

Cyber Security Landscape: An Academic Perspective



APNIC 46 – New Caledonia

10/09/2018

Outline

- ❑ WHO AM I?
- ❑ THREAT LANDSCAPE:
 - ❑ GLOBAL
- ❑ CYBER SECURITY – BACKGROUND
- ❑ TRENDS – WHAT IS OUT THERE:
 - ❑ ACADEMIC – WAIKATO UNIVERSITY
 - ❑ SECURITY VISUALIZATION USE-CASE
 - ❑ LAW ENFORCEMENT USE-CASE
- ❑ WHAT VANUATU IS DOING
 - ❑ NATIONAL SECURITY FRAMEWORK
 - ❑ CERT VANUATU
 - ❑ CYBER LEGISLATION, REGULATIONS AND POLICIES
- ❑ SUMMARY

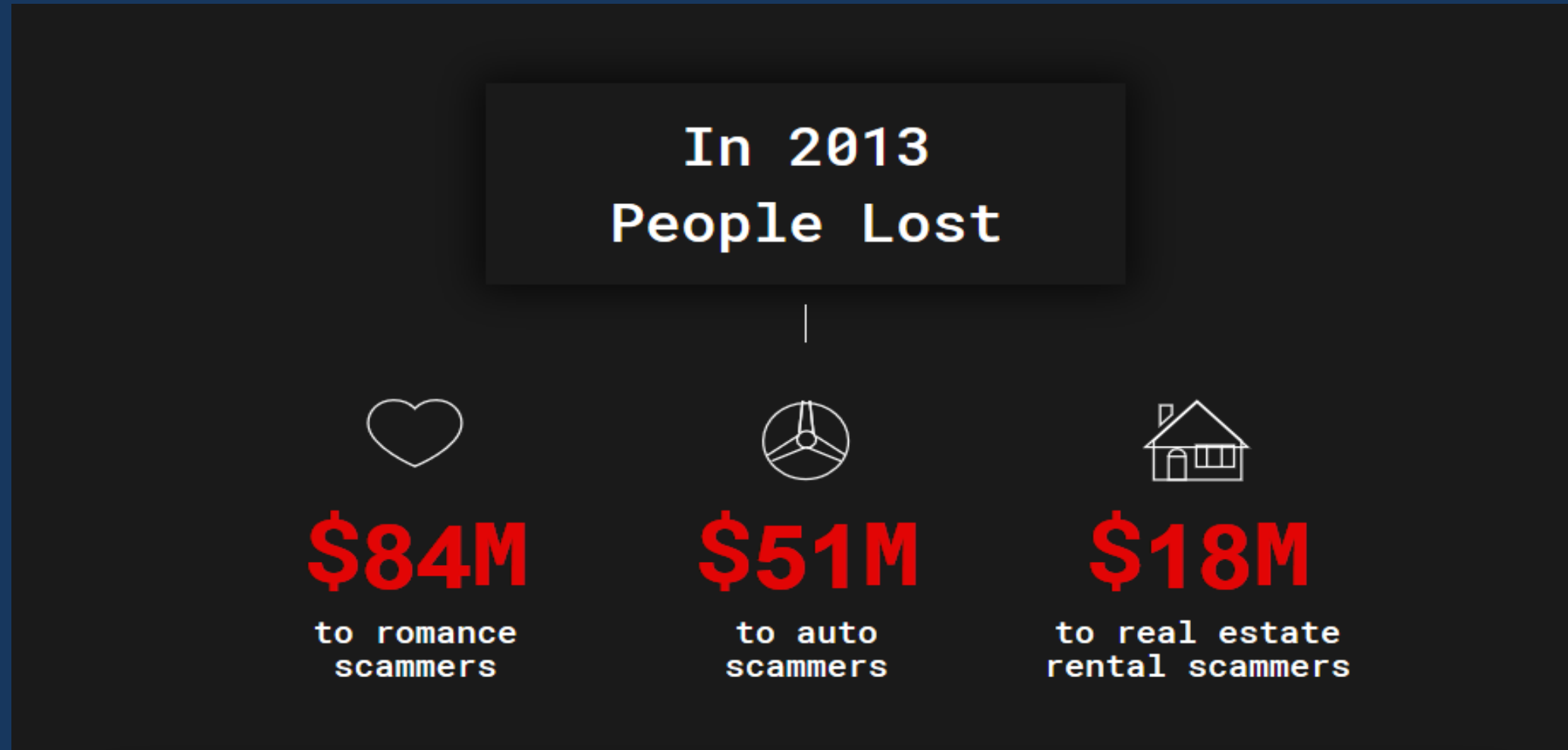
Cyber-threats Landscape



Src: <https://infographicjournal.com/the-trillion-dollar-industry-of-cyber-attacks/>



Cyber-threats Landscape



Src: <https://infographicjournal.com/the-trillion-dollar-industry-of-cyber-attacks/>



Cyber-threats Landscape

Three ways a smartphone is most likely to be hacked:



Unsecure Wi-Fi



Operating
system flaws



Malicious apps

Src: <https://infographicjournal.com/the-trillion-dollar-industry-of-cyber-attacks/>

Cyber-threats Landscape

No business is safe from the threat of a cyber attack



43%

of phishing attacks targeted small businesses in 2015

60%

of small businesses cease operating within the 6 months after they face a cyber attack

68%

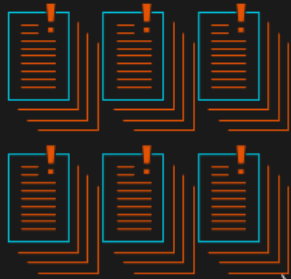
of all funds lost as a result of cyberattacks are likely unrecoverable

Src: <https://infographicjournal.com/the-trillion-dollar-industry-of-cyber-attacks/>



Cyber-threats Landscape

Data that speaks for itself



159M+

records containing sensitive information were compromised in 2015



317M+

pieces of malware released in 2014



100K+

smart devices were hacked at the end of 2013 and the beginning of 2014 and these devices were used to send spam emails



200 BILLION

IoT devices could need to be secured by 2020

Src: <https://infographicjournal.com/the-trillion-dollar-industry-of-cyber-attacks/>



What do We Know?

❑ CYBER SECURITY – BACKGROUND:

❑ Cyber Security:

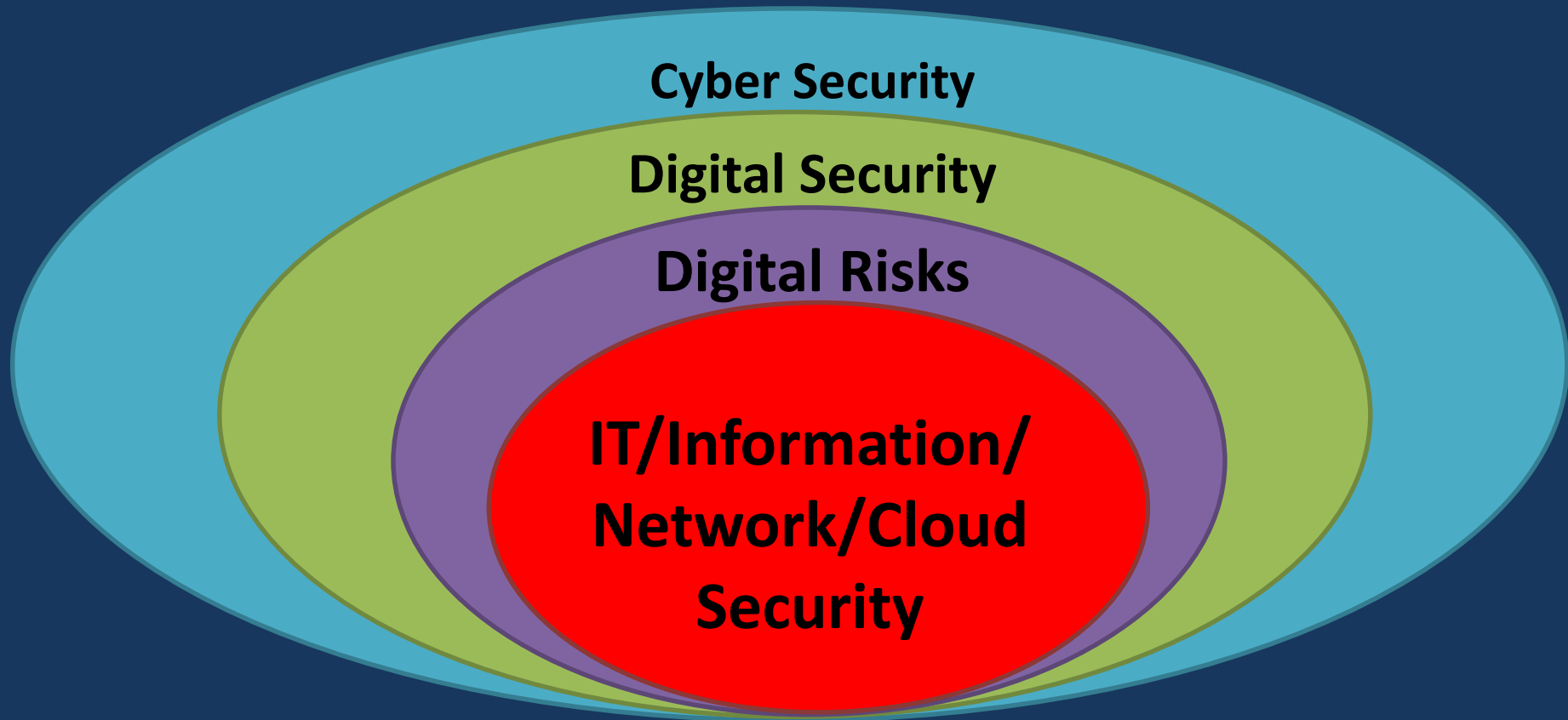
- ❑ Everyone's Problem across society
- ❑ Everyone's Obligation & Responsibility,
- ❑ Every Country Governments, organizations are talking Security.

❑ Cyber Security should be the core of every digital infrastructure, systems and IP communications network.

But ...

What is Cyber Security?

The Buzz Word:



**While various domains define
Cyber Security according to their
perspective, ...**

What is common among all?

Data - *Data is the new Gold*

Threats & Risks - around every
infrastructure, business models, frameworks, domains,
nation, and globally

Cyber Security & Government

WE USUALLY THINK THE GOVERNMENT CAN HELP PROTECT US AND KEEP US SAFE FROM CRIMINALS BUT THERE ARE SOME CHALLENGES:

- 1. THE GLOBAL REACH OF CYBERCRIMINALS**
- 2. THE SPEED AT WHICH THE CRIME CAN BE COMMITTED**
- 3. THE TREMENDOUS SCOPE OF CYBERCRIME IN A VERY SHORT PERIOD OF TIME.**

Trends – What is Out There:

Trend & Prediction



Src: <https://infographicjournal.com/the-trillion-dollar-industry-of-cyber-attacks/>

Academics – University of Waikato:

❑ Cyber Security Researchers of Waikato (CROW Lab) (2013) <https://crow.org.nz/>

❑ Institute of Security & Crime Science (2017) <https://www.waikato.ac.nz/study/qualifications/master-of-security-and-crime-science>

<https://www.waikato.ac.nz/security-crime-science/>

Academics – University of Waikato:

□ New Zealand's 1st Internet Connection (1989)



This ground-breaking work continues the University's proud legacy of online innovation.

In 1989, the University's John Houliker brought the internet to New Zealand via a historic collaboration with NASA.

Today, Dr Ko's team honours this legacy by working to ensure online and internet-linked environments around the world are safe for everyone.

Academics – CROW Lab:

- ❑ Home of:

- ❑ Master of Cyber Security (MCS)

- ❑ The MCS Program has both theoretical and Industry aspects.

- ❑ It also includes a Law paper – “Legal Aspects of Cyber Security”

Carriers:

- ❑ CHIEF INFORMATION SECURITY OFFICER
- ❑ ENTREPRENEURS OF NEW SECURITY
- ❑ PRODUCTS AND SERVICE
- ❑ PENETRATION TESTERS/ SECURITY
- ❑ ASSESSMENT CONSULTANTS
- ❑ IT SECURITY CONSULTANT

Academics – CROW Lab:

❑ Home of:

❑ New Zealand Cyber Security Challenge (NZCSC)



Academics – CROW Lab:

- ❑ Home of:

- ❑ Hosted High Research Visitations from famous people, institutions, agencies, etc.

- ❑ Hosted the ISO/IEC JTC 1/SC 27 Plenary and Working Group Meetings



OBJECTIVE:

“To Return Control to Users”

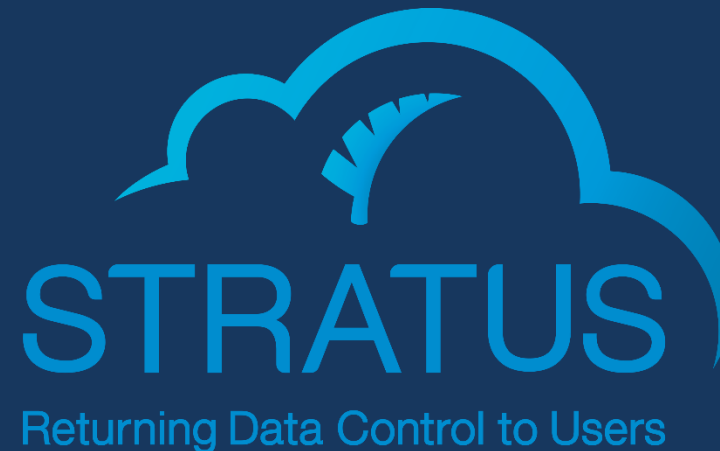
Academics – CROW Lab:

❑ Home of:

❑ **NZD 12.2m MBIE Cyber Security Project Fund: STRATUS**
(*Security Technologies Returning Accountability, Trust and User-centric Services in the Cloud*)

