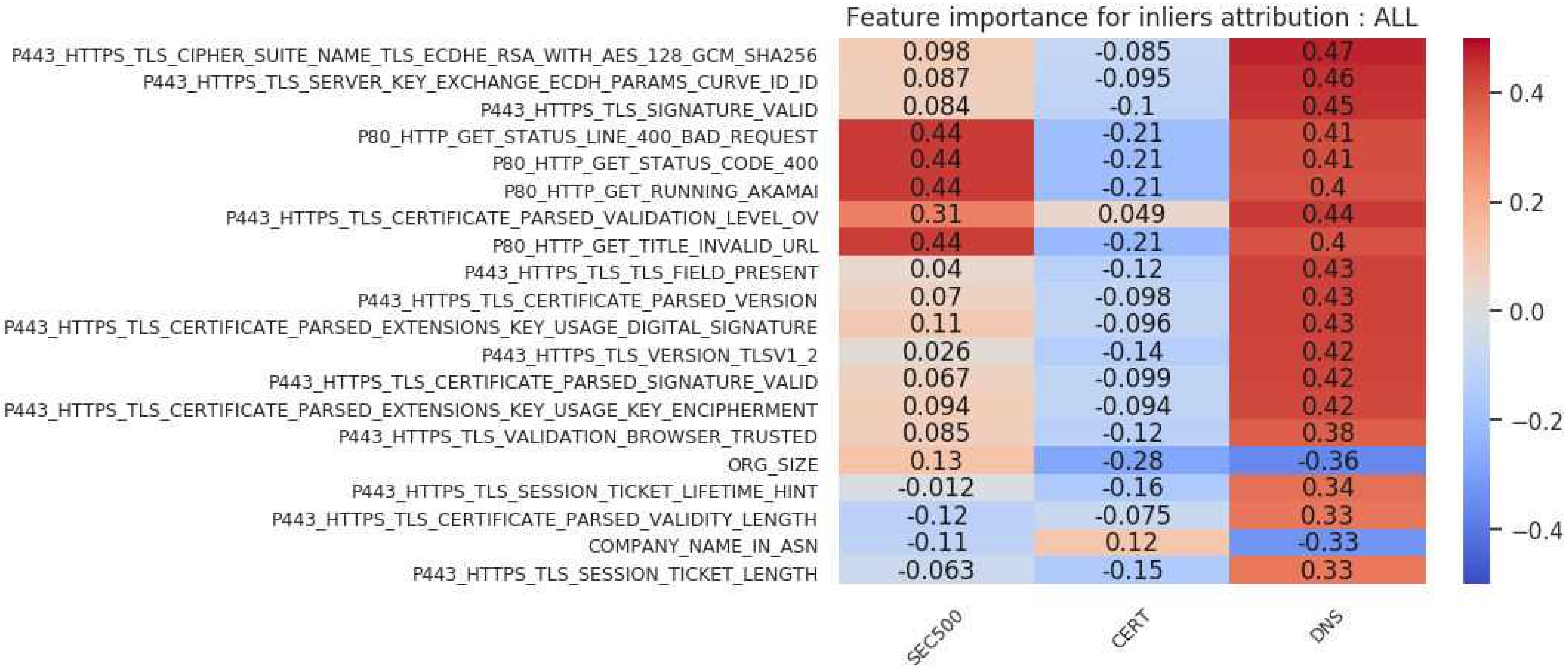


SEC500

CERT

DNS

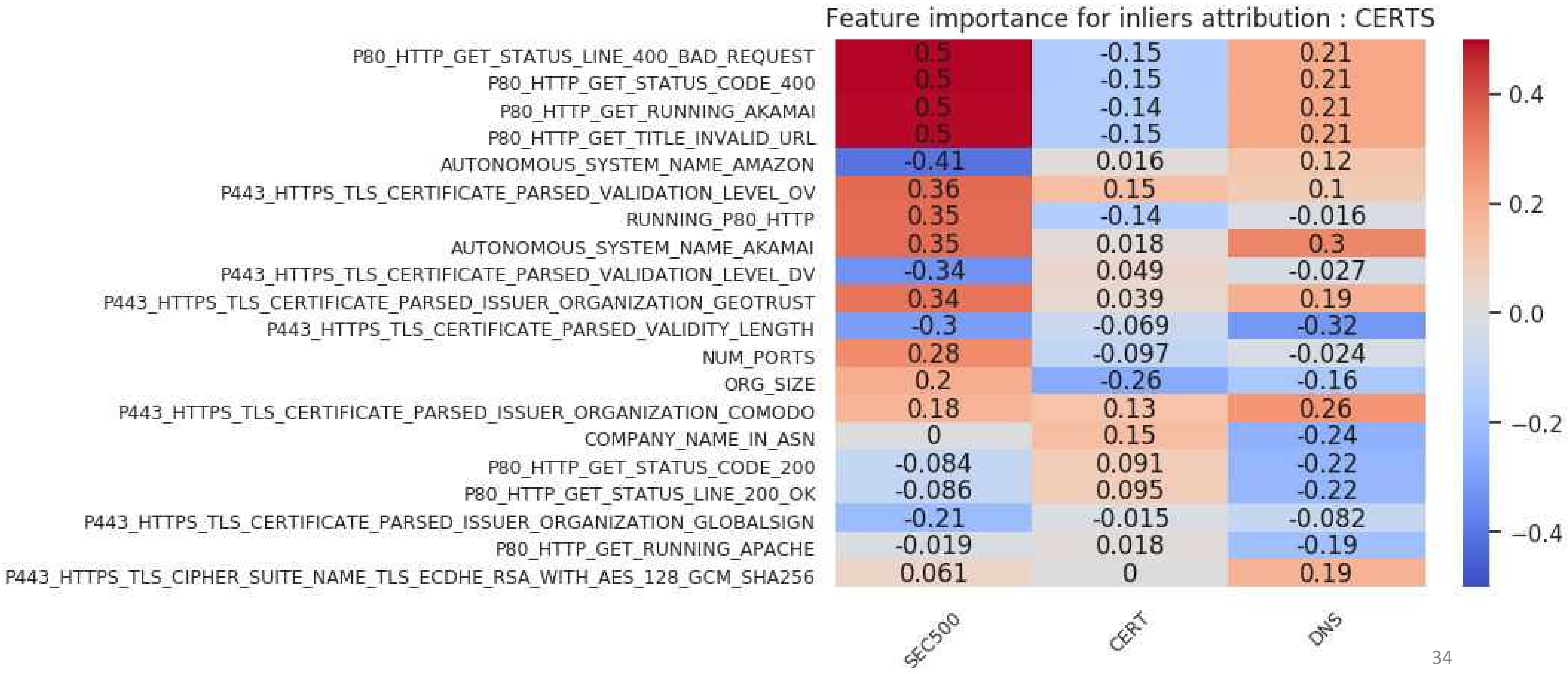
Victim host classification(cont’d) - Inliers



Feature importance for inliers attribution : ALL

	SEC500	CERT	DNS
P443_HTTPS_TLS_CIPHER_SUITE_NAME_TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0.098	-0.085	0.47
P443_HTTPS_TLS_SERVER_KEY_EXCHANGE_ECDH_PARAMS_CURVE_ID_ID	0.087	-0.095	0.46
P443_HTTPS_TLS_SIGNATURE_VALID	0.084	-0.1	0.45
P80_HTTP_GET_STATUS_LINE_400_BAD_REQUEST	0.44	-0.21	0.41
P80_HTTP_GET_STATUS_CODE_400	0.44	-0.21	0.41
P80_HTTP_GET_RUNNING_AKAMAI	0.44	-0.21	0.4
P443_HTTPS_TLS_CERTIFICATE_PARSED_VALIDATION_LEVEL_OV	0.31	0.049	0.44
P80_HTTP_GET_TITLE_INVALID_URL	0.44	-0.21	0.4
P443_HTTPS_TLS_TLS_FIELD_PRESENT	0.04	-0.12	0.43
P443_HTTPS_TLS_CERTIFICATE_PARSED_VERSION	0.07	-0.098	0.43
P443_HTTPS_TLS_CERTIFICATE_PARSED_EXTENSIONS_KEY_USAGE_DIGITAL_SIGNATURE	0.11	-0.096	0.43
P443_HTTPS_TLS_VERSION_TLSV1_2	0.026	-0.14	0.42
P443_HTTPS_TLS_CERTIFICATE_PARSED_SIGNATURE_VALID	0.067	-0.099	0.42
P443_HTTPS_TLS_CERTIFICATE_PARSED_EXTENSIONS_KEY_USAGE_KEY_ENCIPHERMENT	0.094	-0.094	0.42
P443_HTTPS_TLS_VALIDATION_BROWSER_TRUSTED	0.085	-0.12	0.38
ORG_SIZE	0.13	-0.28	-0.36
P443_HTTPS_TLS_SESSION_TICKET_LIFETIME_HINT	-0.012	-0.16	0.34
P443_HTTPS_TLS_CERTIFICATE_PARSED_VALIDITY_LENGTH	-0.12	-0.075	0.33
COMPANY_NAME_IN_ASN	-0.11	0.12	-0.33
P443_HTTPS_TLS_SESSION_TICKET_LENGTH	-0.063	-0.15	0.33

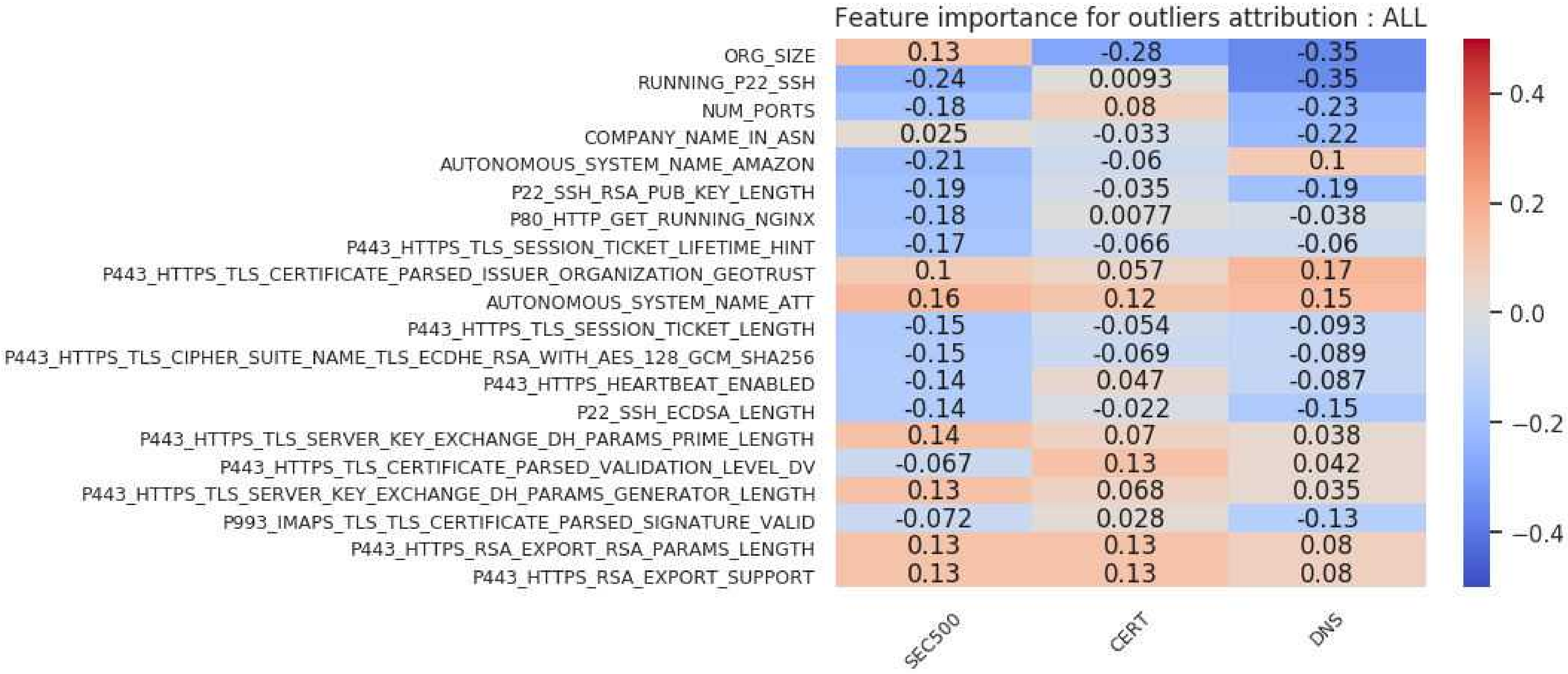
Victim host classification(cont'd) - Inliers



Feature importance for inliers attribution : CERTS

	SEC500	CERT	DNS
P80_HTTP_GET_STATUS_LINE_400_BAD_REQUEST	0.5	-0.15	0.21
P80_HTTP_GET_STATUS_CODE_400	0.5	-0.15	0.21
P80_HTTP_GET_RUNNING_AKAMAI	0.5	-0.14	0.21
P80_HTTP_GET_TITLE_INVALID_URL	0.5	-0.15	0.21
AUTONOMOUS_SYSTEM_NAME_AMAZON	-0.41	0.016	0.12
P443_HTTPS_TLS_CERTIFICATE_PARSED_VALIDATION_LEVEL_OV	0.36	0.15	0.1
RUNNING_P80_HTTP	0.35	-0.14	-0.016
AUTONOMOUS_SYSTEM_NAME_AKAMAI	0.35	0.018	0.3
P443_HTTPS_TLS_CERTIFICATE_PARSED_VALIDATION_LEVEL_DV	-0.34	0.049	-0.027
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_GEOTRUST	0.34	0.039	0.19
P443_HTTPS_TLS_CERTIFICATE_PARSED_VALIDITY_LENGTH	-0.3	-0.069	-0.32
NUM_PORTS	0.28	-0.097	-0.024
ORG_SIZE	0.2	-0.26	-0.16
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_COMODO	0.18	0.13	0.26
COMPANY_NAME_IN_ASN	0	0.15	-0.24
P80_HTTP_GET_STATUS_CODE_200	-0.084	0.091	-0.22
P80_HTTP_GET_STATUS_LINE_200_OK	-0.086	0.095	-0.22
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_GLOBALSIGN	-0.21	-0.015	-0.082
P80_HTTP_GET_RUNNING_APACHE	-0.019	0.018	-0.19
P443_HTTPS_TLS_CIPHER_SUITE_NAME_TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0.061	0	0.19

