3

Logon Script

Installed a script that triggers when a user logs on.

4 4

Draw a card.

2

Accessibility

Hijacking sticky keys and onscreen keyboard..

3 4

Draw a card.

1

Malicious Driver

Loaded a malicious driver into th operating system.

4 3

Draw a card.

Browser Plugin

New endpoint, installed plugins in the browser.

2 5

10

0

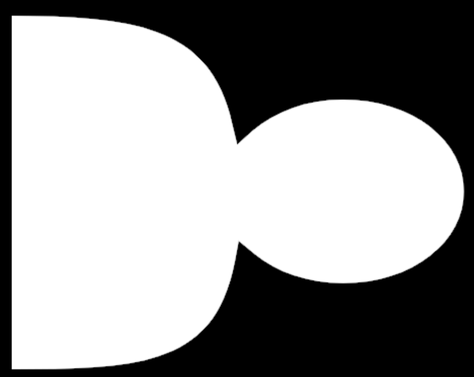
Copy a card in your hand

New Service

Pirates loaded malware in a new service

5 4

New User Added



The pirates add a new user to the local computer.

1 1

Draw a card.

10

0

Draw a card.

1

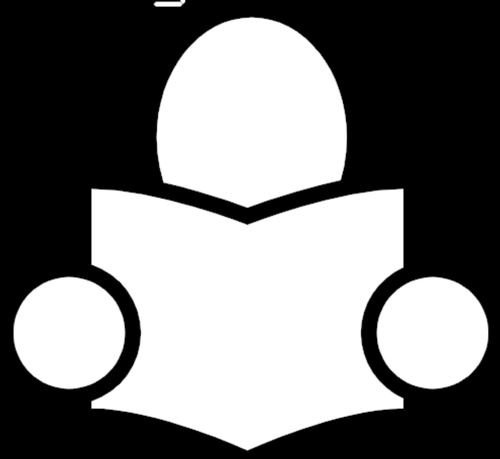
Server Analysis

Baselining systems to that it is running normal.

2 5

Draw a card.

Log Review

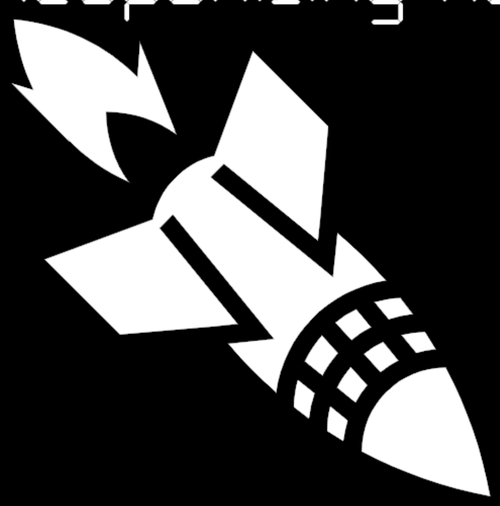


What am I looking for in these firewall logs?

1 6

6

Weaponizing AD



Maping trust relationships in Active Directory Network.

10 1

6

Local Privileges

Gained admin access from local software.

10 1

Use a card from your discard

App Shimming

Used app compatibility toolkit hide ports & files.

8 3

Take a card from the event row for free

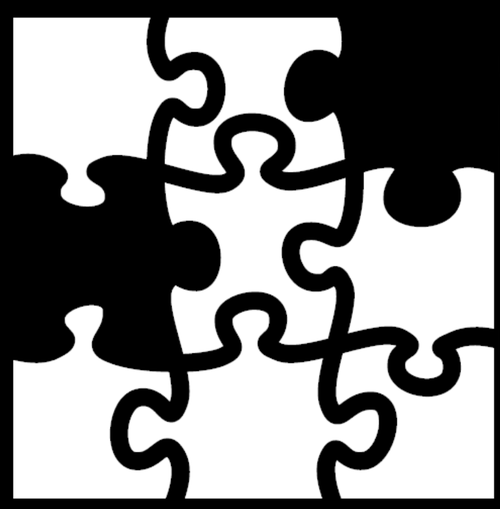
Evil Firmware

Updated the computers firmware with stealthy evil.

