Chernoff Faces

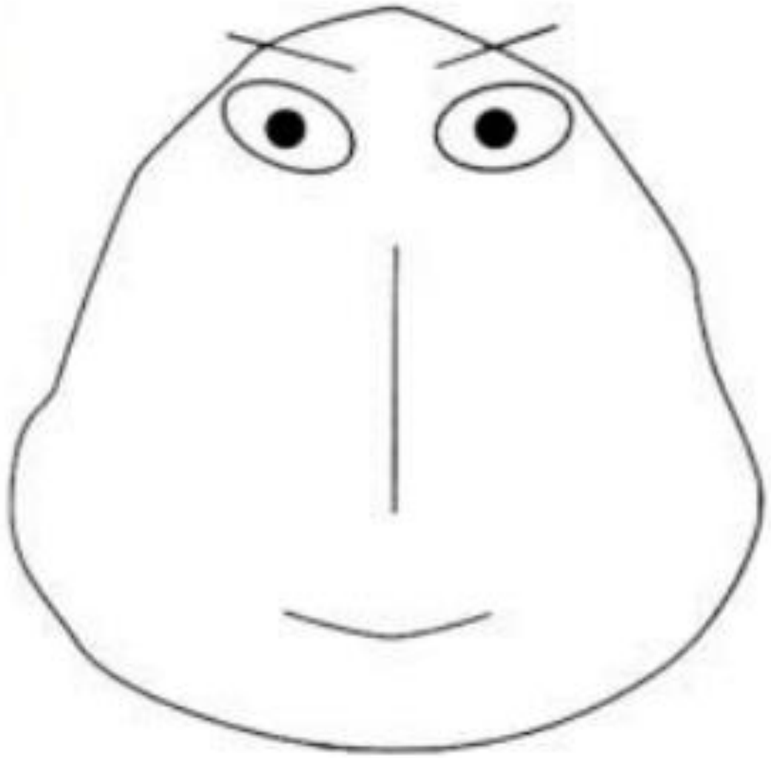
Visualisation des attaques

ADEM CHERIF

- Master en Systèmes d'Information et de Données – Université d’Oran(2019)
- Ingénieur d'État chez Sonatrach, Oran : Première expérience dans l'ingénierie avec des projets dans le secteur pétrolier et gazier.(2019)
- Master en Cybersécurité, Université de Bradford : Études approfondies en sécurité informatique et gestion des risques.(2021)
- Développeur Backend (Ruby on Rails) : Expérience en développement web backend, intégration de fonctionnalités et optimisation.(2020-2021)
- Stage Audit ISO 27001 chez ABC Technologies : Audit de conformité ISO 27001, analyse des risques et recommandations de sécurité.(2021)
- Assistant de Recherche, Université de Bradford : Travail sur un projet de robotique, apport en cybersécurité.(2022-2023)
- Auditeur en Cybersécurité chez Cyber Tech Ltd : Analyse et amélioration des pratiques de sécurité en entreprise.(2023-2024)
- Enseignant en Cybersécurité, LaSalle Saint-Denis : Formation en cybersécurité pour BTS et licences.(actuellement)

chernoff face presentation avec des examples

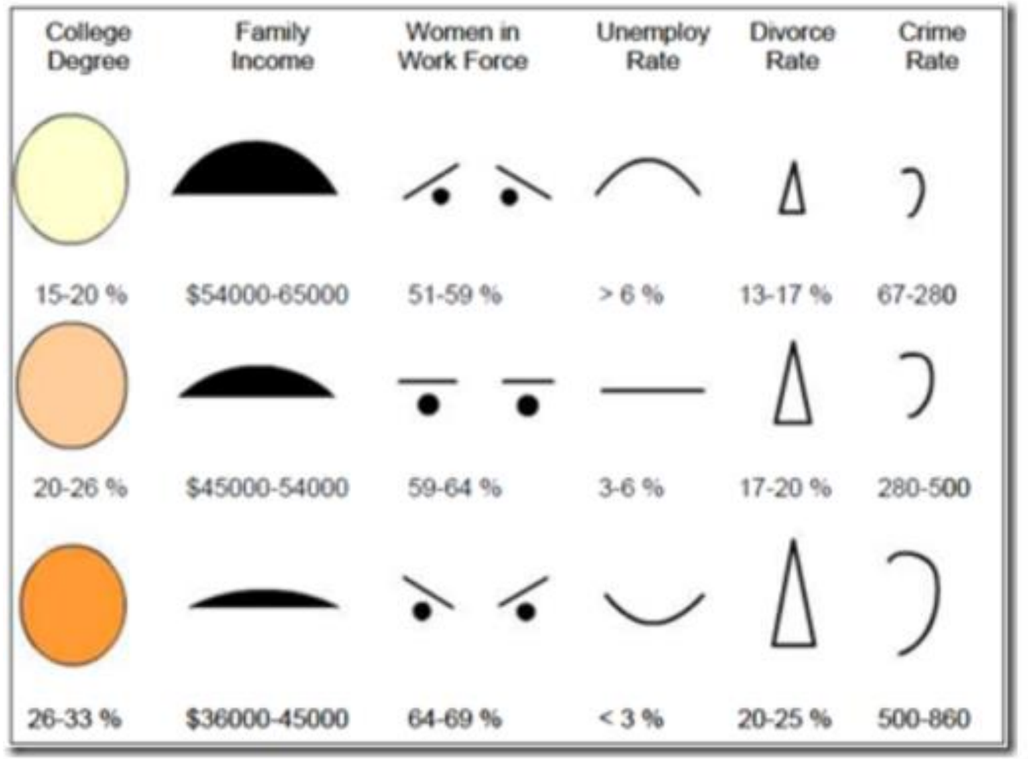
Technique de visualisation nommée d'après Herman Chernoff
Méthode pour représenter des données multivariées (en 1973)
Raisonnement cognitif derrière cette technique : les humains détectent facilement de petits changements dans les visages

