The beginner's guide to Threat Intelligence

Ialle Teixeira
Reverse Engineering/Malwares/C++

#whoami

Ialle Teixeira

Exploit Database Security Papers @author=9833
Linkedin @isDebuggerPresent
Twitter @DbgShell
Reverse Engineering
Threat Intelligence
Malwares

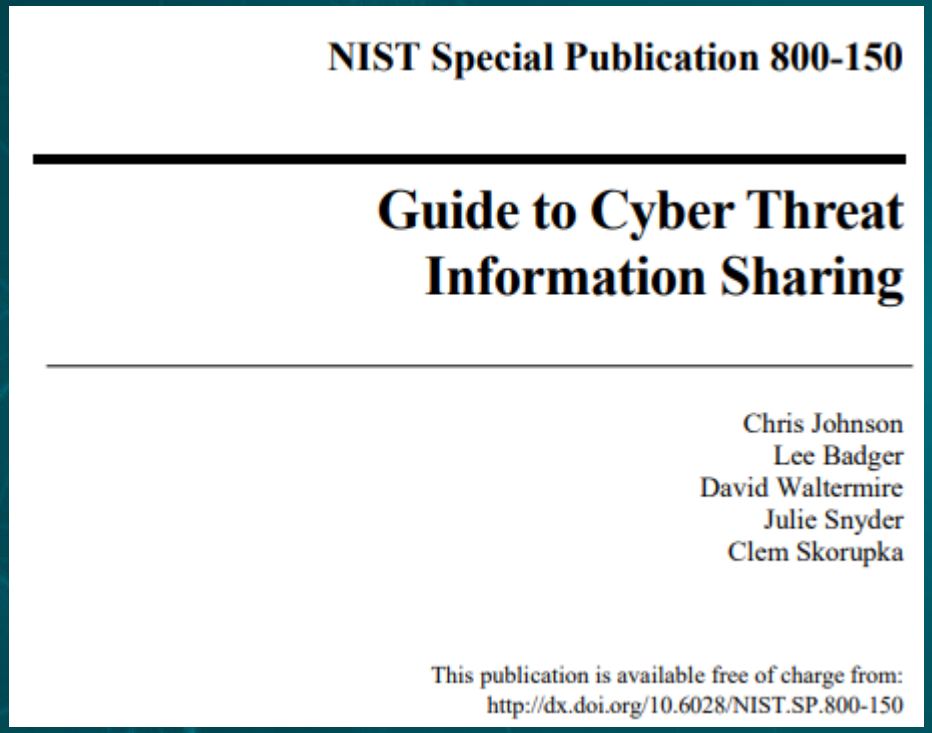
AGENDA

- **Introduction**
  - **Intelligence Foundations - Foundations and Lifecycle**
  - **Operational Threat Intelligence**
- **Strategic Threat Intelligence**
  - Threat Intelligence Platform
- **Threat Intelligence - NIST Guides**
- **Tactical Threat Intelligence Requirements**
  - Using Open Source Intelligence
  - Free Resources

The challenges of today's world

Intelligence Foundations - Foundations and Lifecycle

Tactical Threat Intelligence Requirements (NIST Guides)



