

Detecting Network Intrusions

Janet Carson



3 Million
Records
Stolen Every
Day

- Retail
- Healthcare
- Government

Network logs

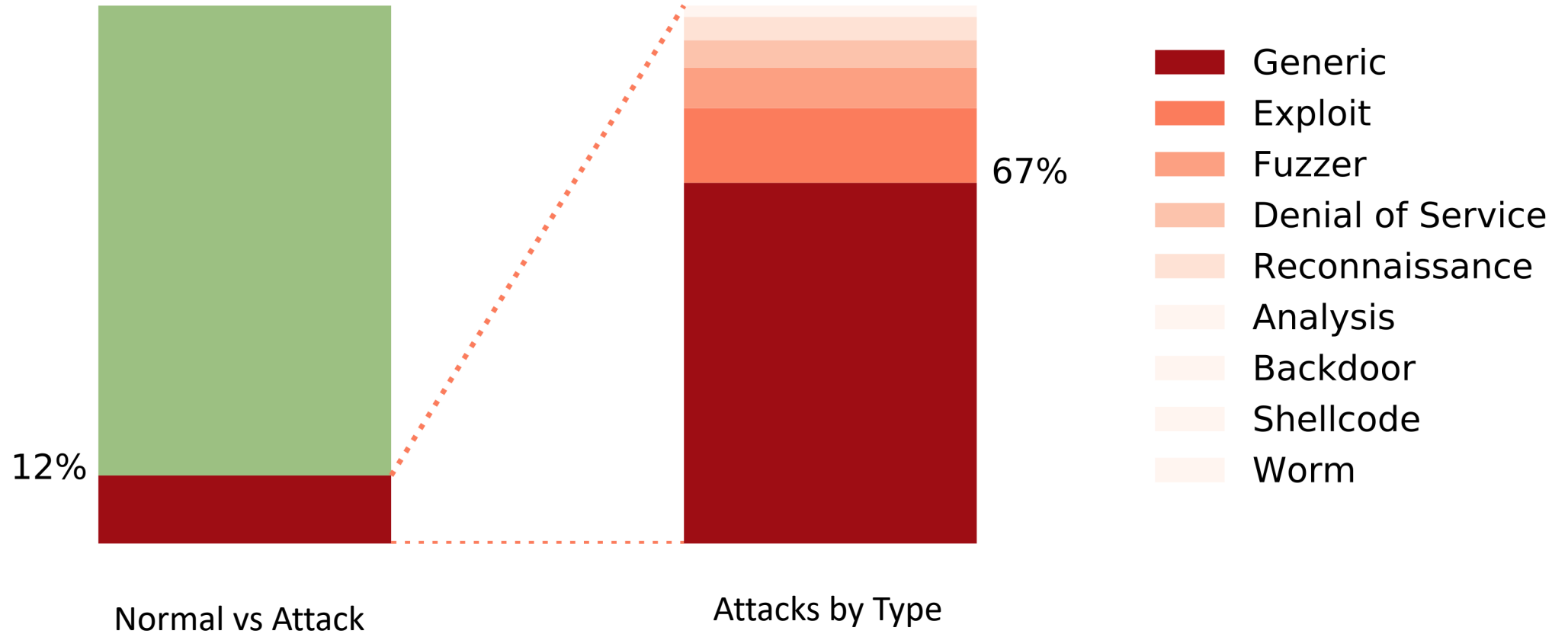
- Records of computer network traffic
- Can be used for real-time analysis or for forensic investigation