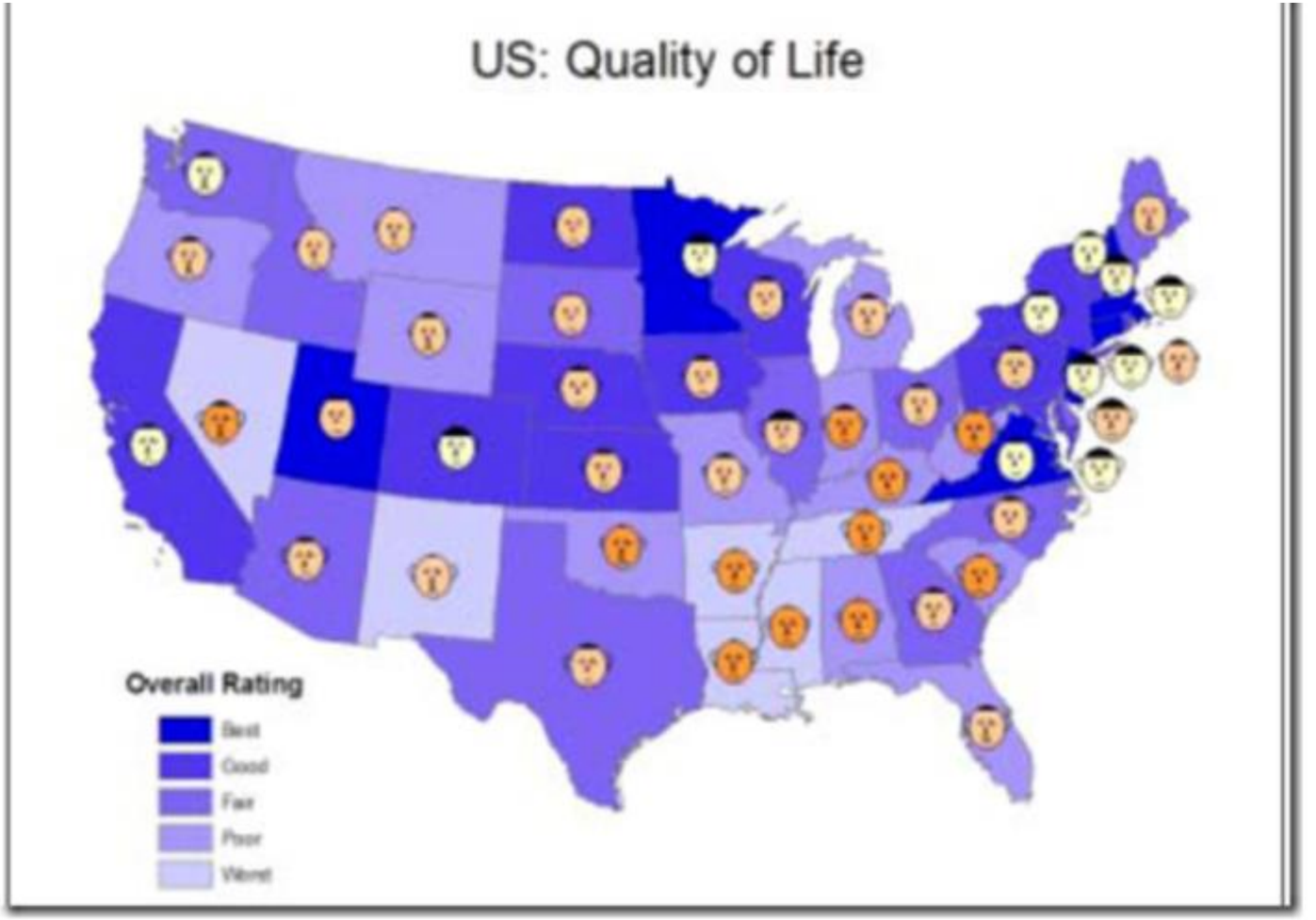


Comment est-elle utilisée ?

