



At the edge of digital innovation

eGov Conference **2024**

Smart Governance with GovTech

Enhancing Citizen Experience and Engagement

08th April 2024

www.sil.mu



Securing the Future: Cybersecurity in Government Ecosystems

Discover key threats, best practices, and the benefits of these solutions in bolstering cybersecurity through the digital transformation of governmental entities.



Agenda



Attack Statistics – based on a Cyber Security report

Why Are Companies being Targeted?

Let's Take a Step Back – Pandemic Era

Critical Role in Government Operations

Why are Companies being Attacked?

Types of Threats

SIL Solutions – adopting the NIST CSF v2.0 Framework

Advanced persistent threat landscape in 2020

Top 10 targets:

- Government
- Banks
- Financial Institutions
- Diplomatic
- Telecommunications
- Educational
- Defense
- Energy
- Military
- IT companies

Top 12 targeted countries:



Top 10 significant threat actors:

- Lazarus
- DeathStalker
- CactusPete
- IAmTheKing
- TransparentTribe
- StrongPity
- Sofacy
- CoughingDown
- MuddyWater
- SixLittleMonkeys

Kaspersky's Global Research and Analysis Team (GReAT) is well-known for the discovery and dissemination of the most advanced cyberthreats.

According to their data, in 2020 the top targets for advanced persistent threats (APT) were governments, and the most significant threat actor was Lazarus.

ept.securelist.com

Report - Attack Statistics



61%

Attacks are clustered in the middle of the work week

43%

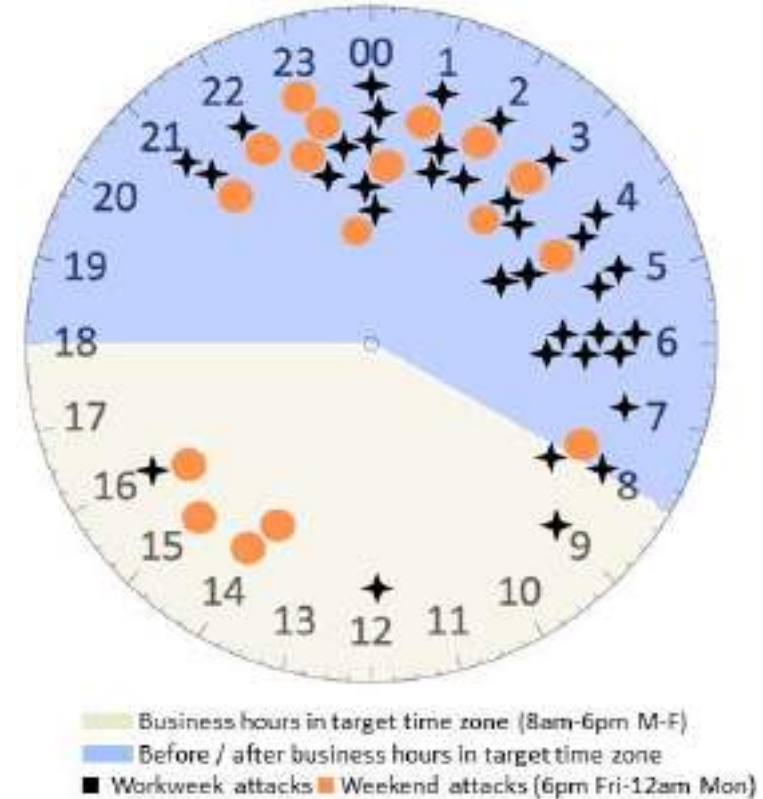
Ransomware attacks launched on either Friday or Saturday

16hrs

Median Time-to-Active Directory for all attacks

43.42%

Data has been exfiltrated



Source: Sophos X-Ops Incident Response Team – Midyear Active Adversary Report (2023)

Attack Statistics Breakdown_{contd.}



Attack Types Detected	Year	
	2022	1H2023
Ransomware	68.42%	68.75%
Network Breach	18.42%	16.25%

Most Active Ransomware Groups	Year	
	2022	1H2023
LockBit	15.38%	14.55%
AlphaVM/BlackCat	12.50%	12.73%

Most Frequently Observed Tools	Year	
	2022	1H2023
Netscan	Did not chart	31.25%
Cobalt Strike	42.76%	30.00%

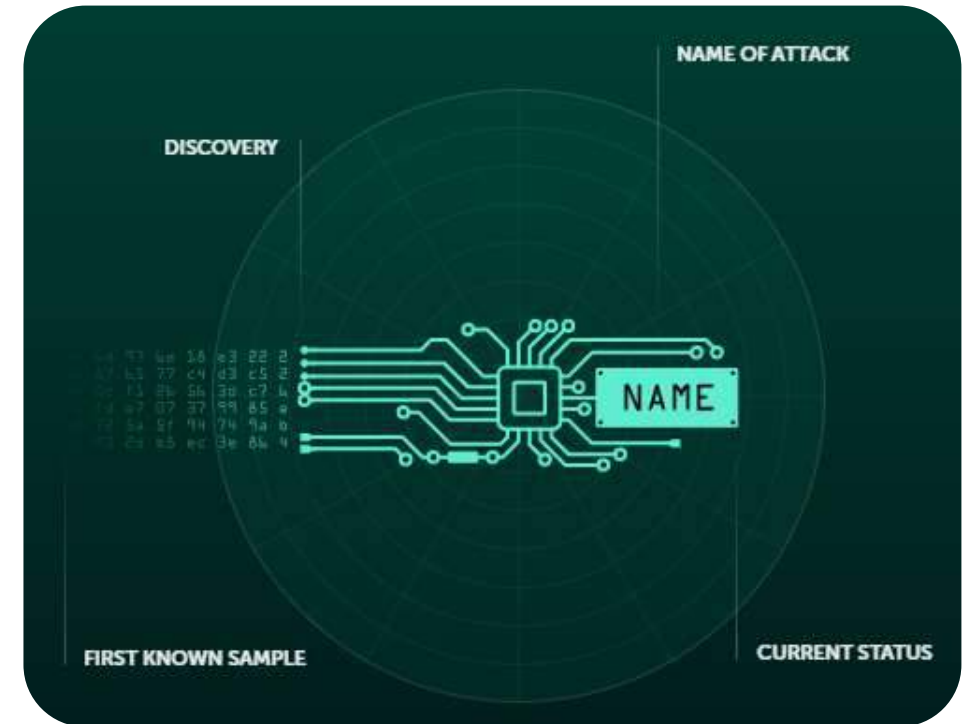
Most Frequently Observed LOLBins	Year	
	2022	1H2023
Powershell	74.34%	78.75%
AlphaVM/BlackCat	12.50%	12.73%

