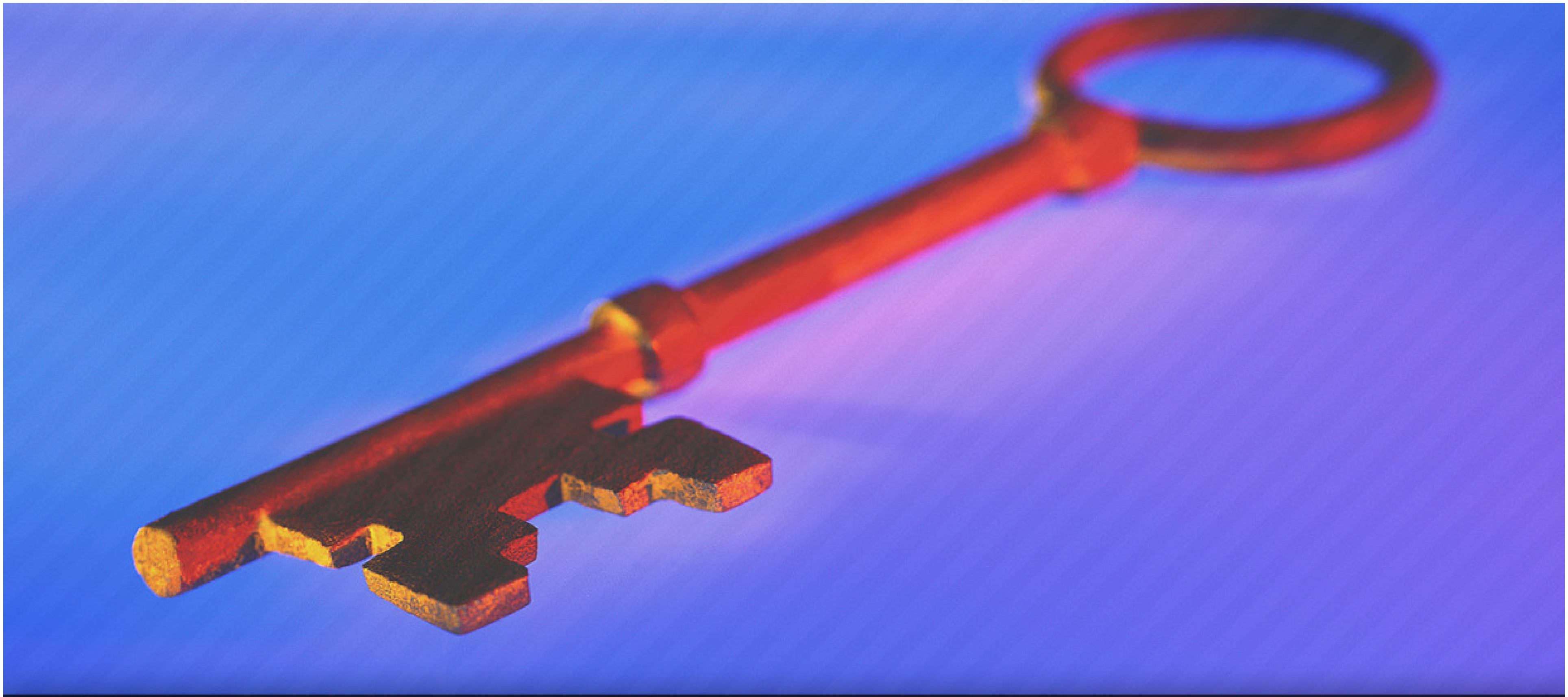