- Prend différentes dimensions des données
- Représente chaque variable comme une partie individuelle d'un visage (yeux, nez, oreilles, bouche)
- Utilise la taille, l'orientation, la forme et la position
- Peut représenter jusqu'à 18 dimensions

Example


College Degree
Family Income
Women in Work Force
Unemploy Rate
Divorce Rate
Crime Rate
15-20 %
$54000-65000
51-59 %
> 6 %
13-17 %
67-280
20-26 %
$45000-54000
59-64 %
3-6 %
17-20 %
280-500
26-33 %
$36000-45000
64-69 %
< 3 %
20-25 %
500-860


US: Quality of Life
Overall Rating
Best
Good
Fair
Poor
Worst

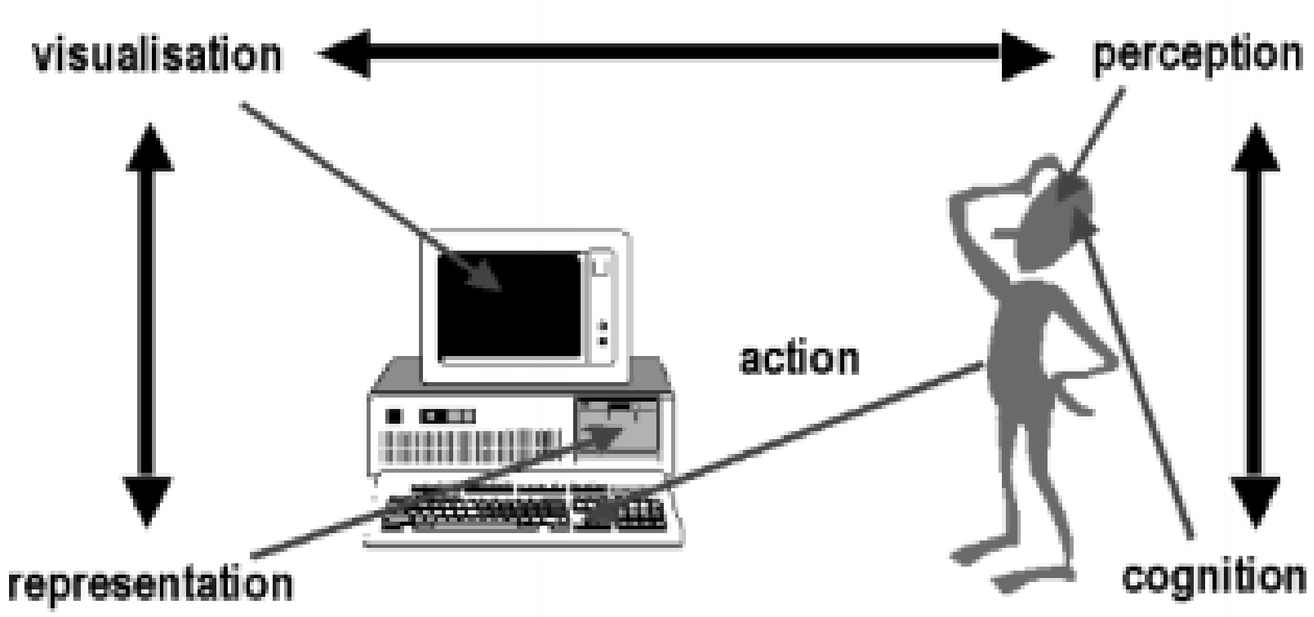
l’importance de la visualisation

Utilisati**ons :**

- **Détection de clusters**
- **Représentation de données multivariées**

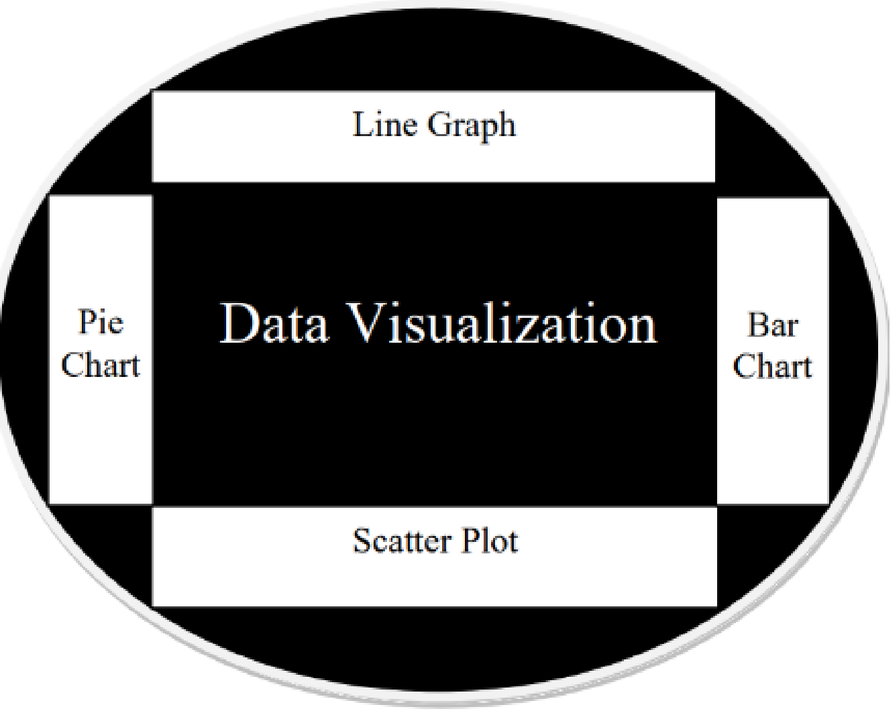
Inconvénients :