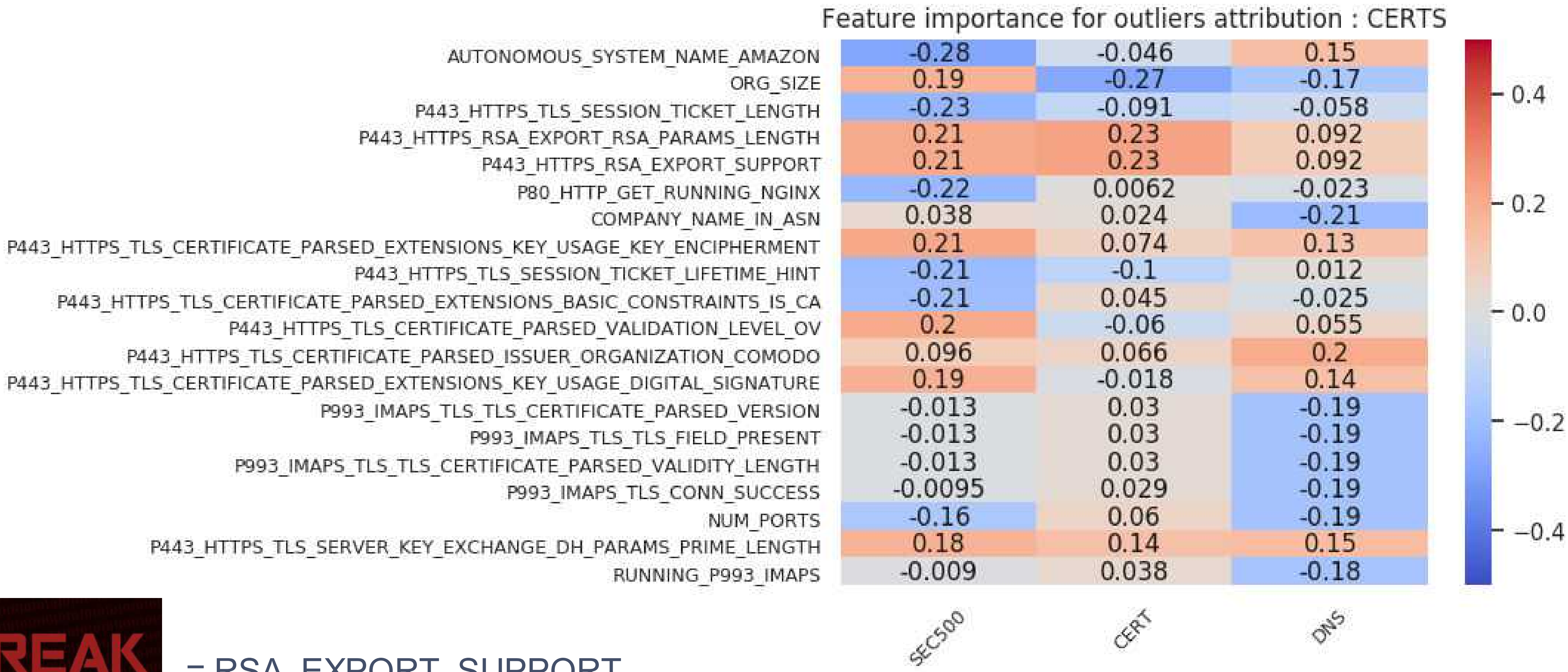
Victim host classification(cont'd) - Outliers



Feature importance for outliers attribution : ALL

	SEC500	CERT	DNS
ORG_SIZE	0.13	-0.28	-0.35
RUNNING_P22_SSH	-0.24	0.0093	-0.35
NUM_PORTS	-0.18	0.08	-0.23
COMPANY_NAME_IN_ASN	0.025	-0.033	-0.22
AUTONOMOUS_SYSTEM_NAME_AMAZON	-0.21	-0.06	0.1
P22_SSH_RSA_PUB_KEY_LENGTH	-0.19	-0.035	-0.19
P80_HTTP_GET_RUNNING_NGINX	-0.18	0.0077	-0.038
P443_HTTPS_TLS_SESSION_TICKET_LIFETIME_HINT	-0.17	-0.066	-0.06
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_GEOTRUST	0.1	0.057	0.17
AUTONOMOUS_SYSTEM_NAME_ATT	0.16	0.12	0.15
P443_HTTPS_TLS_SESSION_TICKET_LENGTH	-0.15	-0.054	-0.093
P443_HTTPS_TLS_CIPHER_SUITE_NAME_TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	-0.15	-0.069	-0.089
P443_HTTPS_HEARTBEAT_ENABLED	-0.14	0.047	-0.087
P22_SSH_ECDSA_LENGTH	-0.14	-0.022	-0.15
P443_HTTPS_TLS_SERVER_KEY_EXCHANGE_DH_PARAMS_PRIME_LENGTH	0.14	0.07	0.038
P443_HTTPS_TLS_CERTIFICATE_PARSED_VALIDATION_LEVEL_DV	-0.067	0.13	0.042
P443_HTTPS_TLS_SERVER_KEY_EXCHANGE_DH_PARAMS_GENERATOR_LENGTH	0.13	0.068	0.035
P993_IMAPS_TLS_TLS_CERTIFICATE_PARSED_SIGNATURE_VALID	-0.072	0.028	-0.13
P443_HTTPS_RSA_EXPORT_RSA_PARAMS_LENGTH	0.13	0.13	0.08
P443_HTTPS_RSA_EXPORT_SUPPORT	0.13	0.13	0.08

Victim host classification(cont'd) - Outliers

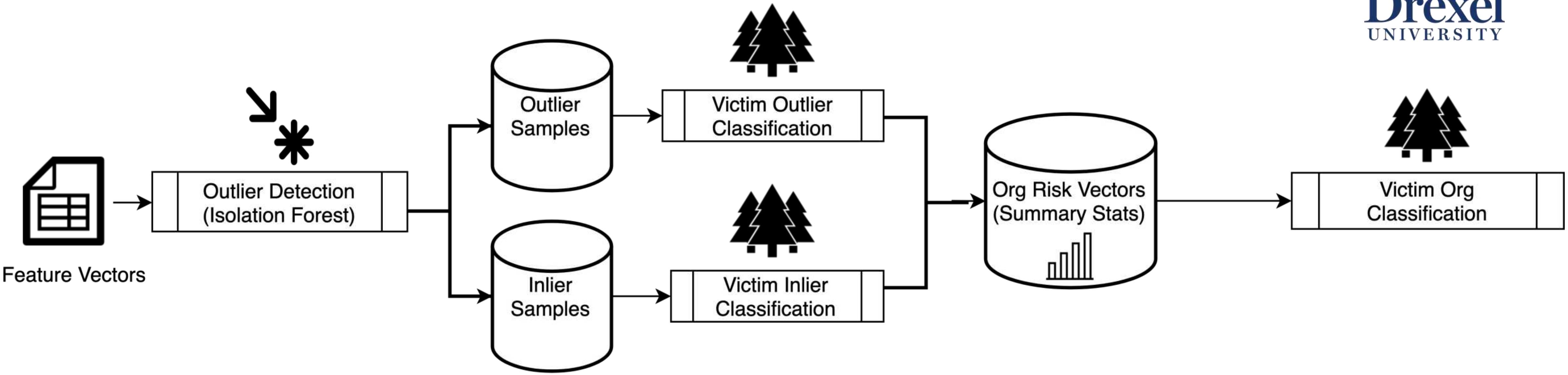


	SEC500	CERT	DNS
AUTONOMOUS_SYSTEM_NAME_AMAZON	-0.28	-0.046	0.15
ORG_SIZE	0.19	-0.27	-0.17
P443_HTTPS_TLS_SESSION_TICKET_LENGTH	-0.23	-0.091	-0.058
P443_HTTPS_RSA_EXPORT_RSA_PARAMS_LENGTH	0.21	0.23	0.092
P443_HTTPS_RSA_EXPORT_SUPPORT	0.21	0.23	0.092
P80_HTTP_GET_RUNNING_NGINX	-0.22	0.0062	-0.023
COMPANY_NAME_IN_ASN	0.038	0.024	-0.21
P443_HTTPS_TLS_CERTIFICATE_PARSED_EXTENSIONS_KEY_USAGE_KEY_ENCIPHERMENT	0.21	0.074	0.13
P443_HTTPS_TLS_SESSION_TICKET_LIFETIME_HINT	-0.21	-0.1	0.012
P443_HTTPS_TLS_CERTIFICATE_PARSED_EXTENSIONS_BASIC_CONSTRAINTS_IS_CA	-0.21	0.045	-0.025
P443_HTTPS_TLS_CERTIFICATE_PARSED_VALIDATION_LEVEL_OV	0.2	-0.06	0.055
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_COMODO	0.096	0.066	0.2
P443_HTTPS_TLS_CERTIFICATE_PARSED_EXTENSIONS_KEY_USAGE_DIGITAL_SIGNATURE	0.19	-0.018	0.14
P993_IMAPS_TLS_TLS_CERTIFICATE_PARSED_VERSION	-0.013	0.03	-0.19
P993_IMAPS_TLS_TLS_FIELD_PRESENT	-0.013	0.03	-0.19
P993_IMAPS_TLS_TLS_CERTIFICATE_PARSED_VALIDITY_LENGTH	-0.013	0.03	-0.19
P993_IMAPS_TLS_CONN_SUCCESS	-0.0095	0.029	-0.19
NUM_PORTS	-0.16	0.06	-0.19
P443_HTTPS_TLS_SERVER_KEY_EXCHANGE_DH_PARAMS_PRIME_LENGTH	0.18	0.14	0.15
RUNNING_P993_IMAPS	-0.009	0.038	-0.18

FREAK
SSL/TLS Vulnerability

= RSA_EXPORT_SUPPORT

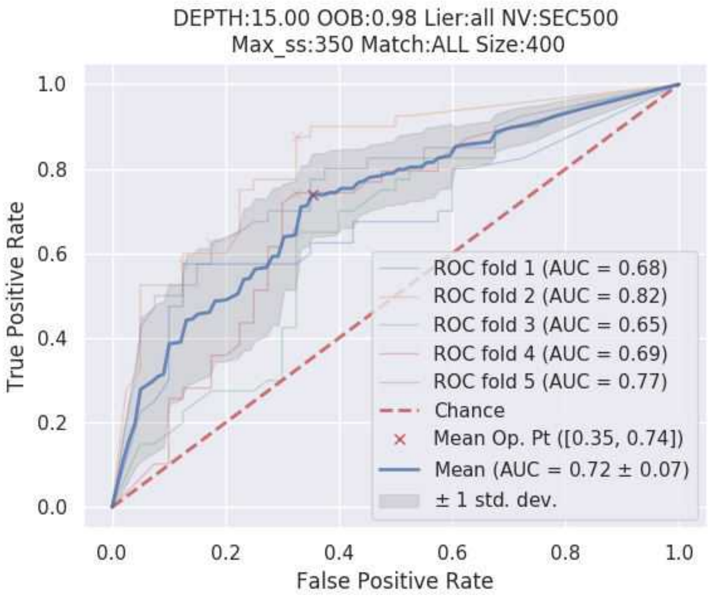
Image Source : [22]

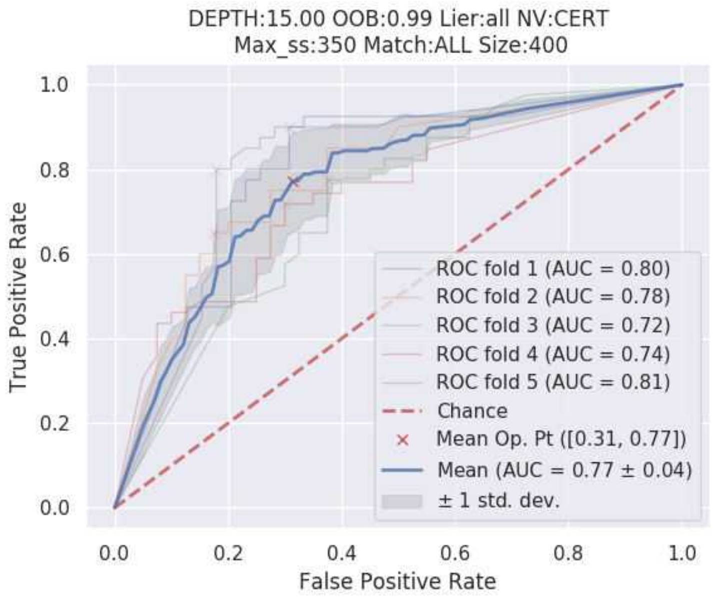

Feature Vectors
Outlier Detection (Isolation Forest)
Outlier Samples
Inlier Samples
Victim Outlier Classification
Victim Inlier Classification
Org Risk Vectors (Summary Stats)
Victim Org Classification

