The Market of Cybersecurity in Europe:
“ Challenges and Opportunity”

Social Envoiremen[redacted]The Market

The cyber security market is estimated to grow to $170 billion (USD) by 2020, at a Compound Annual Growth Rate (CAGR) of 9.8 percent from 2015 to 2020, according to a report from Markets and Markets. The aerospace, defense, and intelligence vertical continues to be the largest contributor to cybersecurity solutions. North America and Europe are the leading cybersecurity revenue contributors, according to a report from TechSci Research. Asia-Pacific is rapidly emerging as a potential market for cyber security solution providers, driven by emerging economies such as China, India and South-East Asian countries, wherein, rising cyber espionage by foreign countries is inducing the need for safeguarding cyber space. The Europe Cyber Security Market is expected to grow to $35.53 billion by 2019, with an expected CAGR of 7.2 percent for the period 2014-2019. This market contributes 26.95 percent of the global market and will slightly fall down to 22.81 percent by 2019.

Governament

Governament are without any dobut , the first stake holder of the cybersecurity topic, they have to protect also pubblic infrastructure and face geopolitical risk linked with the “offensive side” of the cybersecurity.

Corporate

Corporate mainly task is to adopt any countermisure available to avoid data loss, dataloss and service interuption are the biggest treat to corporate, expecilay in fields such as Aerospace,Defense and Finance

Private

Private are mainly focused on end-point security, many research show that peapole tend to protect in a better way the private “cyberspace” thant the corporate ones, so its a realy florid and responsive market, but with huge costs to setup.

Best Market Topics

Pentest
- Zero Knowlege
- Partial Knowlege
- Full Knowlege
- Overt
- Covert

Reporting
- Risk Ranking
- Security Risk Origin
- Risk/Exposure Report

Best of Bread logic
- Corporate size security design
- Budget Analysis
- Best Vendor Enlisting

Identity Access Management
- Continuos Verification
- Document Access Log
- Account level privilges management

Cloud Security
- Virtualization Security
- Elastic Cloud Securiy
- Web Application Security
- IDS/IPS Shield for vulnerabilities

Data Loss Prevention (DLS)
- Endpoint monitoring
- Data flow monitoring
- Intra/extra network data package monitoring
- FDE Monitoring

Mobile Device Security (MDS)
- Custom security ROM
- Custom Backdoor replacement
- BYOD Best Pratice Implementation
- Mobile endpoint security

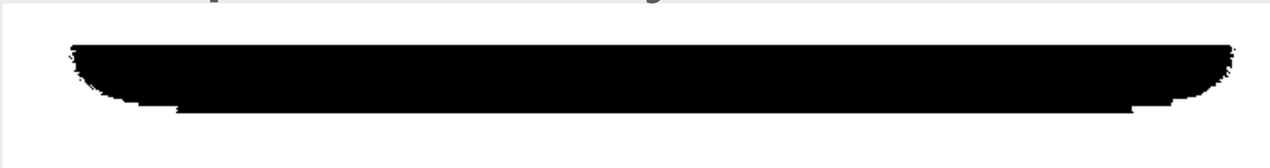
Cyber Forensics and Analysis
- CCFP compliance.
- 0 Day vulnerability Exploitation.
- Global security Risk enlist.

Defensive programming
- Defensive design.
- Security Bug Discover.
- Secure Input and output handling
- Design by code.

