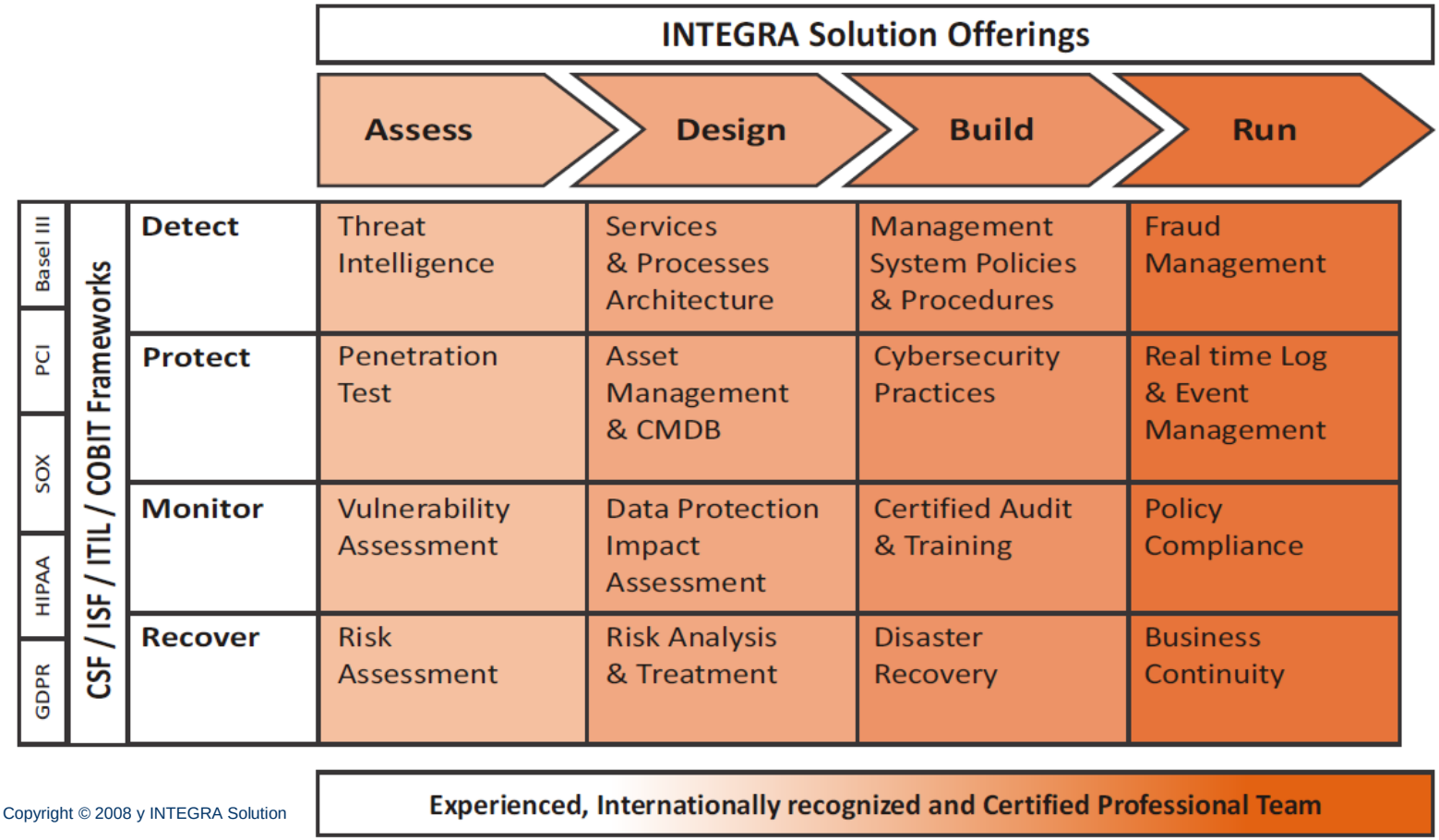
Cybersecurity Case Study

Goran Chamurovski MBA, CISA, CRISC, PMP, CS Manager, CIPP/E
Goran Milev CEH, OSWP, CHFI, MCSE, CCNA Security
INTEGRA Solution