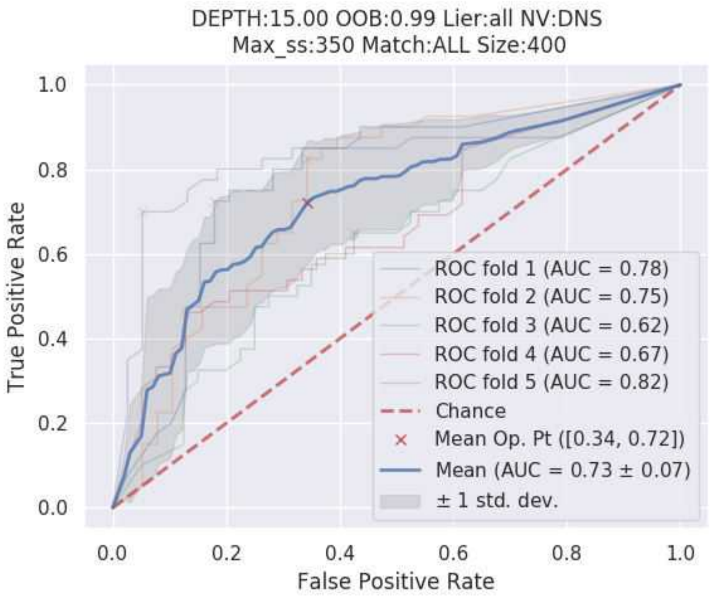
Victim Org Classification

- Challenge now is to reduce these probability scores to an organizational risk profile
- **Solution :** Summary statistics
  - 5 quartiles : [0, 25, 50, 75, 100]
  - Average
  - Variance
  - Amount(count)
- 16 total features

Victim Org Classification

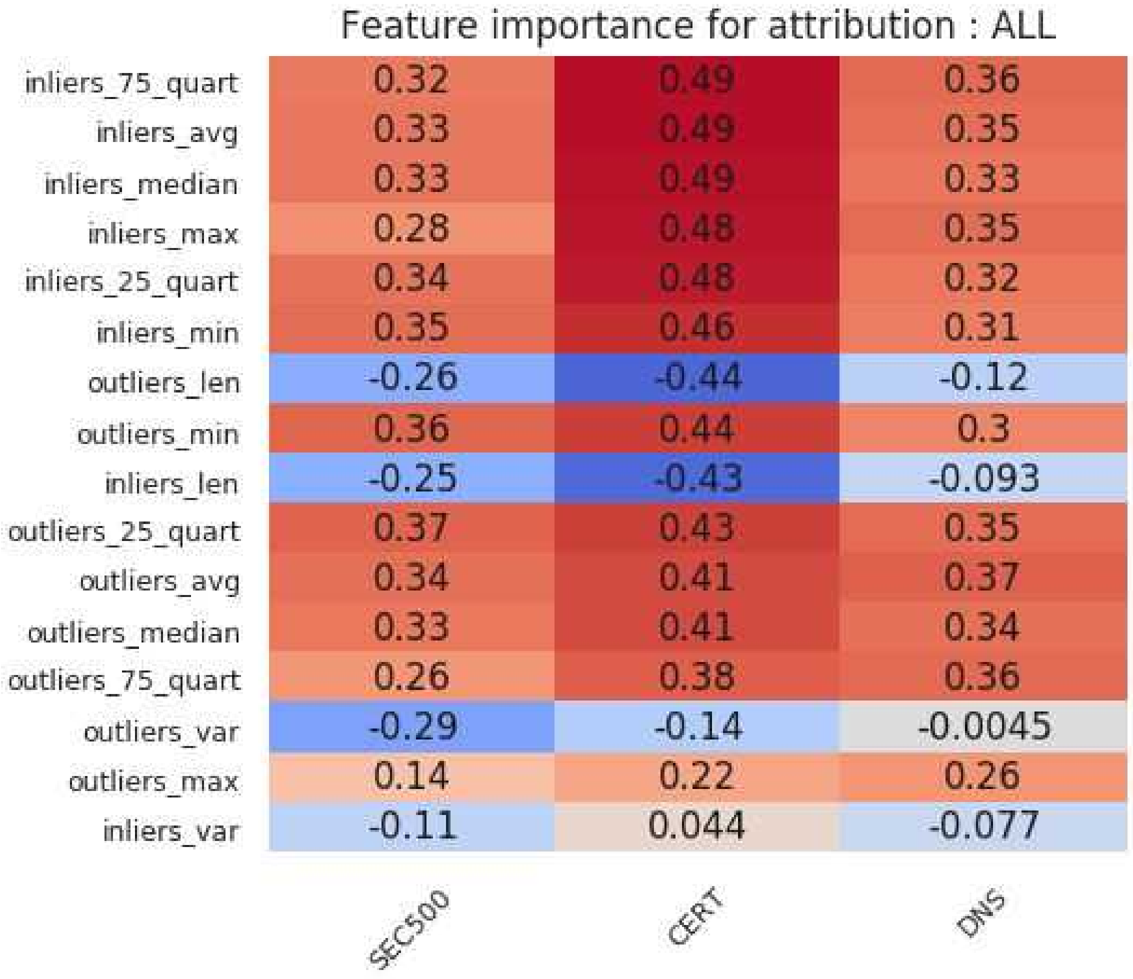






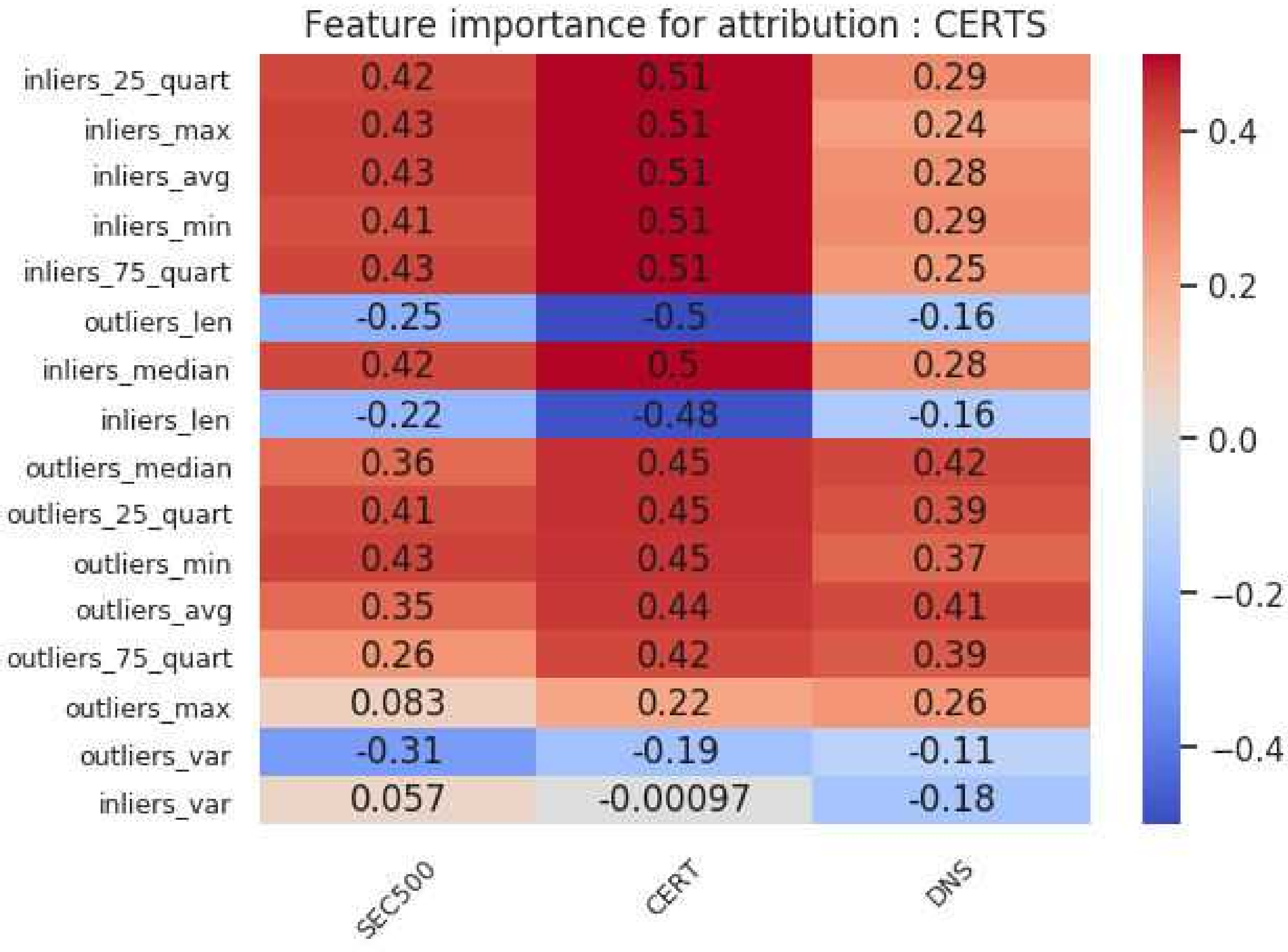
	f1-score	**accuracy**	**fpr**	**supp0**	**supp1**
SEC500	0.72 ± 0.04	0.72 ± 0.04	0.26 ± 0.09	200	199
CERT	0.75 ± 0.05	0.75 ± 0.05	0.27 ± 0.08	198	199
DNS	0.72 ± 0.08	0.72 ± 0.07	0.23 ± 0.14	194	199
Mean	0.73 ± 0.06	0.73 ± 0.05	0.25 ± 0.10	197	199

Victim Org Classification (cont'd)



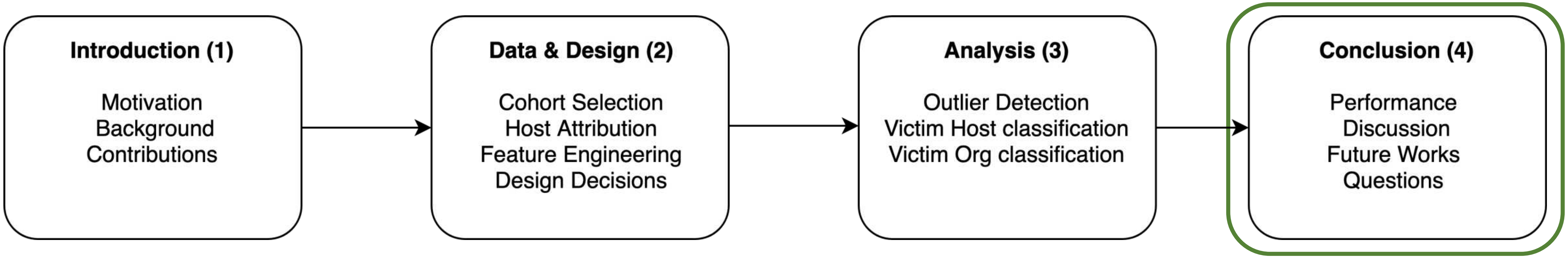
Feature importance for attribution : ALL

	SEC500	CERT	DNS
inliers_75_quart	0.32	0.49	0.36
inliers_avg	0.33	0.49	0.35
inliers_median	0.33	0.49	0.33
inliers_max	0.28	0.48	0.35
inliers_25_quart	0.34	0.48	0.32
inliers_min	0.35	0.46	0.31
outliers_len	-0.26	-0.44	-0.12
outliers_min	0.36	0.44	0.3
inliers_len	-0.25	-0.43	-0.093
outliers_25_quart	0.37	0.43	0.35
outliers_avg	0.34	0.41	0.37
outliers_median	0.33	0.41	0.34
outliers_75_quart	0.26	0.38	0.36
outliers_var	-0.29	-0.14	-0.0045
outliers_max	0.14	0.22	0.26
inliers_var	-0.11	0.044	-0.077



Feature importance for attribution : CERTS

	SEC500	CERT	DNS
inliers_25_quart	0.42	0.51	0.29
inliers_max	0.43	0.51	0.24
inliers_avg	0.43	0.51	0.28
inliers_min	0.41	0.51	0.29
inliers_75_quart	0.43	0.51	0.25
outliers_len	-0.25	-0.5	-0.16
inliers_median	0.42	0.5	0.28
inliers_len	-0.22	-0.48	-0.16
outliers_median	0.36	0.45	0.42
outliers_25_quart	0.41	0.45	0.39
outliers_min	0.43	0.45	0.37
outliers_avg	0.35	0.44	0.41
outliers_75_quart	0.26	0.42	0.39
outliers_max	0.083	0.22	0.26
outliers_var	-0.31	-0.19	-0.11
inliers_var	0.057	-0.00097	-0.18



Introduction (1)

Motivation
Background
Contributions

Data & Design (2)

Cohort Selection
Host Attribution
Feature Engineering
Design Decisions

Analysis (3)

Outlier Detection
Victim Host classification
Victim Org classification

Conclusion (4)

Performance
Discussion
Future Works
Questions

Conclusion (4)

Performance Comparison

	Accuracy	TPR	FPR
"Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents", 2015[8]	0.90	0.90	0.10
"Automatically Detecting Vulnerable Websites Before They Turn Malicious", 2014 [21]	N/A	0.66	0.17
Our Method	0.73	0.77	0.25