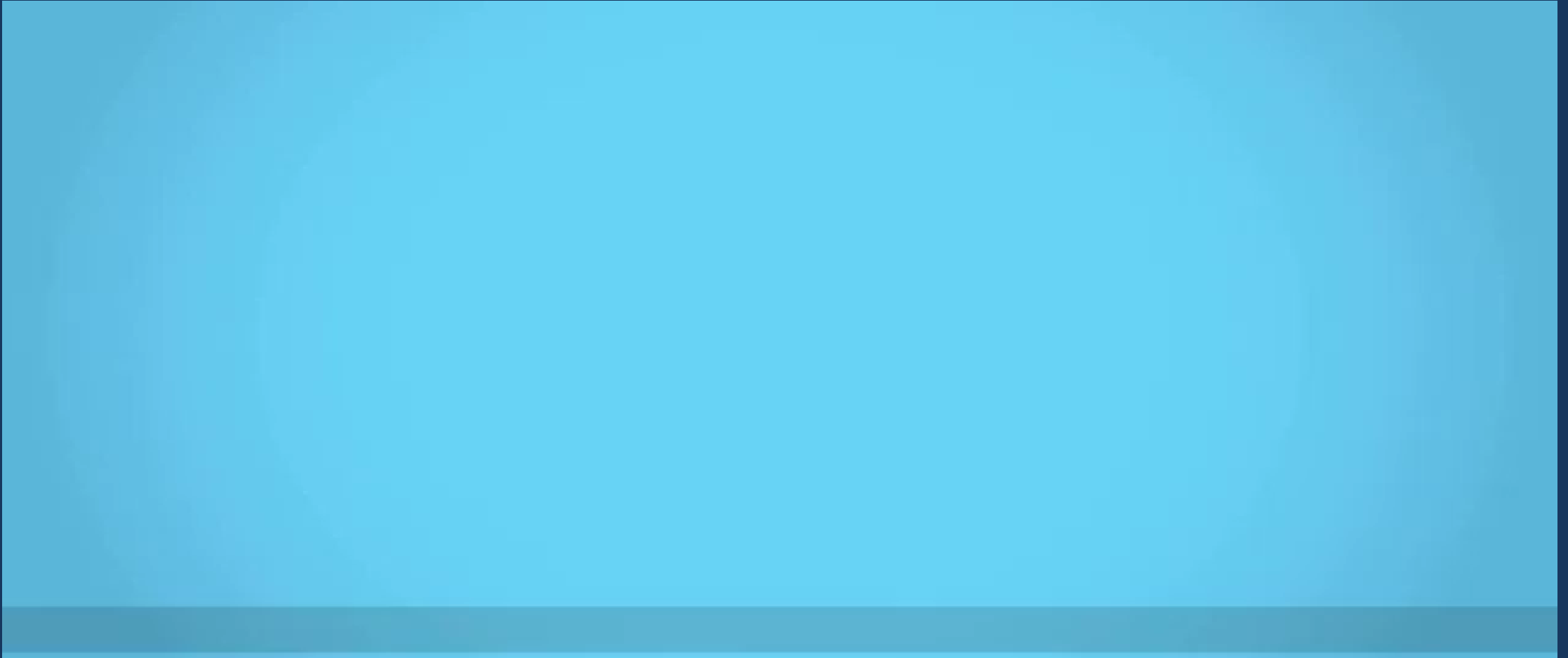
❑ <https://stratus.org.nz/>

❑ https://www.youtube.com/watch?time_continue=123&v=c6fWeHVSPlw



Academics – CROW Lab:

❑ STRATUS:



Src: <https://stratus.org.nz/>

Academics – CROW Lab:

- ❑ Home of:

- ❑ Data Privacy Foundation (DPF)

- ❑ A Rosetta Stone for Data Privacy Laws

- ❑ <https://dataprivacyfoundation.org/>

- ❑ Data Privacy Matrix:

- ❑ <https://dataprivacyfoundation.org/comparison-tool/>

- ❑ <https://dataprivacyfoundation.org/time-series-viz/>
(Visualization Map)

Academics – Institute of Security & Crime Science:

- ❑ Home of:

- ❑ Master of Security & Crime Science (MSCS)

- ❑ The Institute is the primary research partner for the New Zealand Police, and a partner at the Evidence Based Policing Centre in Wellington.

- ❑ research topics will be delivered by world-leading researchers in psychology, statistics, artificial intelligence including machine learning, cyber security, political science, economics, management, law, education, Māori and indigenous development, and demographic research.

- ❑ <https://www.waikato.ac.nz/security-crime-science/>

CROW – Research Directions & Scope:

☐ Provenance

☐ Security Visualization

☐ Hardware Security

☐ Security Economics

☐ User-centricity

☐ Tools & Datasets

Specific Research Approach:

- Thesis:

- “Cyber Security Visualization Effectiveness Measurement”

Definition

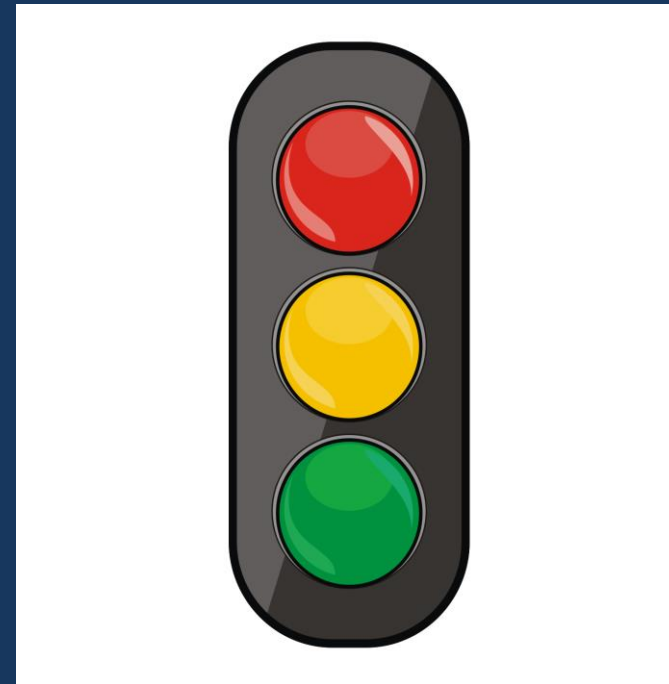
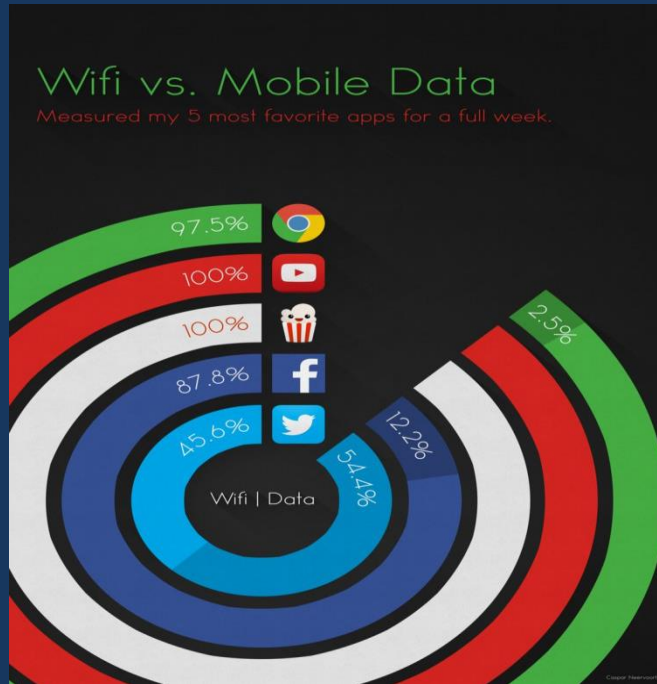
- What is effectiveness?
 - This means executing a process in a faster or efficient way compared to its usual or current way. Improvement has been done to obtain better results.
- What is Security Visualization effectiveness?
 - In Security Visualization, Effectiveness is defined as improving visual clarity, rendering and visual processing within the minimal time required to gain insights.