MKD-CIRT

June 2019

Digital risk management
for regulated industries and environments



INTEGRA SOLUTION
simplify a complex world

AGENDA
Summary

- **Cybersecurity scenario**
- **Cyber attack mechanisms**
- **Attack vector**
- **Mitigation and cybersecurity controls**
- **Evidence and lessons learned**
- **Incident Report**

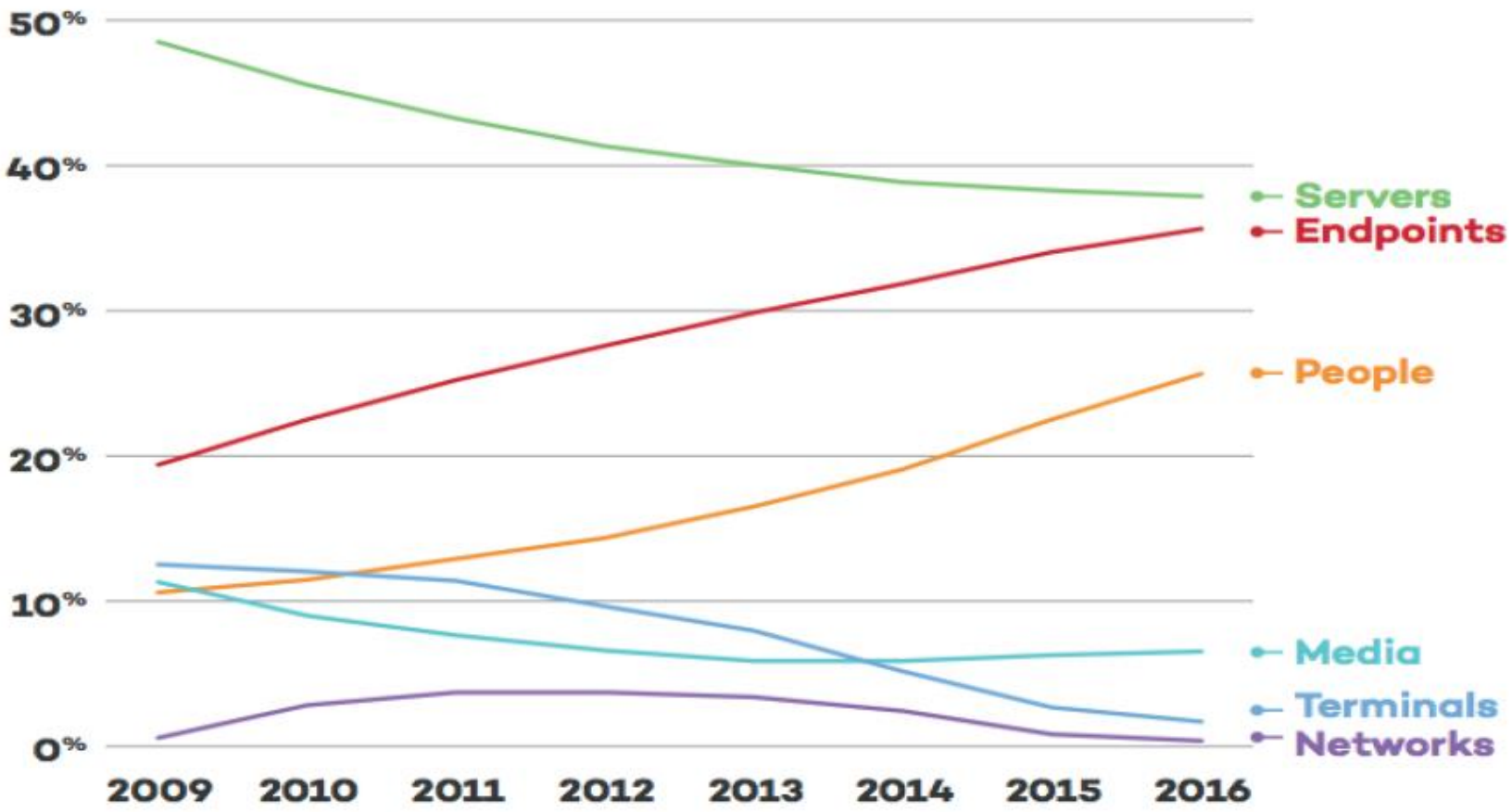
Top cyber threats

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	Stable	1. Malware	Stable	→
2. Web Based Attacks	Increasing	2. Web Based Attacks	Increasing	→
3. Web Application Attacks	Increasing	3. Web Application Attacks	Stable	→
4. Phishing	Increasing	4. Phishing	Increasing	→
5. Spam	Increasing	5. Denial of Service	Increasing	↑
6. Denial of Service	Increasing	6. Spam	Stable	↓
7. Ransomware	Increasing	7. Botnets	Increasing	↑
8. Botnets	Increasing	8. Data Breaches	Increasing	↑
9. Insider threat	Stable	9. Insider Threat	Declining	→
10. Physical manipulation/ damage/ theft/loss	Stable	10. Physical manipulation/ damage/ theft/loss	Stable	→
11. Data Breaches	Increasing	11. Information Leakage	Increasing	↑
12. Identity Theft	Increasing	12. Identity Theft	Increasing	→
13. Information Leakage	Increasing	13. Cryptojacking	Increasing	NEW
14. Exploit Kits	Declining	14. Ransomware	Declining	↓
15. Cyber Espionage	Increasing	15. Cyber Espionage	Declining	→

Legend: Trends: Declining, Stable, Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Source: ENISA

Threat detection



Phishing as attack mechanism

- Phishing is the mechanism of crafting messages that use social engineering emails and messages
- Phishing attacks became more targeted
- Shift from consumer to enterprise targets
- Steady growth in mobile phishing attacks (85% y-over-y)
- Rapid increase in phishing sites using HTTPS (one third)
- The problem of Business Email Compromise (whaling)
- Spearphishing is the de facto delivery method for APT groups (71% of APT as infection vector)
- Trends in malicious attachments (used 28% more malicious attachments compared to malicious URLs)

Attack vectors phishing

- Common techniques: domain typosquatting, domain shadowing, maliciously registered domains, URL shorteners
- Tuesday has been observed as the most popular day for phishers to conduct their campaigns as opposite Friday is less preferred
- BEC phishing attacks were: Purchase Order, Payment, Invoice, Receipt, Slip, Bill, Advice and Transfer