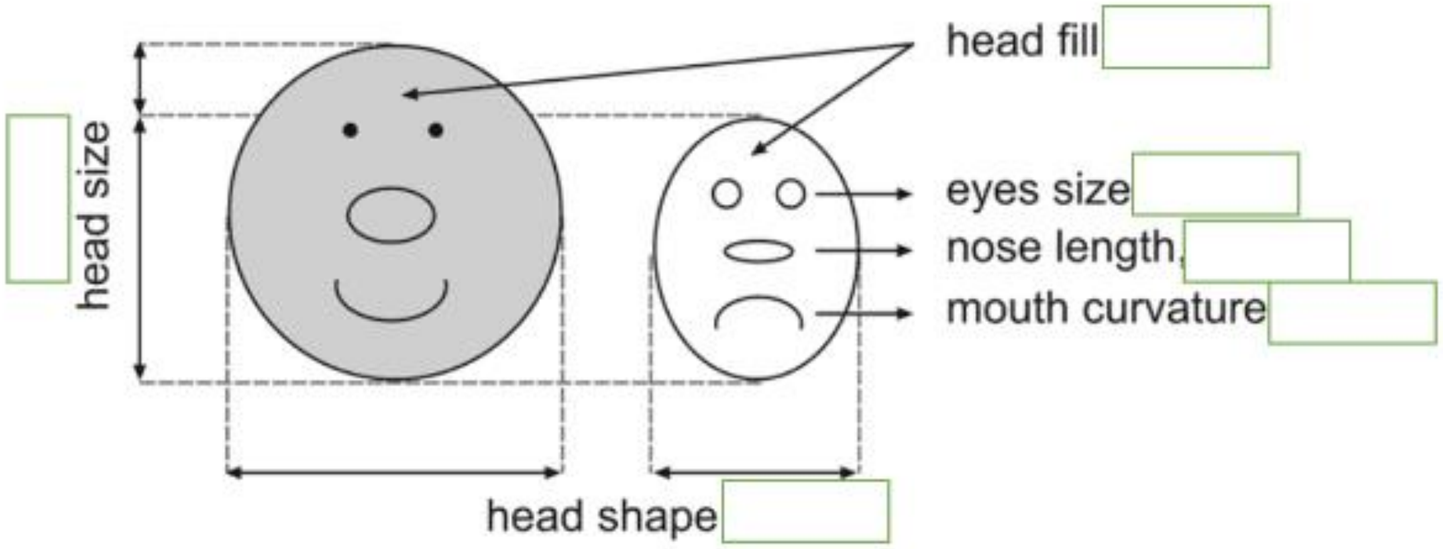
- **Pas d'associations de valeurs quantitatives**
- **Difficile à mettre en œuvre**
- **Difficile à interpréter**



la force de la visualisation avec visage de chernofff

La force du visage de Chernoff réside dans sa capacité élevée de compression des données et sa présentation attrayante. De plus, le balayage répétitif de grandes tables de données est épuisant. Néanmoins, les visages de Chernoff peuvent grandement améliorer la compréhension des données. En outre, le visage de Chernoff offre une représentation complexe des données dans un visage simple, avec la possibilité d'avoir jusqu'à 36 variables.