Defense Cyber Security
- Military Level Pentest
- Virtual & Logical surveliance

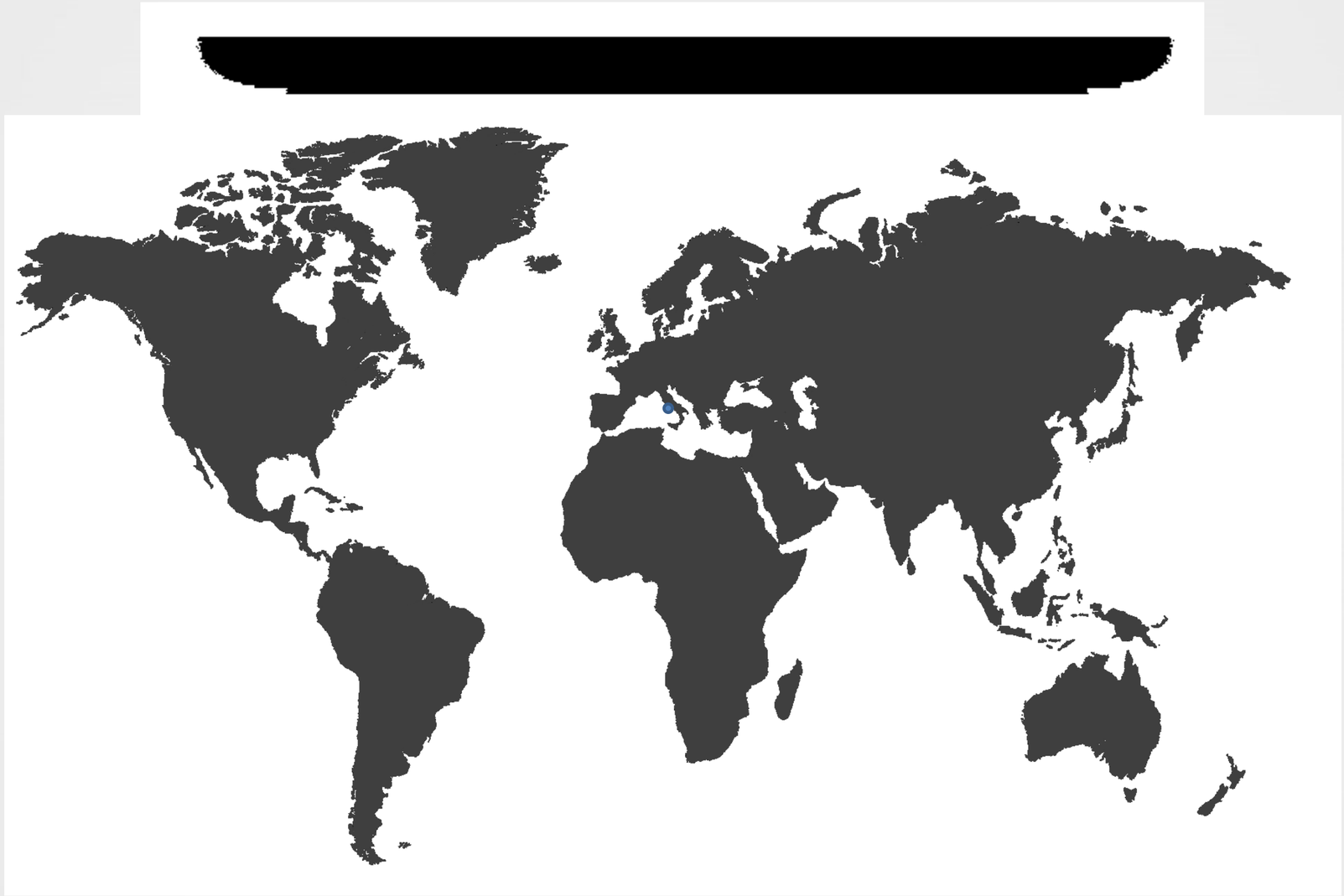
Corporate Security
- Corporate network 24H Watchguard.
- Corporate Doc tracking.
- Corporate phy behaviour tra

The Requirements you NEED to have



- You need to have a custom approch to Cybersecurity.
- Continuous Hw Update and costant presence on sector conferences
- Be your costumer’s watchguard
- You NEED to invest in R/D to have everytime ad updated services offer
- You have to love the open-source community and give back.
- You have to test your infrastructure first
- Be honest with your costumers , you will NOT build the perfect wall.

Globaly Operative



Qualities

Be Fast

Cybersecurity response time must be really short, in case of security breach, time is essential.

Be Smart

Its is important to offer only smart solutions, smart solutions brings smart budget.

Be Passionate

Be passionate to the topic, you got to be part of the underground community to hire the best peapole.

Requirement

[redacted]

Choose the best

Allways choose the best vendor and the best professionalities in the sector.

Reporting

Its important to report on every action taken, by dooing so you will build an exstensive repo wiki that will speed up your next operations.

Private Approach

Never disclose your costumer for “marketing” proposal.