UNSW-NB15 Dataset

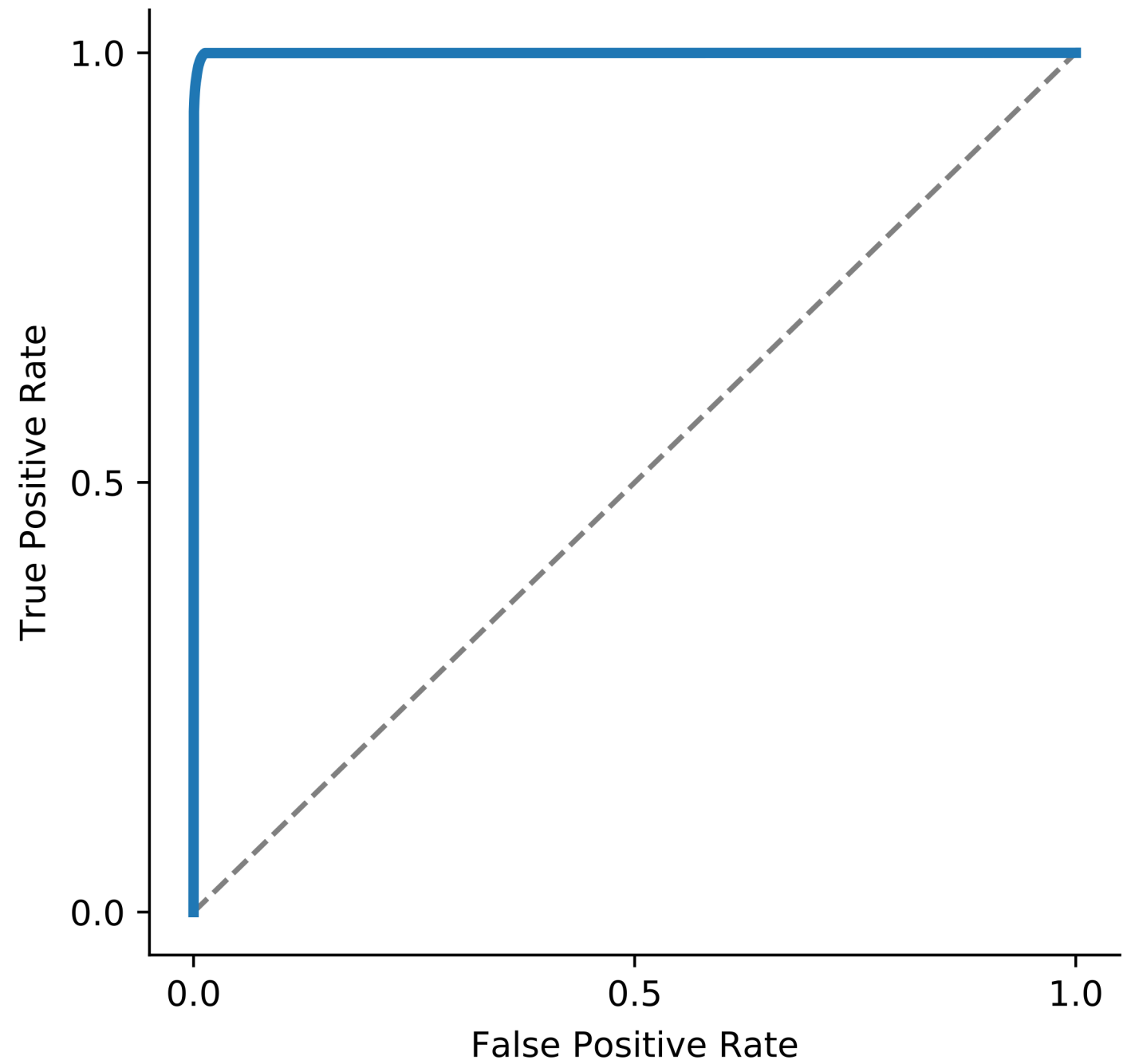
- 2,500,000 records
- 174,000 Attacks
- 3,000 Vulnerabilities

1. Normal
2. Generic
3. Exploits
4. Fuzzers
5. Denial of Service
6. Reconnaissance
7. Analysis
8. Backdoors
9. Shell code
10. Worms

Unbalanced Data



Attack Detection



Attack Labeling

Actual Record Type

Normal	99	0	0	1	0	0	0	0	0	0
Generic	0	98	1	0	1	0	0	0	0	0
Exploit	0	0	60	3	26	2	2	5	0	0
Fuzzer	0	0	1	87	6	1	2	3	0	0
Deny Serv	0	0	22	2	57	1	5	12	1	0
Reconn	0	0	7	1	12	78	1	2	0	0
Analysis	1	0	8	2	49	0	20	21	0	0
Backdoor	0	0	13	4	51	1	14	16	0	0
Shellcode	0	0	6	24	1	5	0	0	64	0
Worm	0	0	68	4	0	1	0	0	0	26
	Normal	Generic	Exploit	Fuzzer	Deny Serv	Reconn	Analysis	Backdoor	Shellcode	Worm