Why Security Visualization?

Motivation

- Research:
 - Security Visualization for Mobile Platforms
 - Effectiveness Measurement in Security Visualization for Mobile Platform

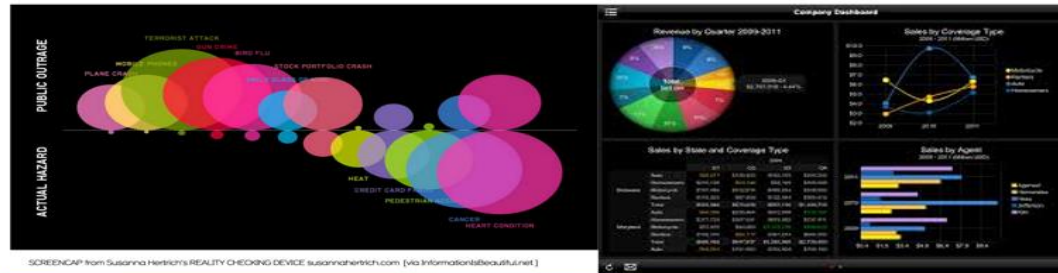


How Users See Visualization

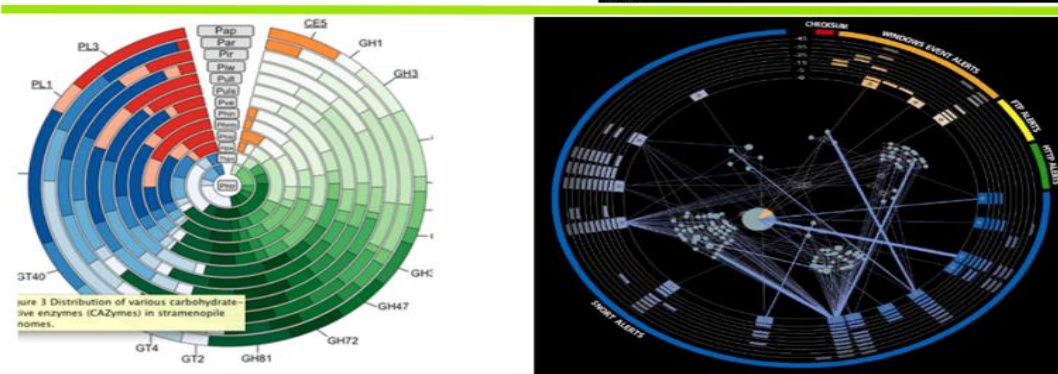
- It is becoming a common medium for reporting findings across academics and industries



What Visualization can Do!



Non-technical
End users,
Top level CEOs
etc,



Tech-savy users,
Advance users,
Some CEOs,
etc,



Developers,
Analysts,
Researchers

Motivation

- Why Visualization or Security Visualization?
 - Users say its simple compared to reading reports and logs
 - Interactive
 - Pretty, captures the eye
 - Most importantly, for **EXPLORING**, **DISCOVERING**, and **REPORTING**
 - And more,



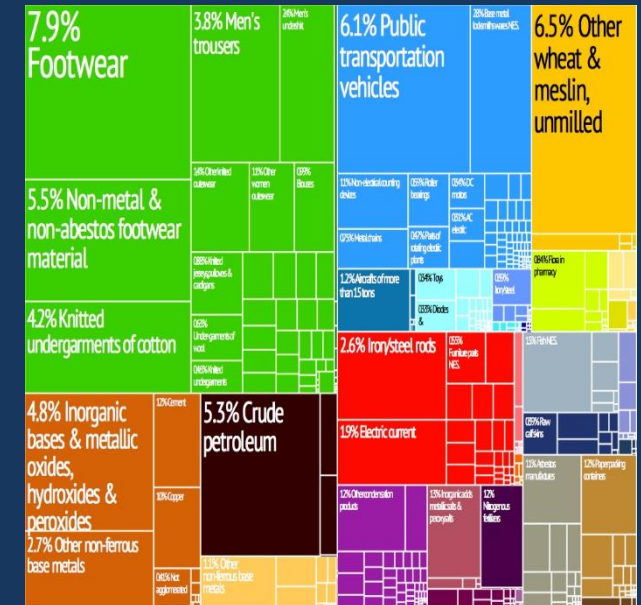
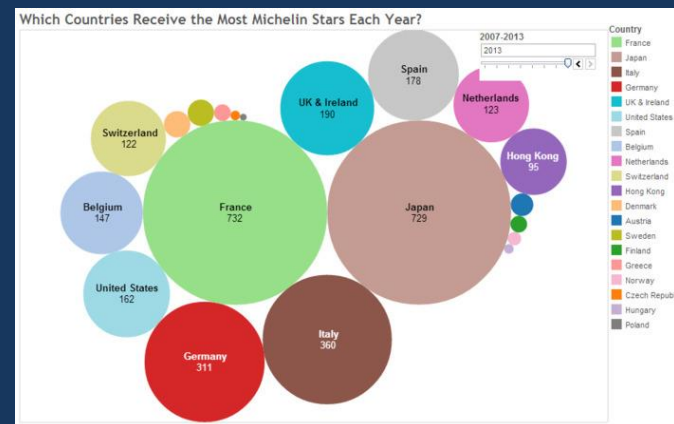
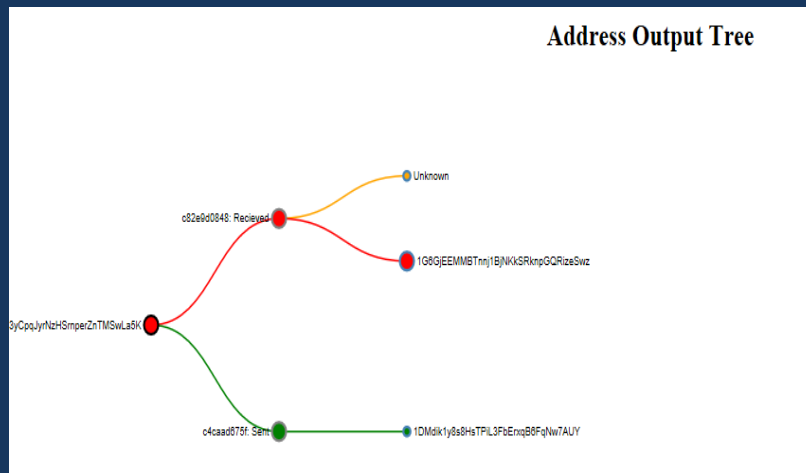
Types of Visualization

- Common Classification of Security Visualization
 - Graph base visualization: dashboards, charts, line graphs, etc.
 - Many eyes type: bubble Vis, Treemaps, etc.
 - Multivariate, multidimensional Visualization: Parallel coordinates, etc.
 - 3D, Virtual Reality, Augmented Reality Visualization



- Others may Classify Security Visualization as/in:

- Qualitative and Quantitative
- Distribution
- Composition
- Comparison
- Relationships



Industry Trends with Visualization

- Security Visualization Trends for Decision making
 - Presentation reasons – bar charts, line graphs, etc.
 - Many eyes visualization – with Dashboards
 - Data Analytics – with Dashboards
 - Tracking and Monitoring Visualization
 - Real-time Visualization