Most Frequently Observed "Other"	Year	
	2022	1H2023
Valid Accounts	71.05%	85.00%
Install Services	63.82%	56.25%
Malicious Scripts	53.29%	50.00%
Browse Networks	43.42%	47.50%
Disable Protection	36.18%	42.50%

Source: Sophos X-Ops Incident Response Team – Midyear Active Adversary Report (2023)

Conclusion of the Report

- 🔍 Lays bare how attackers introduce risks to organisations
- 🔍 Mitigations are possible & have massive positive impacts on the organisations
- 🔍 Budget will not be sufficient – other prioritisations
- 🔍 Requires change in corporate policies – patching & MFA
- 🔍 Store data – analyse periodically
- 🔍 Tools needed to identify assess, identify & respond

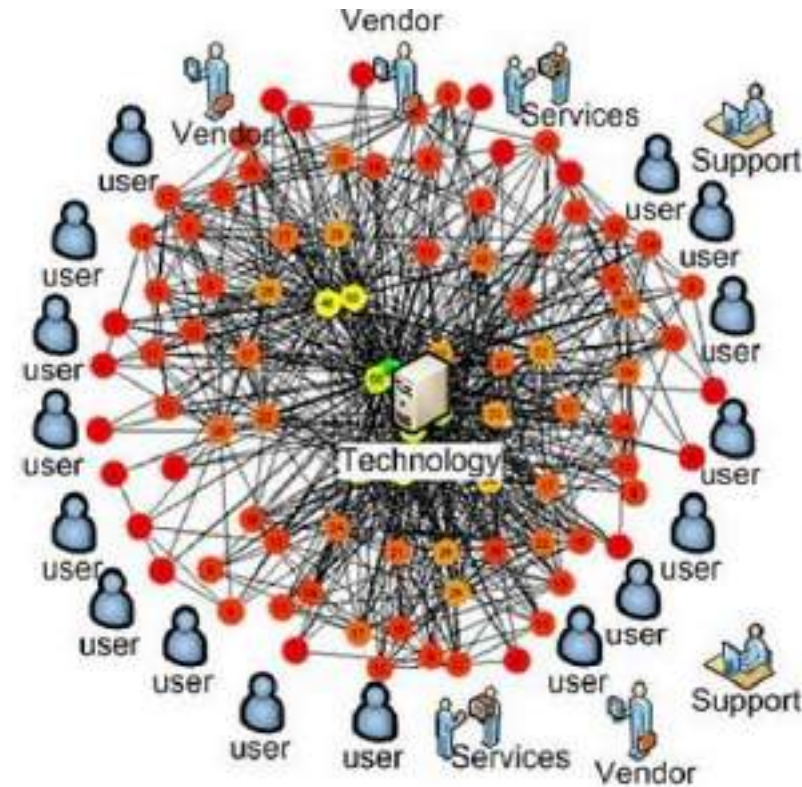


Source: Sophos X-Ops Incident Response Team –
Midyear Active Adversary Report (2023)

Why are Gov. companies being targeted?

Complex Infrastructure

- Extensive and complex IT infrastructures - networks, databases, and legacy systems.
- Managing and securing these diverse systems - significant challenges, especially considering the interconnectedness of government operations.



Why are Gov. companies being targeted?

contd.

■ Limited Resources

- Operate with constrained budgets and limited resources.
- Hinder efforts to:
 - implement robust security measures
 - conduct regular assessments
 - invest in advanced technologies
 - personnel training

My job asked if I can work under limited resources. I showed them this picture. I start next week. 😊



Why are Gov. companies being targeted?

contd.



Legacy Systems & Technology

- Rely on outdated or legacy systems
- Lack adequate security features or receive limited support
- Pose inherent cybersecurity risks due to vulnerabilities that may not be easily patched or mitigated



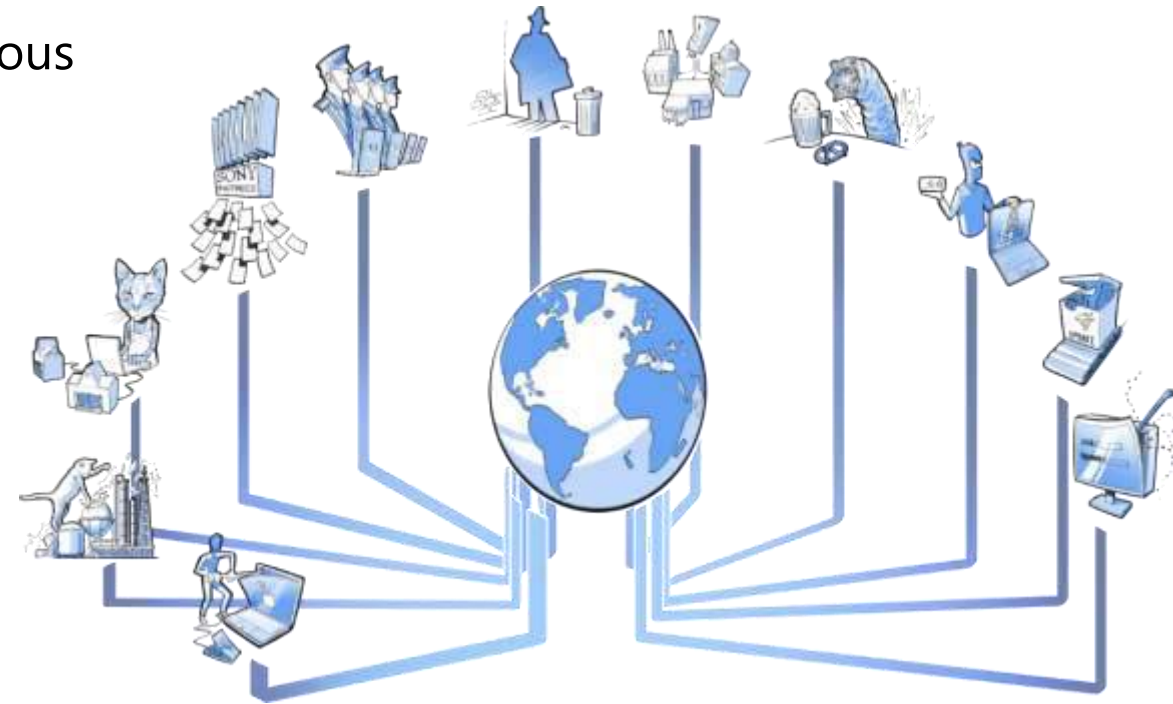
**“What if we don’t change at all ...
and something magical just happens?”**

Why are Gov. companies being targeted?

contd.