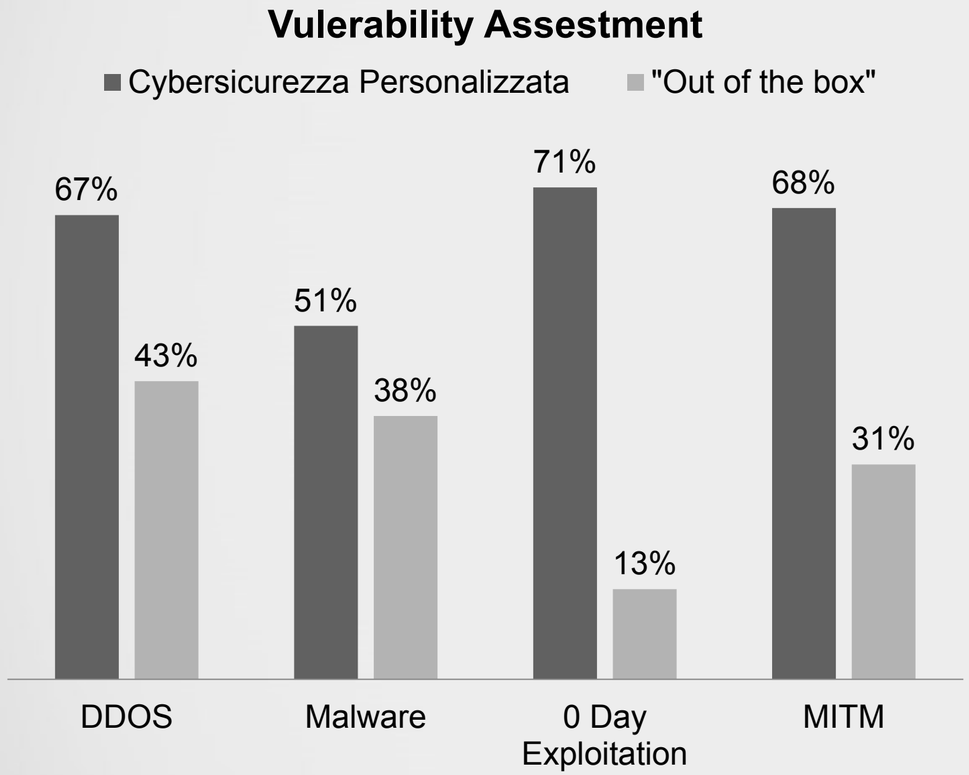
Professional Approch

It’s important to gain professional reputation, sometimes cybersec company are viewed as “grey” entities