10 2

5

OLL Attacks

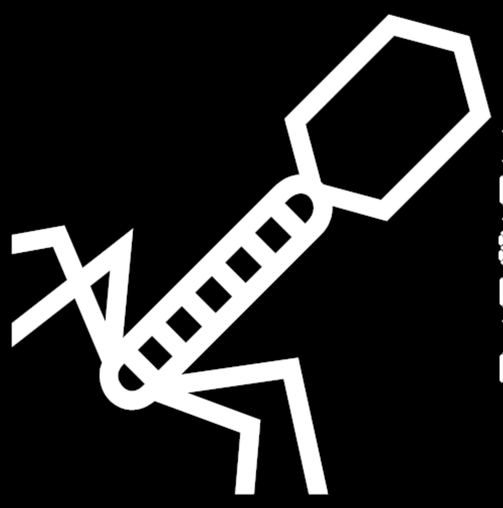


Hijacked the order OLLs are loaded through dractory

8 2

5

Malware



Added a service that starts with the system.

8 2

Draw a card.

2

Endpoint Analysis

Using SANS IR cheat sheets to detect attacts on PCs.

3 4

Draw a card.

2

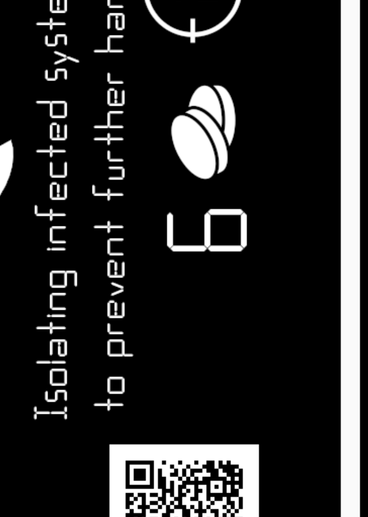
Endpoint Security

Check the anti virus alerts.

4 3

5

Isolation

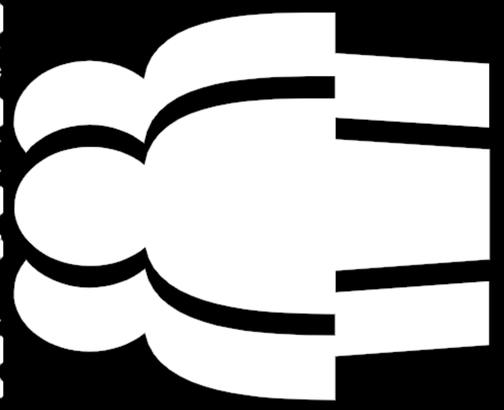


Isolating infected systems to prevent further harm.

6 2

4

User Behavior

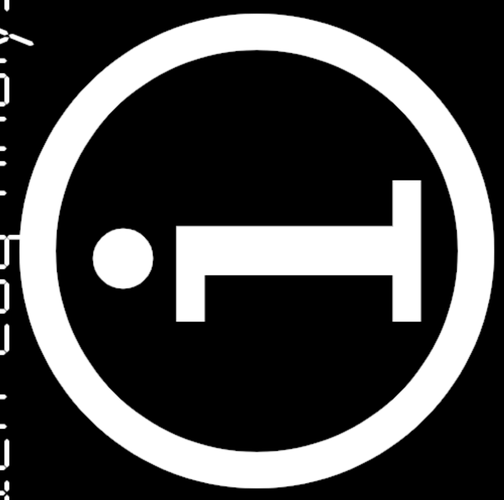


UEBA looks for multiple concurrent&impossible logins

5 3

2

SIEM Log Analysis

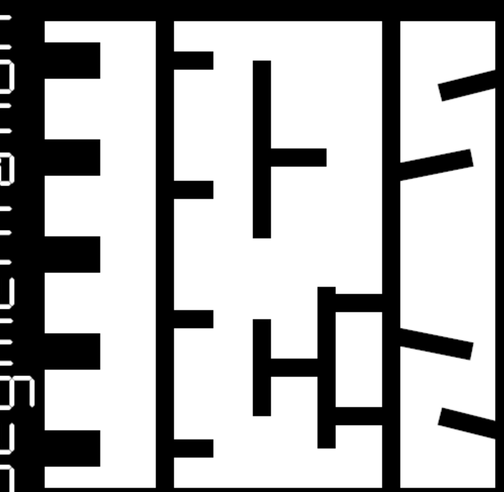


Hope we have been logging the right things.

