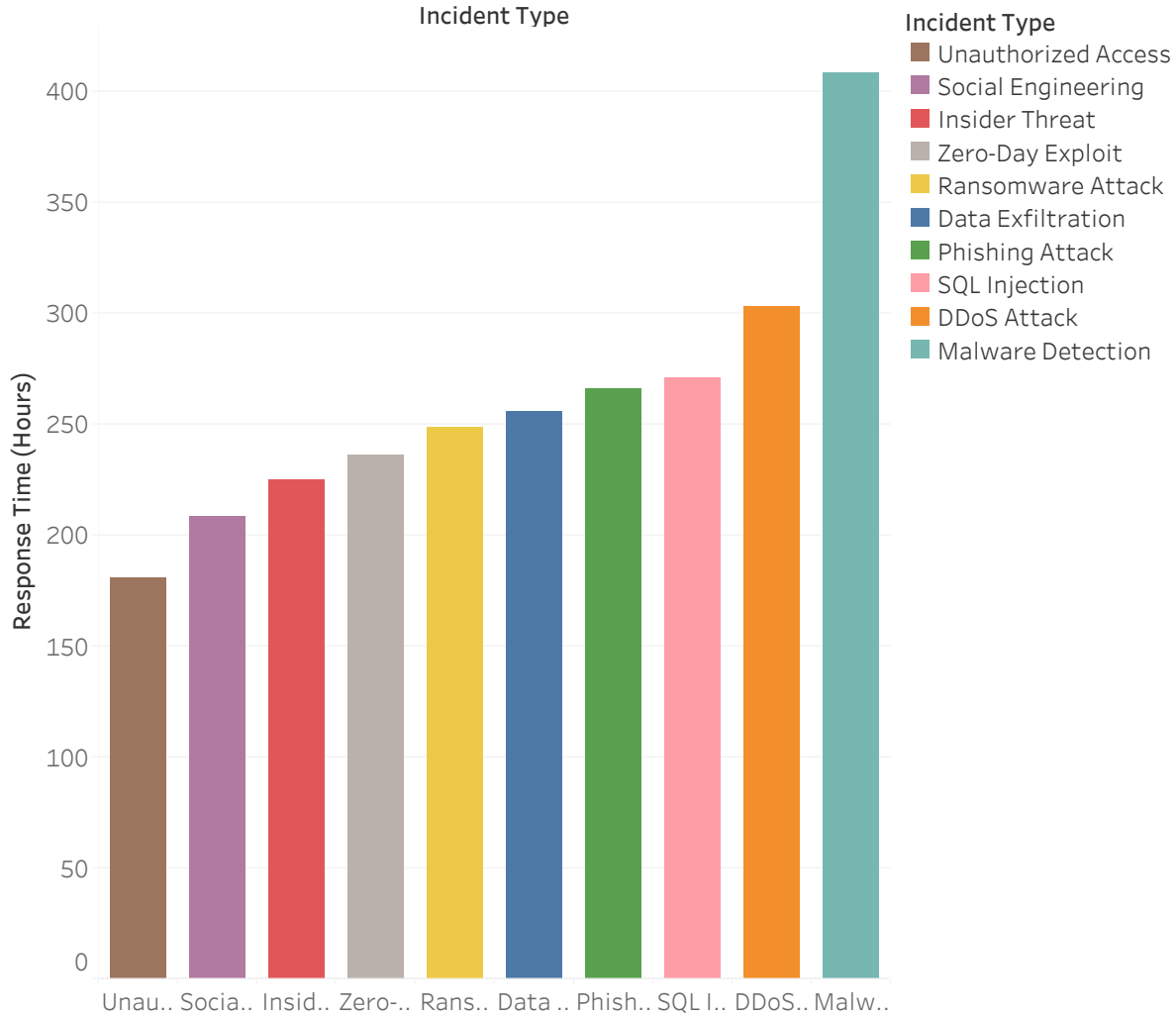
INCIDENT SEVERITY

Severit..	Count of Incide..
Critical	43
High	56
Low	55
Medium	46

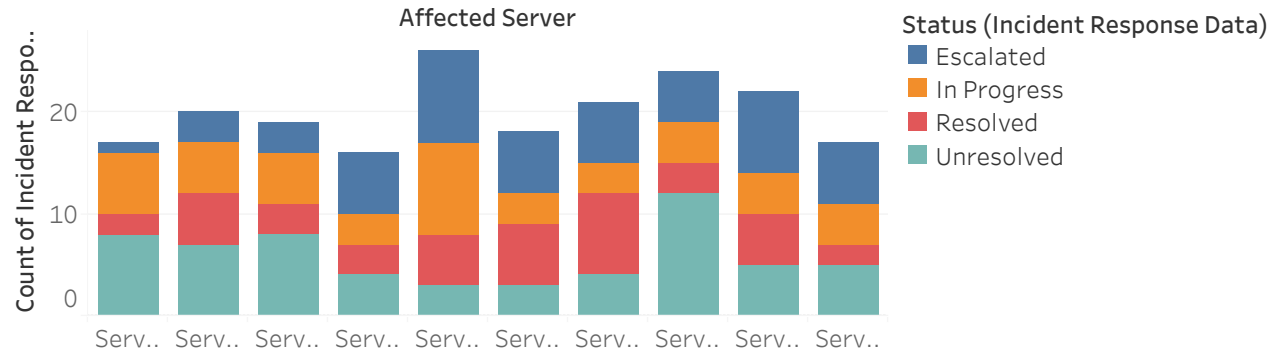
Count of Incident Response Data broken down by Severity (Incident Response Data). Color shows count of Incident Response Data. The marks are labeled by count of Incident Response Data. The data is filtered on Action (Incident Type) and Action (Incident Type,Location (Incident Response Data)). The Action (Incident Type) filter keeps 10 members. The Action (Incident Type,Location (Incident Response Data)) filter keeps 59 members.

INCIDENT VS RESPONSE TIME



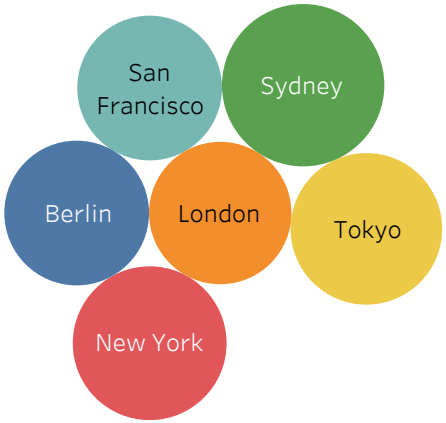
Sum of Response Time (Hours) for each Incident Type. Color shows details about Incident Type. The data is filtered on Affected Server, Action (Incident Type,Location (Incident Response Data)), Action (Incident Type) and Action (Severity (Incident Response Data),Status (Incident Response Data)). The Affected Server filter keeps 10 of 10 members. The Action (Incident Type,Location (Incident Response Data)) filter keeps 59 members. The Action (Incident Type) filter keeps 10 members. The Action (Severity (Incident Response Data),Status (Incident Response Data)) filter keeps 16 members.

Status of Affected Servers



Count of Incident Response Data for each Affected Server. Color shows details about Status (Incident Response Data). The data is filtered on Action (Incident Type,Location (Incident Response Data)), Action (Incident Type) and Action (Severity (Incident Response Data),Status (Incident Response Data)). The Action (Incident Type,Location (Incident Response Data)) filter keeps 59 members. The Action (Incident Type) filter keeps 10 members. The Action (Severity (Incident Response Data),Status (Incident Response Data)) filter keeps 16 members. The view is filtered on Status (Incident Response Data), which keeps Escalated, In Progress, Resolved and Unresolved.