Model Output

Attack Labeling

99% Normal

Actual Record Type

	Normal	Generic	Exploit	Fuzzer	Deny Serv	Reconn	Analysis	Backdoor	Shellcode	Worm
Normal	99	0	0	1	0	0	0	0	0	0
Generic	0	98	1	0	1	0	0	0	0	0
Exploit	0	0	60	3	26	2	2	5	0	0
Fuzzer	0	0	1	87	6	1	2	3	0	0
Deny Serv	0	0	22	2	57	1	5	12	1	0
Reconn	0	0	7	1	12	78	1	2	0	0
Analysis	1	0	8	2	49	0	20	21	0	0
Backdoor	0	0	13	4	51	1	14	16	0	0
Shellcode	0	0	6	24	1	5	0	0	64	0
Worm	0	0	68	4	0	1	0	0	0	26
	Normal	Generic	Exploit	Fuzzer	Deny Serv	Reconn	Analysis	Backdoor	Shellcode	Worm

Model Output

Attack Labeling

1% False alarms

Actual Record Type

	Normal	Generic	Exploit	Fuzzer	Deny Serv	Reconn	Analysis	Backdoor	Shellcode	Worm
Normal	99	0	0	1	0	0	0	0	0	0
Generic	0	98	1	0	1	0	0	0	0	0
Exploit	0	0	60	3	26	2	2	5	0	0
Fuzzer	0	0	1	87	6	1	2	3	0	0
Deny Serv	0	0	22	2	57	1	5	12	1	0
Reconn	0	0	7	1	12	78	1	2	0	0
Analysis	1	0	8	2	49	0	20	21	0	0
Backdoor	0	0	13	4	51	1	14	16	0	0
Shellcode	0	0	6	24	1	5	0	0	64	0
Worm	0	0	68	4	0	1	0	0	0	26
	Normal	Generic	Exploit	Fuzzer	Deny Serv	Reconn	Analysis	Backdoor	Shellcode	Worm