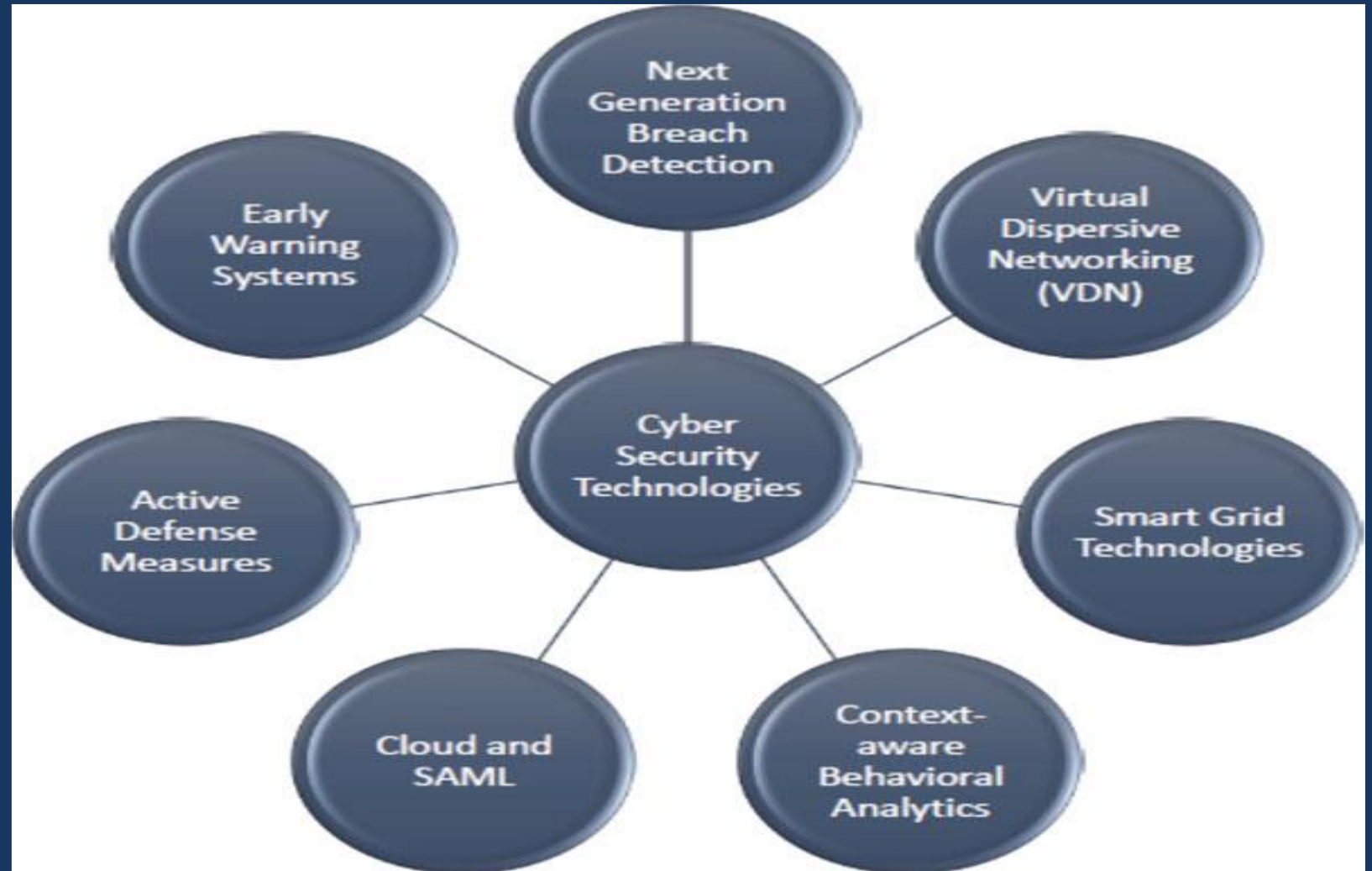
- Security Visualization Trends for Decision making:
 - The use of many eyes type visualization
 - The use of Dashboards (Interactive)
 - The use of Virtual Reality and Augmented Reality
 - Tracking and Monitoring Visualization



Cyber Security Technologies Trends:

- More into security context:

Cyber security technologies trend overview in 2016



- **Security Visualization Trends for Decision making**

However, we start to see a shift!

- Data Analytics still remains the key for visualization
- Visualization for Intelligence, tracking and monitoring
- VR and AR are also coming in strong again
- Machine Learning & Deep Learning are becoming the join force for improving Visualization



- **Security Visualization Trends for Decision making:**

The Demand: Effective security visualization approach depends on the following:

1. Who are the users?
2. What do the users want to see?
3. What security tasks can be performed using these visualizations?
4. When would these security visualization be used?



- **Security Visualization Trends for Decision making**

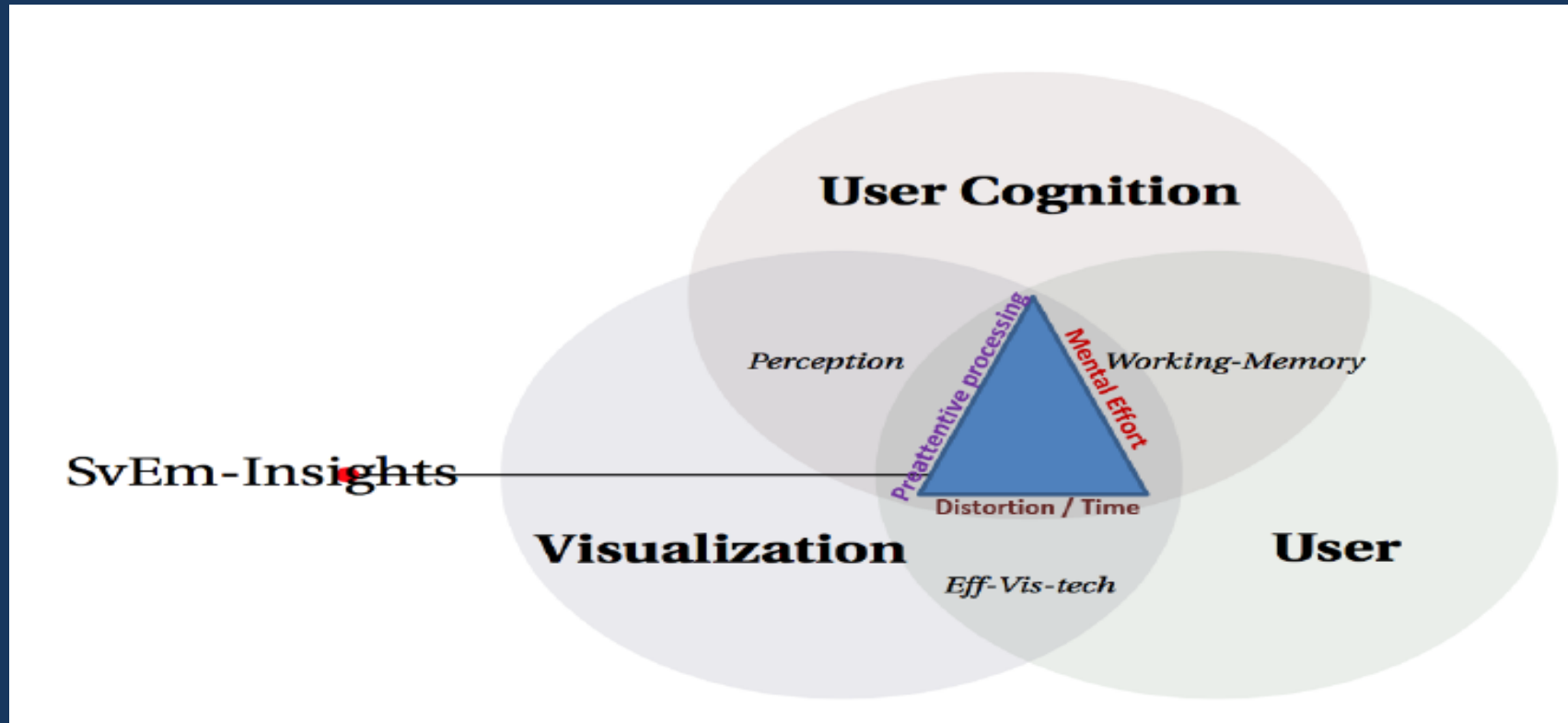
The Attack Landscape: Effective security visualization approach depends on the following,

1. What type of attack is visualized?
2. When did the attack take place?
3. What is the origin (source) and destination of the attack being visualized?
4. What is the reason of visualizing this attack?