1 5

5

Segmentation

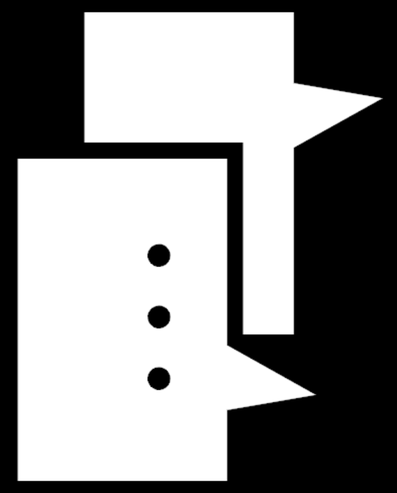


Treating the internal network as hostile.

6 2

2

Social Engineering

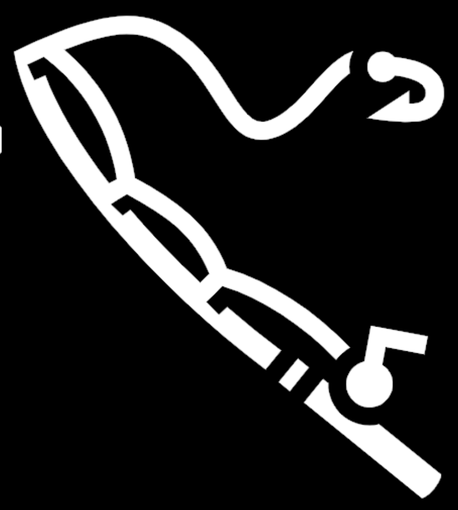


Trying to trick a user into running malware.