Model Output

Attack Labeling

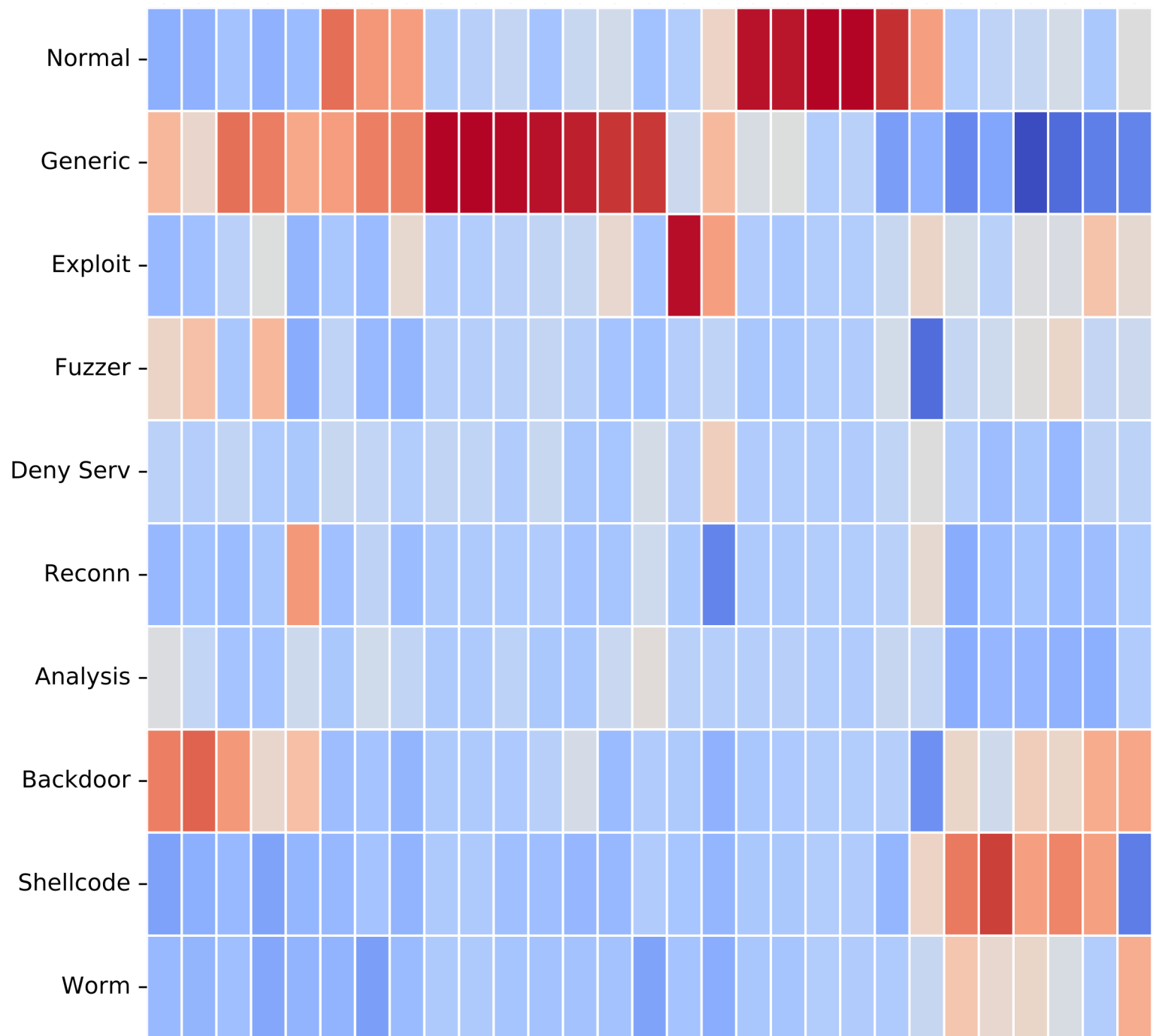
99.99% of attacks
-- 87% correct label

Actual Record Type

	Normal	Generic	Exploit	Fuzzer	Deny Serv	Reconn	Analysis	Backdoor	Shellcode	Worm
Normal	99	0	0	1	0	0	0	0	0	0
Generic	0	98	1	0	1	0	0	0	0	0
Exploit	0	0	60	3	26	2	2	5	0	0
Fuzzer	0	0	1	87	6	1	2	3	0	0
Deny Serv	0	0	22	2	57	1	5	12	1	0
Reconn	0	0	7	1	12	78	1	2	0	0
Analysis	1	0	8	2	49	0	20	21	0	0
Backdoor	0	0	13	4	51	1	14	16	0	0
Shellcode	0	0	6	24	1	5	0	0	64	0
Worm	0	0	68	4	0	1	0	0	0	26
	Normal	Generic	Exploit	Fuzzer	Deny Serv	Reconn	Analysis	Backdoor	Shellcode	Worm

