anubisnetworks™
a BITSIGHT® company

A Eficiência na Resposta a Ameaças

Tecnologias focadas para respostas direcionadas (e confiantes).

10º EIN /
Cyber Intelligence e Situational Awareness no Ciberespaço

29 Abril 2016

Rui Diogo Serra
Sr Product Marketing Manager

Tecnologias focadas para respostas direcionadas

Nationwide Defense Organizations

CyberDefesa

~13000M	~ 35% de 7000M	15 Triliões de Gigabytes
Connected devices 2015	Pessoas online 2015	Total Dados

In: NATO, National Cybersecurity framework, 2016
The Hague HCSS Report 2015

Nationwide Defense Organizations

CyberDefesa > Mandatos

Cyber Warfare	Proteção de CIS das Infraestruturas Críticas	Computer Incident Response	...	...
& Militar, Counter, Intelligence, etc..		& Resposta a crises		

Nationwide Defense Organizations

CyberDefesa > Operacional >

Cyber Warfare

Proteção de CIS de Infraestruturas Críticas

Computer Incident Response

...

...

Cyber Threat Intelligence

- Defensivo (reativo)
- Preventivo (proativo)

Nationwide Defense Organizations

CyberDefesa > Objetivo

Proteção de Infraestruturas Críticas

Computer Incident Response

Cyber Threat Intelligence

Situational Awareness & Response

Eficiência na **Resposta a Ameaças**

Cyber Threat Intelligence  **Situational Awareness & Response**

Como obter uma *threat perspective* de diferentes geografias, e de diferentes "portfolios"

E como operacionalizar estes dados?

(*) Portfolios: Critical Infrastructures vs. Threat Landscape (País) vs. Threat Landscape internacional

Eficiência na **Resposta a Ameaças**

Cyber Threat Intelligence → **Situational Awareness & Response**

Atividade ↓

Como obter uma *threat perspective* de diferentes geografias, e de diferentes "portfolios"

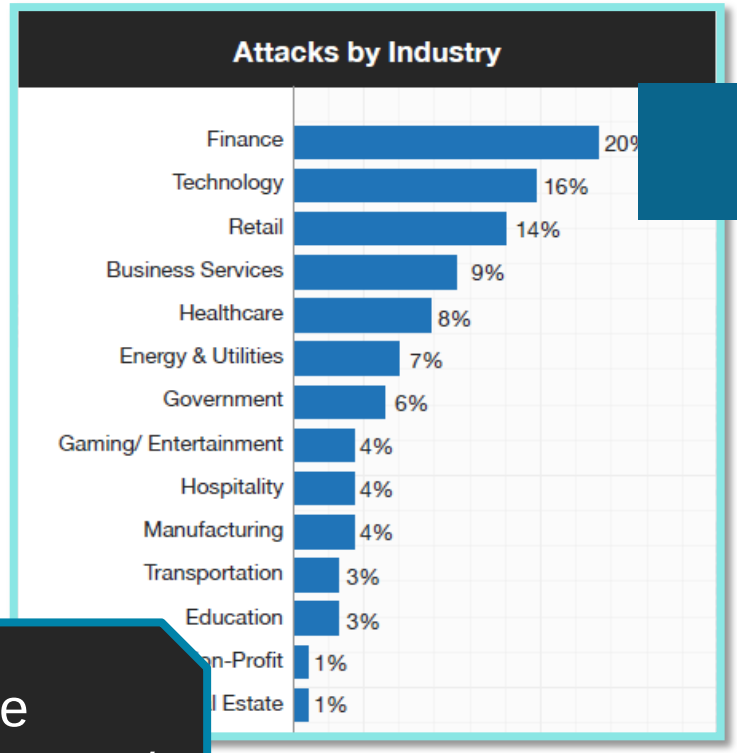
E como operacionalizar estes dados?