- Phishing related to cryptocurrencies and ICO
- Social media phishing has increased by 200% from 2016 to 2017.

Malware as attack mechanism

- Malware is the most frequently encountered cyber threat involved in 30% of all data breach incidents reported
- Command and Control communication has increased by 300%
- The mobile malware landscape is steadily increasing and IoT devices are targeted
- Fileless attack techniques are the new norm
- Continued growth in the usage of open-source malware
- 79% of the detected malware in organisations were targeting Windows, 18% Linux and 3% Mac systems
- 94% of all malicious executables have been polymorphic

Attack vectors (malware)

- Compromised email (phishing, spam and spear-phishing) is the dominating attack vector for malware infections
- email compromise was the attack vector for 92,4% of detected malware, web and browser was the attack vector for 6,3% and 1,3% has been attributed to other attack vectors (Verizon)
- Special attention should be given to the abuse of Remote Desktop Protocol (RDP) as an attack vector
- Finally, supply chain attacks is another attack vector can be utilised for delivering the malicious payload

Information leakage as attack mechanism

- Information leakage is one of the significant cyberthreats covering a wide variety of compromised information, from personal data collected by internet enterprises and online services to business data stored in IT infrastructures
- Most reported reasons for information leakage are hacking and malware, however
- Users voluntarily forget their PII ownership
- Human error is the most crucial factor for data disclosure
- Governmental organizations take the majority of data leakage incidents
- Geopolitics become an even stronger factor

Attack vectors information leakage

- Q3 2018, a 20% increase in confidential data leaks compared with Q3 2017
- H1 2018, USB sticks and other removable media accounted for 2,1% of the leaks worldwide
- March 2018, ca. 500.000 email accounts with passwords were priced at US $90 in the Dark Web
- Fines to be paid to the European Regulators (according to GDPR) from £1.4bn in 2015 to £122bn
- The total amount of business data being stored is estimated to double every 12 to 18 months
- Internal actors are 29% of those who are involved in data disclosures (26% of the internal actors are system administrators, 22% are end-users,…)