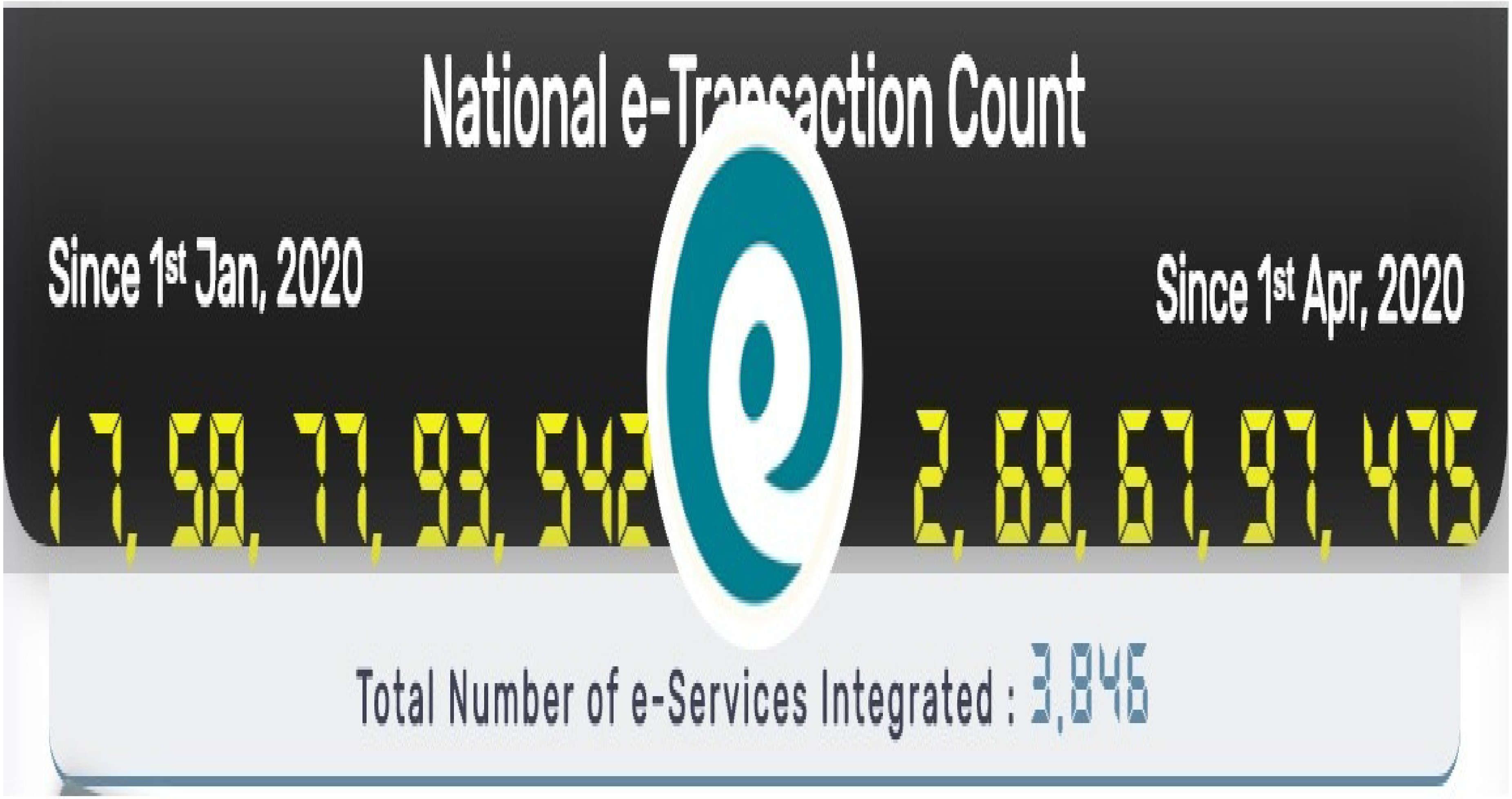