1 5

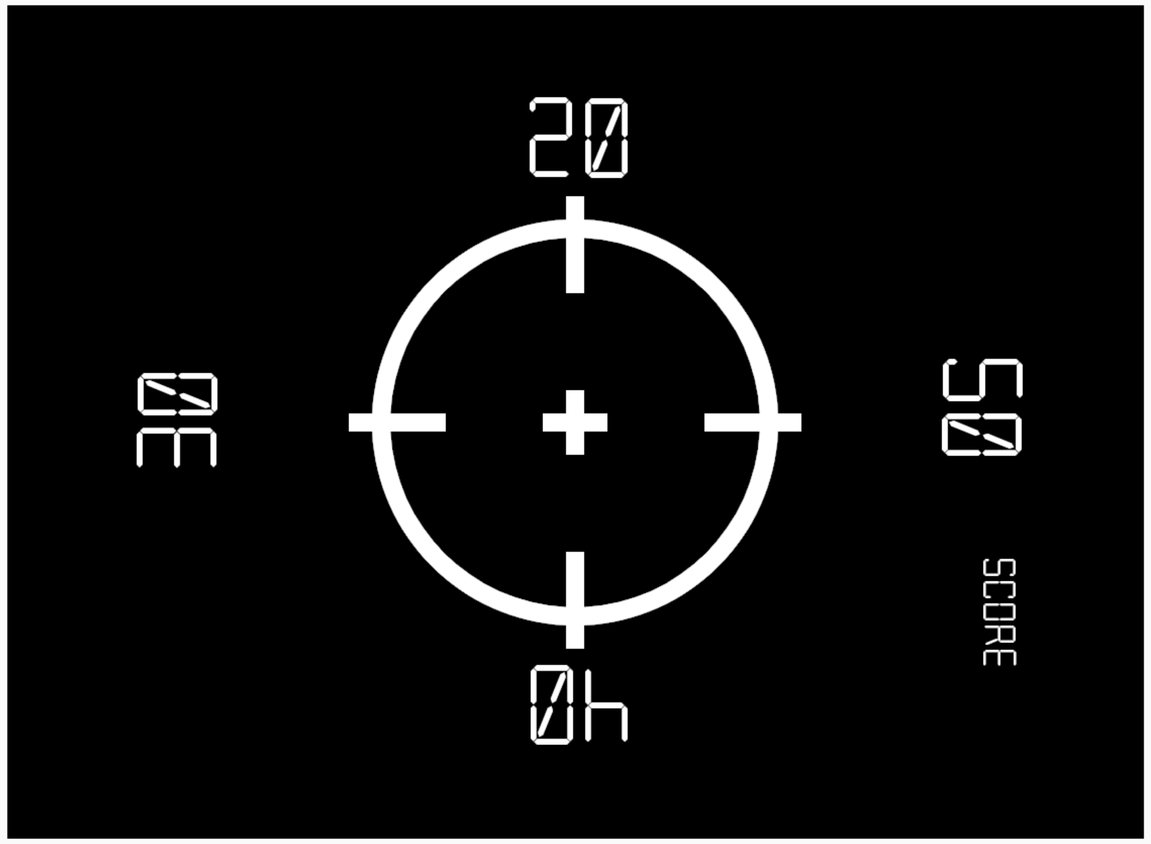
1

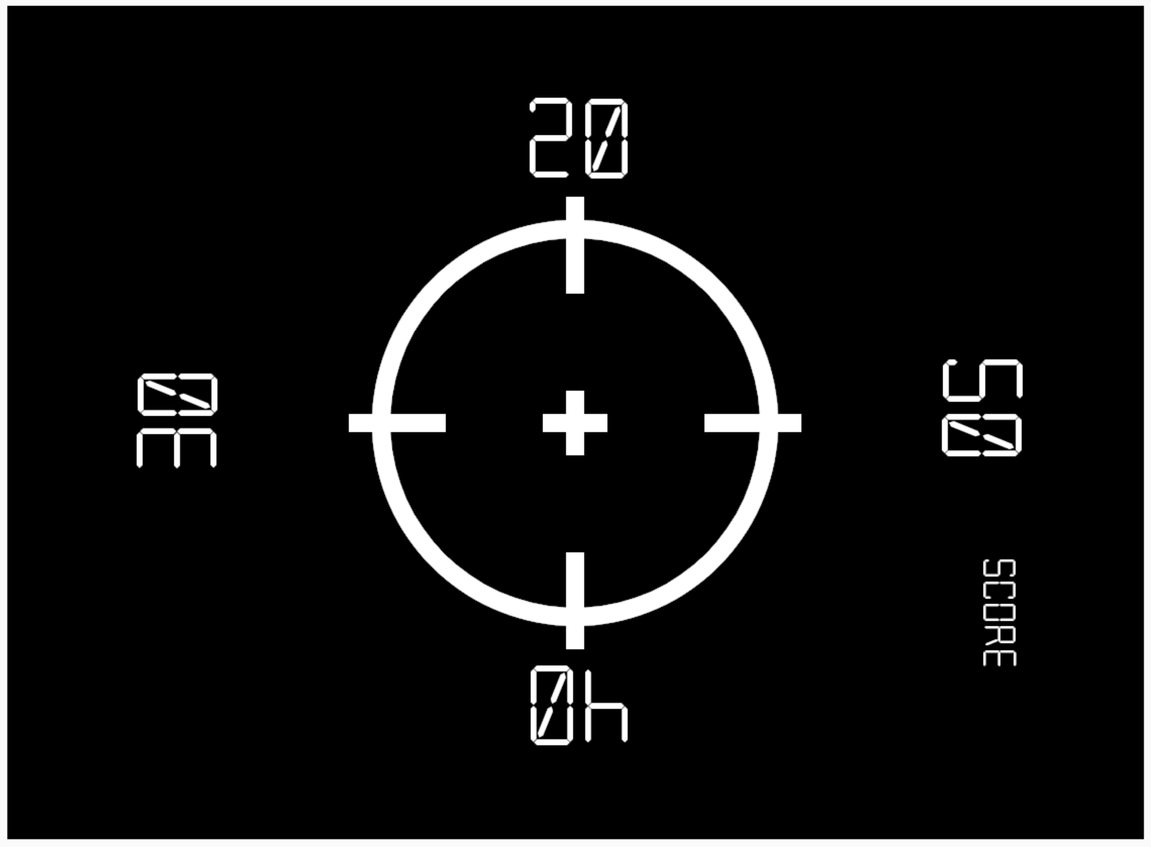
Phishing