NIST Special Publication 800-150

Guide to Cyber Threat Information Sharing

Chris Johnson
Lee Badger
David Waltermire
Julie Snyder
Clem Skorupka

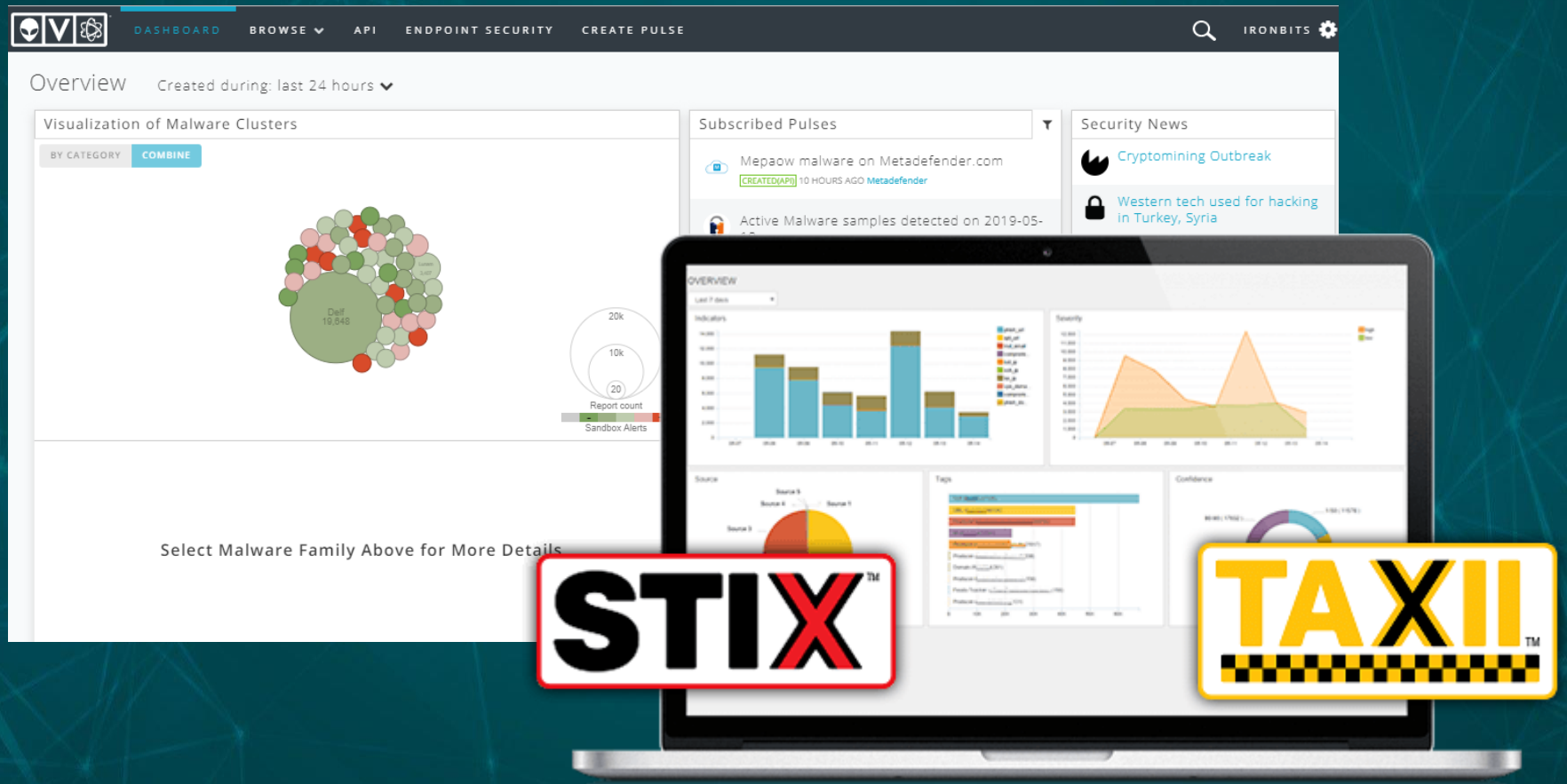
This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-150