Mitigating phishing controls

- Educate staff to identify fake and malicious emails and stay vigilant
- Perform social engineering pentest as an exercise with many different scenarios and attack vectors
- Disable automatic execution of code, macros, rendering of graphics and preloading mailed links
- Implement a fraud and anomaly detection system at network level for both inbound and outbound
- Enable two factor-authentication whenever applicable
- Unencrypted and unsigned emails should not be trusted, especially for sensitive use-cases
- Consider applying security solutions that use machine learning techniques to identify phishing sites in real time

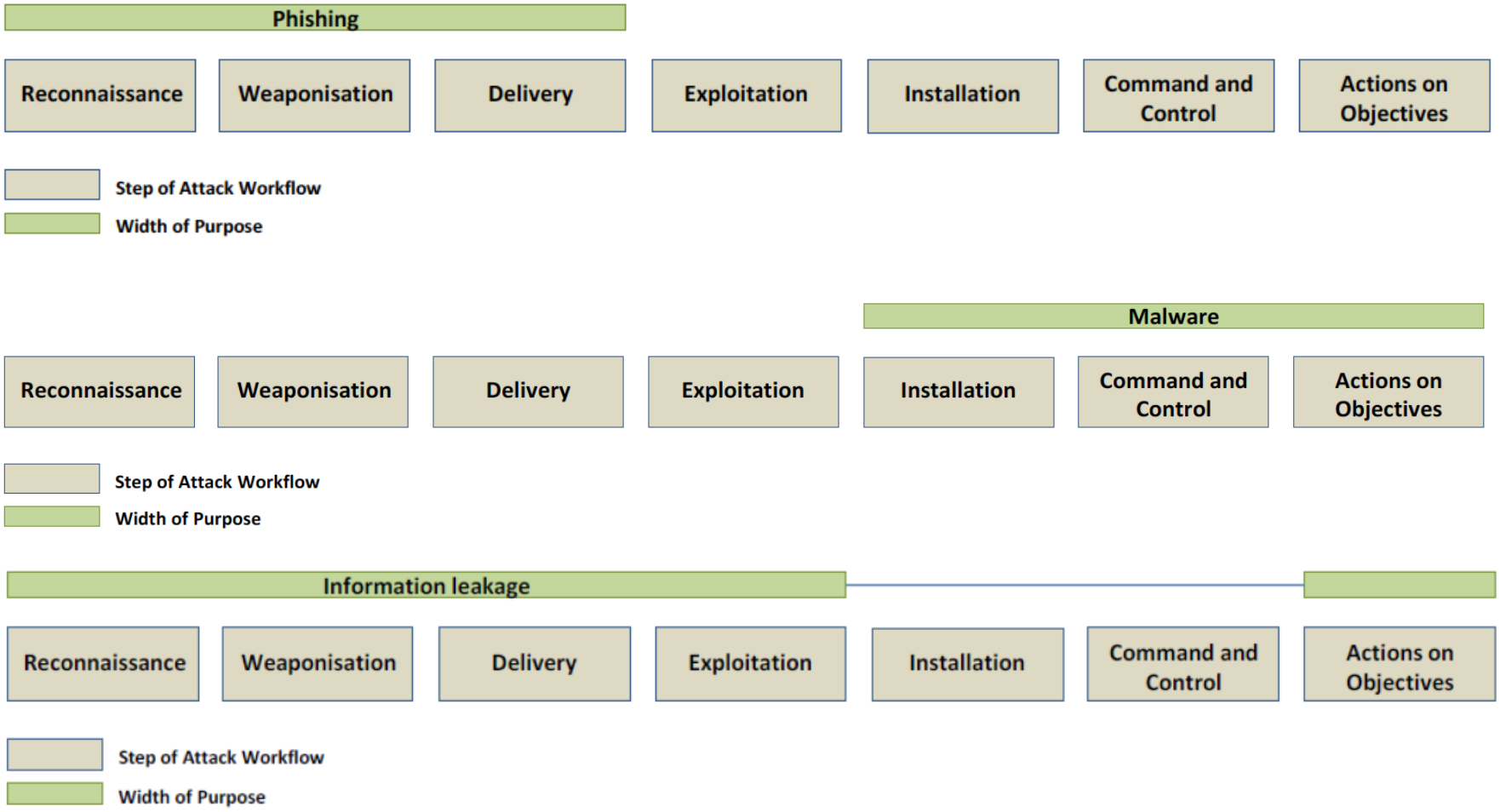
Mitigation malware controls

- Malware detection should be implemented for all inbound/outbound channels
- Tools on malware analysis as well as sharing of malware information and malware mitigation
- Incident response security policies that specify the processes followed in cases of infection
- Identify gaps and apply defence-in-depth principle
- Monitor the antivirus tests regularly
- Interfaces of malware detection functions (intelligence led threat hunting)

Mitigating information leakage

- Perform data classification to assess and reflect the level of protection needed
- Anonymise, pseudonymise, minimise and encrypt data according to the provisions
- Store data only on secure IT assets (data mapping)
- Limit user access privileges under the need-to-know principle
- Orchestrate the patch management and updates system in line with a vulnerability management framework
- Utilise technology tools to avoid possible data leakages, such as vulnerability scans, malware scans
- Monitor the log's via a SIEM solution and data loss prevention