Cyber Security for Public Sectors

Golok Kumar Simli
Chief of Technology, Pssport Seva
Ministry of External Affairs
Government of India
Twitter @ctopassportseva

Backdrop

Every single task and activity, we as individuals perform in today’s Digital World involves some or other form of Data Transactions. Data is the new vital economical input as well as essence of our daily life, therefore its protection is equally important



National e-Transaction Count

Since 1st Jan, 2020

17,58,77,93,542

Since 1st Apr, 2020

2,69,67,97,475

Total Number of e-Services Integrated : 3,846

* *Source:eTaal.gov.in*

Approach to Cyber Security

- Effective cyber security is about much more than technology solutions and tools deployed
- Government has a large employee base, it is much more exposed to the security vulnerabilities caused by security mistakes, inadequate training, and illegal activity from within
- Though cyber attacks seems oriented from outside organisations, employees remain the largest security risk in any organization
- Primarily careless user groups, who accidently reveal information that helps others carry out attacks, majority due to lack of awareness about how to minimize risk

Get the Basics Right – Rest Will Follow

- Password Policies and Adherence - deploy 2-FA wherever possible
- Phishing and Social Engineering – employees must be trained how to recognize phishing scams
- We must exercise caution around emails, videos or websites that seem suspicious
- Doubly ascertain and check email domains before clicking on URL links to make certain that it originated from a legitimate source
- Misspellings, Grammatical errors are other indicators of risk and should be careful if someone asks for your user credentials

Get the Basics Right – Rest Will Follow

- Device policies - Users must be trained about how to use, secure, and store devices. E.g., leaving machines unlocked when you are away from your desks. Mobile devices should also support remote wipe functions

- Physical security - Devices shouldn’t be left unattended in unsafe areas

- Critical and sensitive data should never be on display out in the open, such as leaving printed content unattended

- Continuously monitor and enforce the cyber security posture and training road map of your organisation