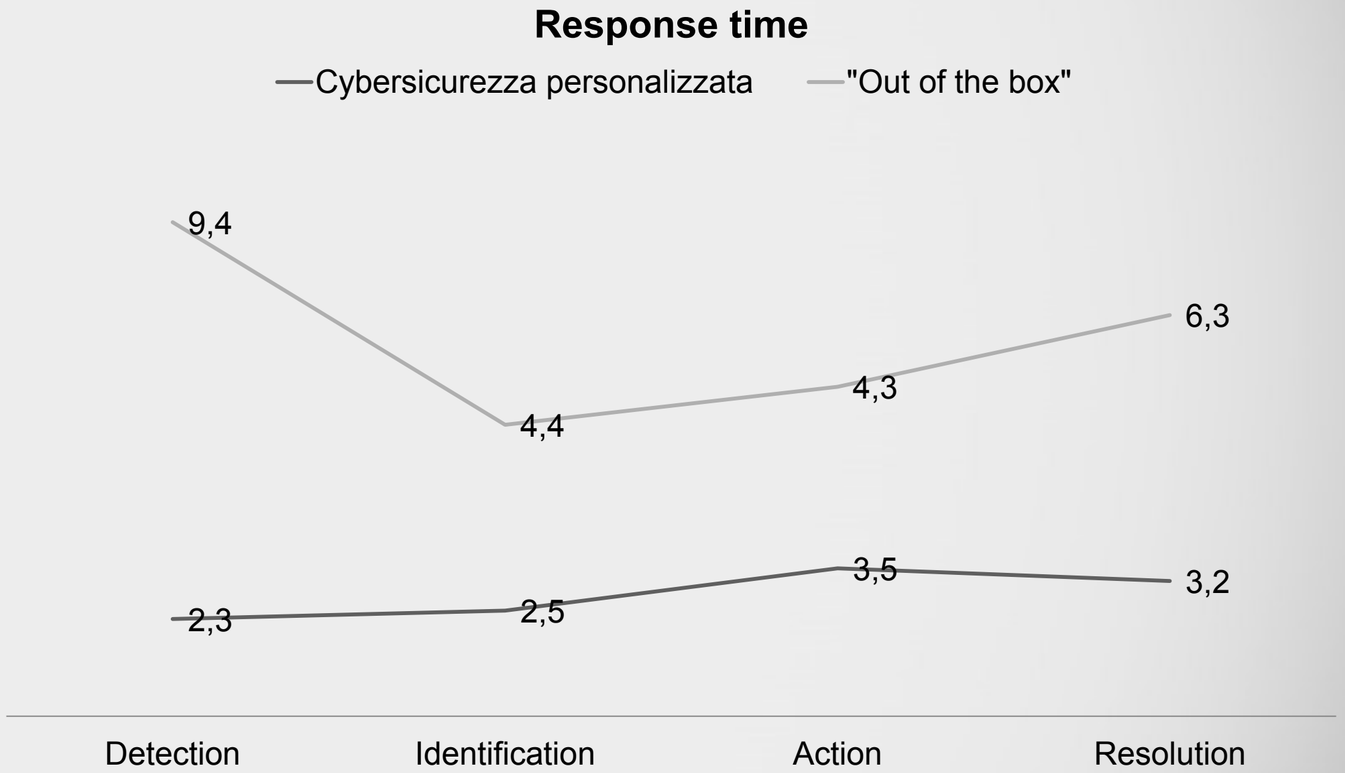
Case Study 1

Cybersicurezza personalizzata VS Cybersicurezza “out of the box”

[redacted]



Contrast percentage based on 100 Attacks*



Response times in minutes*

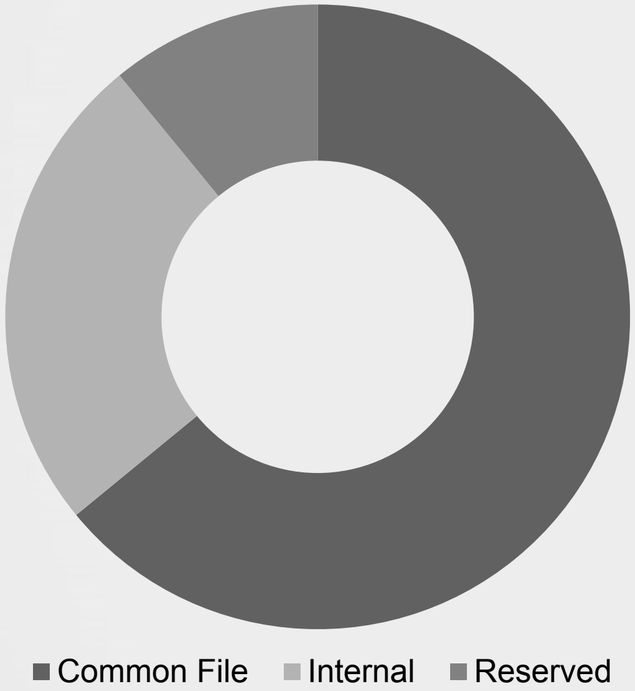
*Source Gartner

Case Study 2

Data Loss Prevention

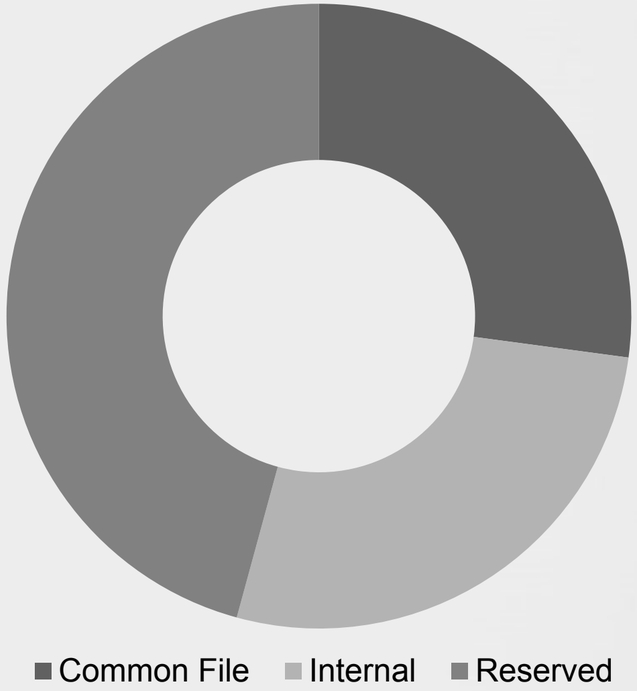
[redacted]