Cyber kill chain

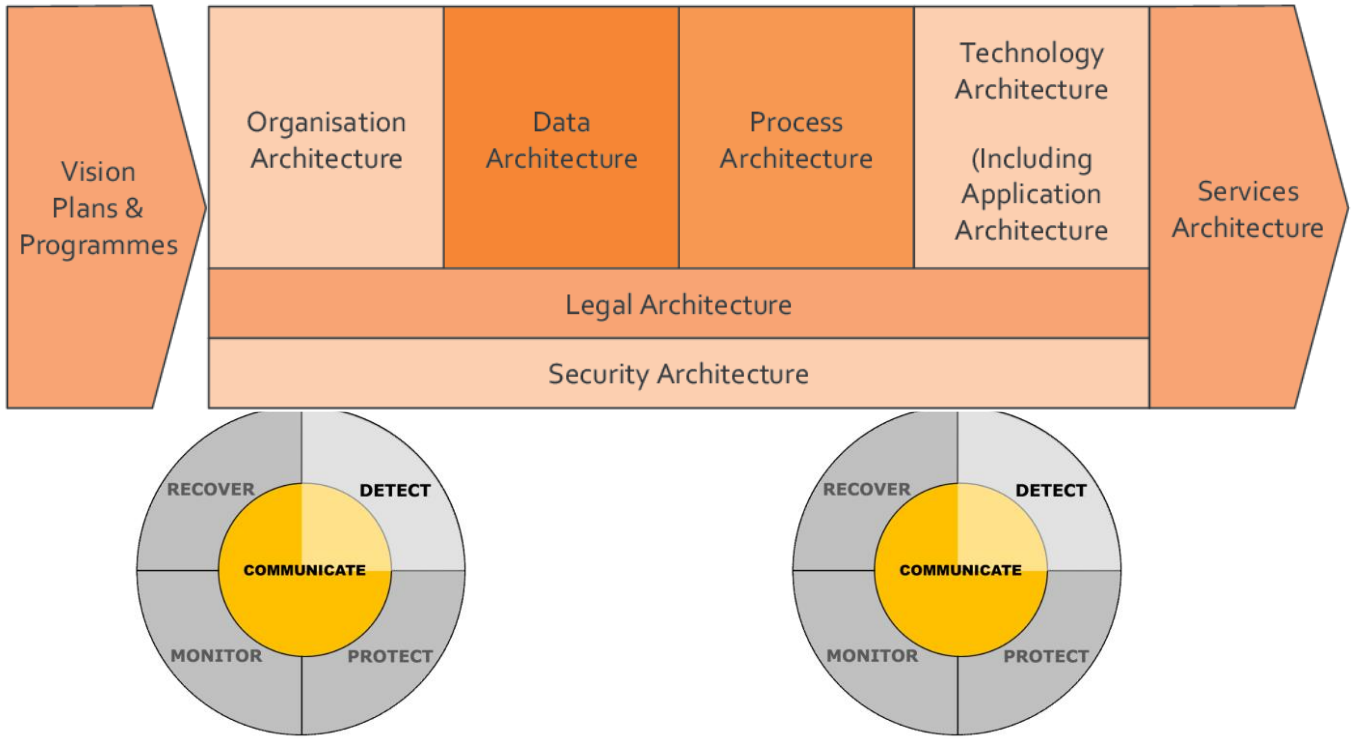


Threat Agents

	THREAT AGENTS						
	Cyber-criminals	Insiders	Nation States	Corporations	Hacktivists	Cyber-terrorists	Script kiddies
Malware	✓	✓	✓	✓	✓	✓	✓
Web-based attacks	✓		✓	✓	✓	✓	✓
Web application attacks	✓		✓	✓	✓	✓	✓
Denial of Service	✓		✓	✓	✓	✓	✓
Botnets	✓		✓	✓	✓	✓	✓
Phishing	✓	✓	✓	✓	✓		✓
Spam	✓	✓	✓	✓			
Ransomware	✓	✓	✓	✓			✓
Insider threat	✓		✓	✓		✓	
Physical manipulation / damage / theft / loss	✓	✓	✓	✓	✓	✓	✓
Exploit kits	✓		✓	✓			