The Full-Scale EM Model

- **User** → **Framework (tool)** → **Visualization**
 - Aim is to address performance & time spent to gain insights (patterns, behaviours, statistics, trends, etc.)



Framework Features

- User Cognitive Activators:
 - Security Visualization Colour Standard

	Malicious Content: payload, event (file,process, etc.)
	Suspicious Content: payload, event (file,process, etc.)
	Normal Content: data traffic
	Intelligence Content: tracking files, tagged files, etc.
	Trafficking Content: drug trafficking, etc.
	Fraud Content: currencies, account details, etc.

Security visualization Colour Standard

- How can we achieve our Security Visualization framework
- Goal:
 - Create a “Set of Markers – flash screen”
 - Markers => Cognition activator
 - Security Visual Markers

Security Visualization Standard

Visual => Data Representation









- => Malicious Payload (file, video, etc.)
- => Suspicious Content (file, IP address, etc.)
- => Normal Content (file, net-traffic, etc.)
- => Intelligence (tagged file, bitcoin address, etc.)
- => Trafficking Content (images, videos, etc.)
- => Fraud Content (files, acc.no#, etc.)

Security Visualization Colour Standard

- How can we achieve our Security Visualization framework
- Goal:
 - Create a “Set of Markers – flash screen”
 - Markers => Cognition activator
 - Security Visual Markers

Security Visualization Standard

Visual => *Data Representation*

	=> Malicious Payload (file, video, etc.)
	=> Suspicious Content (file, IP address, etc.)
	=> Normal Content (file, net-traffic, etc.)
	=> Intelligence (e.g. file, IP address, etc.)
	=> Trafficking Content (images, videos, etc.)
	=> Fraud Content (files, acc.no#, etc.)

**Main
Color
Identifiers**

Security Visualization Colour Standard

- How can we achieve our Security Visualization framework
- Goal:
 - Create a “Set of Markers – flash screen”
 - Markers => Cognition activator
 - Security Visual Markers

Security Visualization Standard

Visual => *Data Representation*



=> Malicious Payload (file, video, etc.)

=> Suspicious Content (file, IP address, etc.)

=> Normal Content (file, net-traffic, etc.)

=> Intelligence (tagged file, bitcoin address, etc.)

=> Trafficking Content (images, videos, etc.)

Added Color Identifiers

=> Fraud Content (files, acc.no#, etc.)

- **Security Visualization Sample:**

- **Visual Progger:**

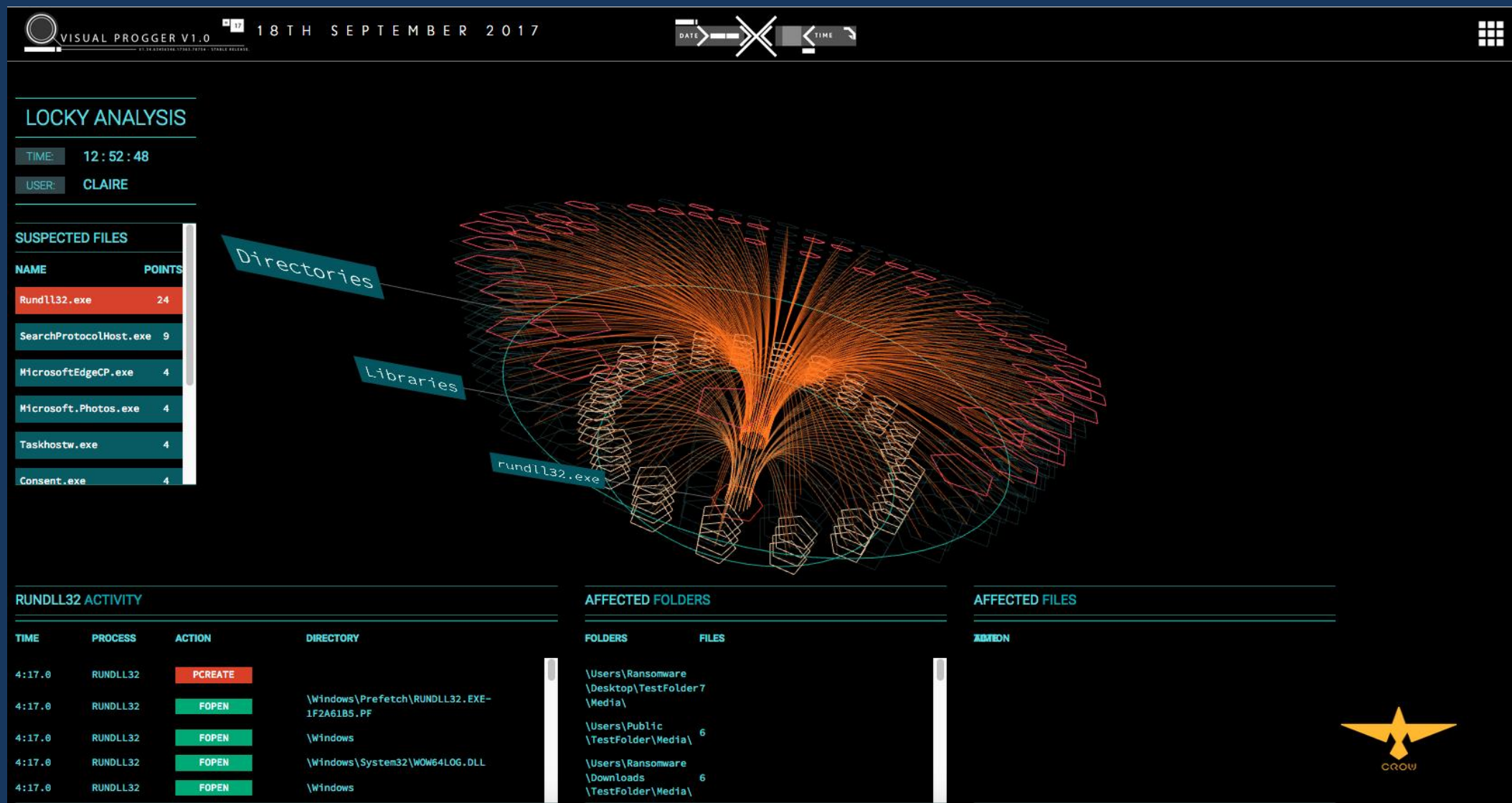
- **Locky Ransomware**
 - **Real-time Monitoring**