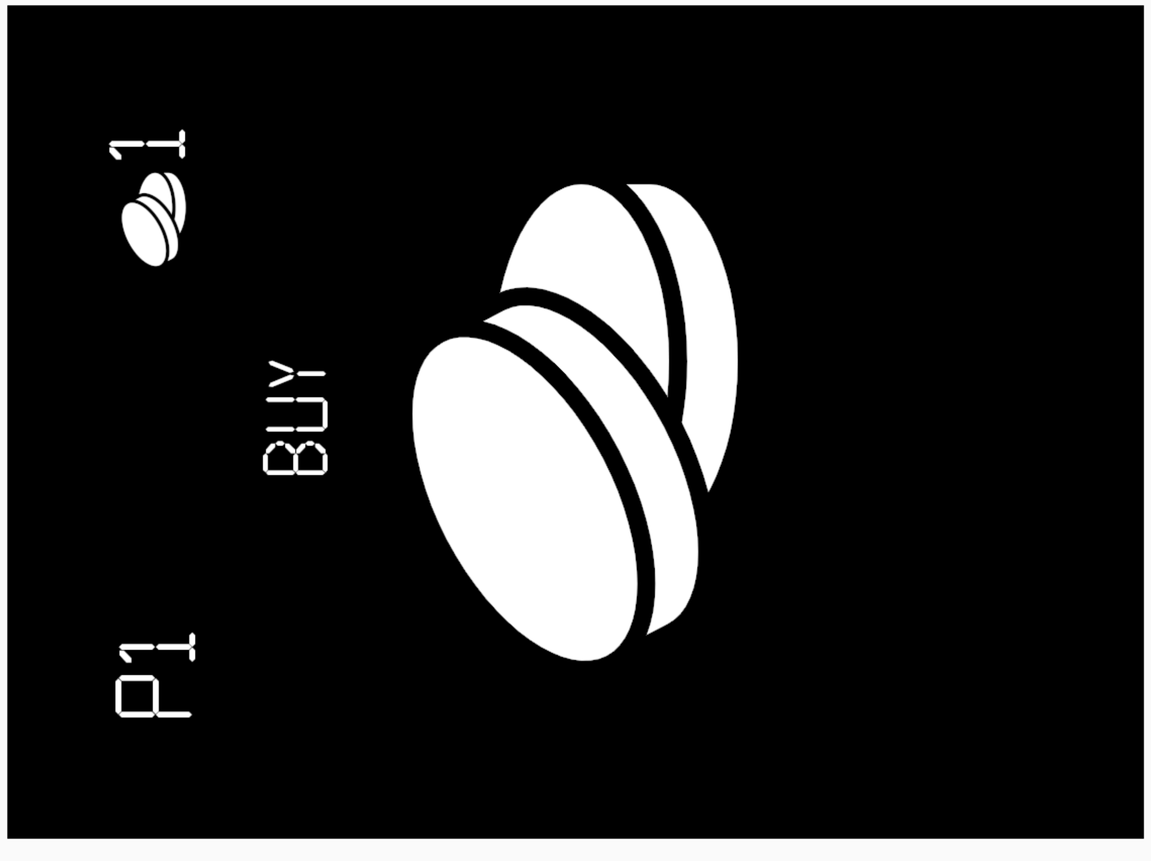


Sending emails to users. Lets see if we get a catch.