- Foco
- Direção
- Confiança

Mindset

Tecnologias **Focadas**

Cyber Threat Intelligence → **Situational Awareness & Response**



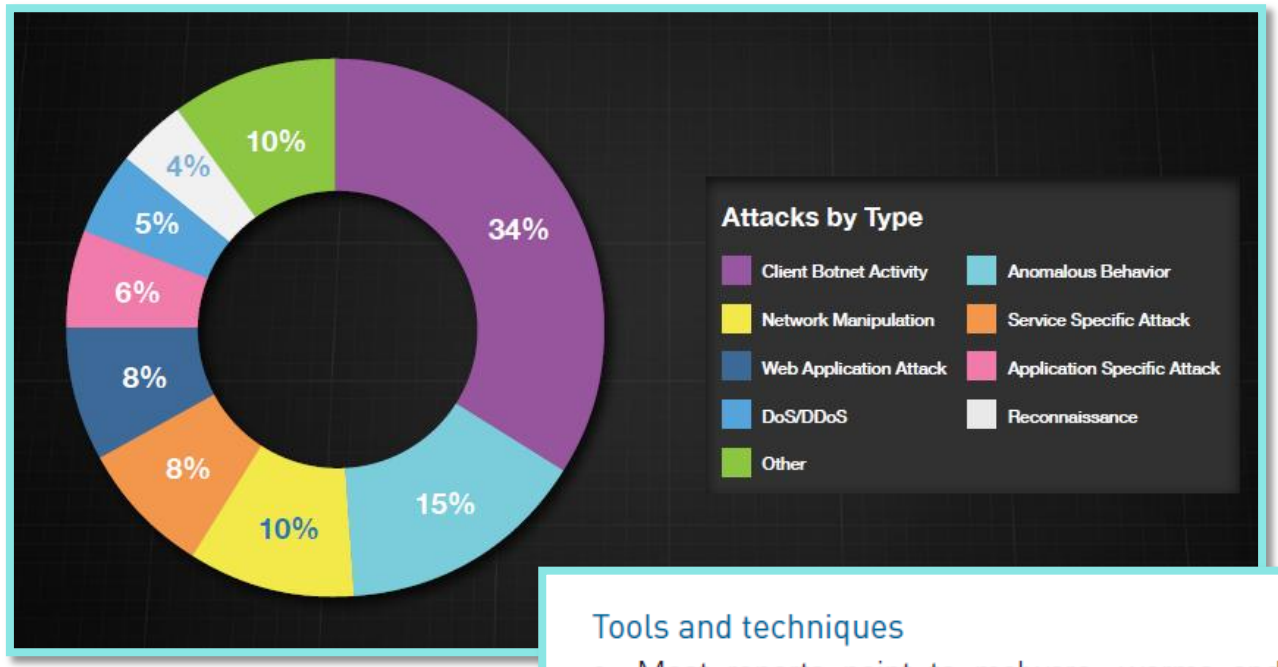
Foco

50M de Cyber Incidentes / ano

IN: The Hague HCSS Report 2015, PWC 2015

Tecnologias **Focadas**

Cyber Threat Intelligence → **Situational Awareness & Response**



Foco

Tools and techniques

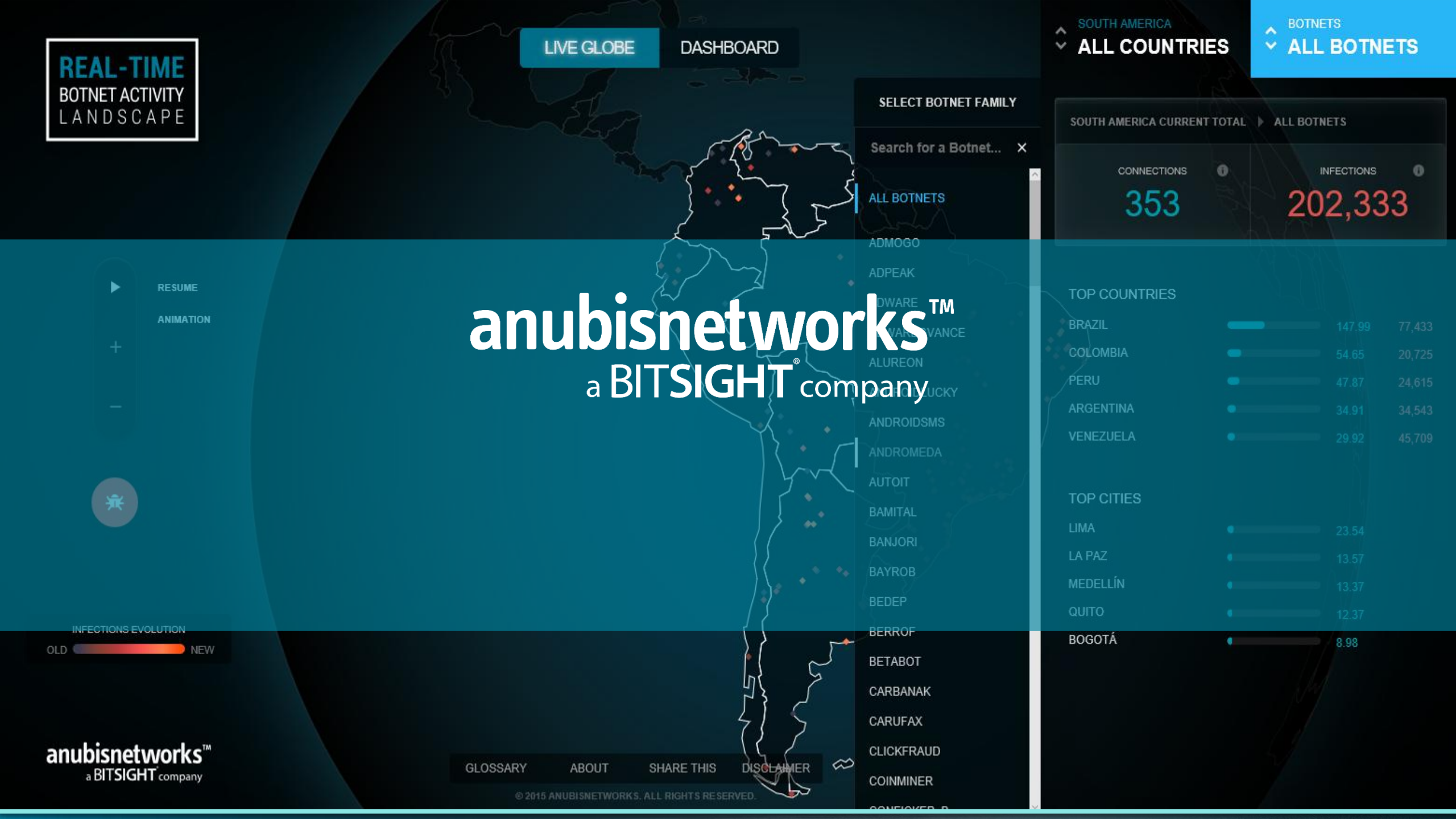
- Most reports point to malware, worms and trojans as most prevalent attack techniques used.

IN: NTT Global Threat report, 2014

... **Respostas** Direcionadas

Uma Framework de Situational Awareness & Resposta a Incidentes:

- Ingestão e correlação de CTI em tempo real
- Capacidades de **Situational Awareness**: Reporting, monitorização, data mining, que permitam identificação rápida de anomalias, tendências, padrões
- Informação **confiável, profunda** sobre o ataque (vector, campanha, sistema, organização)
- **Portfolio vs. Threat Landscape** Setores, Indústrias, Geografias / nacional vs. internacional