Persistent Threat Landscapes

- Face a relentless onslaught of cyber threats from various sources:
 - Nation-states
 - Cybercriminals
 - Hacktivists
 - Insider Threats
- Sophisticated Attacks:
 - Aimed at stealing sensitive information
 - Disrupting operations
- Indiscriminate Attacks – seeking to exploit vulnerabilities



Why are Gov. companies being targeted?

contd.



🚩 Insider Threats

- Intentional
 - Malicious insiders with privileged access exploit their positions to:
 - steal sensitive information
 - sabotage systems
 - facilitate external attacks
- Unintentional
 - inadvertent actions can inadvertently expose government networks to vulnerabilities or breaches



Why are Gov. companies being targeted?

contd.



Regulatory Compliance

- Subject to various regulatory frameworks & compliance requirements - data protection & cybersecurity frameworks
- Adds another layer of complexity to efforts, requiring:
 - continuous
 - monitoring, reporting &
 - adherence to standards



"Uh oh, here come more regulations."

Critical Role in Government Operations

- Protection of Sensitive Area
- Critical Infrastructure Protection
- Intellectual Properties
- Prevention of Cyber Warfare
- National Security



Let's take a step back – Pandemic Era

Weak Areas Exposed

- Work from home system
- Remote collaboration
- Employees were less likely to have access to IT or security patches and updates.
- There was an increase in the transfer of sensitive information via email.
- Internet of Things - wearable technologies ballooned the number of existing communicating devices - increased the attack surface creating new vulnerabilities.



Why are Gov. inst. being attacked? (1)

❖ Compromise Sensitive Information

- Names
- Addresses
- Drivers' license numbers
- Forms for payment
- Social Security Numbers & more

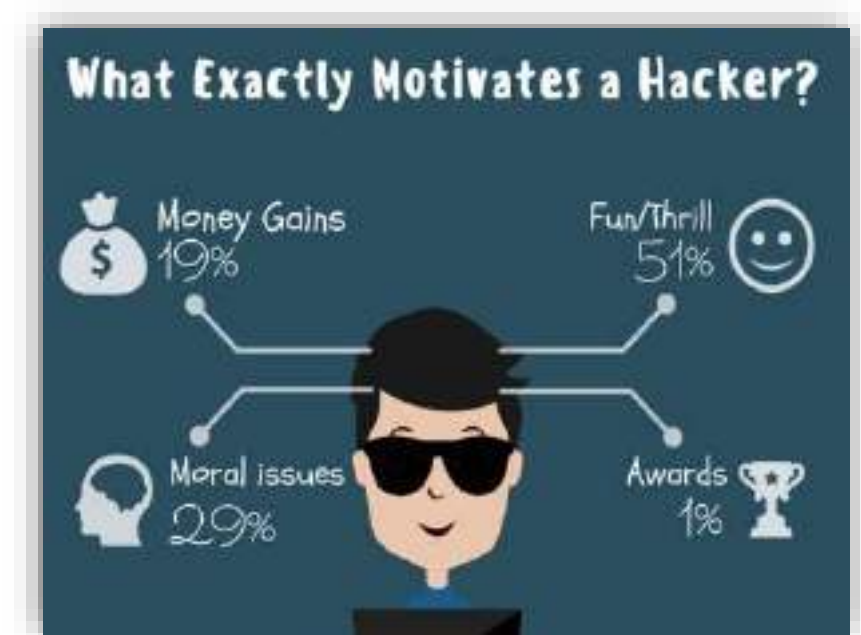
High value for cyber-criminals to capture, sell, or hold for ransom.



"This is *my* spot, Ciswell."

🚩 Motives

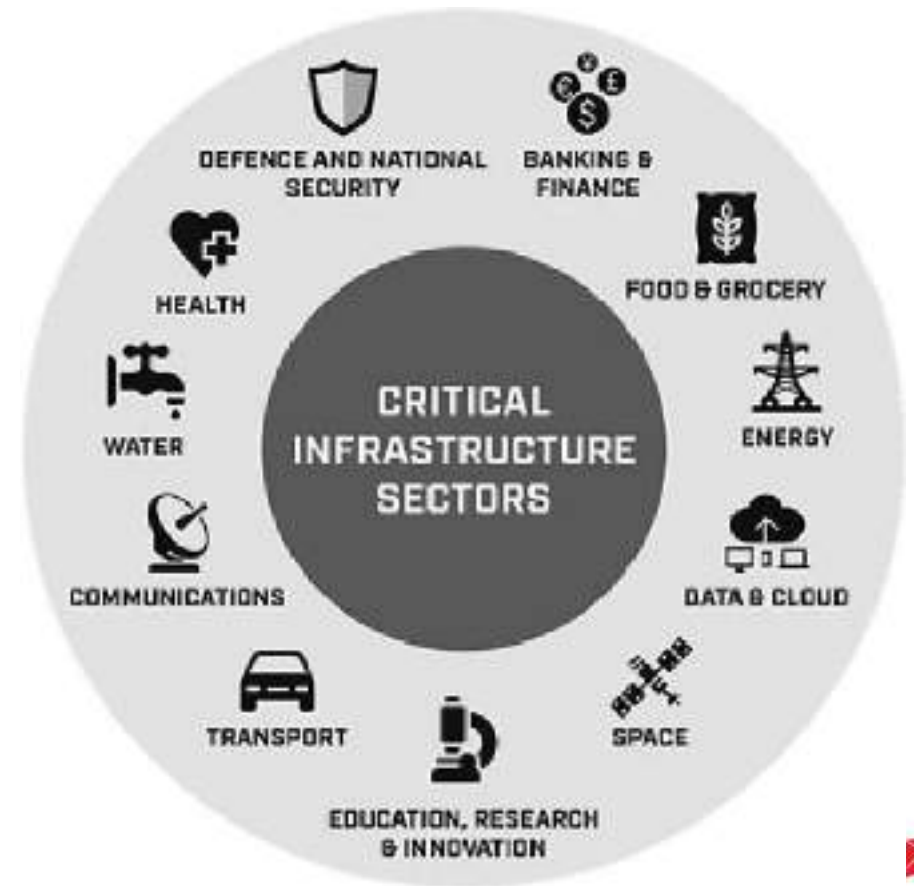
- Aim to shake the public's confidence in local systems and eventually, endangering them.
- Governmental entities are the ones running critical systems as power grids, communicating systems, now the transport system...imagine the risks if all of these go down.