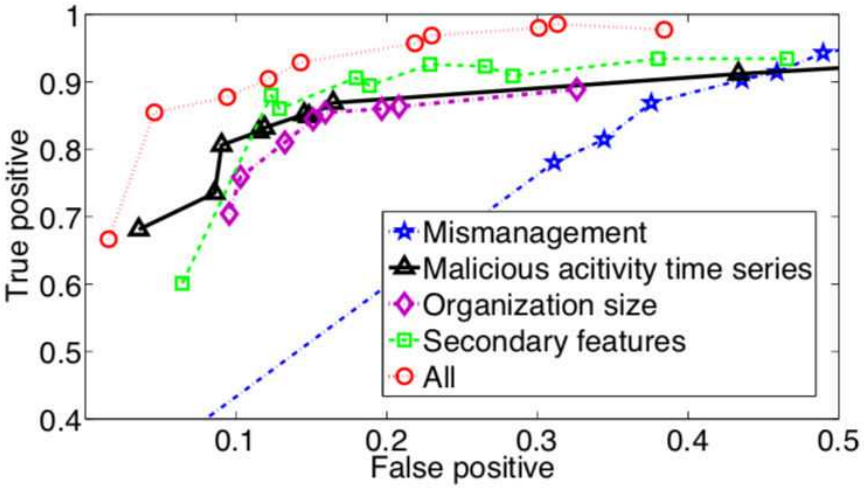
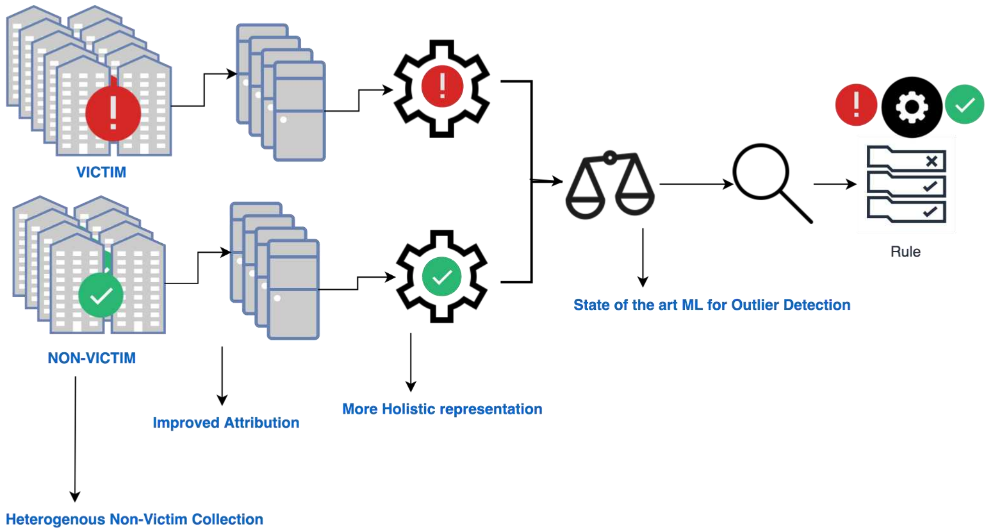


Image Source : [8]

Discussion

- Takeaways
  - SSH is outlier most likely to appear in a non-victim
  - Misconfigured HTTPS server is outlier most likely to appear in a victim
  - Important rules depend on non-victims
  - Non-victims have more outliers and higher variance in outliers


VICTIM
NON-VICTIM
Rule
State of the art ML for Outlier Detection
More Holistic representation
Improved Attribution
Heterogenous Non-Victim Collection

Future Work

- More data
  - Methods of collecting non-victims
  - Organizations than 200 per cohort subset
  - Configuration features. E.g. Protocols like RDP

- Graphical approach (instead of outlier detection)
  - Handle the inter host features

- Time series analysis
  - Network configurations (and vulnerabilities) are constantly evolving
  - Create an adaptive model

Questions?

References

[1] Privacy Rights Clearing House. Breaches for 2017-18. URL: https : / / www.privacyrights.org/data-breaches?title=&taxonomy_vocabulary_ 11_tid%5B%5D=2436&taxonomy_vocabulary_11_tid%5B%5D=2434.

[2] Benjamin Edwards, Steven Hofmeyr, and Stephanie Forrest. “Hype and heavy tails: A closer look at data breaches”. In: Journal of Cybersecurity 2.1 (2016), pp. 3–14.

[3] “Krebs on Security.” Brian Krebs, krebsonsecurity.com/tag/cyber-risk-score/

[4] Inloox.com. (2019). The Importance of the Internet of Things (IoT) for Project Management - InLoox. [online] Available at: https://www.inloox.com/company/blog/articles/the-importance-of-the-internet-of-things-iot-for-project-management/ [Accessed 2 Jun. 2019].

[5] "Individuals using the Internet 2005 to 2014", Key ICT indicators for developed and developing countries and the world (totals and penetration rates), International Telecommunication Union (ITU). Retrieve 25 May 2015.

[6] Engineers dailys. *Computer Networks.* URL : http://www.engineersdaily.com/2011/02/computer-networks.html

[7] Zhang, Jing, et al. "On the Mismanagement and Maliciousness of Networks." NDSS. 2014.

[8] Liu, Yang, et al. "Cloudy with a chance of breach: Forecasting cyber security incidents." 24th {USENIX} Security Symposium ({USENIX} Security 15). 2015.

[9] Durumeric, Zakir, et al. "A search engine backed by Internet-wide scanning." Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015.

[10] Durumeric, Zakir, Eric Wustrow, and J. Alex Halderman. "ZMap: Fast Internet-wide scanning and its security applications." Presented as part of the 22nd {USENIX} Security Symposium ({USENIX} Security 13). 2013.

[11] RISKIQ. RISKIQ. URL: https://www.riskiq.com/.

[12] Binary Edge. Binary Edge. URL: https://app.binaryedge.io/.

[13] Security Trails. Security Trails. URL: https://securitytrails.com/.

[14] Virus Total. Virus Total. URL: https://www.virustotal.com.

[15] Liu, Fei Tony, Kai Ming Ting, and Zhi-Hua Zhou. "Isolation forest." 2008 Eighth IEEE International Conference on Data Mining. IEEE, 2008

[16] Random Forest. *Neural Regeneration Research*. http://www.nrronline.org/viewimage.asp?img=NeuralRegenRes_2018_13_6_962_233433_f2.jpg

[17] scikit-learn. *Recursive Feature Elimination*. https://scikit-learn.org/stable/auto_examples/feature_selection/plot_rfe_with_cross_validation.html

[18] The Tech Check. *Different types of validations in machine learning(Cross Validation)*. https://blog.contactsunny.com/data-science/different-types-of-validations-in-machine-learning-cross-validation

[19] StackExchange. *Accuracy vs. area under the ROC curve*. https://stats.stackexchange.com/questions/225210/accuracy-vs-area-under-the-roc-curve

[20] Censys. *The FREAK Attack.* https://censys.io/blog/freak

[21] Soska, Kyle, and Nicolas Christin. "Automatically detecting vulnerable websites before they turn malicious." 23rd {USENIX} Security Symposium ({USENIX} Security 14). 2014.

[22] The Hacker News. *'FREAK' — New SSL/TLS Vulnerability Explaine*d. https://thehackernews.com/2015/03/freak-openssl-vulnerability.html

[23] FICO. Cyber Risk Score. URL: https://www.fico.com/en/products/cyber-risk-score.

[24] BitSight. BitSight. URL: https://www.bitsight.com/.

[25] SecurityScorecard. SecurityScorecard. URL: https://securityscorecard. com/.

[26] UpGuard. UpGuard. URL: https://www.upguard.com/.

Appendix

Other Relevant Works

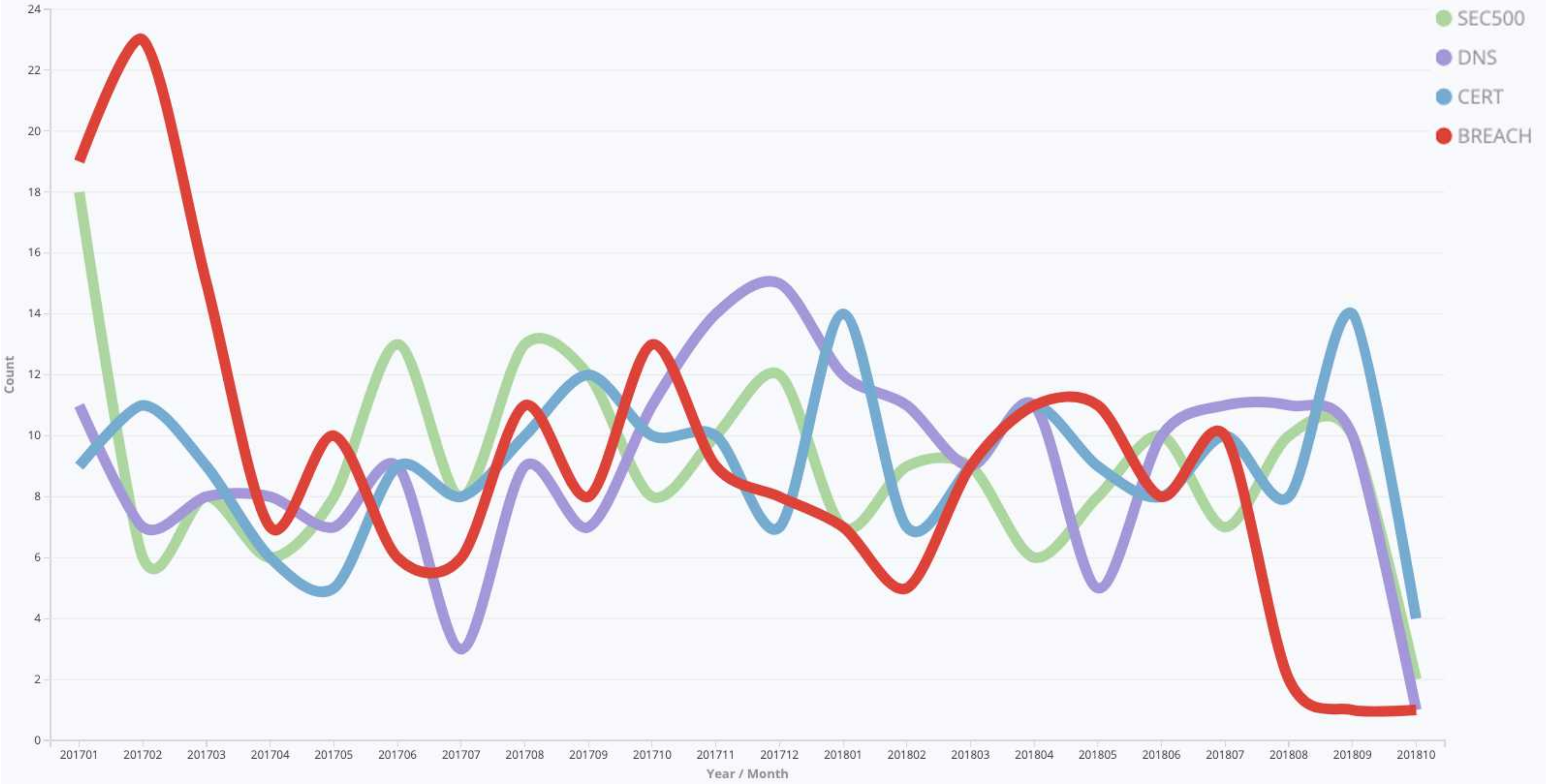
- Sarabi et al. examine the extent that business details about an organization can help forecast its risk of experiencing different types of data incidents [23].

- Vasek et al. analyzed features from sampled web servers to identify risk factors for web server compromise [17].

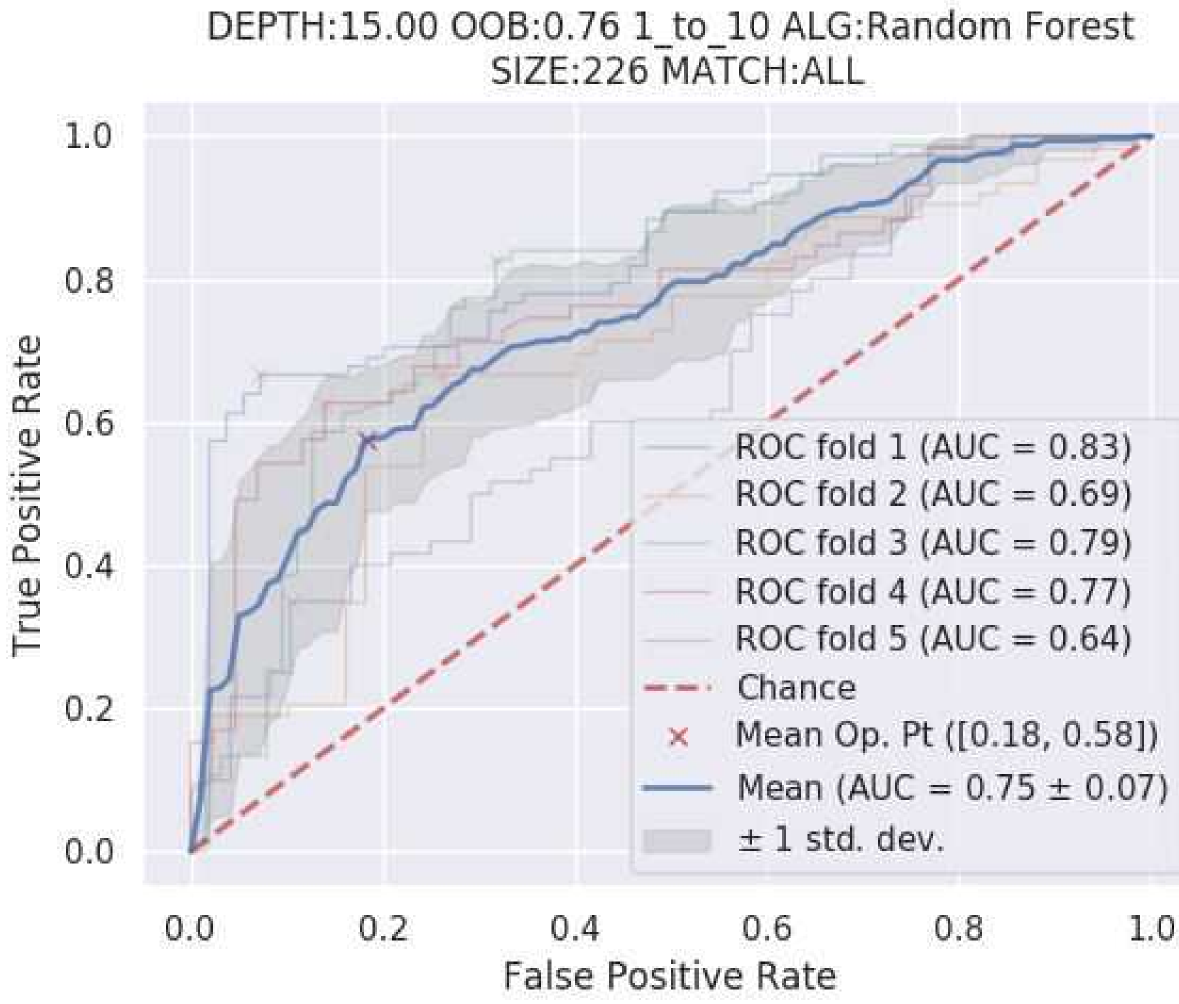
- Thonnard et al. looked at organization risk factors (number of employees and business sector) and individual level factors (job type and location) that are related with experiencing spear phishing targeted attacks [24].