1 6

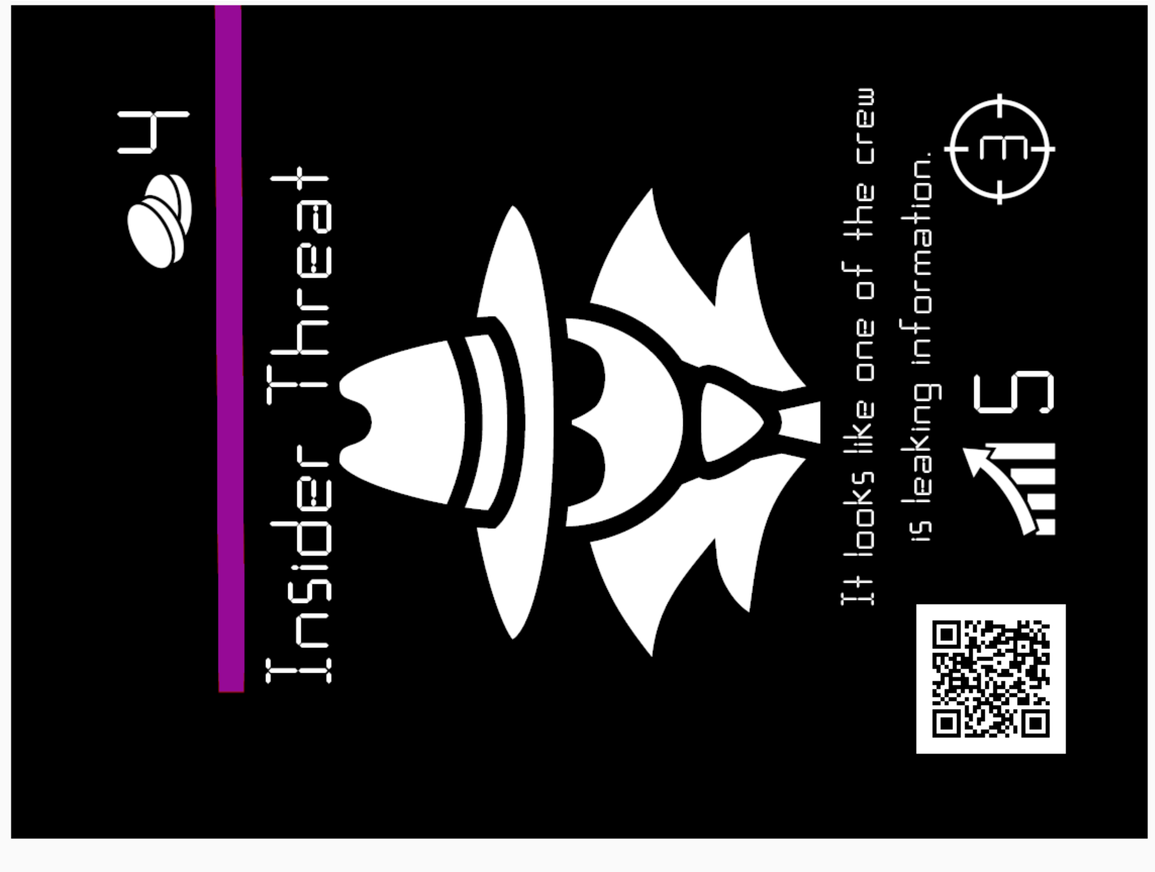

30
20
0h
SCORE
05


30
20
0h
SCORE
05


P1
1
BUY


Draw a card.
2
Cred Stuffing
Got IDs & passwords from a third party breach.
4
3


Draw a card.
1
Web Server
Taking over an external web server. Trying to get internal.
2
5


4
Insider Threat
It looks like one of the crew is leaking information.
5
3


3
Cloud Access
Gaining access to cloud resources. Trying to pivot.
4
4


Draw a card.
1
Relationships
Got into a third party with access to the network
4
3