Why are Gov. inst. being attacked? (3)

▀ Cripple Critical Infrastructure

- Police Force
- Healthcare Systems
- Banking
- Government Information Highway



Why are Gov. inst. being attacked? (4)

▀ Limited Resources

Financial Constraints:

- Limit ability to acquire and implement state of the art practice of cybersecurity technology, policies, and practices.
- Struggle to match the job market demands in recruiting and retaining qualified cybersecurity personnel
- Many operate ageing infrastructure and outdated systems...making them more vulnerable to cyber attacks.



Types of Threats

- Ransomware
- Phishing
- DoS/DDoS
- Advanced Persistent Threats (APTs)
- Artificial Intelligence



Ransomware

Warning Message!!

We are sorry to say that your computer and your files have been encrypted, but wait, don't worry. There is a way that you can restore your computer and all of your files

06 Days 22:59:44 Hours

When countdown ends your files will be lost forever

You must send at least 1.0 Bitcoin to our wallet and you will get your files back

Your personal unique ID:

Send 1.0BTC to this address:

Warning Message!!

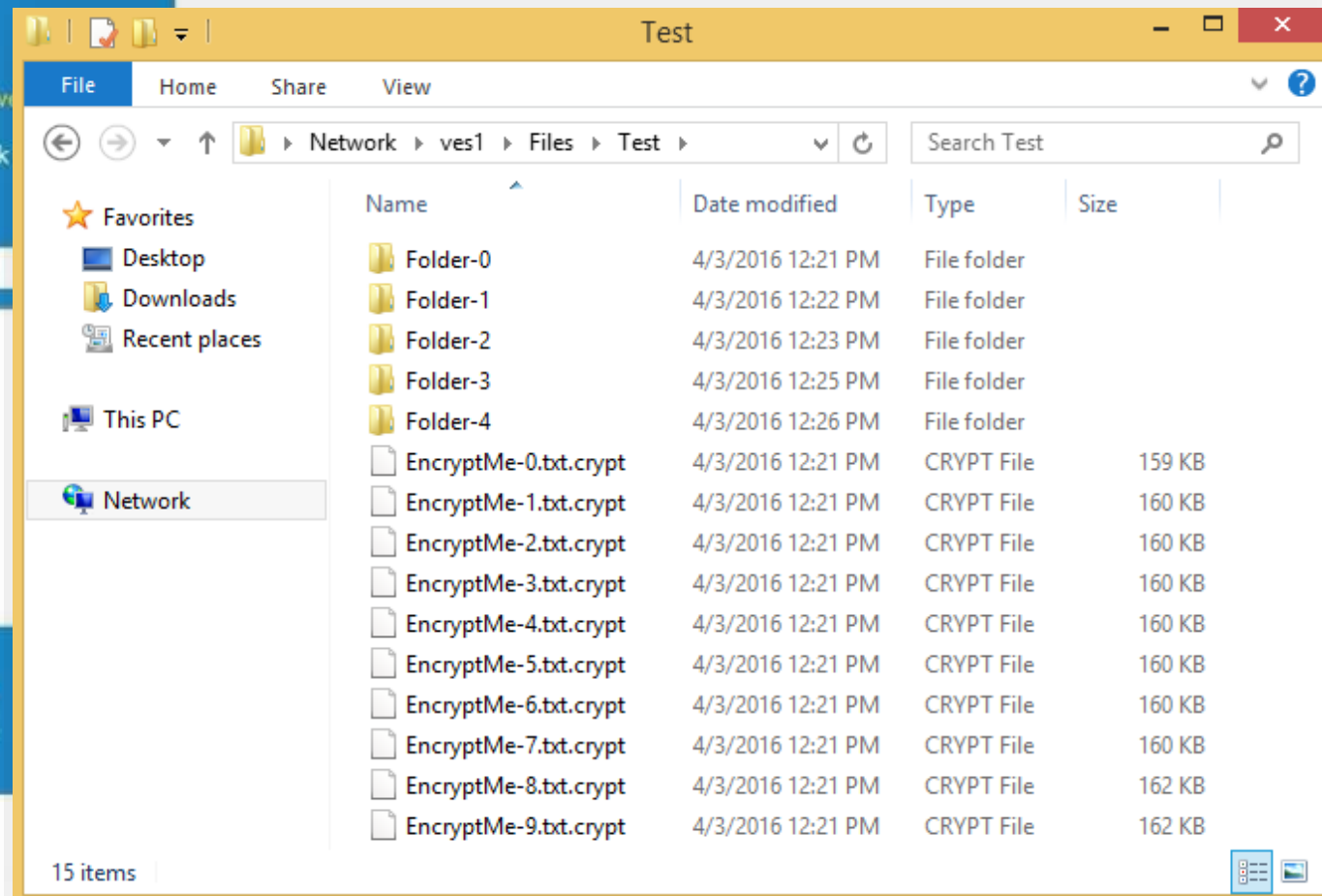
We are sorry to say that your computer and your files have been encrypted, but wait, don't worry. There is a way that you can restore your computer and all of your files

Your personal unique ID: "[redacted]"

You must send at least "1.0" Bitcoin to address "[redacted]" to get your files back

After you've made the payment, you will get a code, please insert it here:

Decrypt



Test

File Home Share View

Network > ves1 > Files > Test

Search Test

Name	Date modified	Type	Size
Folder-0	4/3/2016 12:21 PM	File folder	
Folder-1	4/3/2016 12:22 PM	File folder	
Folder-2	4/3/2016 12:23 PM	File folder	
Folder-3	4/3/2016 12:25 PM	File folder	
Folder-4	4/3/2016 12:26 PM	File folder	
EncryptMe-0.txt.crypt	4/3/2016 12:21 PM	CRYPT File	159 KB
EncryptMe-1.txt.crypt	4/3/2016 12:21 PM	CRYPT File	160 KB
EncryptMe-2.txt.crypt	4/3/2016 12:21 PM	CRYPT File	160 KB
EncryptMe-3.txt.crypt	4/3/2016 12:21 PM	CRYPT File	160 KB
EncryptMe-4.txt.crypt	4/3/2016 12:21 PM	CRYPT File	160 KB
EncryptMe-5.txt.crypt	4/3/2016 12:21 PM	CRYPT File	160 KB
EncryptMe-6.txt.crypt	4/3/2016 12:21 PM	CRYPT File	160 KB
EncryptMe-7.txt.crypt	4/3/2016 12:21 PM	CRYPT File	160 KB
EncryptMe-8.txt.crypt	4/3/2016 12:21 PM	CRYPT File	162 KB
EncryptMe-9.txt.crypt	4/3/2016 12:21 PM	CRYPT File	162 KB

15 items

HSBC | The world's local bank



Dear HSBC customer,

Due to some issues we hold against your account(s), we temporarily suspended access to your online use. You may be getting this message because you recently signed on from a different location or computer. In order to avoid further actions taken by our security department, please identify yourself and continue using our service as normal:

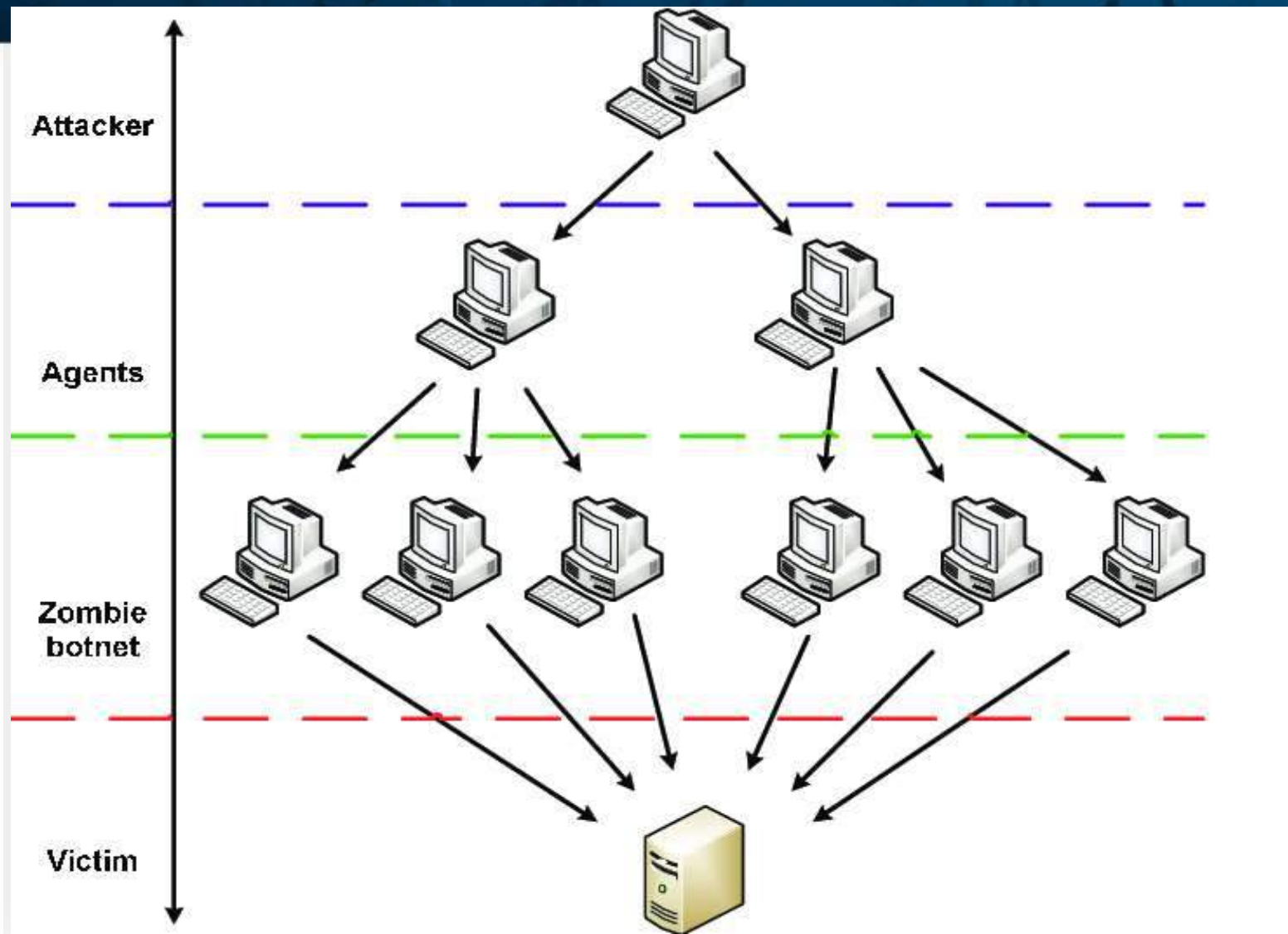
https://hsbc.co.uk/1/2/HSBCINTEGRATION/CAM10;jsessionid=0tva9duIDV_URL=hsbc.MyHSBC_pib/

Thank you.