anubisnetworks™

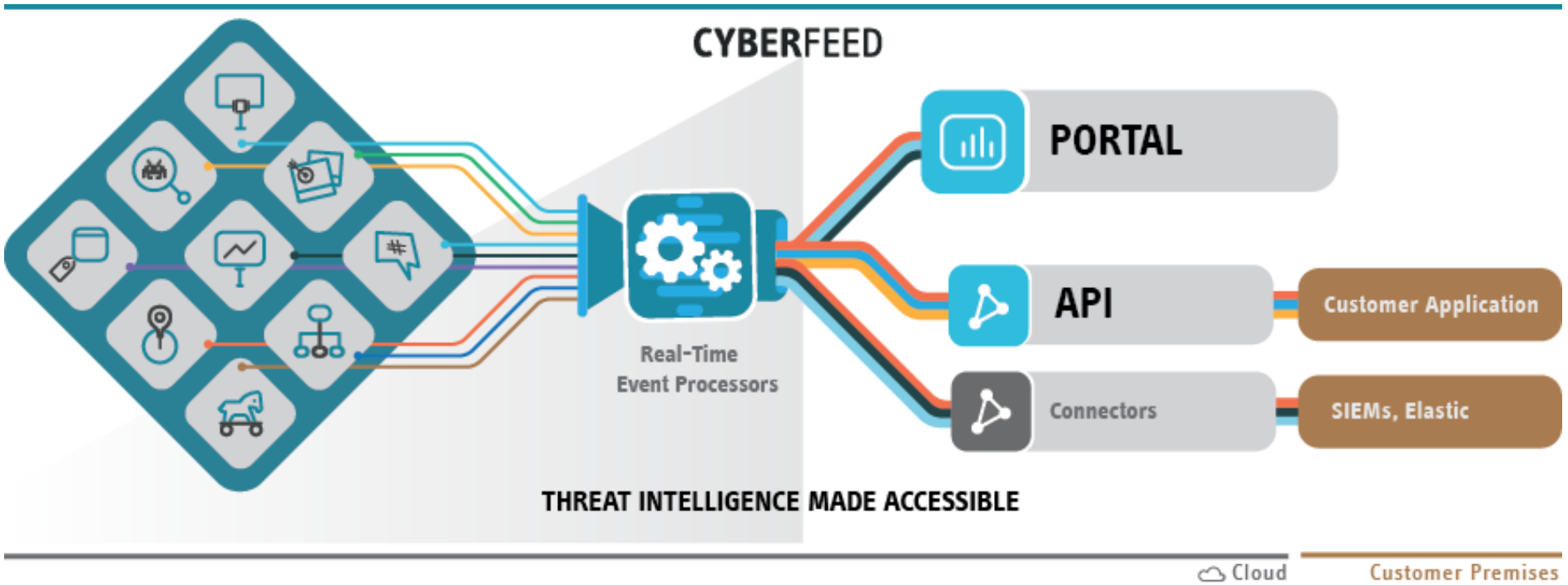
a BITSIGHT® company

Anubis > Threat Intelligence

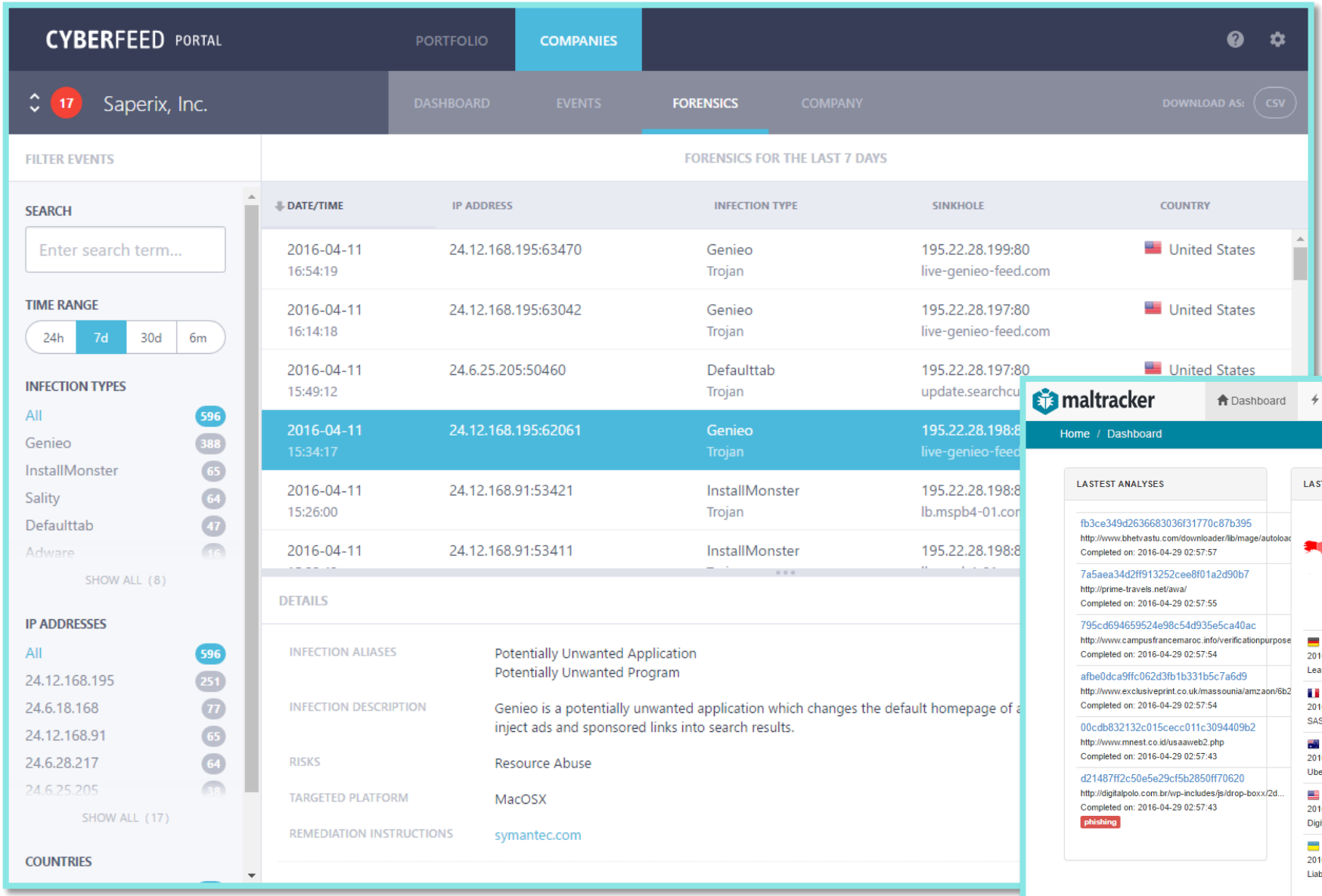