techniques utiliser pour la visualisation

les variables dans le visage que on peut utiliser et combien de combinaison

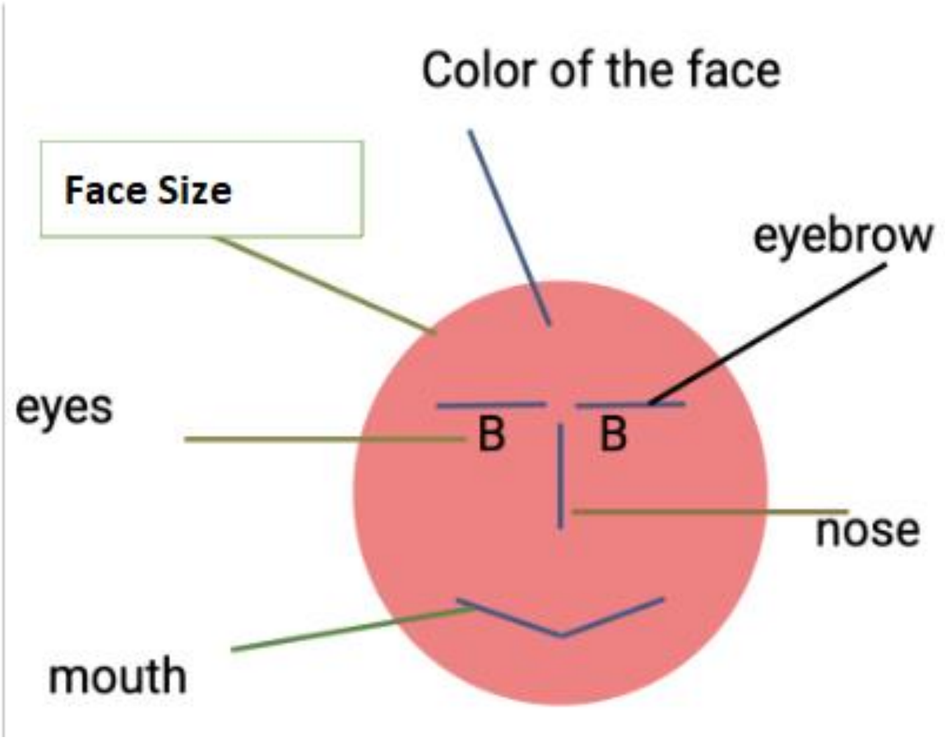
KFSensor

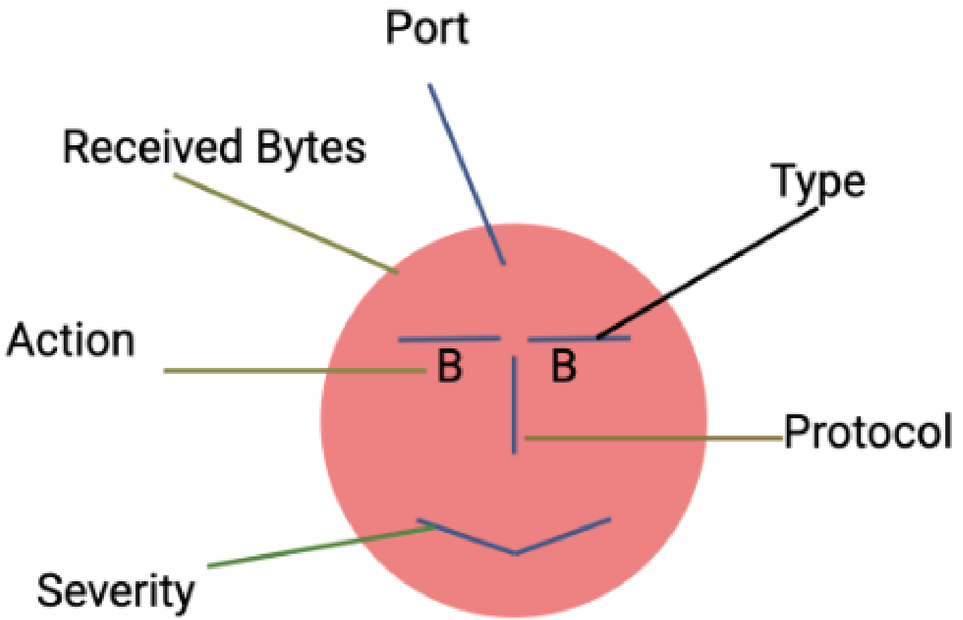
KFSensor est un système de détection d'intrusion (IDS) de type honeypot, conçu pour les environnements Windows (KFsensor, 2001-2016). Cette application est particulièrement bien adaptée aux environnements professionnels, notamment dans les entreprises utilisant des systèmes Windows, car elle offre plusieurs fonctionnalités uniques et innovantes, telles que la gestion à distance, un moteur de signatures compatible avec Snort (Roesch, 1999), ainsi qu'une émulation du réseau Windows.
La version d'essai de KFSensor permet de travailler sur deux protocoles : le premier est le protocole TCP avec 22 ports, et le second est le protocole UDP avec 14 ports (Grimes, 2005).