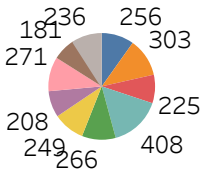
Incidents in locations



Location (Incident Response Data)
- Berlin
- London
- New York
- San Francisco
- Sydney
- Tokyo

Location (Incident Response Data). Color shows details about Location (Incident Response Data). Size shows count of Incident Response Data. The marks are labeled by Location (Incident Response Data). The data is filtered on Action (Incident Type) and Action (Severity (Incident Response Data),Status (Incident Response Data)). The Action (Incident Type) filter keeps 10 members. The Action (Severity (Incident Response Data),Status (Incident Response Data)) filter keeps 16 members.

TOP 3 INCIDENT - RESPONSE TIME



Incident Type (color) and sum of Response Time (Hours) (size). The data is filtered on Action (Severity (Incident Response Data),Status (Incident Response Data)), which keeps 16 members. The view is filtered on Incident Type, which keeps 10 of 10 members.

Response Time (Hours)

2,603

Incident Type

- Data Exfiltration
- DDoS Attack
- Insider Threat
- Malware Detection
- Phishing Attack
- Ransomware Attack
- Social Engineering
- SQL Injection
- Unauthorized Access
- Zero-Day Exploit

Severit..	Status (Incident Response Data)			
	In Progress	Resolved	Escalated	Unresolved
Critical	10	10	11	12
Low	14	13	14	14
Medium	11	7	12	16
High	11	12	16	17

Count of Incide..
7 17

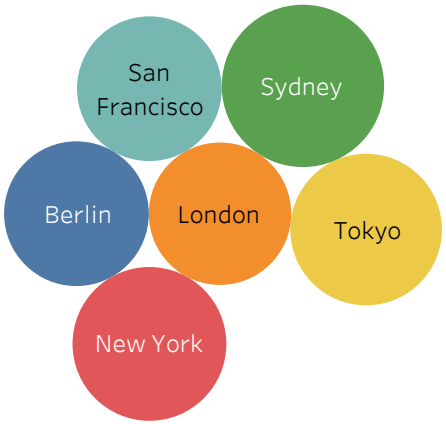
Count of Incident Response Data broken down by Status (Incident Response Data) vs. Severity (Incident Response Data). Color shows count of Incident Response Data. The marks are labeled by count of Incident Response Data.

INCIDENT RESPONSE DASHBOARD

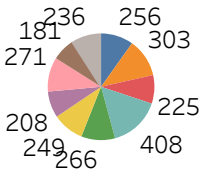
Status (Incident Response Data)

Severit..	In Progress	Resolved	Escalated	Unresolved
Critical	10	10	11	12
Low	14	13	14	14
Medium	11	7	12	16
High	11	12	16	17