Cybersecurity infrastructure + Security Labs

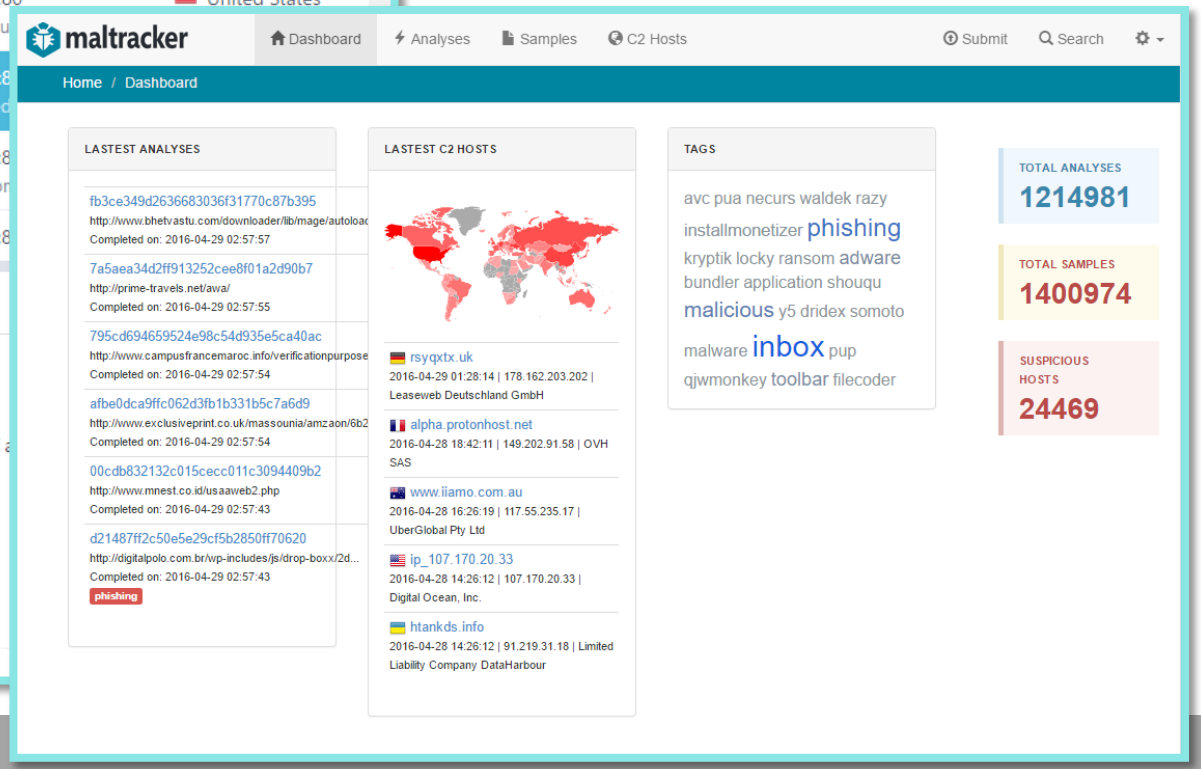
Real-time Events > **infections and vulnerabilities**