- Canali et al. analyzed user browsing behavior to predict whether a user will encounter a malicious page achieving 87% accuracy [15]

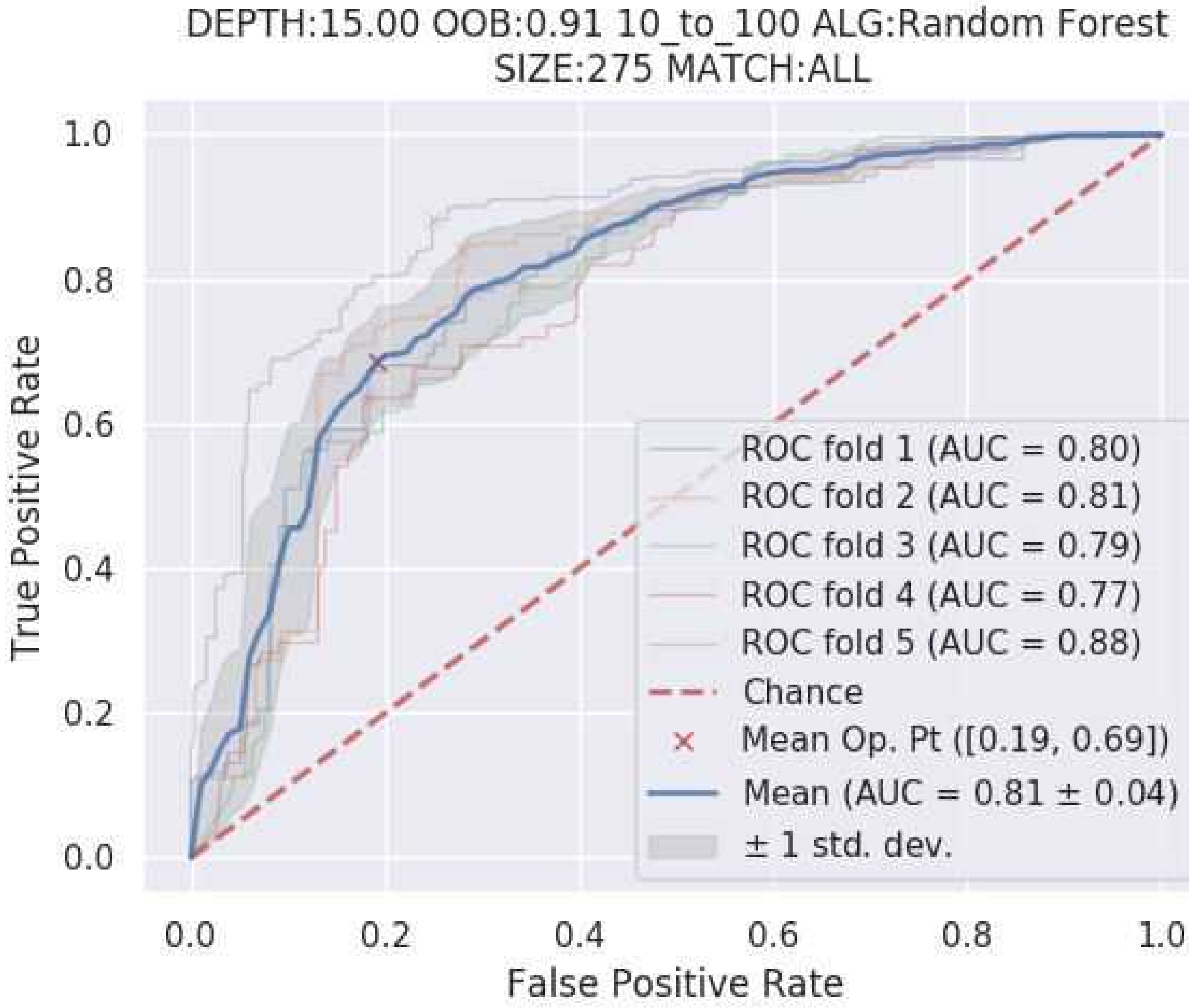
Lookup Dates



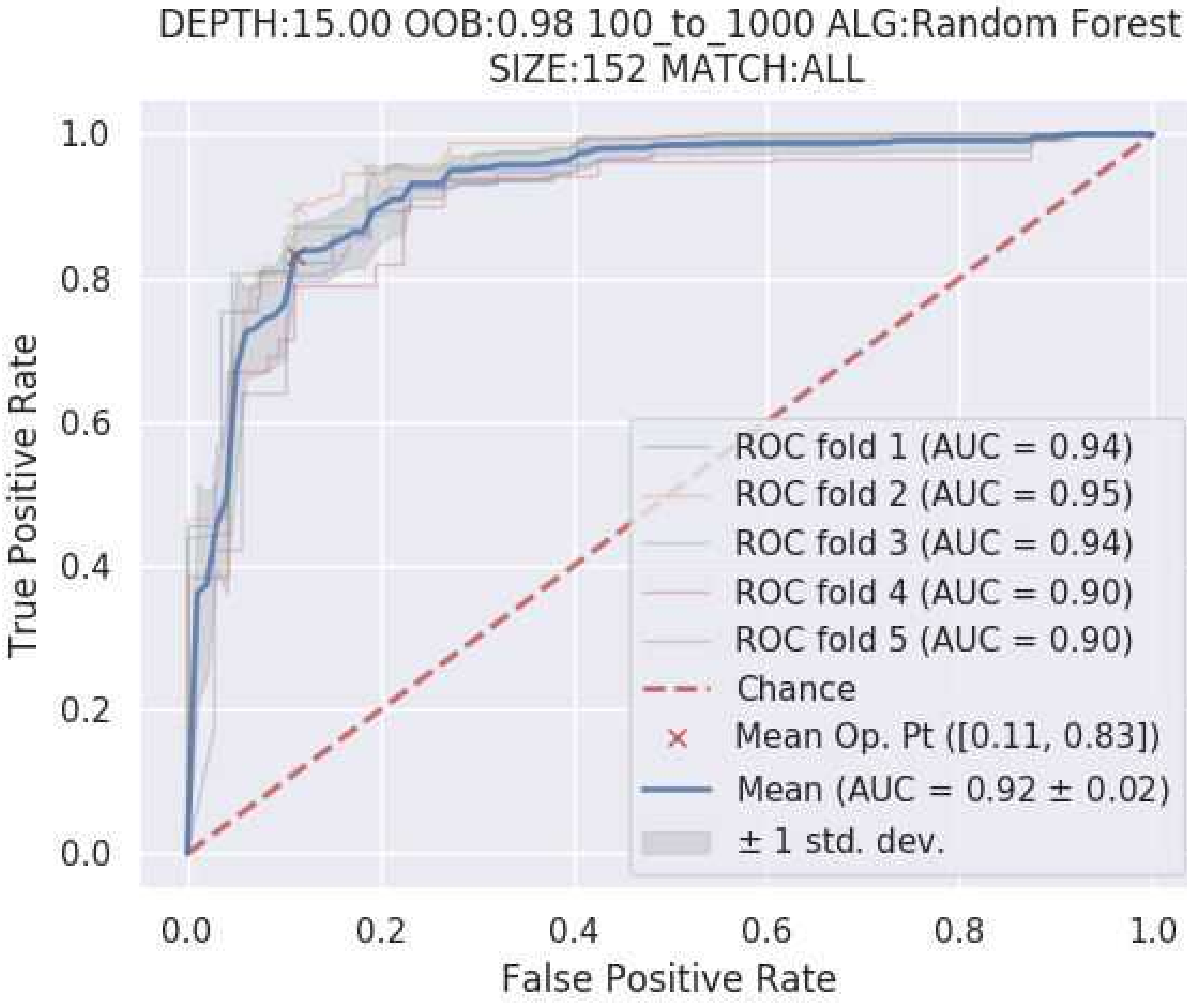
Outlier classification – >= 10



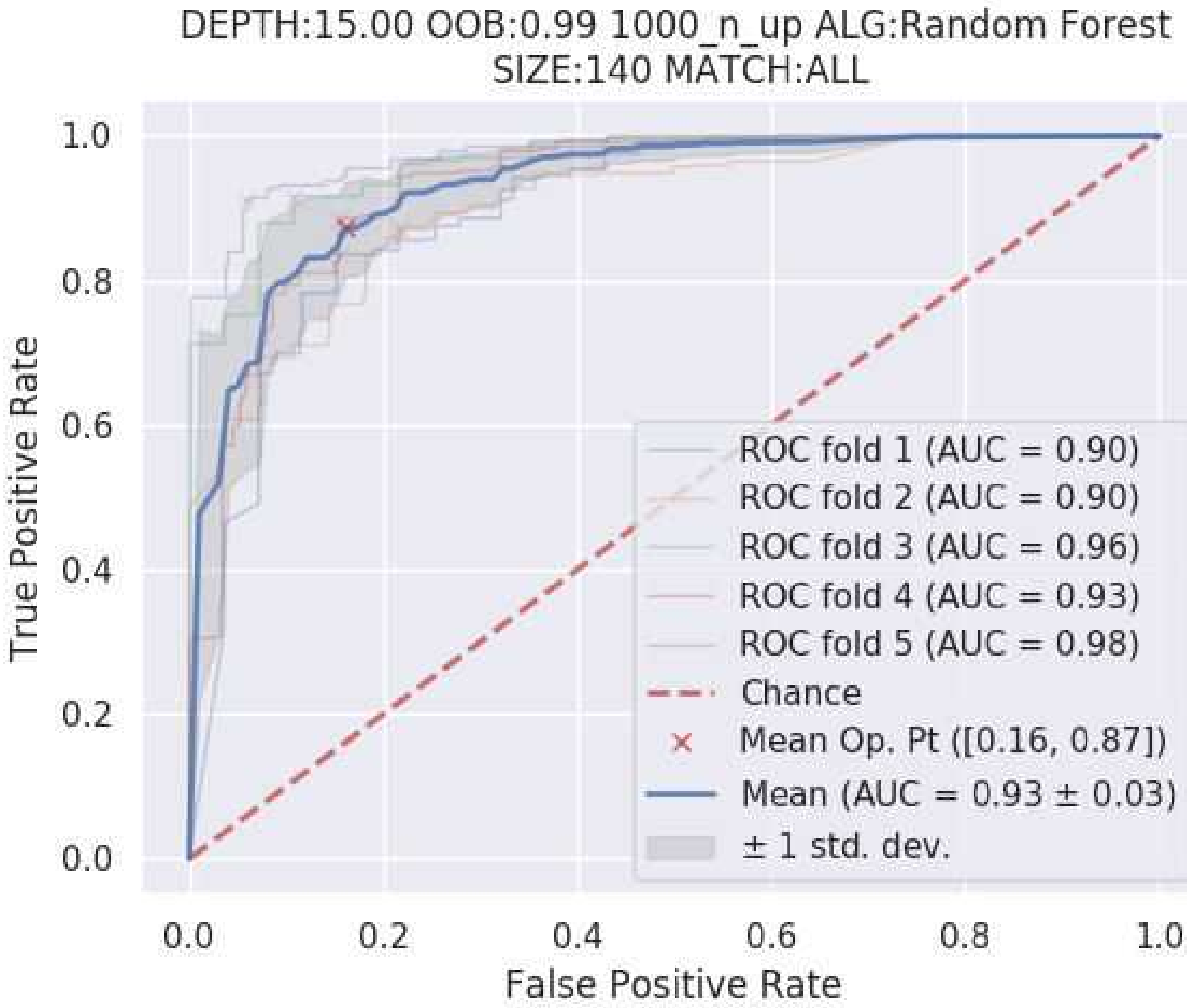
Outlier classification : [10, 100]



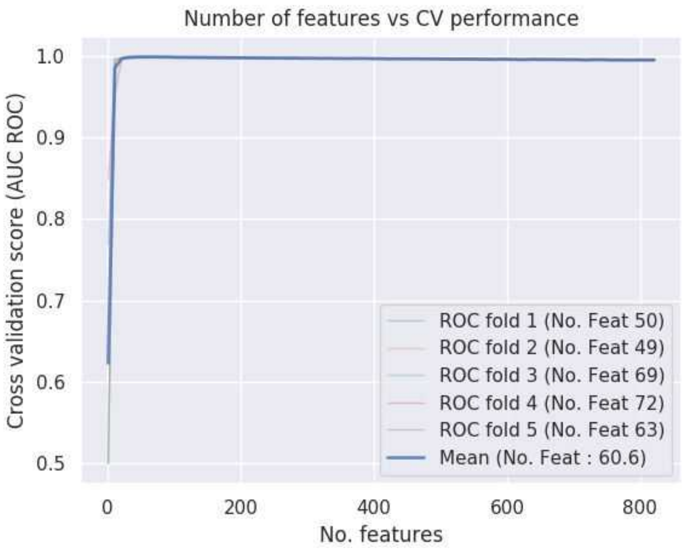
Outlier classification : [100, 1000]