Incidents in locations

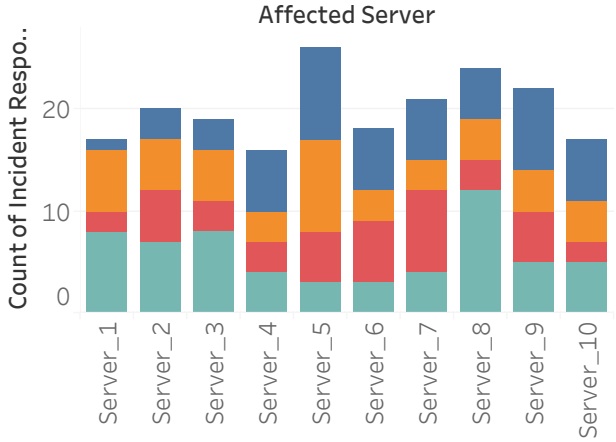


TOP 3 INCIDENT - RESPONSE TIME

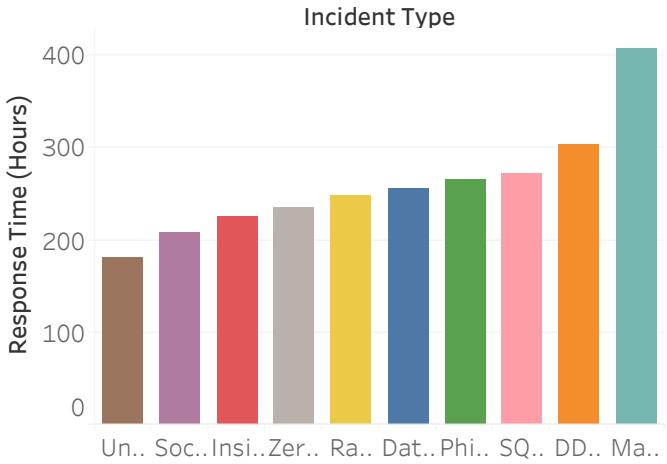


Incident Type
- Data Exfiltrati..
- DDoS Attack
- Insider Threat
- Malware Dete..
- Phishing Attack
- Ransomware ..
- Social Enginee..