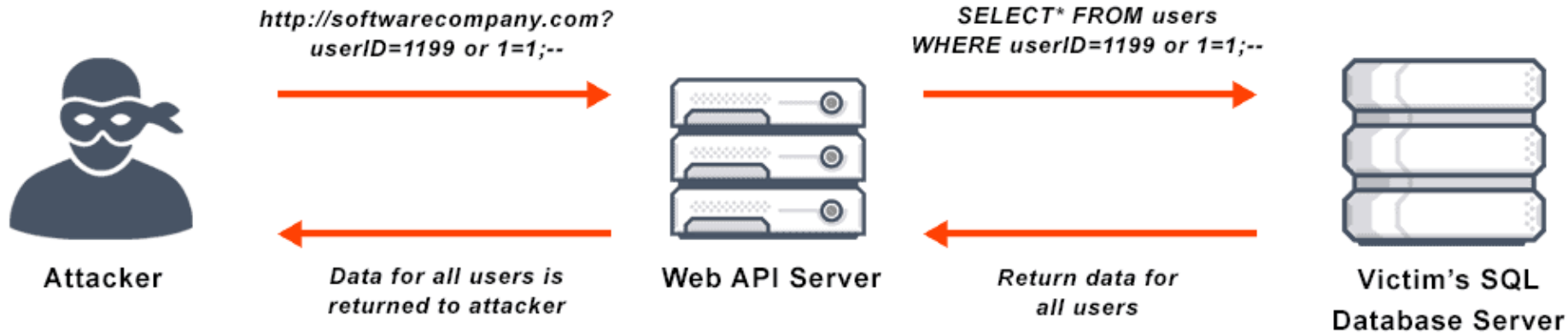
http://hsbc-online.wpew.info/1/2/HSBCINTEGRATION/CAM10;jsessionid=0000tva9NQkofu4NIM7pUeI5Tvn11j5bfvduIDV_URL=hsbc.MyHSBC_pib/index.html

© HSBC Bank plc 2002 – 2010 | Email ID: #4316451

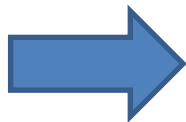
DoS/DDoS Attacks



SQL Injection



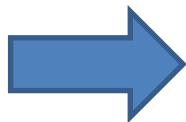
Legitimate SQL query



If the administrator should use "admin@company.com" and "password", like this:

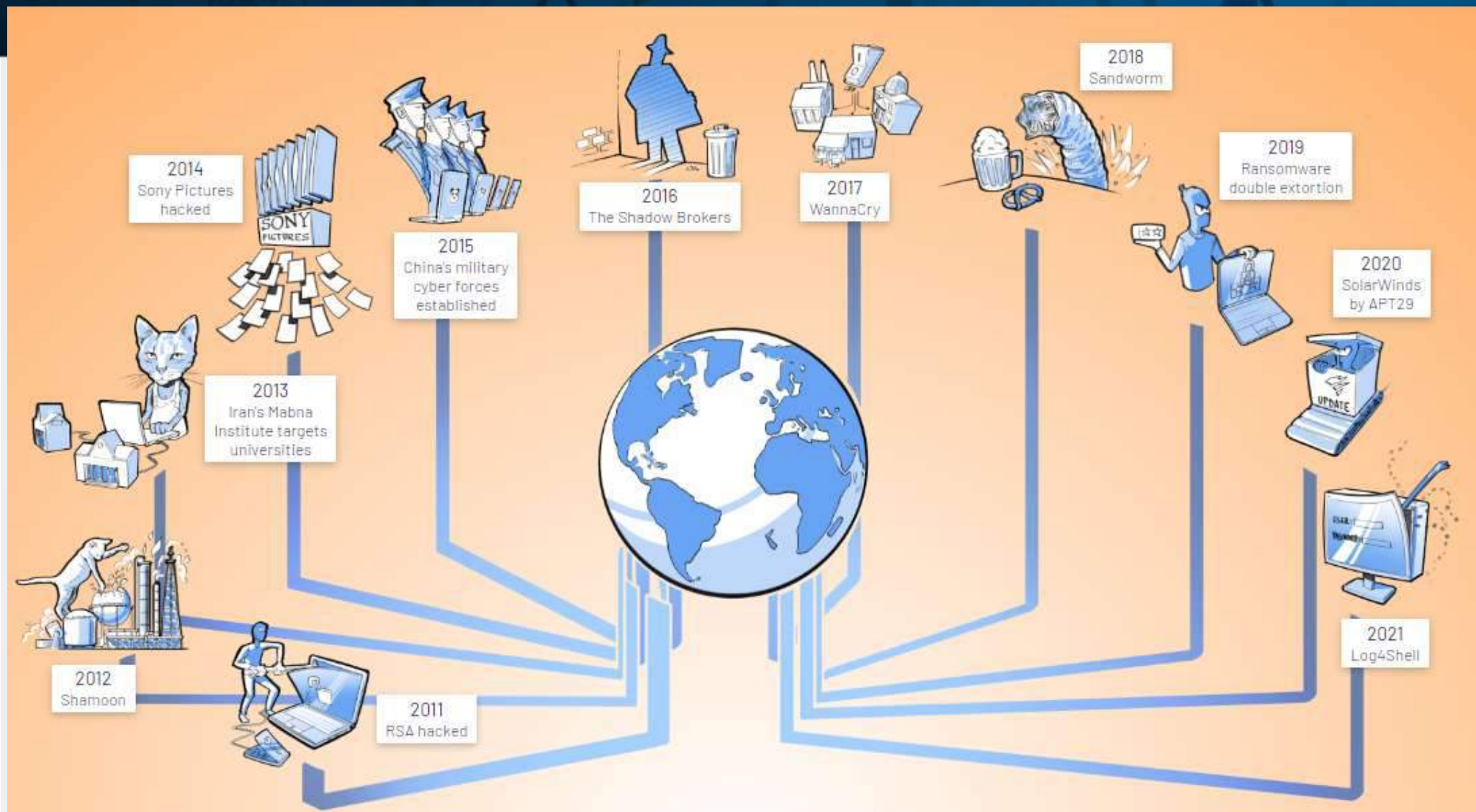
```
SELECT * FROM users WHERE email = 'admin@company.com' AND password = md5('password');
```