P2 6

ENGINES

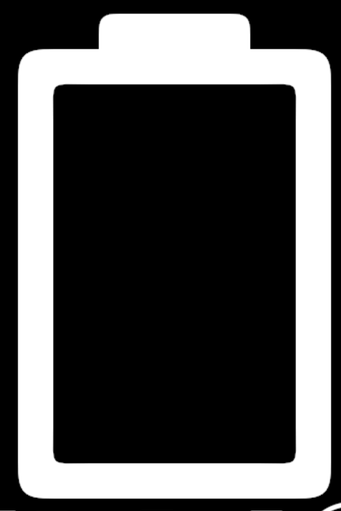
MISSION

P1 6

ENGINES

MISSION

EMP



EVERYONE 10

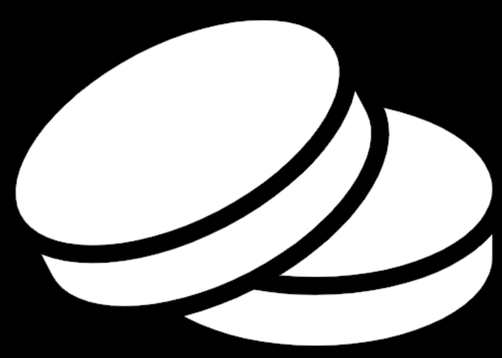
P2 6

COM

MISSION

P1 1

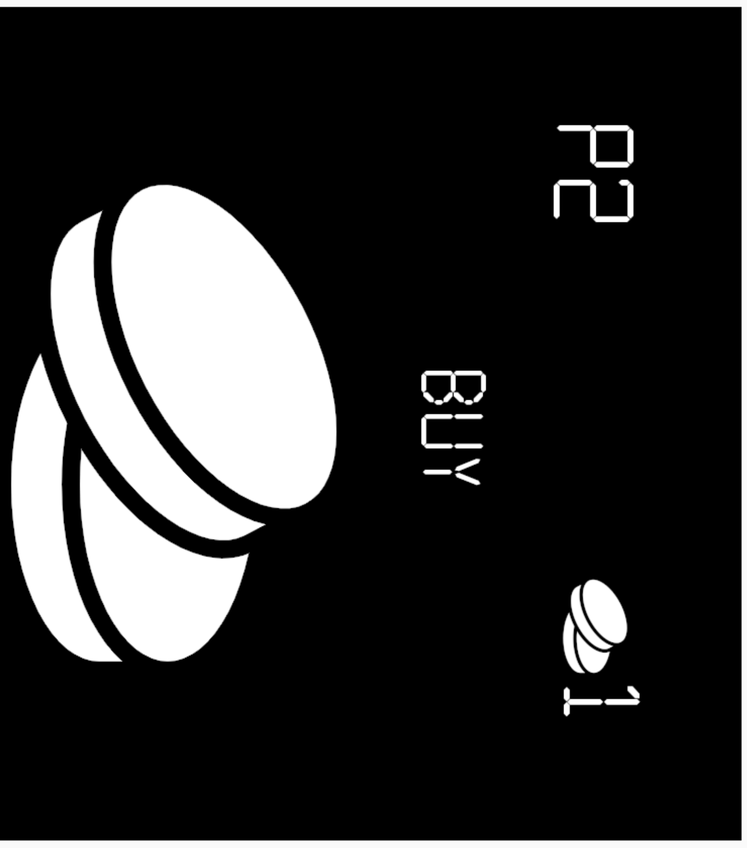
BUY



P1 6

COM

MISSION



SETUP:

1. Shuffle event cards together to make a draw pile.
2. Take top the top 6 cards from the draw pile and put them in a row in the center of the table.
3. Shuffle the player cards to make a draw pile.
4. Set the score tracker to 50.
5. Place the four mission cards in front of each player.

Game Ends: when you complete all missions or your health runs out.

For more complete rules got to games.webdesk.me

By: Black Hills & WebDesk Games

SETUP:

1. Shuffle event cards together to make a draw pile.
2. Take top the top 6 cards from the draw pile and put them in a row in the center of the table.
3. Shuffle the player cards to make a draw pile.
4. Set the score tracker to 50.
5. Place the four mission cards in front of each player.

Game Ends: when you complete all missions or your health runs out.

For more complete rules got to games.webdesk.me

By: Black Hills & WebDesk Games

GAMEPLAY:

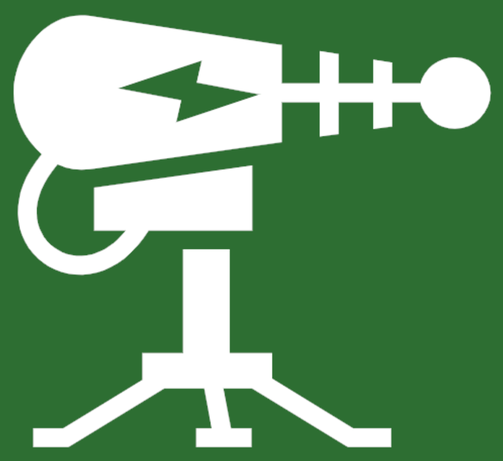
1. Draw four cards
2. Play cards to buy cards from the event row or attack the pirate ship. Purchased cards go into your discard.
3. Lose server integrity equal to the card farthest right in the event row. Discard that card to the events discard pile.
4. Refill the event row to 6 cards whenever it has less than six.
5. When any draw pile is empty take the cards in the corresponding discard pile and shuffle them to make a new draw pile.
6. Repeat.

