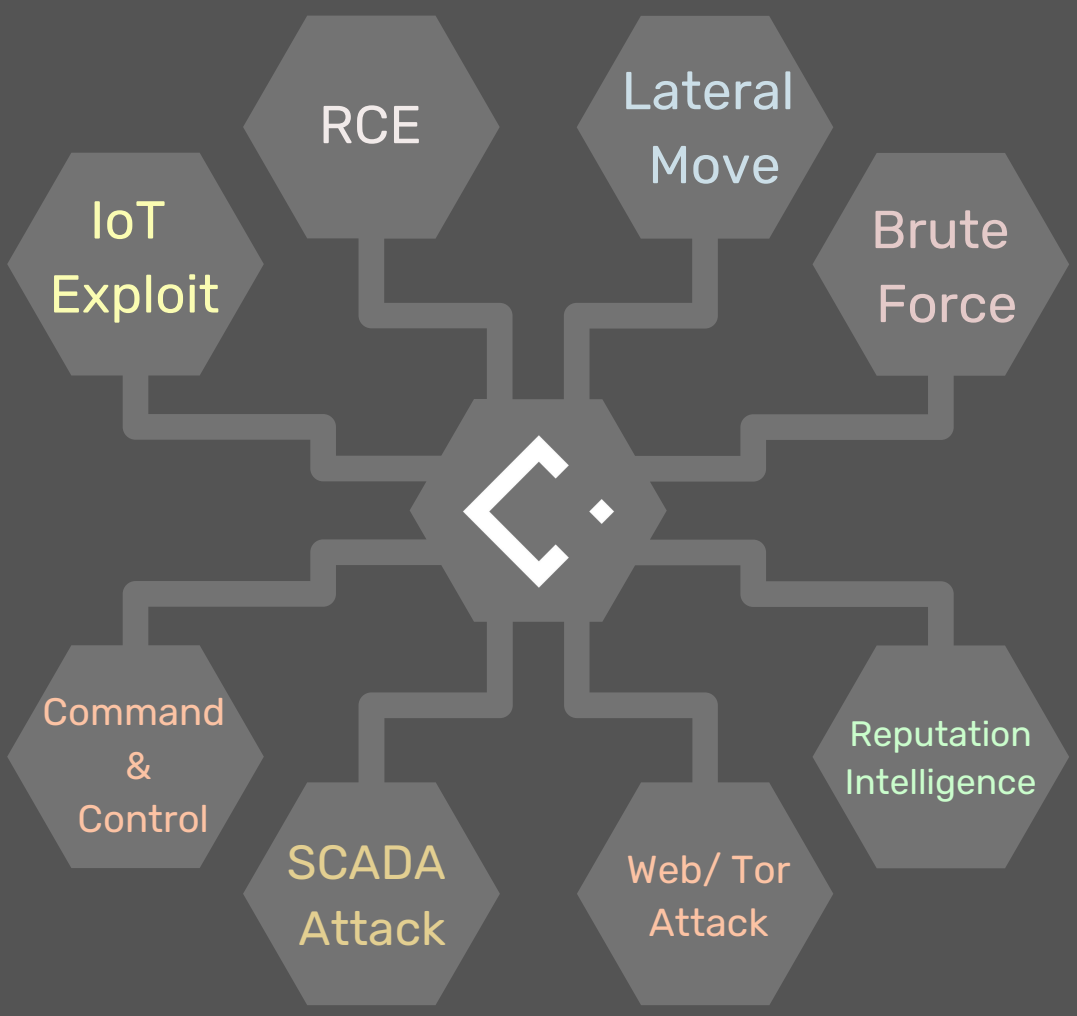
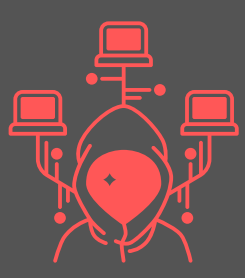
LECS
DETECTION INFOCHART





RCE / Attack / Malware

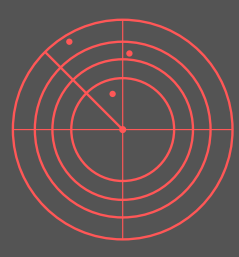
Of **thousands** service and vendor supported:
[With most dangerous CVE > 9 CVSS Score]

- SMB
- DNS
- FTP
- Laravel
- QNAP
- SolarWinds
- Various DBMS
- Microsoft Service...

- **Powershell**
  - Lateral Movement
  - Weel-Know base64 Command-Invoke
  - C2C
  - Kerberos

- **SQL Injection**
  - MSSQL
  - MySQL
  - noSQL
  - ..Other DB

- **Malware**
  - Adware_PUP
  - Loader
  - Various Payload [doc,pdf, Java..]
  - IOC of APT [Advanced Persistence Threat]
  - Many more...



Network Recon Category

Over **hundreds type** of malicious reconing, and Gathering Ops in different classification:

- Stealth Scan
- Aggressive Port Scan
- OS Fingerprinting
- Service Scan
  - Service Enumeration
  - Port triggering
- Slow Scan
- Fragmented Scan
- Kerberos
- Intra-Extra Net Conn. [TCP,UDP,SNMP..]
- Many more...

- **Industrial Scan - SCADA**
  - Modbus
  - SIEMENS
  - PcVue
  - DATAC...

Some Example:
- Mirai scan
- Tool: Zmap, MassScan, Hydra...
- Malware: Varius Ransomware scan
- HTTP Verbs
- UpnP Scan, VoIP....

DOS Attack

- GreatCannon
- LOIC
- Flood [NTP, HTTP...]
- IRC Based...and many

LECS also allows monitoring exploits to devices without a "standard" OS and/or anomalies in the traffic, as:

- **IoT Exploit**
  - Router
  - Firewall
  - IP Camera
  - A lot of Network device...

- **Weak Credentials/ Config**
  - Default login
  - Clear traffic
  - Weak TLS/SSL
  - Many more...

- **Brute Forcing**
  - Dictionary Attack
  - Pure Brute Force
  - Mask Attack
  - SMTP Brute...

> *"The tactical advantage of LECS is to detect and block a threat when it is most exposed."*