Injected codes in the SQL query

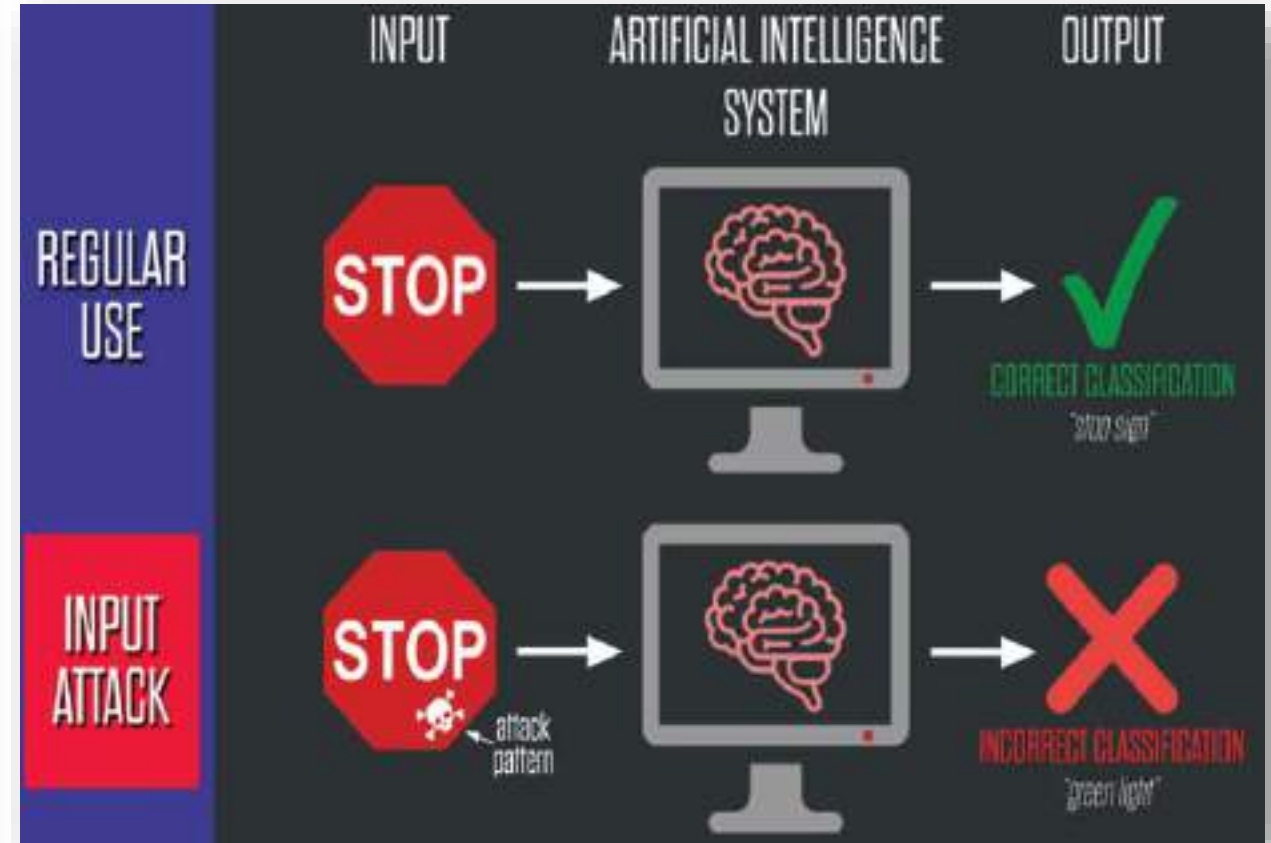
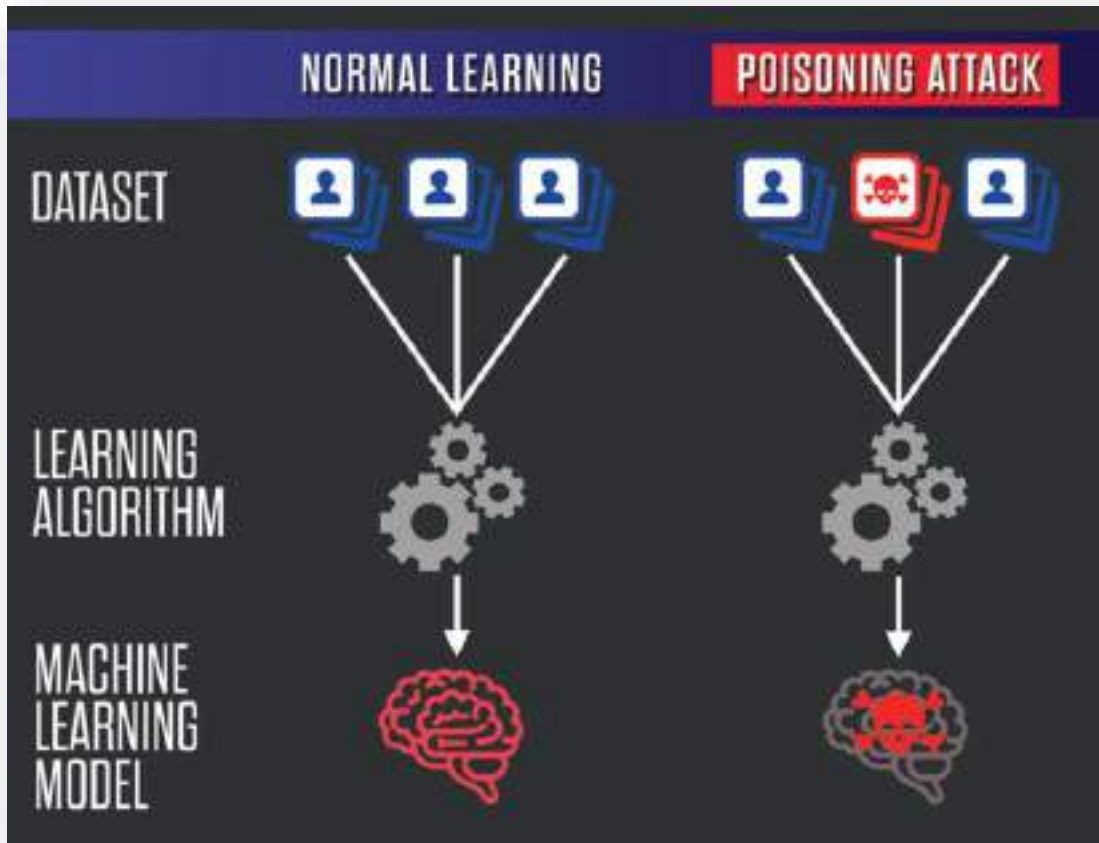


```
SELECT * FROM users WHERE email = 'xxx@xxx.xxx' OR 1 = 1 LIMIT 1 -- ' ] AND password = md5('password').
```


Advanced Persistent Threats



Artificial Intelligence



Safeguarding our digital assets



- As business organizations depend more and more on digital systems to store data and information, cyber-attacks are becoming more and more sophisticated.
- This brings in the need of the hour: to deploy cyber security solutions to safeguard organizations.
- Even though companies are moving to the cloud model, it is the individual duty of the organization to protect itself from security breaches and malicious attacks.