Table 3-3: Traffic Light Protocol, Version 1.0

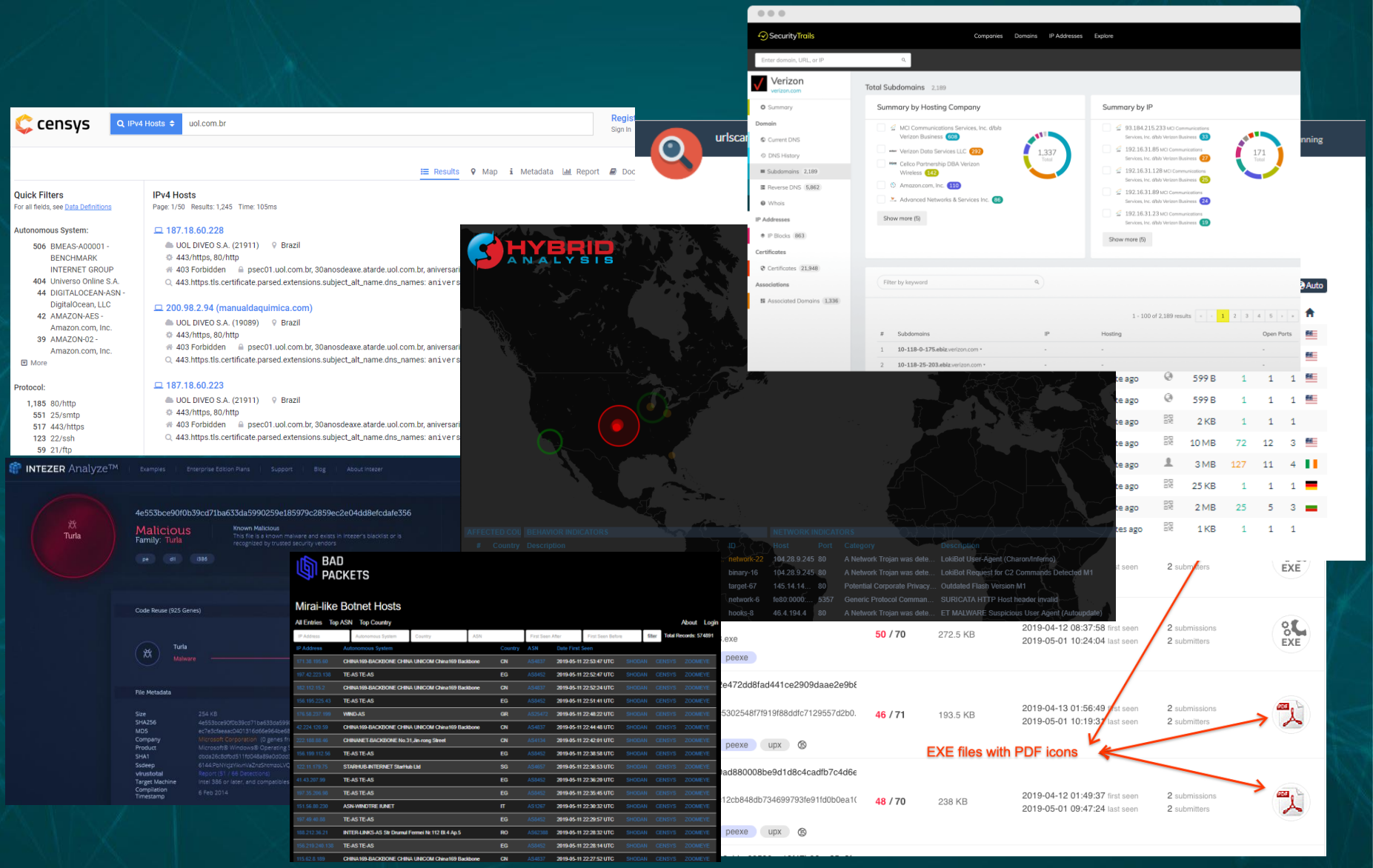
Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules.	TLP:WHITE information may be distributed without restriction.