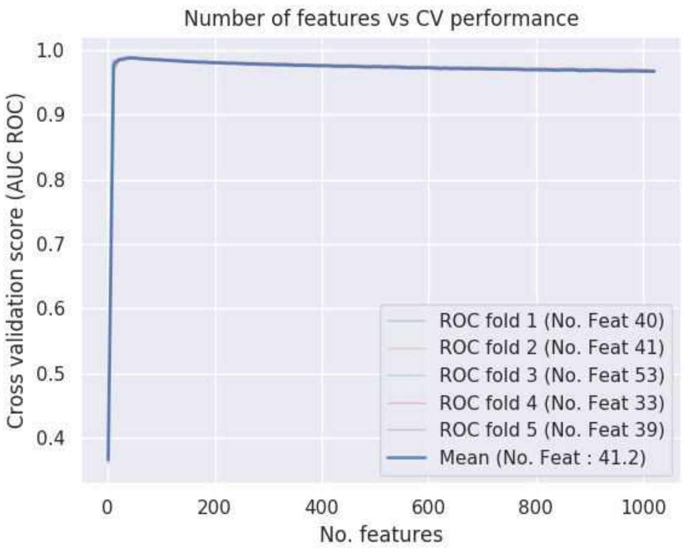
Outlier classification : >= 1000



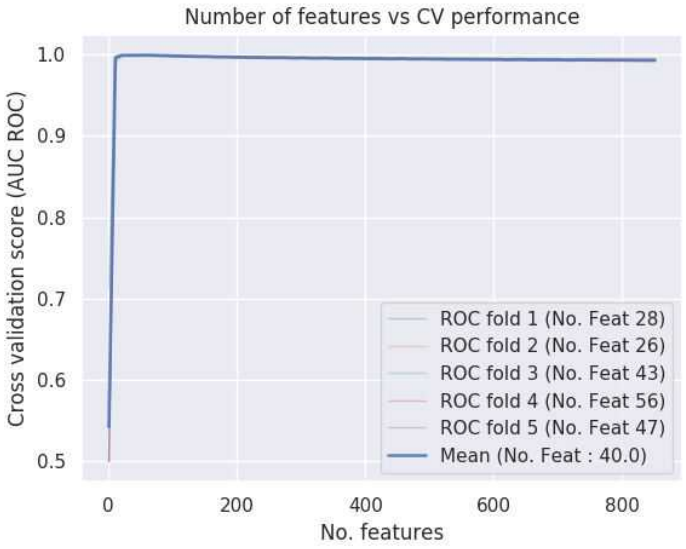
RFE



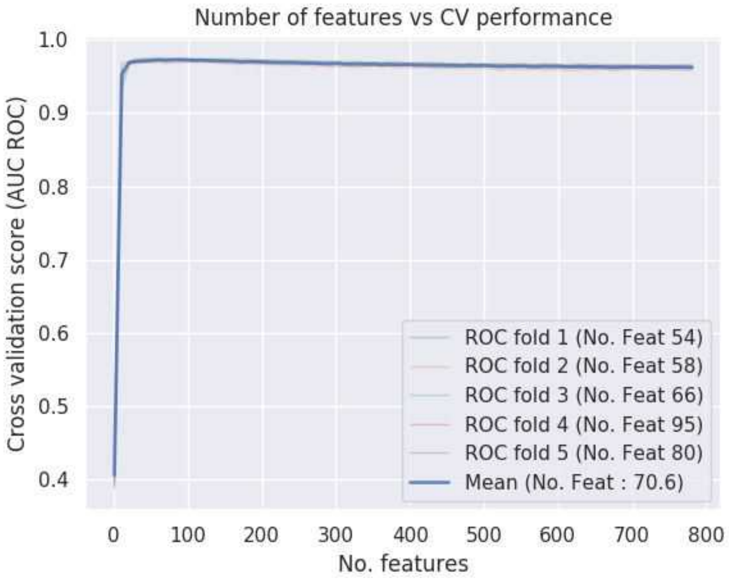
Number of features vs CV performance
Cross validation score (AUC ROC)
1.0
0.9
0.8
0.7
0.6
0.5
0
200
400
600
800
No. features
ROC fold 1 (No. Feat 50)
ROC fold 2 (No. Feat 49)
ROC fold 3 (No. Feat 69)
ROC fold 4 (No. Feat 72)
ROC fold 5 (No. Feat 63)
Mean (No. Feat : 60.6)



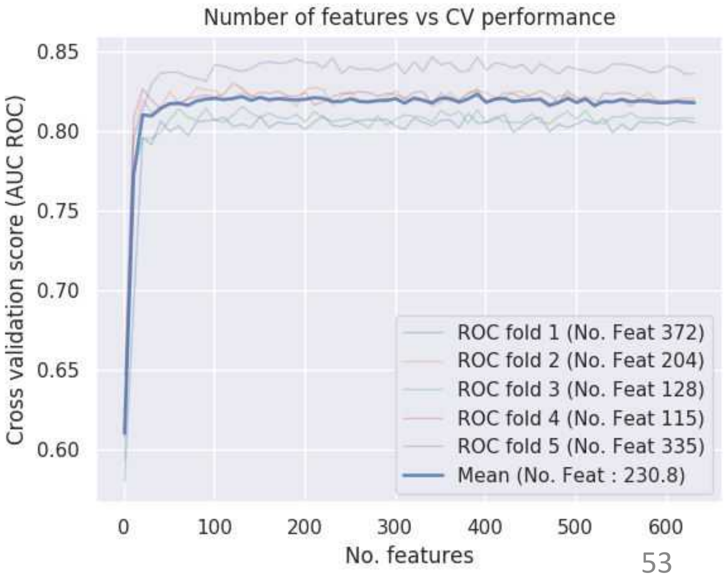
Number of features vs CV performance
Cross validation score (AUC ROC)
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0
200
400
600
800
1000
No. features
ROC fold 1 (No. Feat 40)
ROC fold 2 (No. Feat 41)
ROC fold 3 (No. Feat 53)
ROC fold 4 (No. Feat 33)
ROC fold 5 (No. Feat 39)
Mean (No. Feat : 41.2)



Number of features vs CV performance
Cross validation score (AUC ROC)
1.0
0.9
0.8
0.7
0.6
0.5
0
200
400
600
800
No. features
ROC fold 1 (No. Feat 28)
ROC fold 2 (No. Feat 26)
ROC fold 3 (No. Feat 43)
ROC fold 4 (No. Feat 56)
ROC fold 5 (No. Feat 47)
Mean (No. Feat : 40.0)



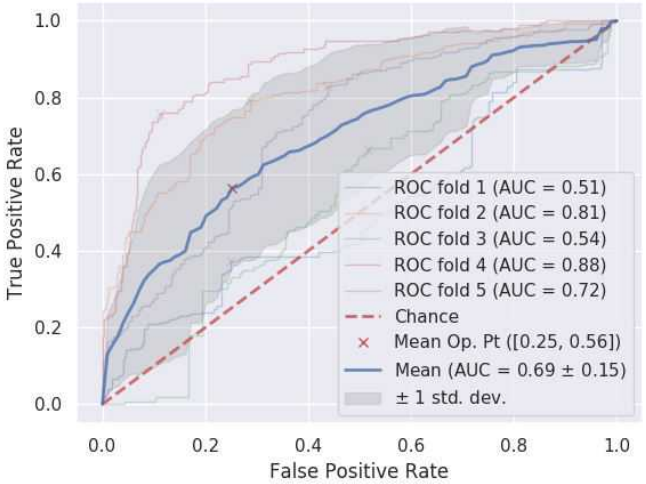
Number of features vs CV performance
Cross validation score (AUC ROC)
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0
100
200
300
400
500
600
700
800
No. features
ROC fold 1 (No. Feat 54)
ROC fold 2 (No. Feat 58)
ROC fold 3 (No. Feat 66)
ROC fold 4 (No. Feat 95)
ROC fold 5 (No. Feat 80)
Mean (No. Feat : 70.6)



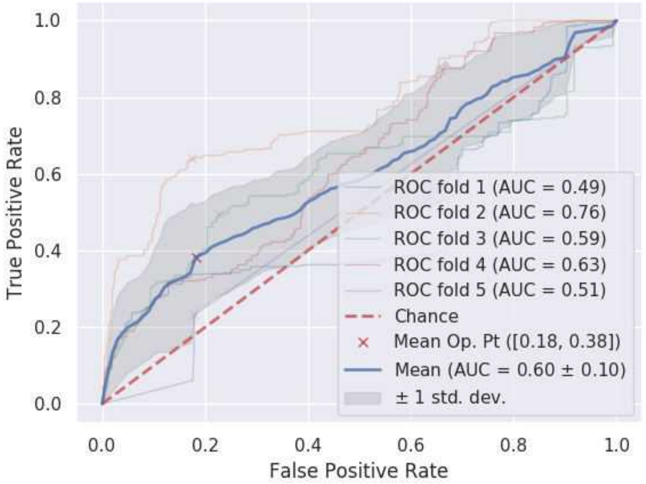
Number of features vs CV performance
Cross validation score (AUC ROC)
0.85
0.80
0.75
0.70
0.65
0.60
0
100
200
300
400
500
600
No. features
ROC fold 1 (No. Feat 372)
ROC fold 2 (No. Feat 204)
ROC fold 3 (No. Feat 128)
ROC fold 4 (No. Feat 115)
ROC fold 5 (No. Feat 335)
Mean (No. Feat : 230.8)

Victim Lier classification (cont'd) CERT ONLY

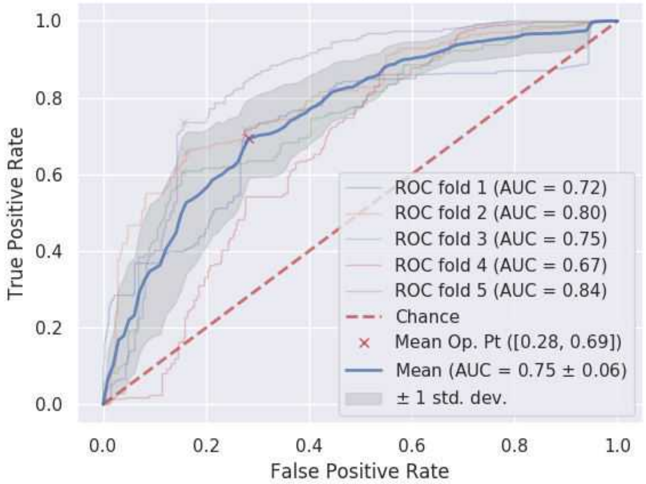
DEPTH:15.00 OOB:0.93 Lier:outliers NV:SEC500
Max_ss:350 Match:CERTS Size:400



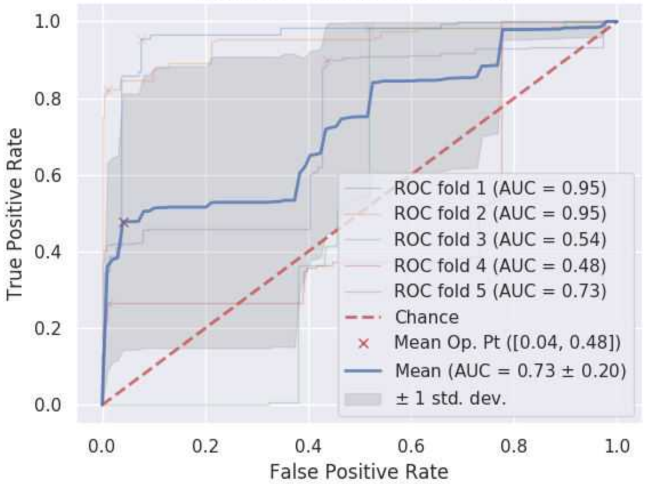
DEPTH:15.00 OOB:0.95 Lier:outliers NV:CERT
Max_ss:350 Match:CERTS Size:400



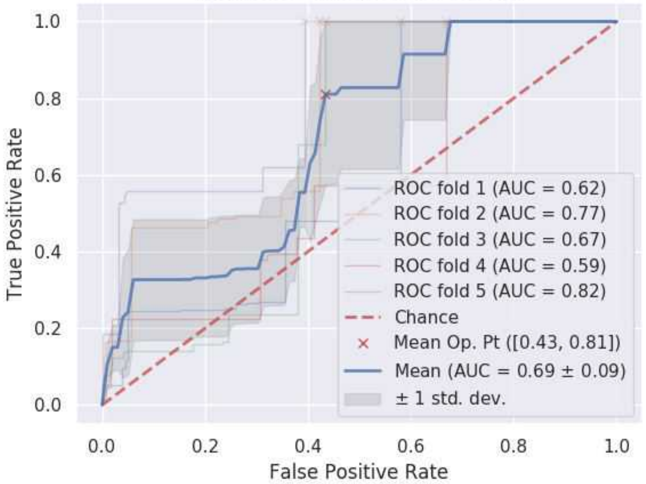
DEPTH:15.00 OOB:0.94 Lier:outliers NV:DNS
Max_ss:350 Match:CERTS Size:400



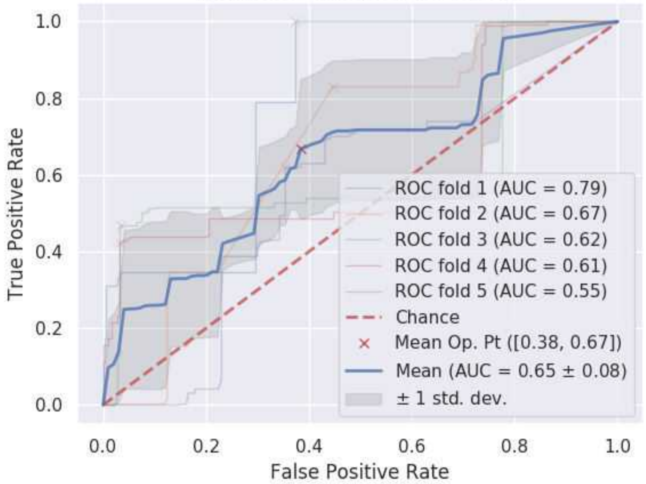
DEPTH:15.00 OOB:0.99 Lier:inliers NV:SEC500
Max_ss:350 Match:CERTS Size:400