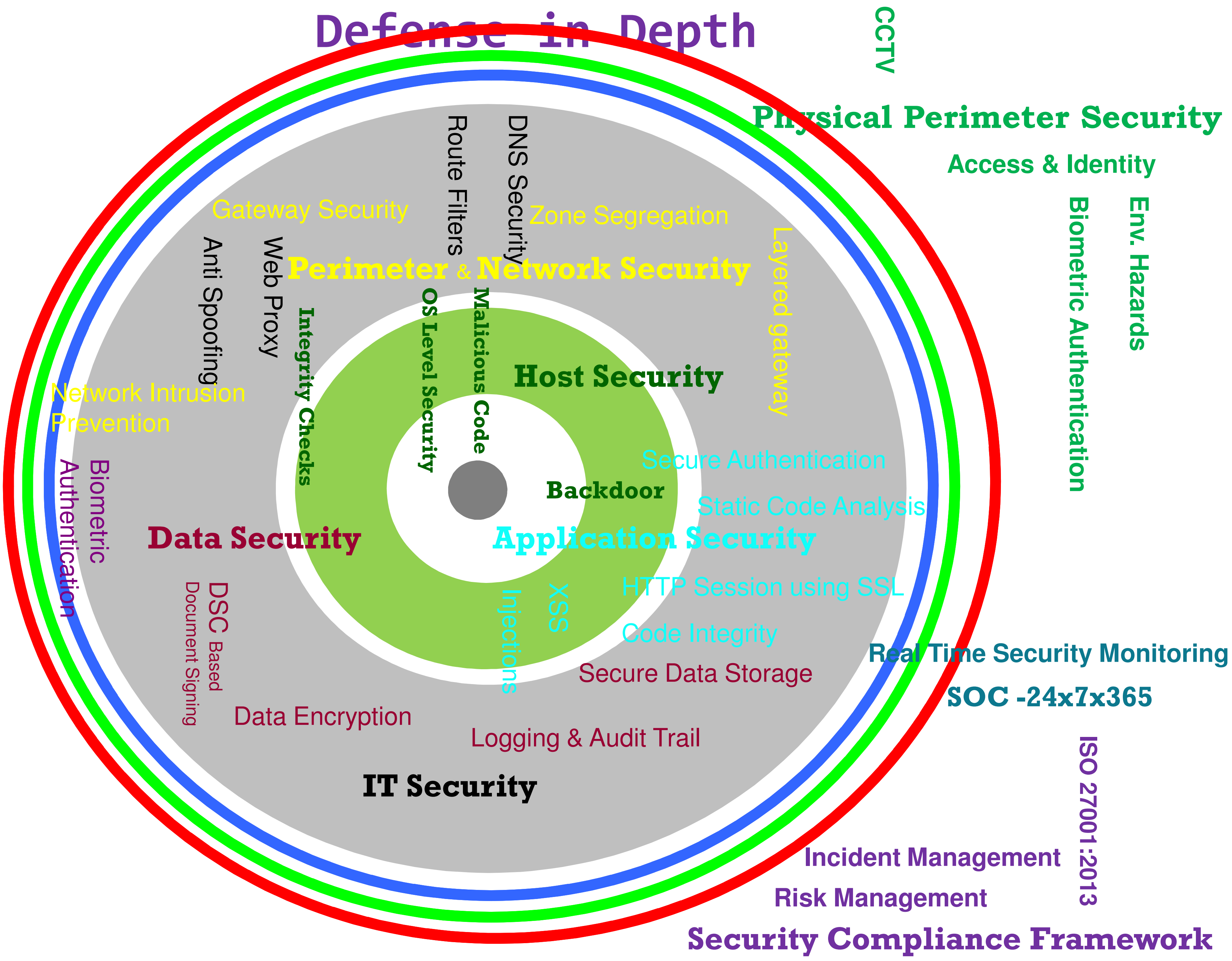
Process and Functional Visibility

- Know your employees
- Know your stakeholders and implementing agency
- Identify sovereign and non-soveriegn tasks
- Define access and authorization based on above
- Know your access and authorization routes
- Identify and classify your data sets, data points

Let the Data Speak

- Establish a Data Governance Model and Visibility
- It must reflects Principal Owner and Custodian of the Data
- We must know how Data is being collected, collected data is stored at rest, governed and shared
- Does the data being collected, governed and shared guided by legal and regulatory compliances
- Enterprise must be able to identify between Sovereign and Non-sovereign functions
- Authorization, Access and Accounting must be based on data categorization and classification

Defense in Depth



Production Deployment

360 enterprise wide Information Security Design, Deployment and Monitoring
across Project entities