ID	Received Bytes	Severity	Type	Protocol	Sensor Port	Name	Visitor	Description	Visitor IP	Action
1	0	High	Scan	TCP	22	SSH	192.168.16.1	Syn Scan	192.168.16.1	Sniff
2	0	High	Scan	TCP	80	IIS	192.168.16.1	Syn Scan	192.168.16.1	Sniff
3	0	High	Scan	TCP	443	IIS HTTPS	192.168.16.1	Syn Scan	192.168.16.1	Sniff
4	0	High	Scan	TCP	443	IIS HTTPS	192.168.16.1	Syn Scan	192.168.16.1	Sniff
5	0	High	Scan	TCP	80	IIS	192.168.16.1	Syn Scan	192.168.16.1	Sniff
6	0	High	Closed Port	TCP	49994	TCP Packet	52.97.161.2	Out of sync pac...	52.97.161.2	Sniff
7	49	High	Closed Port	TCP	49356	TCP Connection	again-chastise.bloggab.com	Long running c...	162.255.45.114	Sniff
8	201	High	Connection	TCP	443	IIS HTTPS	DESKTOP-5KT8FFV.lan	Long running c...	192.168.16.7	Sniff
9	332	High	Connection	TCP	443	IIS HTTPS	DESKTOP-5KT8FFV.lan	Long running c...	192.168.16.7	Sniff
10	240	High	Closed Port	TCP	49355	TCP Connection	52.230.222.68	Long running c...	52.230.222.68	Sniff
11	0	High	Closed Port	TCP	49363	TCP Connection	100.64.250.1	Long running c...	100.64.250.1	Sniff
12	853	High	Connection	TCP	443	IIS HTTPS	DESKTOP-5KT8FFV.lan	Long running c...	192.168.16.7	Sniff
13	54	High	Connection	TCP	443	IIS HTTPS	DESKTOP-5KT8FFV.lan	Long running c...	192.168.16.7	Sniff
14	54	High	Connection	TCP	443	IIS HTTPS	DESKTOP-5KT8FFV.lan	Long running c...	192.168.16.7	Sniff
15	758	High	Connection	TCP	443	IIS HTTPS	DESKTOP-5KT8FFV.lan	Long running c...	192.168.16.7	Sniff
16	53	High	Connection	TCP	443	IIS HTTPS	DESKTOP-5KT8FFV.lan	Long running c...	192.168.16.7	Sniff
17	0	High	Closed Port	TCP	49355	TCP Packet	52.230.222.68	Out of sync pac...	52.230.222.68	Sniff
18	784	High	Closed Port	TCP	49363	TCP Packet	100.64.250.1	Out of sync pac...	100.64.250.1	Sniff
19	0	High	Closed Port	TCP	49363	TCP Packet	100.64.250.1	Out of sync pac...	100.64.250.1	Sniff
20	39906557	High	Closed Port	TCP	49364	TCP Connection	again-chastise.bloggab.com	Long running c...	162.255.45.114	Sniff