Model Output

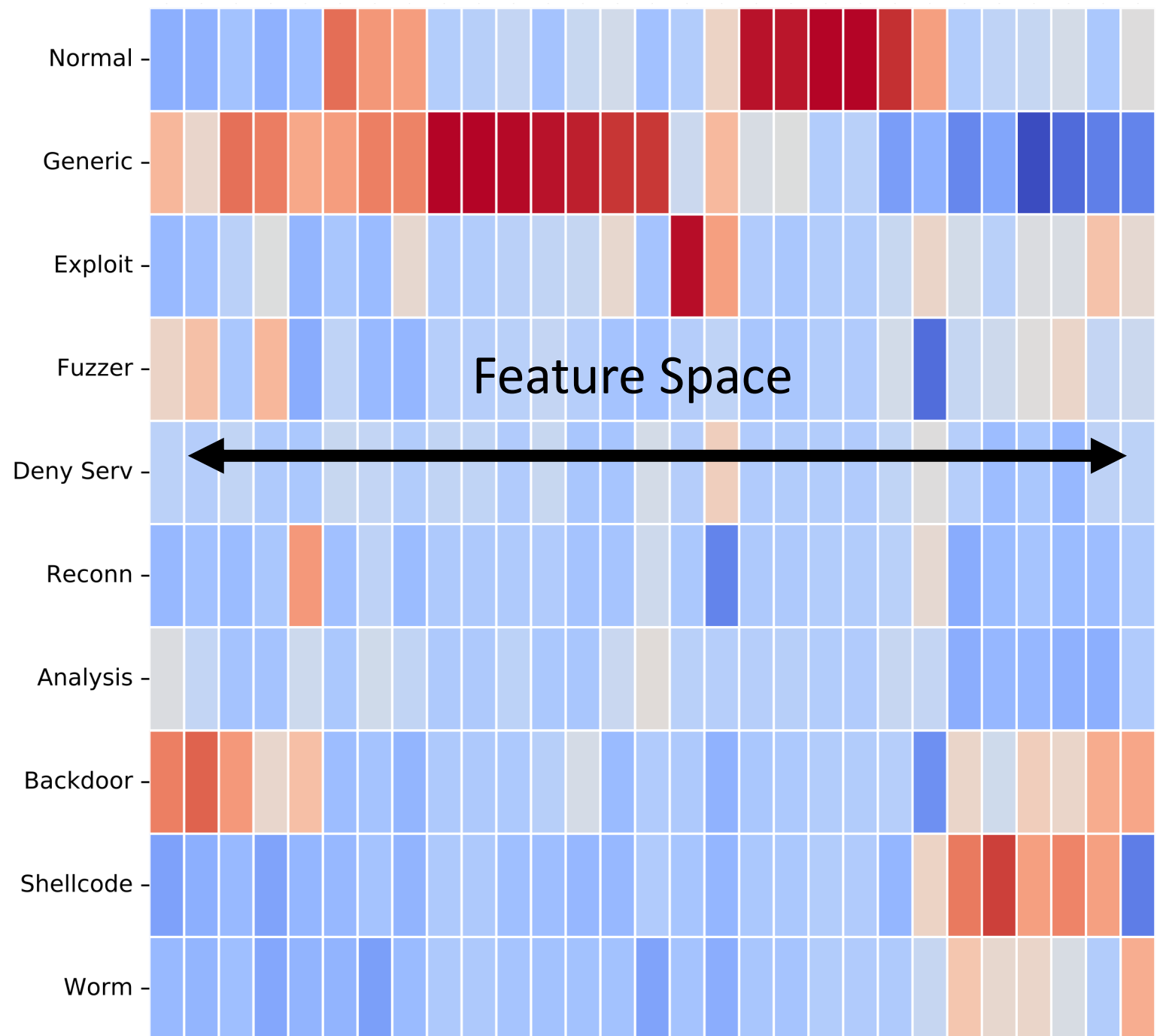
Underlying Data



Underlying Data

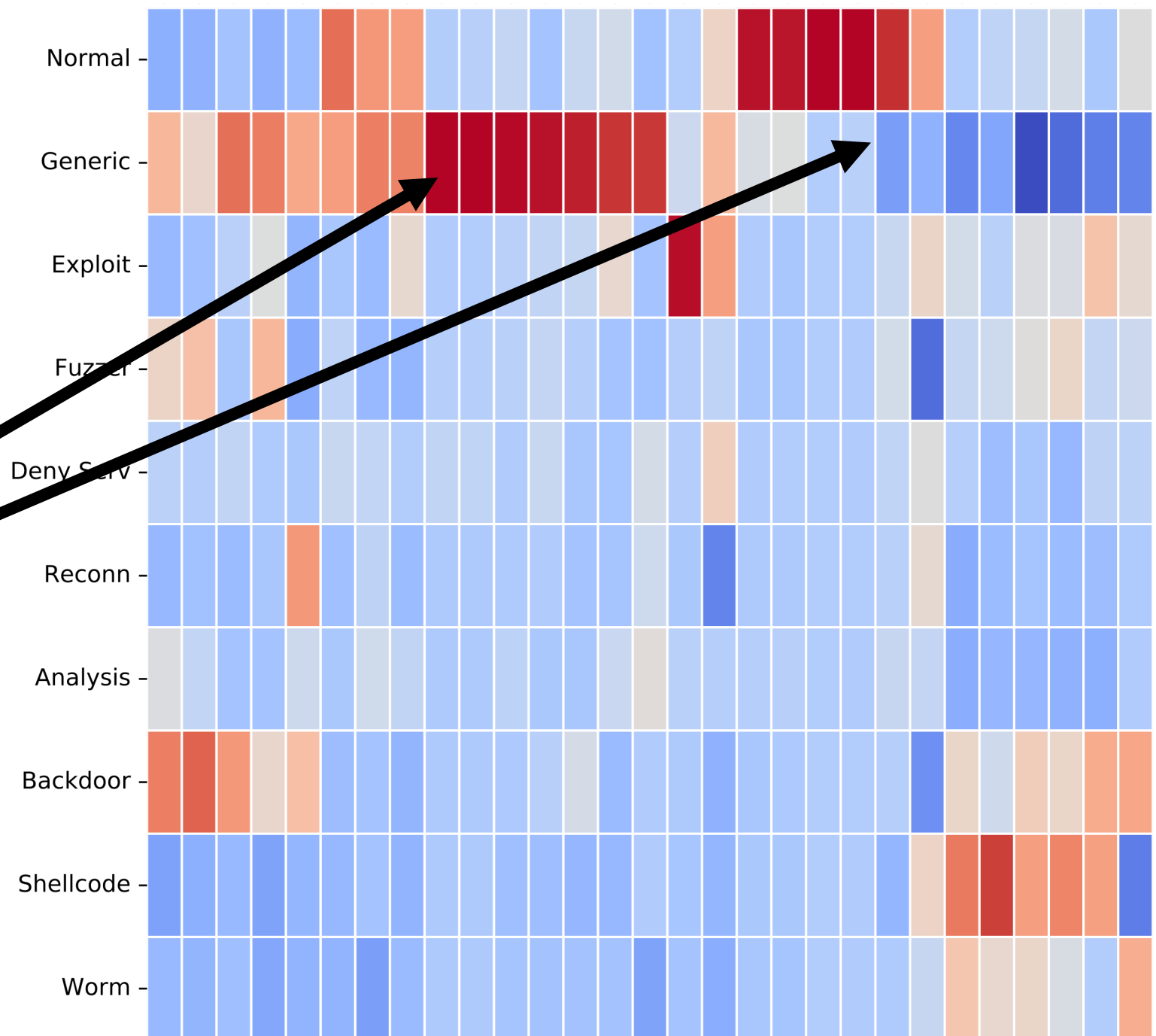


Underlying Data