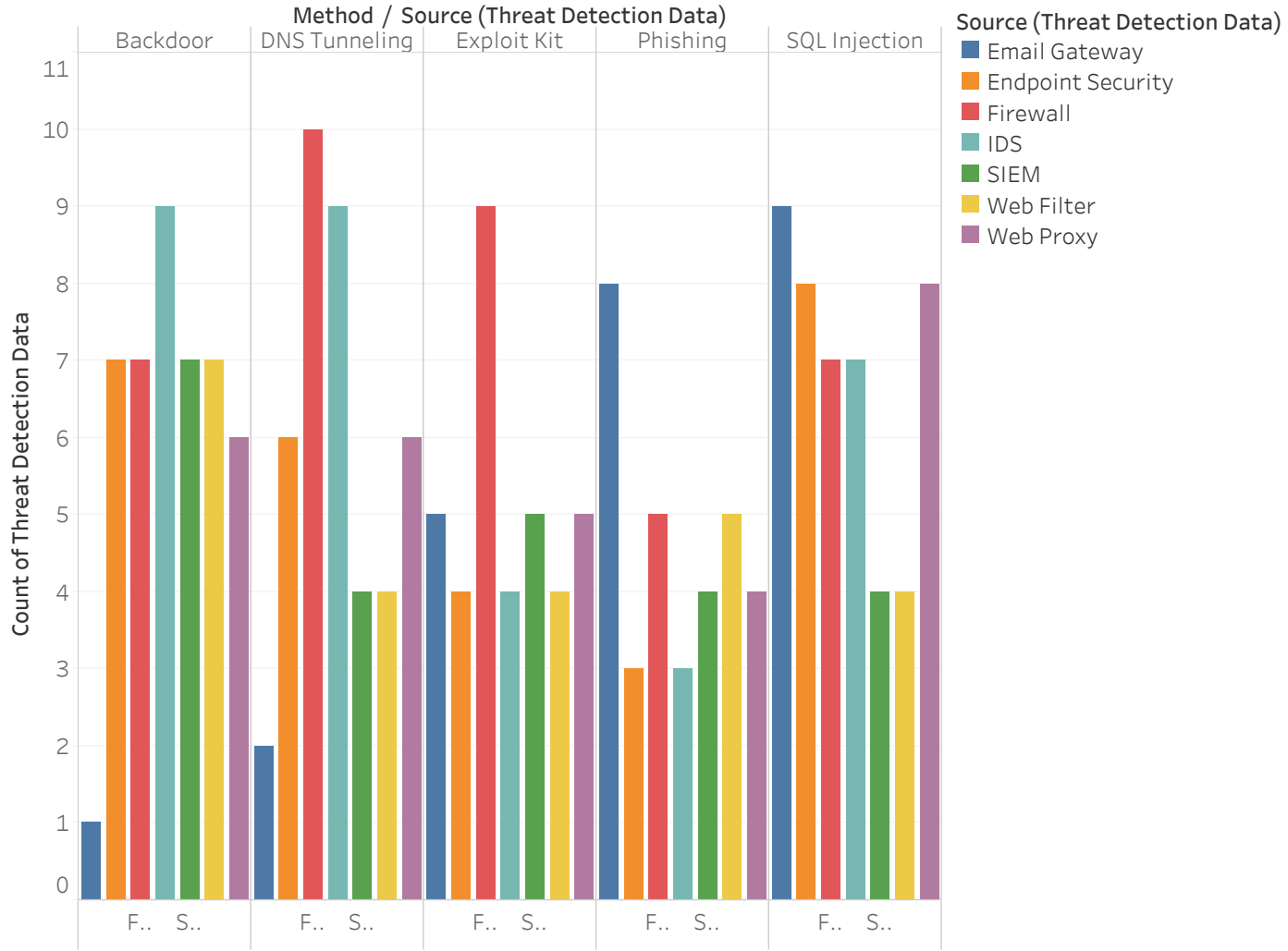
Status of Affected Servers



INCIDENT VS RESPONSE TIME



Threat source/Method



Count of Threat Detection Data for each Source (Threat Detection Data) broken down by Method. Color shows details about Source (Threat Detection Data). The data is filtered on Affected Systems (Threat Detection Data), which keeps 50 of 50 members. The view is filtered on Method, which excludes Null.

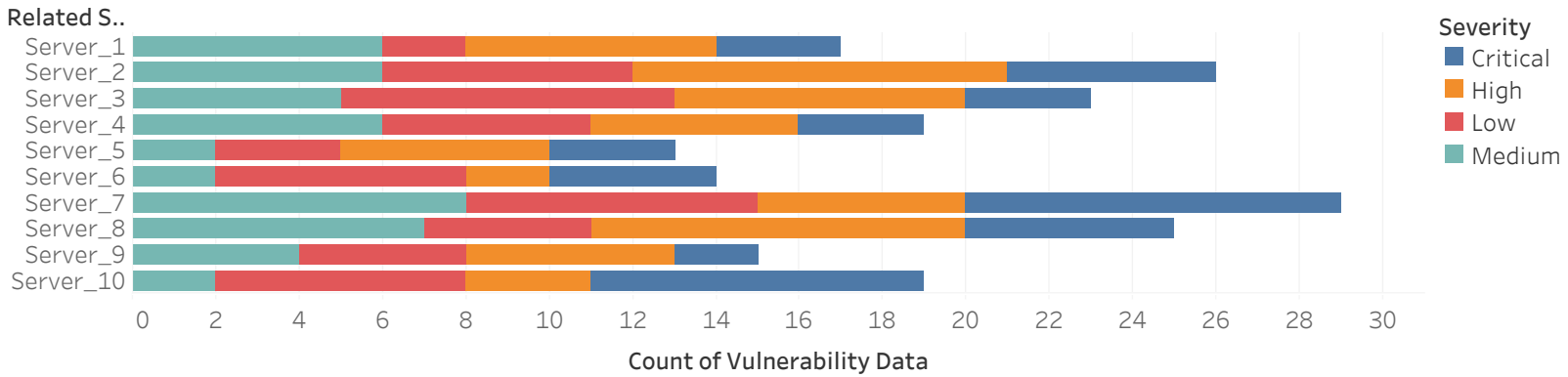
LOGIN STATUS

Status	Action	
Failed	Attempted Unau..	31
	Data Export	47
	Failed Login	34
Successful	Access Critical S..	34
	File Download	28
	Login	26

Count of User ..
26 47

Count of User Activity Data broken down by Status and Action. Color shows count of User Activity Data. The marks are labeled by count of User Activity Data.

Vulnernability of servers



Count of Vulnerability Data for each Related Server. Color shows details about Severity.