Custom CyberSecurity Solutions



Data Loss percentage by Type of Data

“Out of the box”

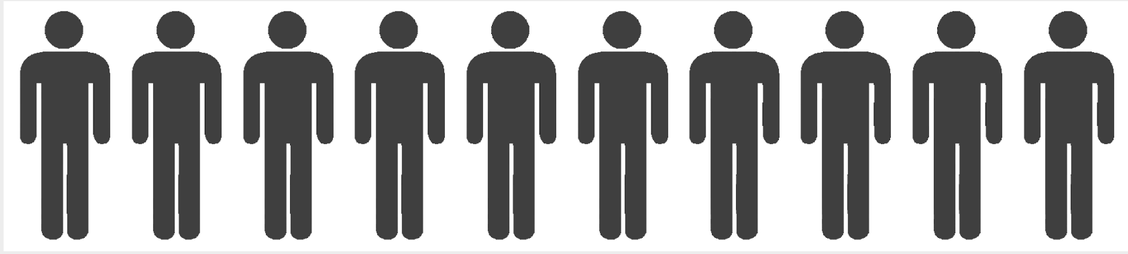


Data Loss percentage by Type of Data

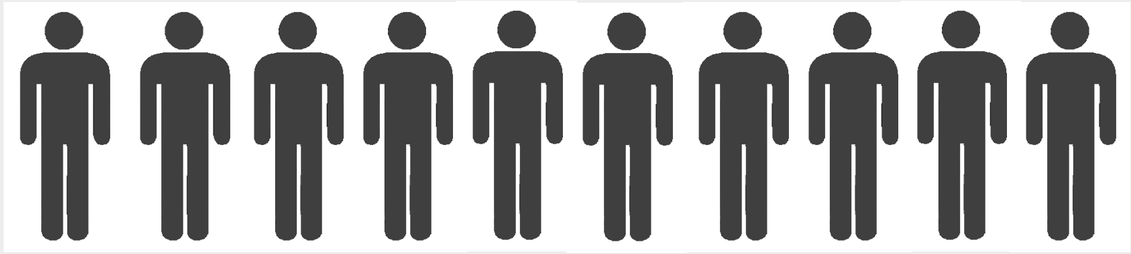
*Source Gartner

Case Study 3

“The Cost Saving” Approch.



Human Resources “inside” needed to guarantee an accettable level of security



Risorse umane “Security” necessarie per garantire un elevato grado di sicurezza con approccio personalizzato e security out-sourcing*

*Source Gartner

Contact Us


[redacted]2sec.com


c2security


Facebook/C2sec

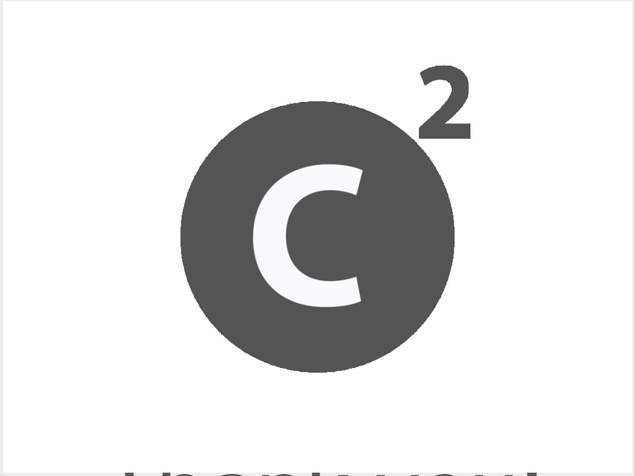

@c2sec


info@c2sec.com


@c2security

“To competently perform rectifying security service, two critical incident response elements are necessary: information and organization.”

- Robert E.Davis



Thank you!

[redacted]

[redacted]