Log Events in KFSensor

integration avec honeypot et comment j'ai choisis les variables





couleur de chaque port

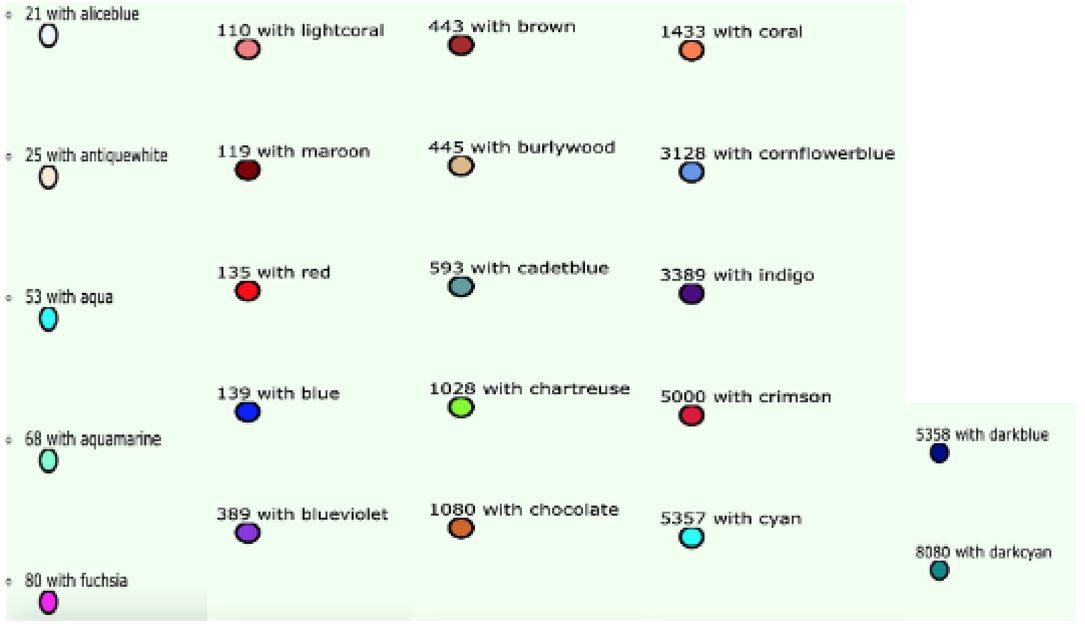


Figure Q: color of each TCP ports

Figure R: color of each UDP port

Figure S: size of the face

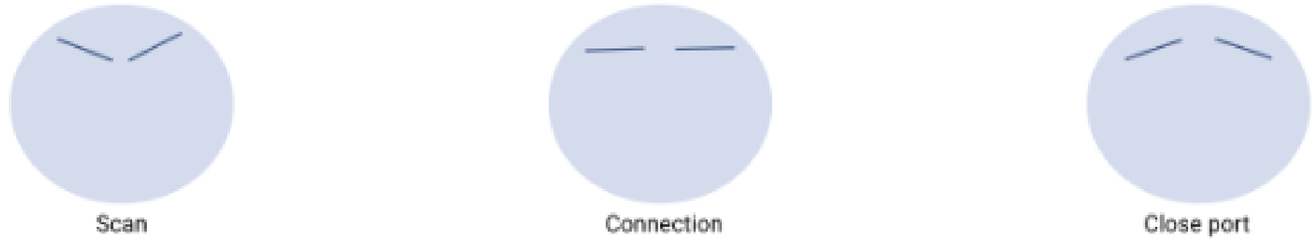


Figure T: representation of type of attack with evebrow in Chernoff face

Figure V: representation of protocols in Chernoff face with nose

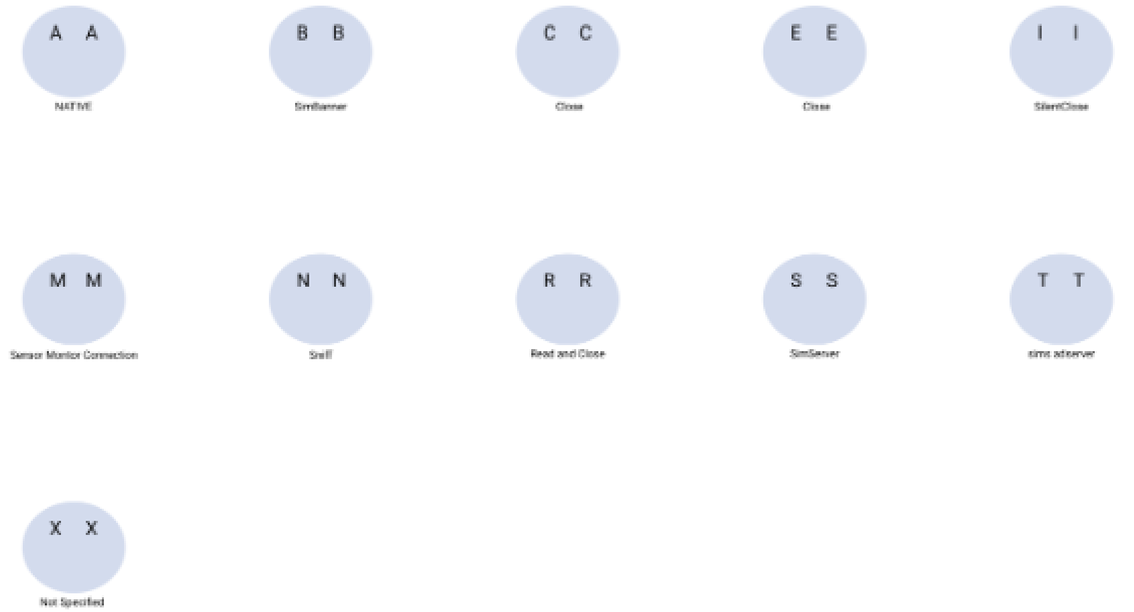


Figure U: representation of different action in Chernoff face

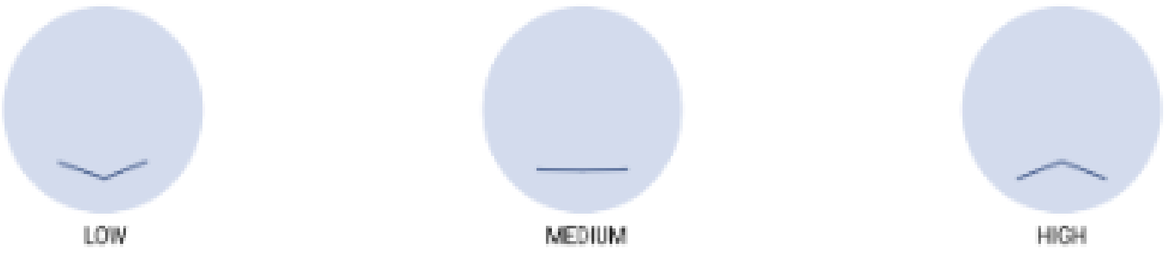
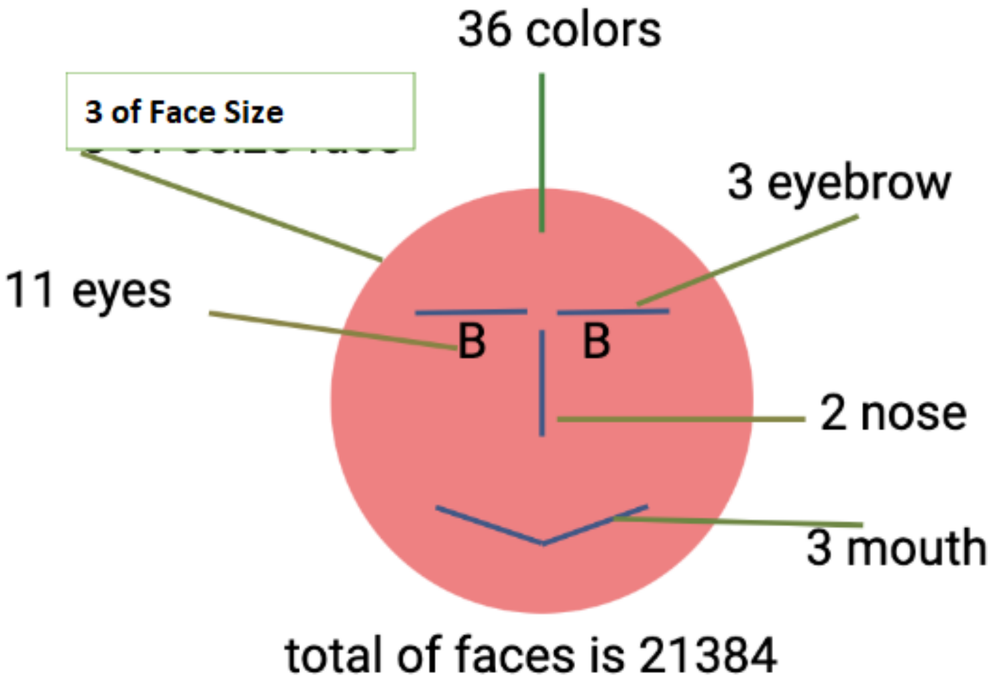