Managing Secrecy of Sovereign data & processes

Layered Security & White List based approach

Robust Security Architecture … effective Threat Modeling

Focus on **Blended Attacks, New Generation, Cyber Security threats**

Looking beyond traditional security

Dynamic Threat Prevention System

Production Deployment

Security of additional real world layers Logic Bypass, Functionality Exploits

Electronic Surveillance security systems

Advanced Application Security design, implementation, real-time monitoring

Focus on Cyber Espionage global events on security threats

Cryptography applied for Data Security : Digital Signature Certificate

Enterprise wide ISMS Framework based on ISO27001 :2013

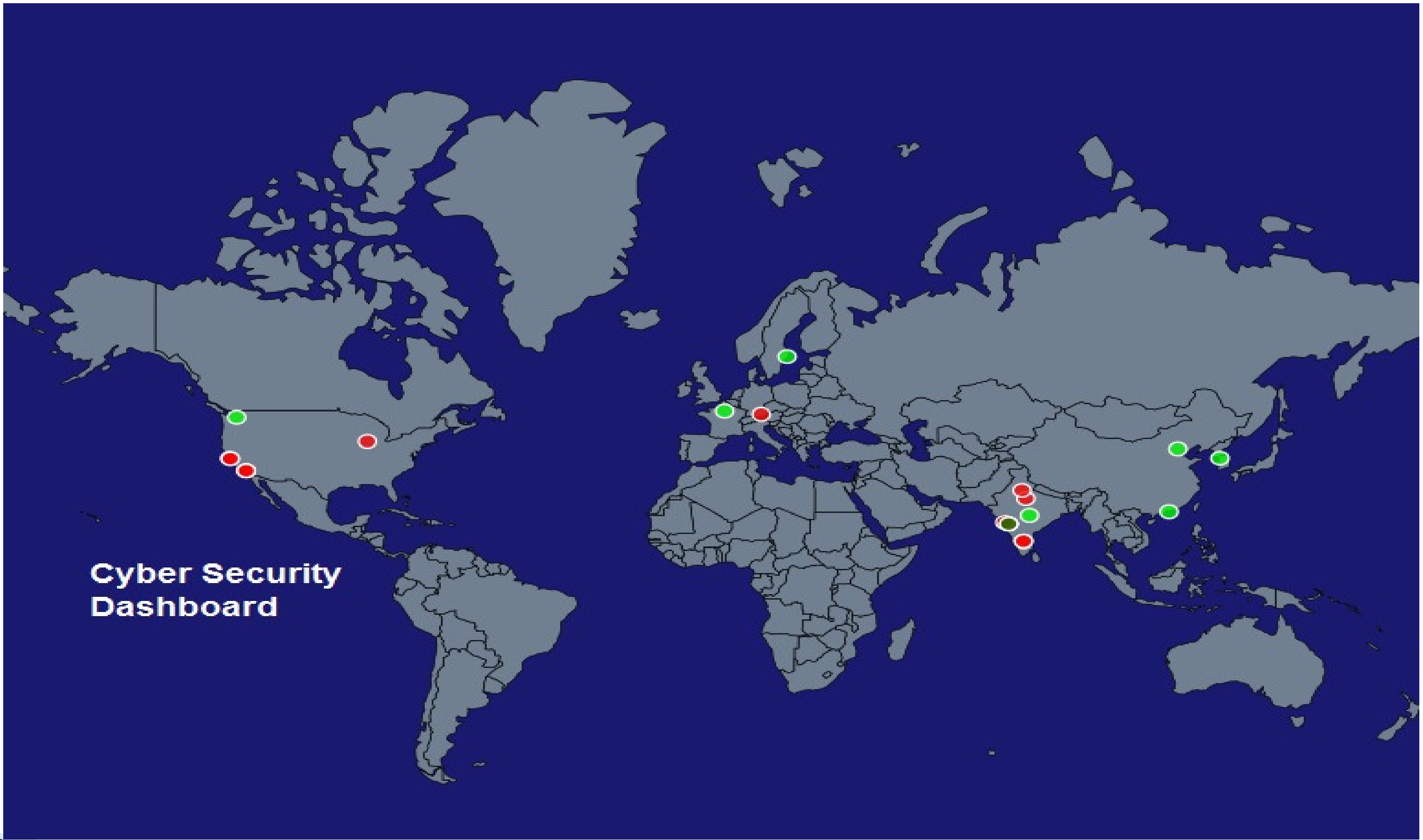
24x7x365 **SOC Real-time** Security Operations