GAMEPLAY:

1. Draw four cards
2. Play cards to buy cards from the event row or attack the pirate ship. Purchased cards go into your discard.
3. Lose server integrity equal to the card farthest right in the event row. Discard that card to the events discard pile.
4. Refill the event row to 6 cards whenever it has less than six.
5. When any draw pile is empty take the cards in the corresponding discard pile and shuffle them to make a new draw pile.
6. Repeat.

P1 12

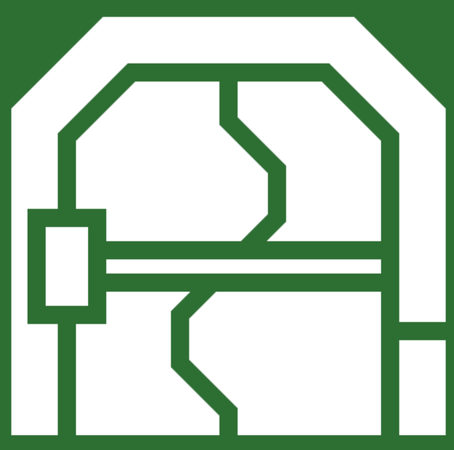
GUNS



MISSION

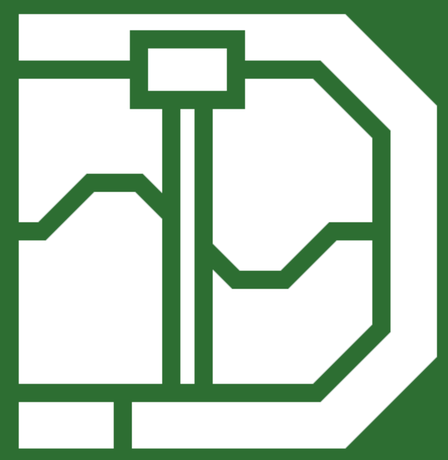
P2 7

PORT



Spend any 7 cards in hand

MISSION



Spend any 7 cards in hand

MISSION

P1 7

PORT

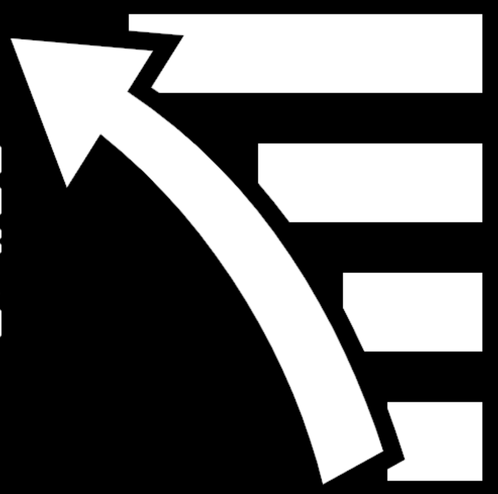
P2 12

GUNS

MISSION

P1 1

SKILL



P1 1

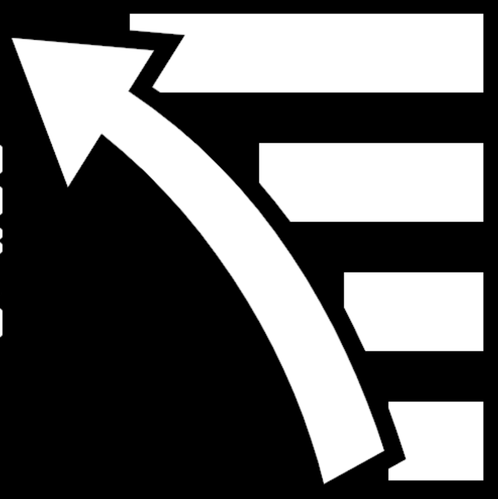
SKILL

SCORE

1 2 3 4 5 6 7 8 9

P2 1

SKILL



SCORE

1 2 3 4 5 6 7 8 9

P1 1

SKILL

P2 1

SKILL

P1 1

SKILL

P1 1

SKILL


P2
1
SKILL


P2
1
SKILL