Figure W: representation of severity in Chernoff face with mouth

Default Values:

Action	Action name
A	Native
B	SimBanner
C	Close
E	SimExternal
I	SilentClose
M	SensorMonitorConnection
N	Sniff
R	ReadAndClose
S	SimServer
T	SimStdServer
X	NotSpecified

Figure X: special letters of each action



visitor IP	action	sensor port	protocol	type	severity	received
52.97.161.2	native	21	tcp	close port	high	0
162.255.45.114	simbanner	110	tcp	connection	low	100
104.133.43.26	close	119	tcp	scan	low	3320
101.32.228.11	simexternal	25	tcp	close port	high	33
1.24.0.21	silentclose	1433	tcp	scan	medium	120

Figure Z: log event exported in csv format

visitor IP	action	sensor port	protocol	type	severity	received	longitude	Latitude	id
52.97.161.2	native	21	tcp	close port	high	0	-6.2433300018311	53.353889465332	1
162.255.45.114	simbanner	110	tcp	connection	low	100	18.056	59.3247	2
104.133.43.26	close	119	tcp	scan	low	3320	-9.1927795410156	38.722221374512	3
101.32.228.11	simexternal	25	tcp	close port	high	33	72.8479	19.0144	4
1.24.0.21	silentclose	1433	tcp	scan	medium	120	111.62370300293	40.808601379395	5
102.22.100.43	sensormontorconnection	1080	tcp	connection	high	450	-4.0082998275757	5.3600001335144	6
107.172.16.11	sniff	8080	tcp	close port	low	0	-5.3724	35.5711	7
103.100.102.45	readandclose	42	udp	close port	low	1600	174.69830322266	-36.725898742676	8
103.139.131.132	simserver	53	udp	scan	medium	200	2.3488	48.8534	9
103.100.160.20	sims adserver	88	udp	connection	high	0	106.6549987793	10.779999732971	10
103.253.42.23	notspecified	500	udp	scan	high	0	114.15239715576	22.248310089111	11
103.4.98.7	sniff	67	udp	close port	medium	0	103.85178375244	1.2879500389099	12

Figure BB: adding longitude and latitude in csv log event

Figure GG: visualization of faces with their position on the map

Figure II: final result of Chernoff faces

En quoi la visualisation des attaques à l'aide des visages de Chernoff peut-elle être utile ?

La visualisation des attaques à l'aide des visages de Chernoff permet une lecture rapide et une analyse efficace, facilitant l'évaluation des menaces et la prise de décisions initiales. Un des atouts majeurs de cette méthode est qu'elle rend l'interprétation des attaques accessible aussi bien aux professionnels IT et non IT, grâce à une visualisation intuitive basée sur des expressions faciales émotionnelles.

difficultés que j’ai rencontrées avec la méthode de Chernoff

Les difficultés que j'ai rencontrées incluent la localisation des adresses IP : il est impossible d'obtenir des emplacements précis des attaquants, car la plupart utilisent des VPN.

mes projets actuelle avec chernoff face en informatique

- Dans le d**omaine bancaire, j'intègre les visages de Chernoff pour visualiser la sécurité et l'état de chaque compte bancaire.**
- **J'applique également cette méthode à la visualisation des contrôles techniques des véhicules pour représenter leur état de manière intuitive.**

merci