100000+ **Non Stop Shifts** Since March 2010

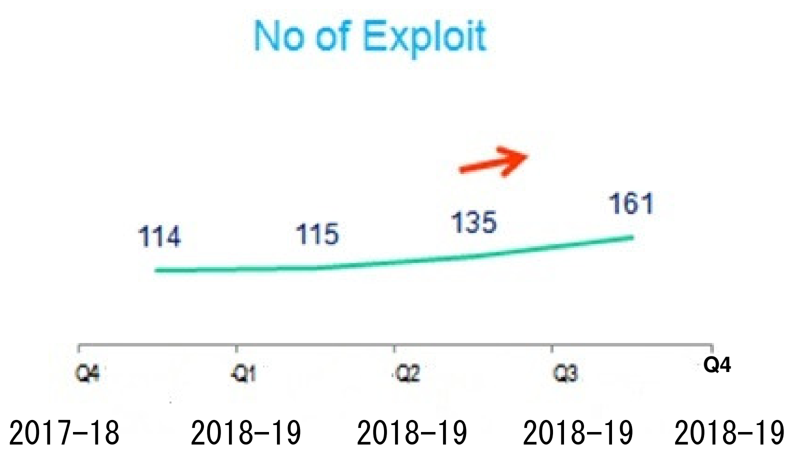
Raw Events **200+** Billion

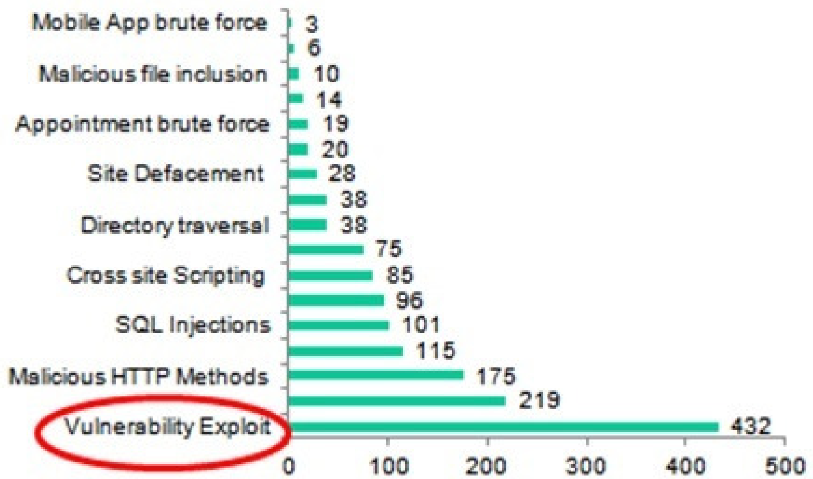
Processed Events **5.2** Million

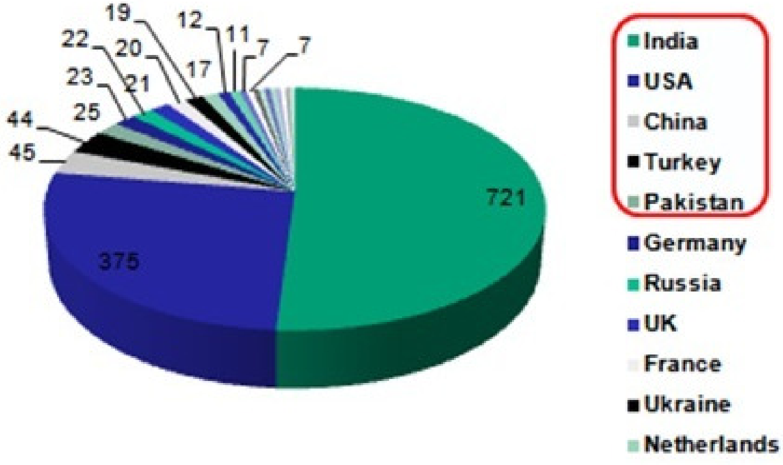
LIVE Cyber Security Operations - **SoC**