NIST CSF Framework Version 1.0



Capability

Description

Identify (ID)

What processes and assets need protection

Protect (PR)

Implement appropriate safeguards to ensure protection of the enterprise's assets

Detect (DE)

Implement appropriate mechanisms to identify the occurrence of incidents

Respond (RS)

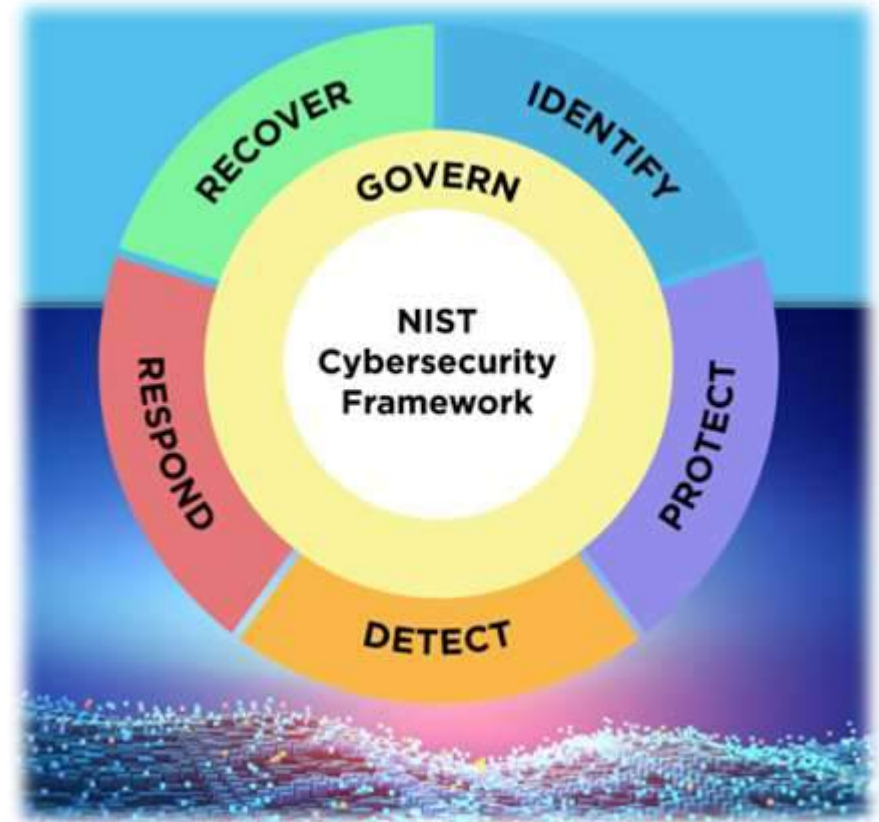
Develop techniques to contain the impacts of events

Recover (RC)

Implement the appropriate processes to restore capabilities and services impaired to adverse events

🚩 Govern (GV)

- Addresses an understanding of organizational context;
- goes beyond protecting critical infrastructure
- cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy;
- and the oversight of cybersecurity strategy



SIL's Solution based on NIST CSF V2.0



Identify

- Identification and Access Management (IAM)
- Data Protection

Protect

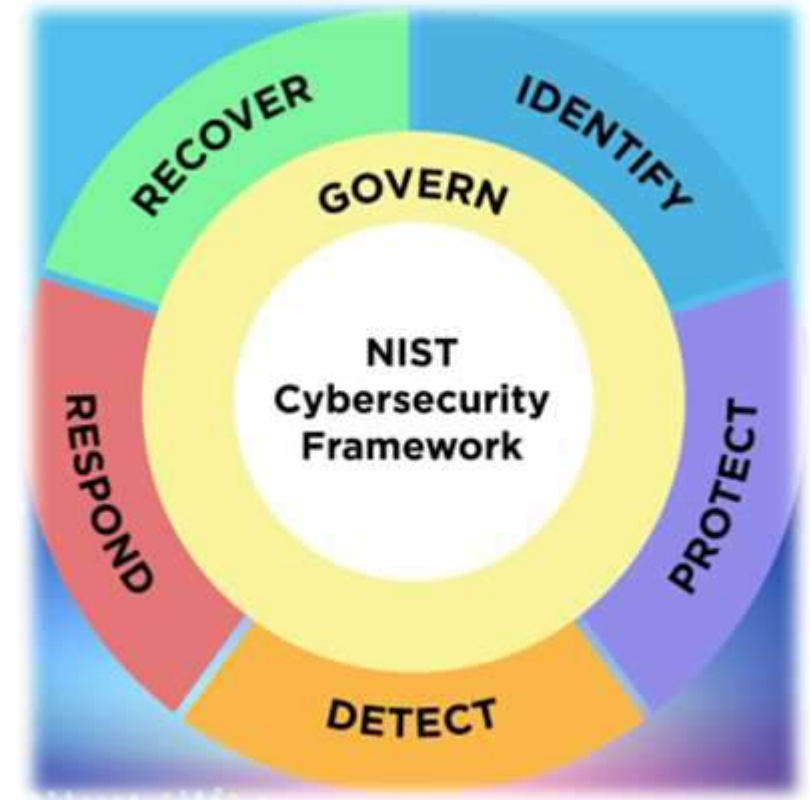
- Endpoint Security
- Threat Intelligence

Detect

- Network Monitoring
- Code Review
- Vulnerability Assessment & Penetration Testing (VAPT)

Respond & Recover

- Endpoint Security
- Disaster Recovery & Business continuity



We Help You Take Decisions



🚩 Govern



- ❖ Cyber Security is indispensable to government operations, given the critical nature of the data and systems that governments manage.
- ❖ Overall, Cyber Security offers valuable tools and resources for government agencies to enhance their cybersecurity capabilities effectively, ensuring the protection of sensitive information, safeguarding national security, and mitigating cyber threats.

“Better cybersecurity outcomes are possible, and tech leaders are the ones that can turn a possibility into a reality. It has to start somewhere, it has to start sometime. What better place than here, what better time than now?”

Thank You

SIL

2, Saint Georges Street, Port Louis

Republic of Mauritius



207 8000



silmail@sil.mu