NIST National Institute of Standards and Technology
U.S. Department of Commerce

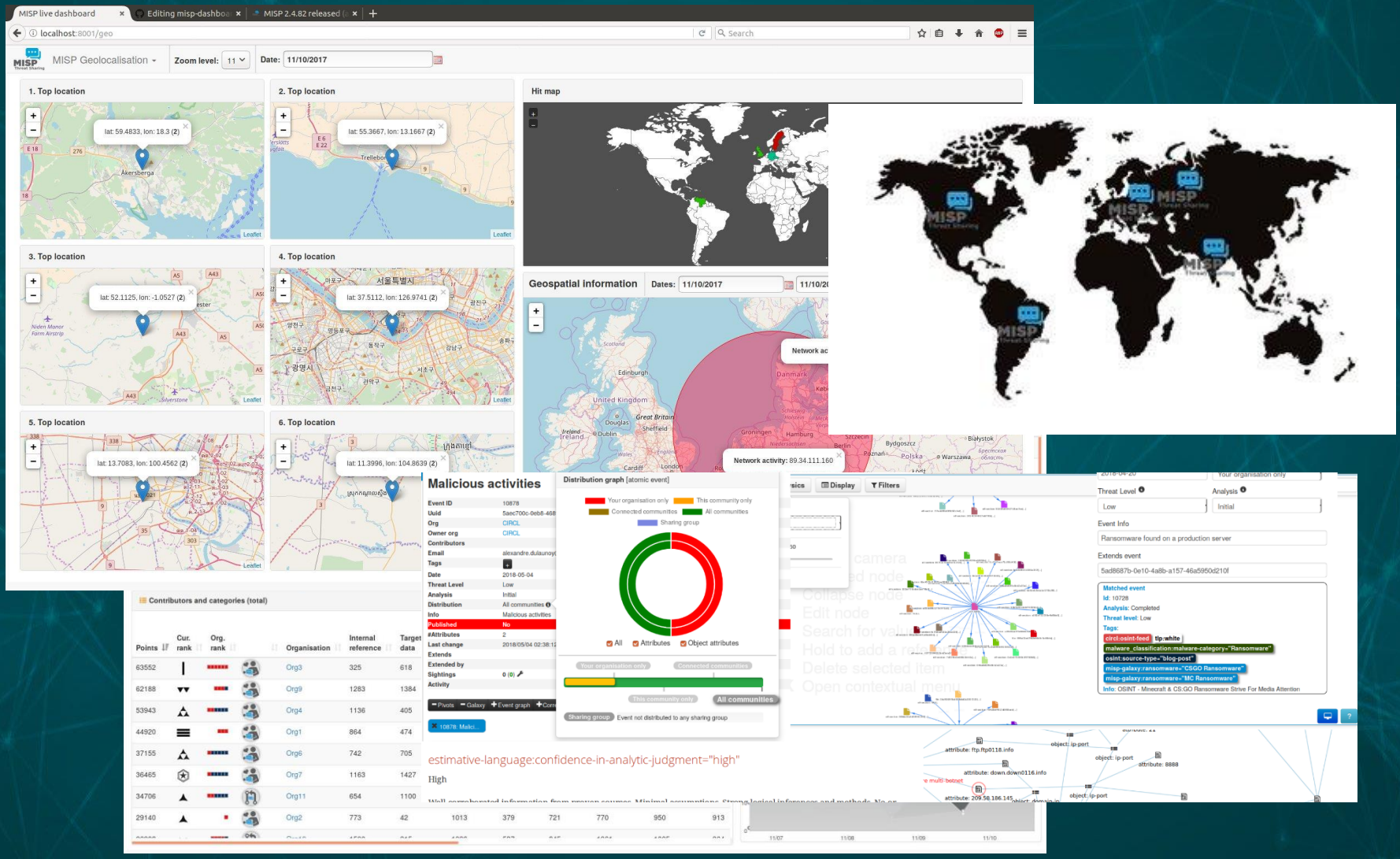
- Threat Intelligence Platform



- # Threat Intelligence Sharing/Resources



Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing



The challenges of today's world

Questions?!
Questions?!?
Questions?!?!