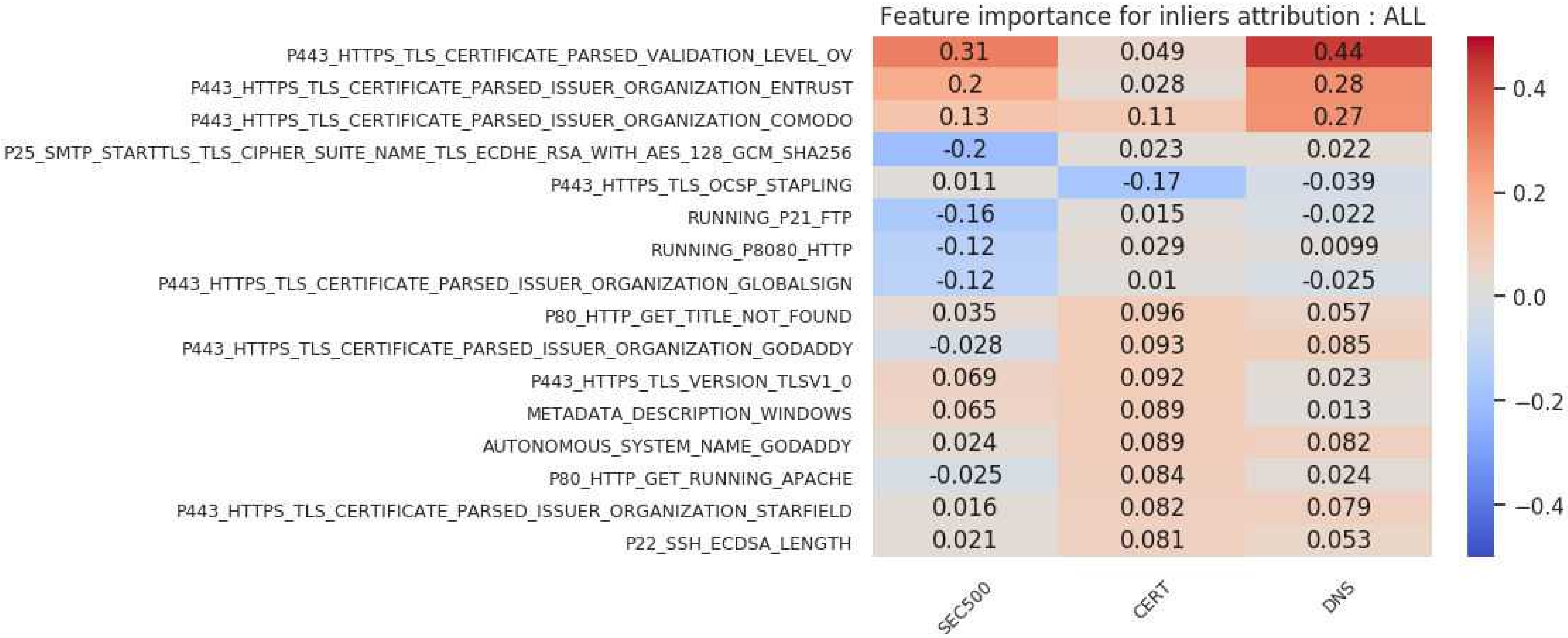
DEPTH:15.00 OOB:1.00 Lier:inliers NV:CERT
Max_ss:350 Match:CERTS Size:400



DEPTH:15.00 OOB:0.99 Lier:inliers NV:DNS
Max_ss:350 Match:CERTS Size:400



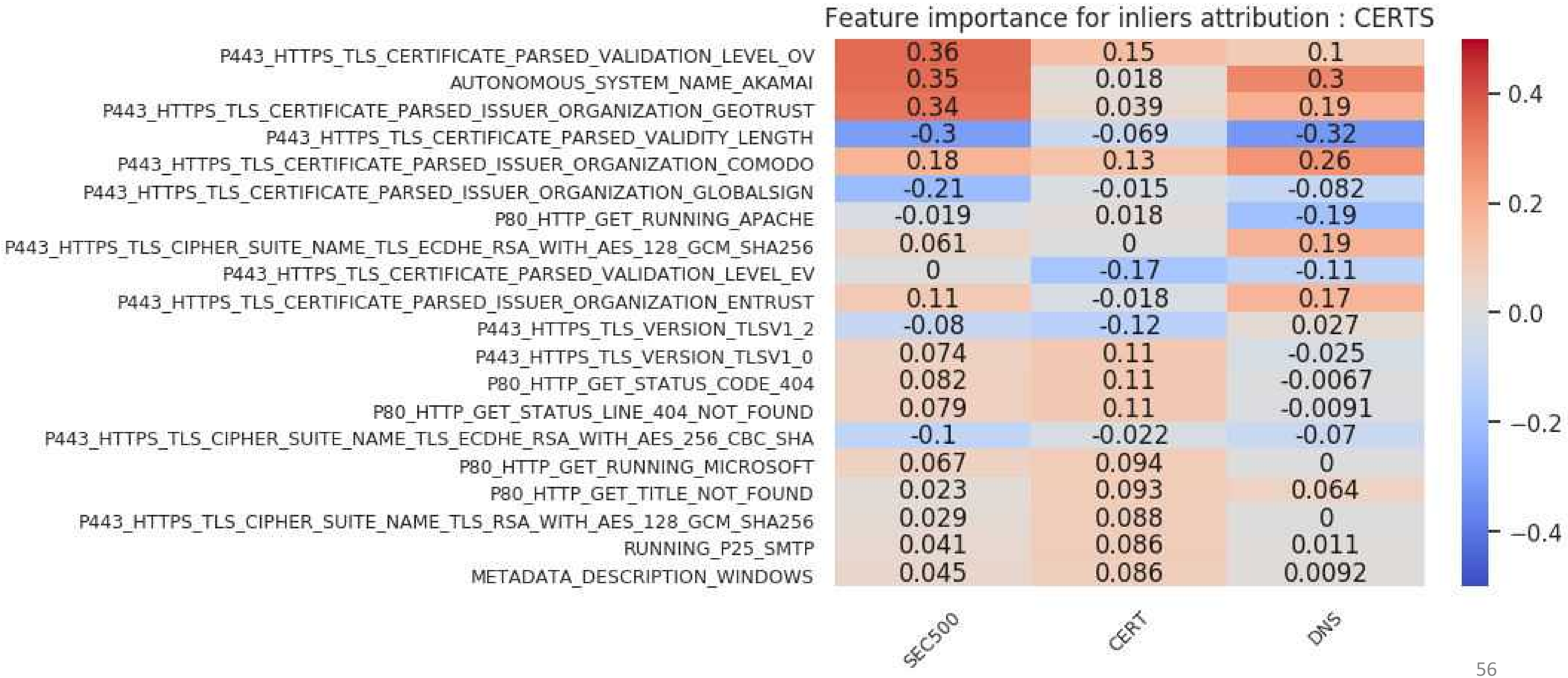
Victim Lier Classification- Inliers



Feature importance for inliers attribution : ALL

	SEC500	CERT	DNS
P443_HTTPS_TLS_CERTIFICATE_PARSED_VALIDATION_LEVEL_OV	0.31	0.049	0.44
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_ENTRUST	0.2	0.028	0.28
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_COMODO	0.13	0.11	0.27
P25_SMTP_STARTTLS_TLS_CIPHER_SUITE_NAME_TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	-0.2	0.023	0.022
P443_HTTPS_TLS_OCSP_STAPLING	0.011	-0.17	-0.039
RUNNING_P21_FTP	-0.16	0.015	-0.022
RUNNING_P8080_HTTP	-0.12	0.029	0.0099
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_GLOBALSIGN	-0.12	0.01	-0.025
P80_HTTP_GET_TITLE_NOT_FOUND	0.035	0.096	0.057
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_GODADDY	-0.028	0.093	0.085
P443_HTTPS_TLS_VERSION_TLSV1_0	0.069	0.092	0.023
METADATA_DESCRIPTION_WINDOWS	0.065	0.089	0.013
AUTONOMOUS_SYSTEM_NAME_GODADDY	0.024	0.089	0.082
P80_HTTP_GET_RUNNING_APACHE	-0.025	0.084	0.024
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_STARFIELD	0.016	0.082	0.079
P22_SSH_ECDSA_LENGTH	0.021	0.081	0.053

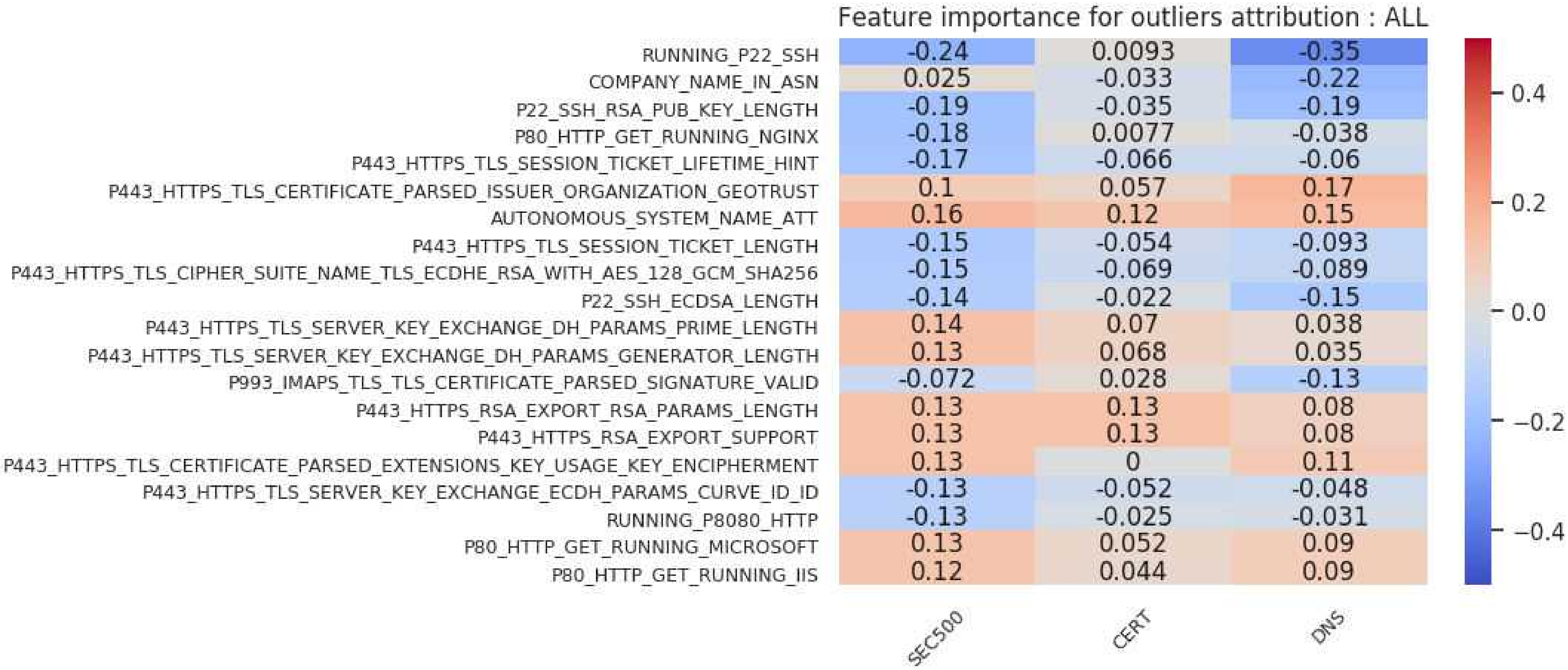
Victim Lier Classification- Inliers



Feature importance for inliers attribution : CERTS

	SEC500	CERT	DNS
P443_HTTPS_TLS_CERTIFICATE_PARSED_VALIDATION_LEVEL_OV	0.36	0.15	0.1
AUTONOMOUS_SYSTEM_NAME_AKAMAI	0.35	0.018	0.3
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_GEOTRUST	0.34	0.039	0.19
P443_HTTPS_TLS_CERTIFICATE_PARSED_VALIDITY_LENGTH	-0.3	-0.069	-0.32
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_COMODO	0.18	0.13	0.26
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_GLOBALSIGN	-0.21	-0.015	-0.082
P80_HTTP_GET_RUNNING_APACHE	-0.019	0.018	-0.19
P443_HTTPS_TLS_CIPHER_SUITE_NAME_TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0.061	0	0.19
P443_HTTPS_TLS_CERTIFICATE_PARSED_VALIDATION_LEVEL_EV	0	-0.17	-0.11
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_ENTRUST	0.11	-0.018	0.17
P443_HTTPS_TLS_VERSION_TLSV1_2	-0.08	-0.12	0.027
P443_HTTPS_TLS_VERSION_TLSV1_0	0.074	0.11	-0.025
P80_HTTP_GET_STATUS_CODE_404	0.082	0.11	-0.0067
P80_HTTP_GET_STATUS_LINE_404_NOT_FOUND	0.079	0.11	-0.0091
P443_HTTPS_TLS_CIPHER_SUITE_NAME_TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	-0.1	-0.022	-0.07
P80_HTTP_GET_RUNNING_MICROSOFT	0.067	0.094	0
P80_HTTP_GET_TITLE_NOT_FOUND	0.023	0.093	0.064
P443_HTTPS_TLS_CIPHER_SUITE_NAME_TLS_RSA_WITH_AES_128_GCM_SHA256	0.029	0.088	0
RUNNING_P25_SMTP	0.041	0.086	0.011
METADATA_DESCRIPTION_WINDOWS	0.045	0.086	0.0092