Data breaches	✓	✓	✓	✓	✓	✓	✓
Identity theft	✓	✓	✓	✓	✓	✓	✓
Information leakage	✓	✓	✓	✓	✓	✓	✓
Cyber espionage		✓	✓	✓			

Legend:
Primary group for threat: ✓
Secondary group for threat: ✓

Business perspective
Value Chain

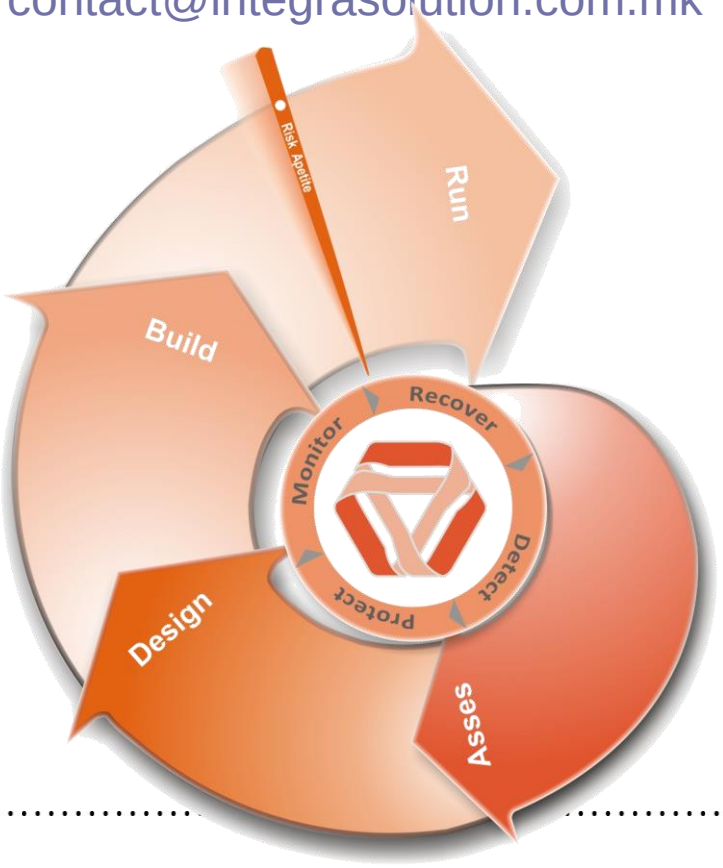


Cybersecurity risk is a reality that organizations must understand and manage to the level of fidelity of other business risks that can have critical impacts.

Q&A

Thank You

contact@integrasolution.com.mk



INTEGRA SOLUTION
simplify a complex world