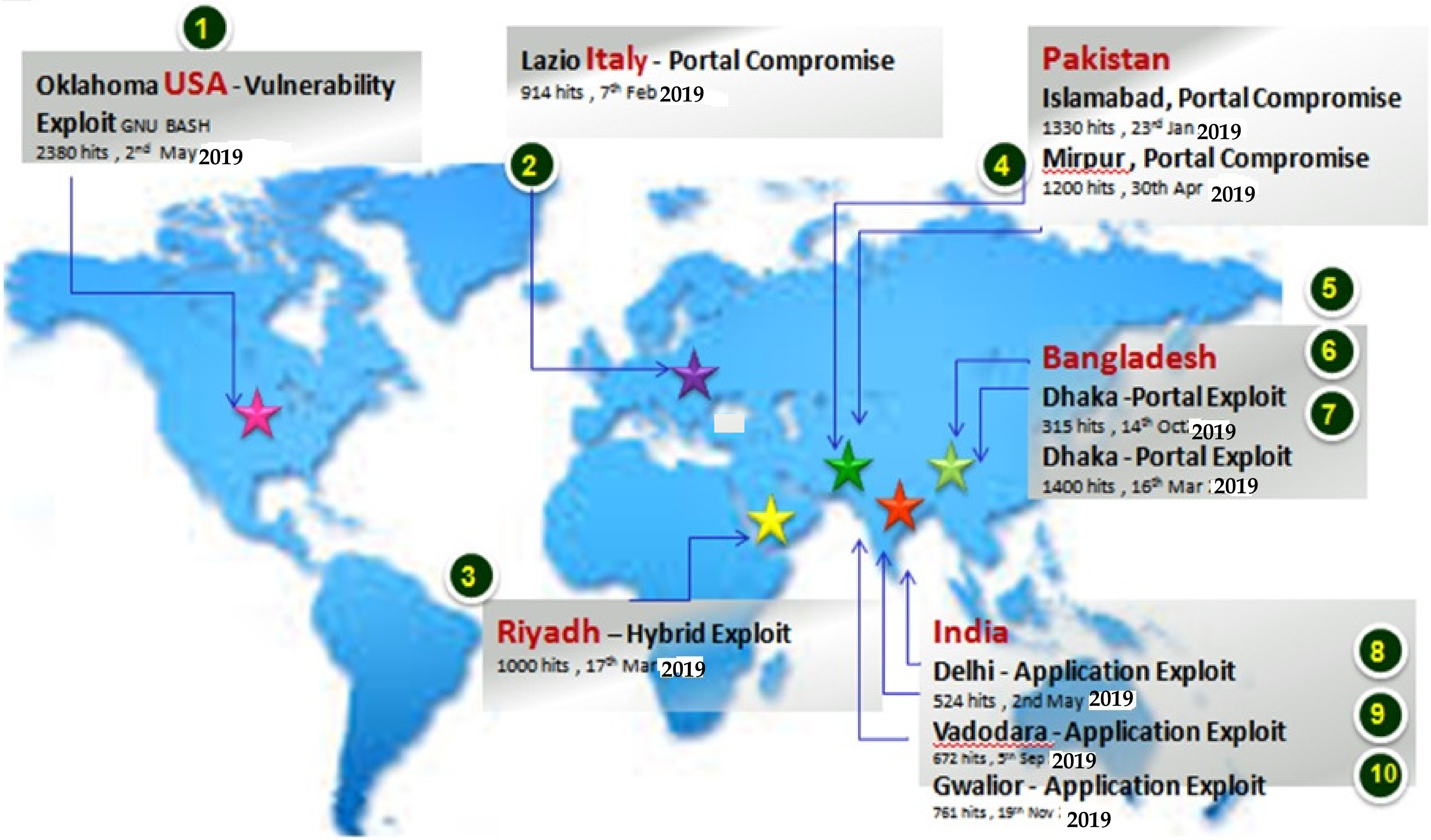
SoC Exploits







Cyber Exploit Map: Top 10 Attacks in 2019



1 Oklahoma USA - Vulnerability Exploit GNU BASH

2380 hits , 2nd May 2019

2 Lazio Italy - Portal Compromise

914 hits , 7th Feb 2019

3 Riyadh – Hybrid Exploit

1000 hits , 17th Mar 2019

4 Pakistan

Islamabad, Portal Compromise

1330 hits , 23rd Jan 2019

5 Mirpur , Portal Compromise

1200 hits , 30th Apr 2019

6 Bangladesh

Dhaka -Portal Exploit

315 hits , 14th Oct 2019

7 Dhaka - Portal Exploit

1400 hits , 16th Mar 2019

8 India

Delhi - Application Exploit

524 hits , 2nd May 2019

9 Vadodara - Application Exploit

672 hits , 5th Sep 2019

10 Gwalior - Application Exploit

761 hits , 19th Nov 2019

- Government of India has not yet enacted any specific legislation on data protection and privacy. Information Technology Act (2000) and its amendment in 2008, Section 43A and Section 72A give power to the principal owner of the data, a right to compensation for improper disclosure of sensitive personal data or information and thereby causing wrongful loss or wrongful gain to the person by a body Corporate

- The upcoming Data protection regime will widen the scope by offering a comprehensive data protection framework which shall apply to processing of personal data by any means, and to processing activities carried out by both the Government as well as the private entities- not only Body Corporate

Security design and implementation must start with a preliminary risk assessment e.g. business risk, technology risk, employee risk, regulatory and compliance risk, organizational risk etc. A data/information breach is about both privacy and security, therefore, a dynamic security framework and its adherence becomes very, very important because you can't have privacy unless you have a well defined security structure. Process and data points visibility are the two essential ingredients for defining security road map of any organizations.

Thank You