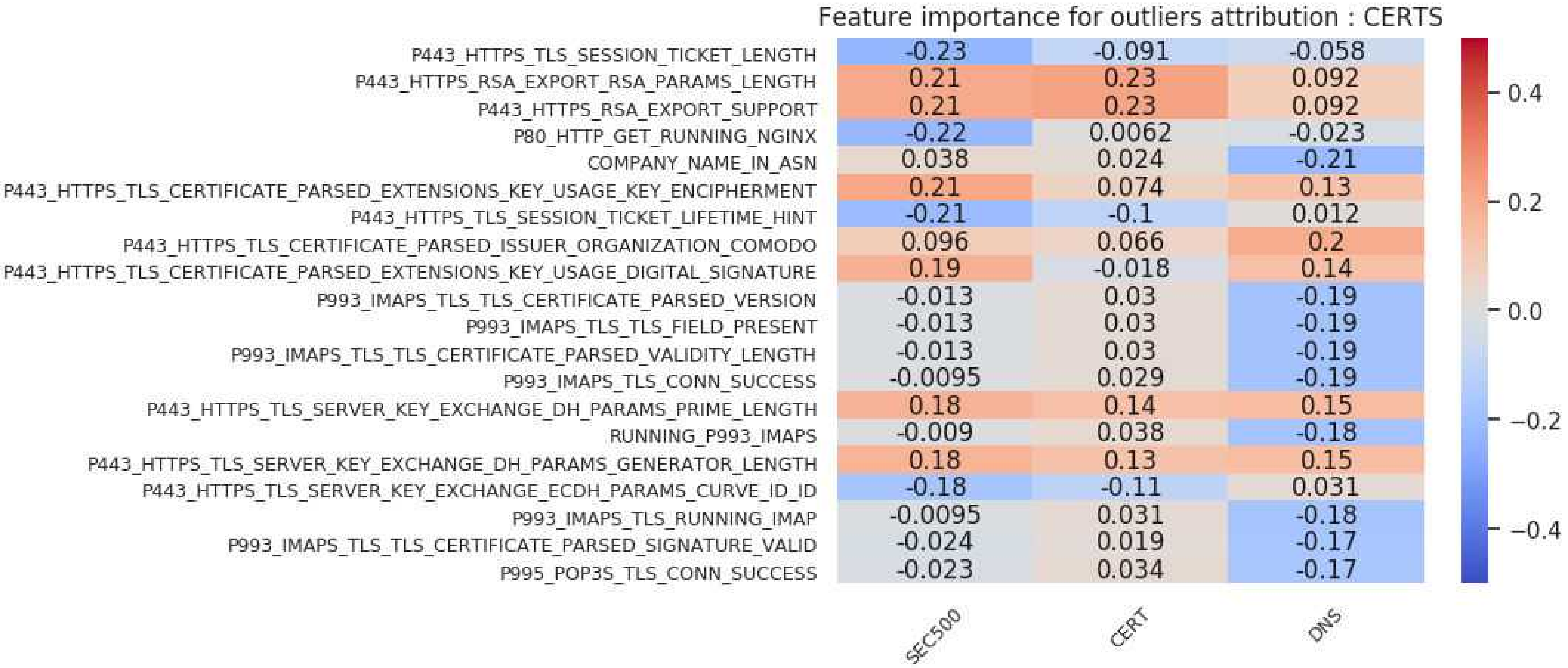
Victim Lier Classification- Outliers



Feature importance for outliers attribution : ALL

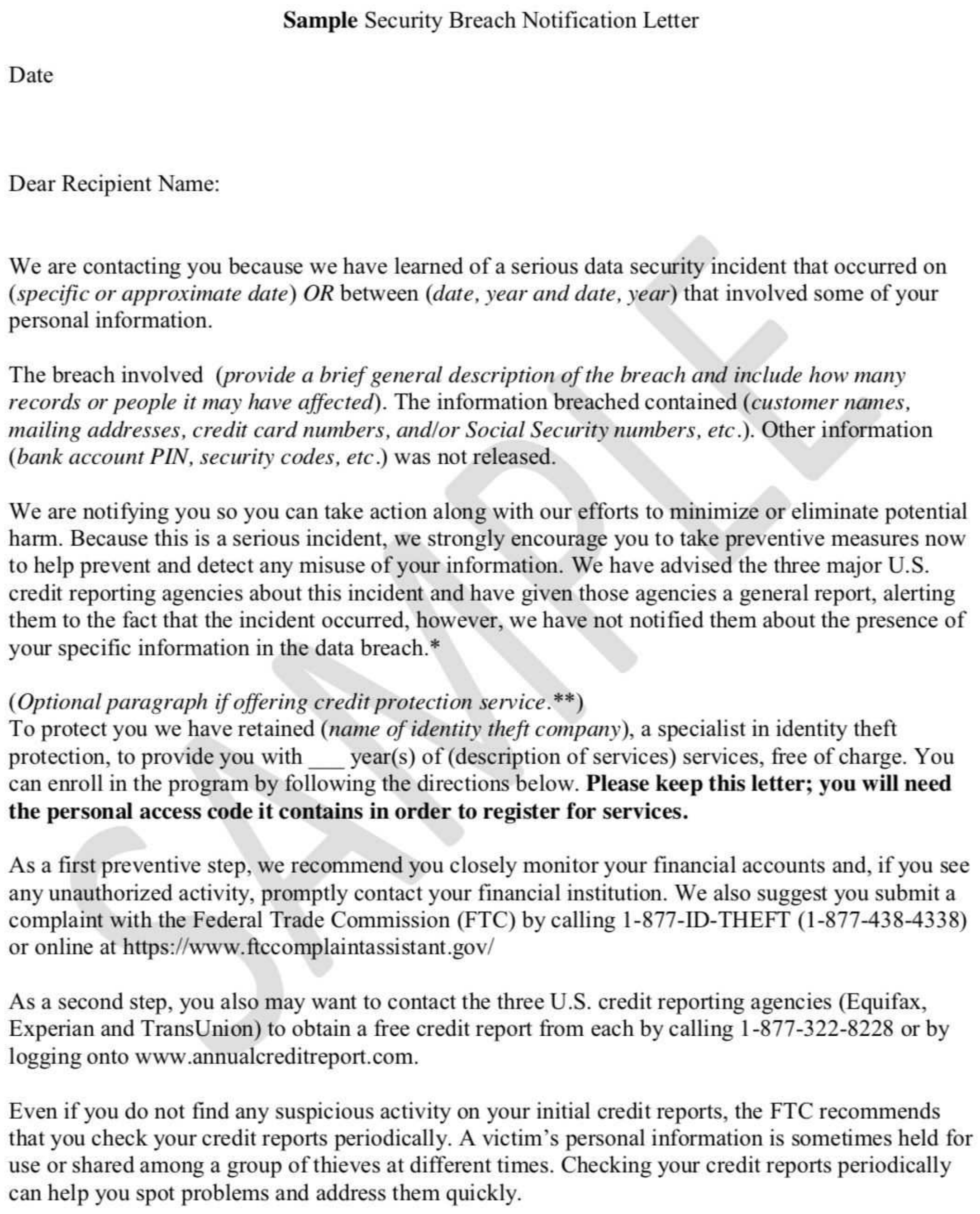
	SEC500	CERT	DNS
RUNNING_P22_SSH	-0.24	0.0093	-0.35
COMPANY_NAME_IN_ASN	0.025	-0.033	-0.22
P22_SSH_RSA_PUB_KEY_LENGTH	-0.19	-0.035	-0.19
P80_HTTP_GET_RUNNING_NGINX	-0.18	0.0077	-0.038
P443_HTTPS_TLS_SESSION_TICKET_LIFETIME_HINT	-0.17	-0.066	-0.06
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_GEOTRUST	0.1	0.057	0.17
AUTONOMOUS_SYSTEM_NAME_ATT	0.16	0.12	0.15
P443_HTTPS_TLS_SESSION_TICKET_LENGTH	-0.15	-0.054	-0.093
P443_HTTPS_TLS_CIPHER_SUITE_NAME_TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	-0.15	-0.069	-0.089
P22_SSH_ECDSA_LENGTH	-0.14	-0.022	-0.15
P443_HTTPS_TLS_SERVER_KEY_EXCHANGE_DH_PARAMS_PRIME_LENGTH	0.14	0.07	0.038
P443_HTTPS_TLS_SERVER_KEY_EXCHANGE_DH_PARAMS_GENERATOR_LENGTH	0.13	0.068	0.035
P993_IMAPS_TLS_TLS_CERTIFICATE_PARSED_SIGNATURE_VALID	-0.072	0.028	-0.13
P443_HTTPS_RSA_EXPORT_RSA_PARAMS_LENGTH	0.13	0.13	0.08
P443_HTTPS_RSA_EXPORT_SUPPORT	0.13	0.13	0.08
P443_HTTPS_TLS_CERTIFICATE_PARSED_EXTENSIONS_KEY_USAGE_KEY_ENCIPHERMENT	0.13	0	0.11
P443_HTTPS_TLS_SERVER_KEY_EXCHANGE_ECDH_PARAMS_CURVE_ID_ID	-0.13	-0.052	-0.048
RUNNING_P8080_HTTP	-0.13	-0.025	-0.031
P80_HTTP_GET_RUNNING_MICROSOFT	0.13	0.052	0.09
P80_HTTP_GET_RUNNING_IIS	0.12	0.044	0.09

Victim Lier Classification- Outliers



Feature importance for outliers attribution : CERTS

	SEC500	CERT	DNS
P443_HTTPS_TLS_SESSION_TICKET_LENGTH	-0.23	-0.091	-0.058
P443_HTTPS_RSA_EXPORT_RSA_PARAMS_LENGTH	0.21	0.23	0.092
P443_HTTPS_RSA_EXPORT_SUPPORT	0.21	0.23	0.092
P80_HTTP_GET_RUNNING_NGINX	-0.22	0.0062	-0.023
COMPANY_NAME_IN_ASN	0.038	0.024	-0.21
P443_HTTPS_TLS_CERTIFICATE_PARSED_EXTENSIONS_KEY_USAGE_KEY_ENCIPHERMENT	0.21	0.074	0.13
P443_HTTPS_TLS_SESSION_TICKET_LIFETIME_HINT	-0.21	-0.1	0.012
P443_HTTPS_TLS_CERTIFICATE_PARSED_ISSUER_ORGANIZATION_COMODO	0.096	0.066	0.2
P443_HTTPS_TLS_CERTIFICATE_PARSED_EXTENSIONS_KEY_USAGE_DIGITAL_SIGNATURE	0.19	-0.018	0.14
P993_IMAPS_TLS_TLS_CERTIFICATE_PARSED_VERSION	-0.013	0.03	-0.19
P993_IMAPS_TLS_TLS_FIELD_PRESENT	-0.013	0.03	-0.19
P993_IMAPS_TLS_TLS_CERTIFICATE_PARSED_VALIDITY_LENGTH	-0.013	0.03	-0.19
P993_IMAPS_TLS_CONN_SUCCESS	-0.0095	0.029	-0.19
P443_HTTPS_TLS_SERVER_KEY_EXCHANGE_DH_PARAMS_PRIME_LENGTH	0.18	0.14	0.15
RUNNING_P993_IMAPS	-0.009	0.038	-0.18
P443_HTTPS_TLS_SERVER_KEY_EXCHANGE_DH_PARAMS_GENERATOR_LENGTH	0.18	0.13	0.15
P443_HTTPS_TLS_SERVER_KEY_EXCHANGE_ECDH_PARAMS_CURVE_ID_ID	-0.18	-0.11	0.031
P993_IMAPS_TLS_RUNNING_IMAP	-0.0095	0.031	-0.18
P993_IMAPS_TLS_TLS_CERTIFICATE_PARSED_SIGNATURE_VALID	-0.024	0.019	-0.17
P995_POP3S_TLS_CONN_SUCCESS	-0.023	0.034	-0.17



Sample Security Breach Notification Letter

Date

Dear Recipient Name:

We are contacting you because we have learned of a serious data security incident that occurred on (*specific or approximate date*) *OR* between (*date, year and date, year*) that involved some of your personal information.

The breach involved (*provide a brief general description of the breach and include how many records or people it may have affected*). The information breached contained (*customer names, mailing addresses, credit card numbers, and/or Social Security numbers, etc*.). Other information (*bank account PIN, security codes, etc*.) was not released.

We are notifying you so you can take action along with our efforts to minimize or eliminate potential harm. Because this is a serious incident, we strongly encourage you to take preventive measures now to help prevent and detect any misuse of your information. We have advised the three major U.S. credit reporting agencies about this incident and have given those agencies a general report, alerting them to the fact that the incident occurred, however, we have not notified them about the presence of your specific information in the data breach.*

(*Optional paragraph if offering credit protection service.***)
To protect you we have retained (*name of identity theft company*), a specialist in identity theft protection, to provide you with ___ year(s) of (description of services) services, free of charge. You can enroll in the program by following the directions below. **Please keep this letter; you will need the personal access code it contains in order to register for services.**

As a first preventive step, we recommend you closely monitor your financial accounts and, if you see any unauthorized activity, promptly contact your financial institution. We also suggest you submit a complaint with the Federal Trade Commission (FTC) by calling 1-877-ID-THEFT (1-877-438-4338) or online at https://www.ftccomplaintassistant.gov/

As a second step, you also may want to contact the three U.S. credit reporting agencies (Equifax, Experian and TransUnion) to obtain a free credit report from each by calling 1-877-322-8228 or by logging onto www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically. A victim's personal information is sometimes held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.