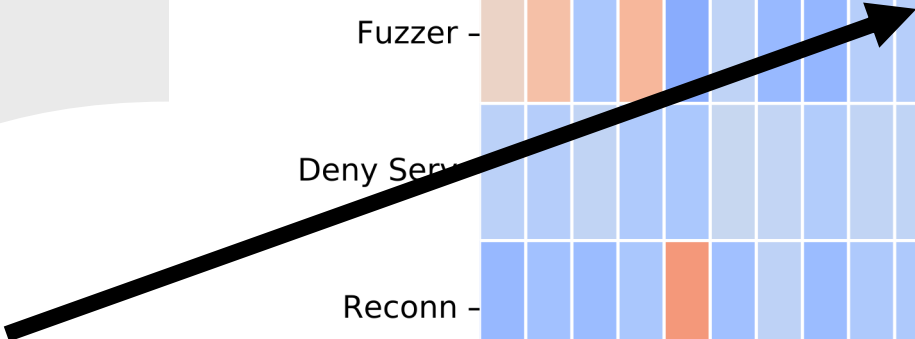


Underlying Data

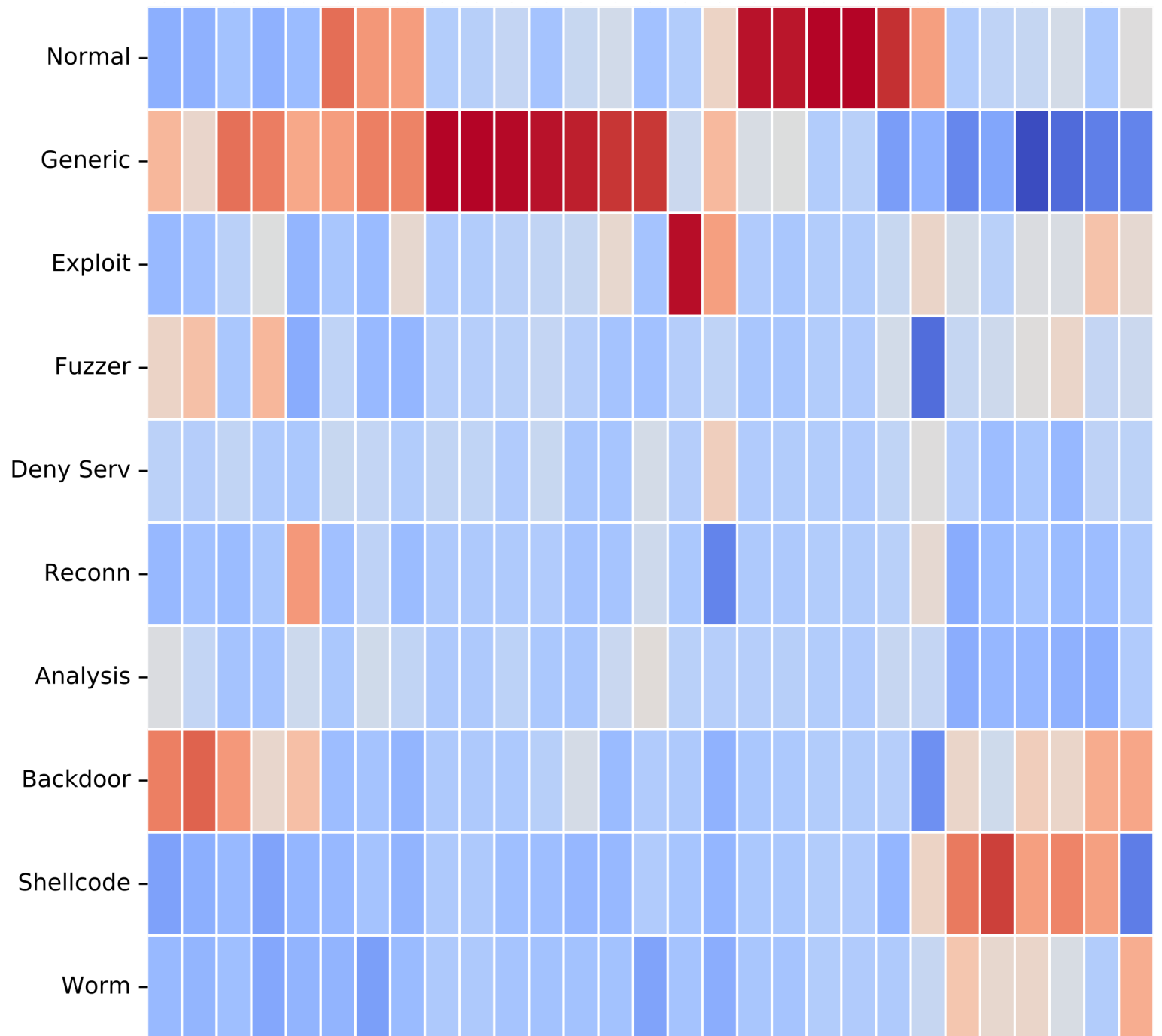
Distinctive features



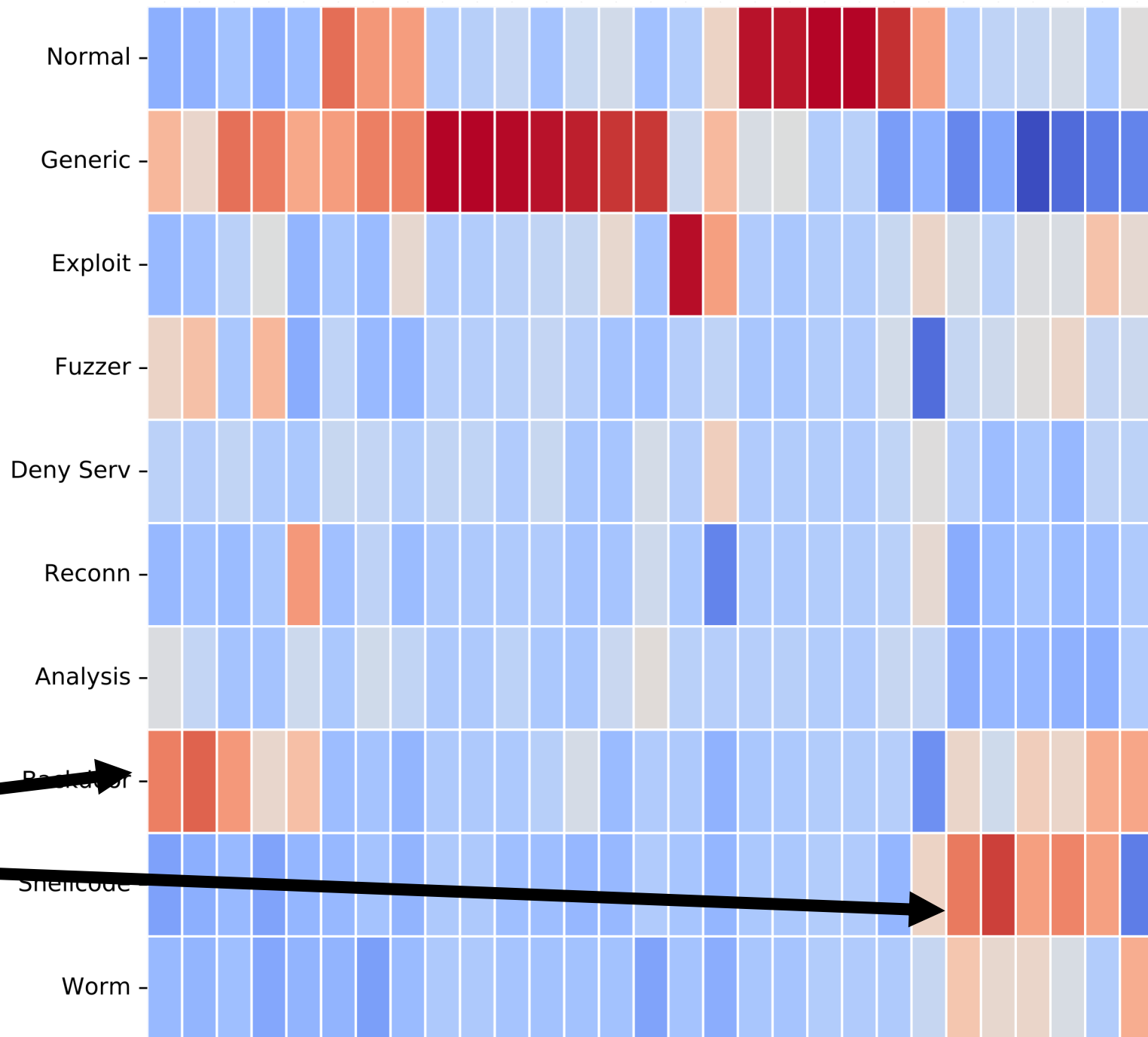
Underlying Data



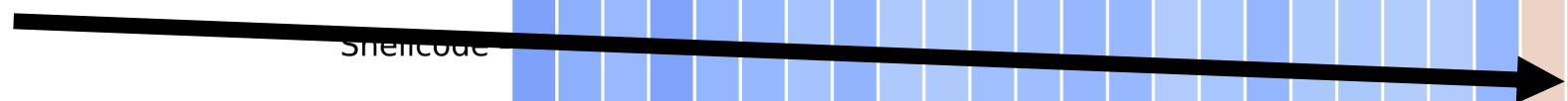
Underlying Data



Underlying Data



Fewer
strong
indicators



Conclusions and Future Work

- Successfully detected attacks, often their subtype
- Better training data would help
 - More balanced training examples
 - Feature extraction

Thank You

Janet Carson

 [carsondata](#)