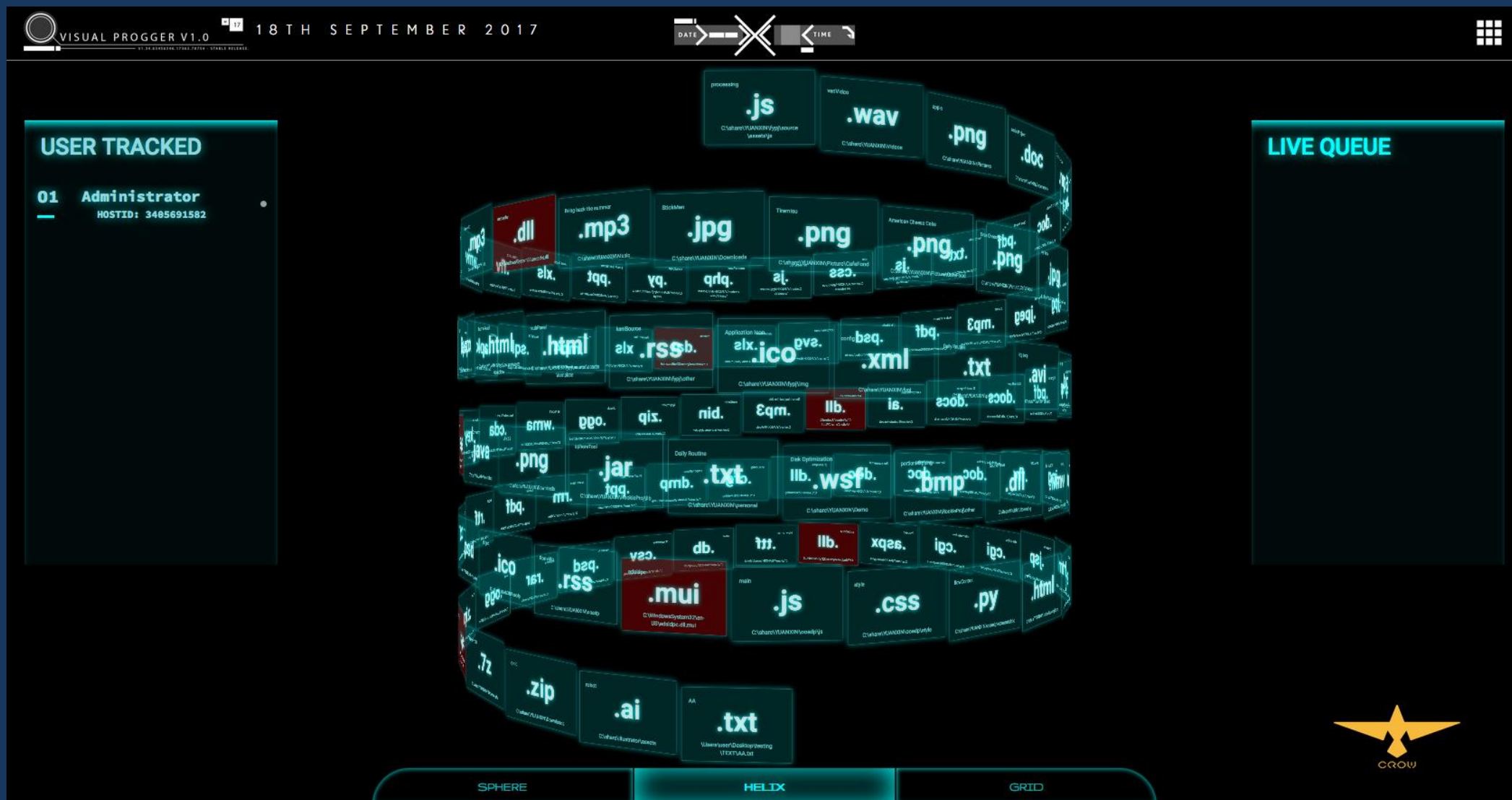
- **Security Visualization Sample 1: Visual Progger – Locky Ransomware**



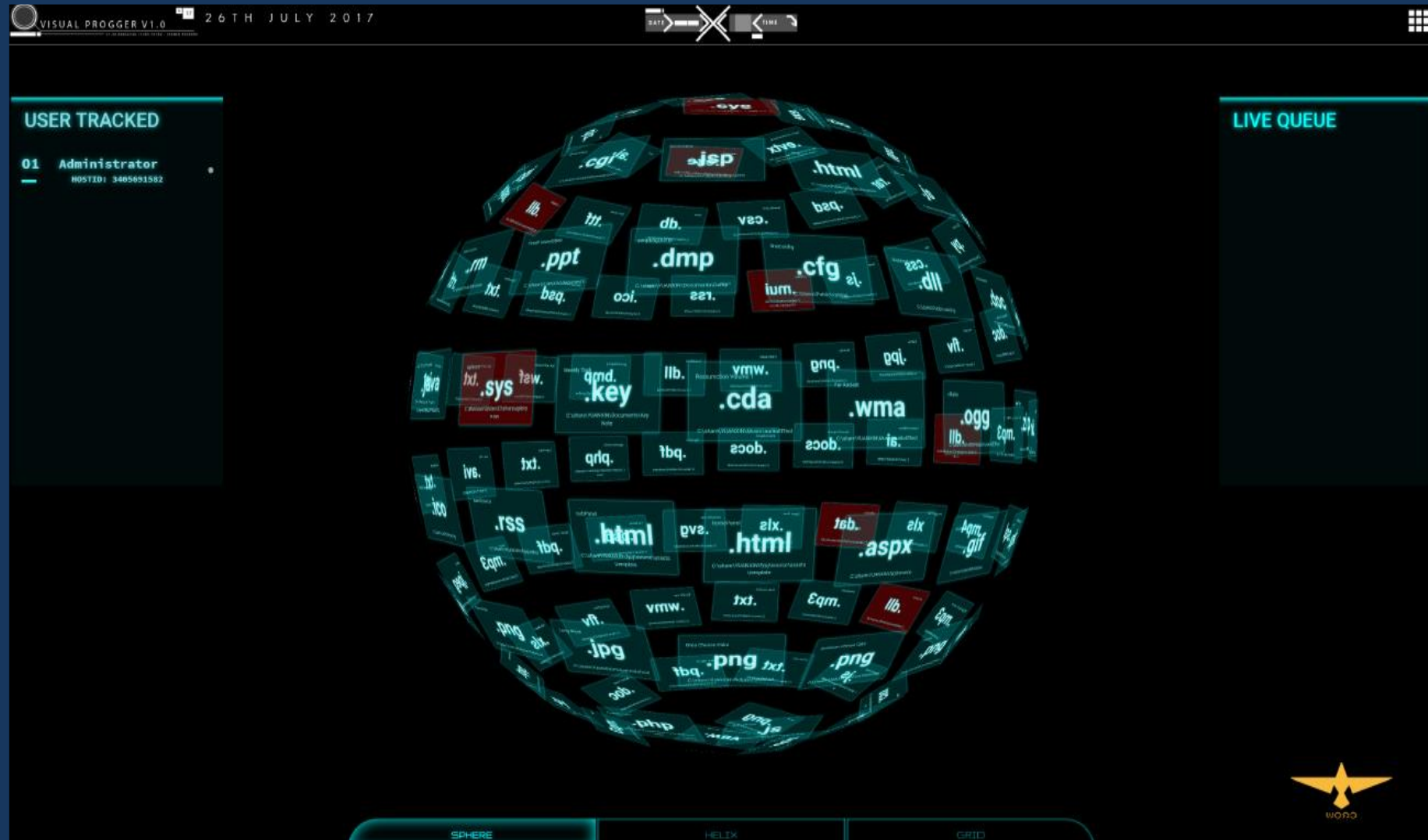
- Security Visualization: Locky Analysis:



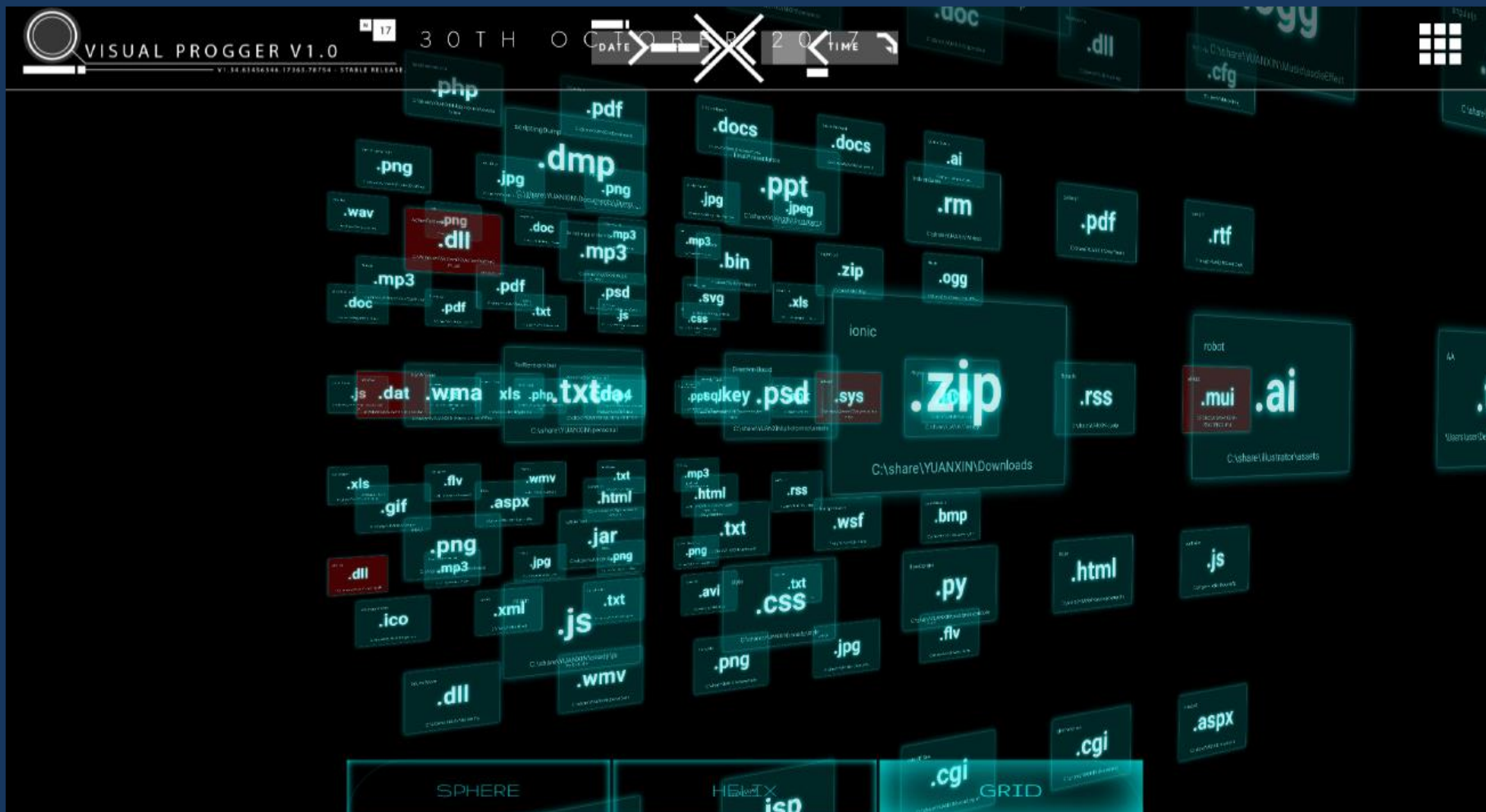
- **Security Visualization: Real-time Monitoring:**



- Security Visualization: Real-time Monitoring:



- **Security Visualization: Real-time Monitoring:**



- **More reading if interested**



2 Book Chapter Contents

- Springer Book Chapter 1 (02/07/2017):
“Visualization and Data Provenance Trends in Decision Support for Cybersecurity”
- Chapter Authors: Jeff Garae & Ryan K.L.Ko
- Editors: Palomares Carrascosa, Ivan, Kalutarage, Harsha Kumara, Huang, Yan (Eds.)
- Part of Data Analytics book series (DAANA)
- https://doi.org/10.1007/978-3-319-59439-2_9



2 Book Chapter Contents

- IET Book Chapter 2 (Sept. 2017):

“Security Visualization for Cloud Computing: An Overview”

- Chapter Authors: Jeff Garae, Ryan K.L.Ko & mark Apperley
- Editors: Vimal Kumar, Ryan Ko & Sivadon Chaisiri (Eds.)
- Source: Data Security in Cloud Computing, 2017
- Part of IET Digital Library
- Book DOI: [10.1049/PBSE007E](https://doi.org/10.1049/PBSE007E)
- Chapter DOI: [10.1049/PBSE007E_ch13](https://doi.org/10.1049/PBSE007E_ch13)
- e-ISBN: 9781785612213



Vanuatu's Computer Emergency Response Team (CERT VANUATU | CERT VU)

CERT VANUATU (CERT VU)

❑ Launched Date:

❑ 19 of June 2018

❑ Workshop by APNIC



AWARENESS AUDIENCE

Awareness Audience:

1. Government Users
2. Organization users
3. IT Technicians, Technical staff, Law Enforcement
4. Teachers
5. Students
6. End-users / Users
7. Kids
8. Banks, ISPs, etc.
9. And more ...

AWARENESS LOCATION

Awareness Locations:

1. Port Vila
2. Luganville
3. Islands – Through Schools, Provincial Headquarter, Community Centers, UAP Centers (Note: See TRBR)
4. And more ...

CAPACITY BUILDING

Capacity Building Plan:

1. In-house Trainings (CERT VU Staff)
2. External Trainings (CERT VU staff, Gov IT Staff, Law Enforcement staff, others)
3. Specific Trainings (e.g. malware analysis, forensics training, security tool trainings, etc.)
4. And more ...

Cyber Security - Future Work

1. The NATIONAL SECURITY & ICT REGULATORY PANEL (NSICTRP)
2. Vanuatu Government Ethics Panel (Basically around data collection, handling, sharing & privacy, etc.)
3. Vanuatu National Cyber Security Centre (VNCSC)
4. Cyber Security Capacity Building & Awareness

Acknowledgement

Special thank you to:

- APNIC
- CERT Vanuatu / OGCIO
- CROW Researchers
- Waikato University
- Stratus Project
- Interpol
- NICT - Japan



Thank You!

Contact: gjeffery@vanuatu.gov.vu