+ **Depth and Breadth**:
  - sectors, companies and industries,
  - malware remediation and severity, communication
  - payloads, forensics, CVEs, IOCs.

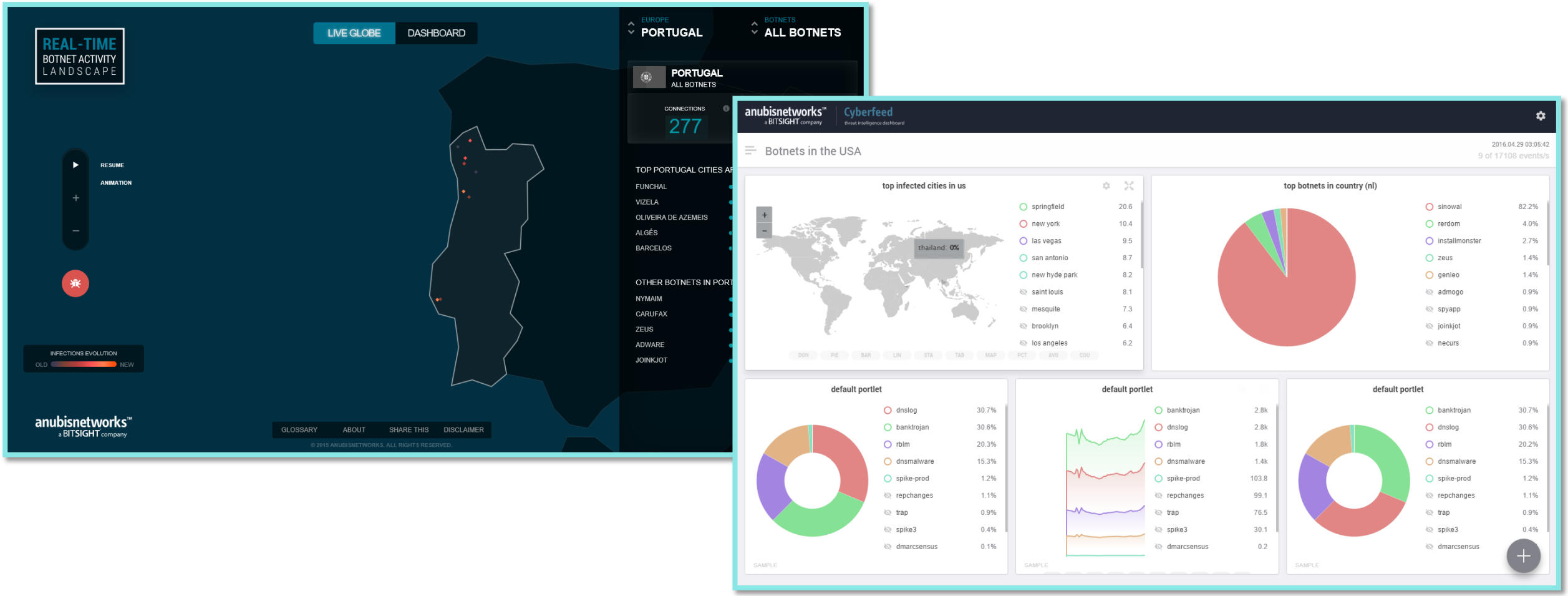


Threat Intelligence Platform

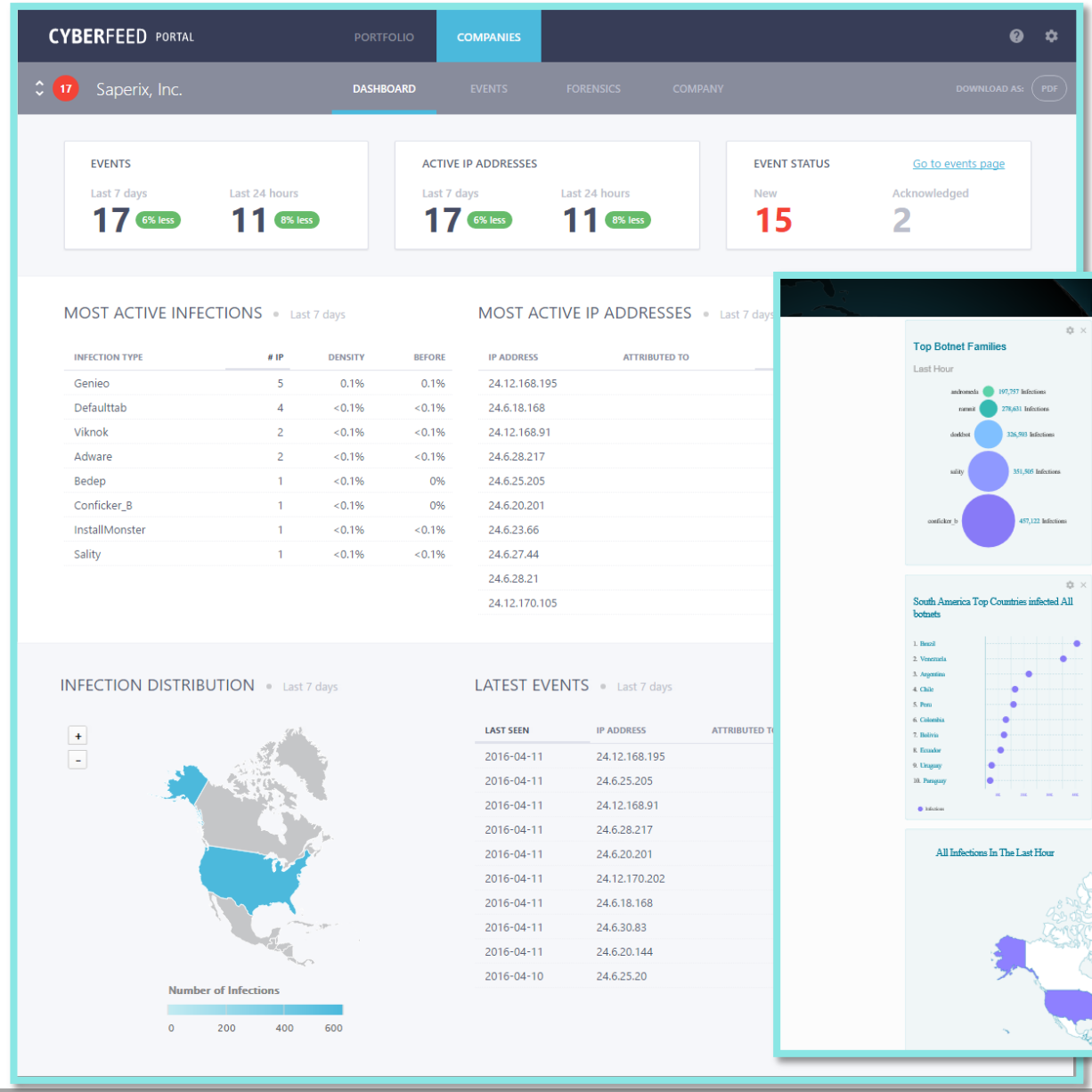


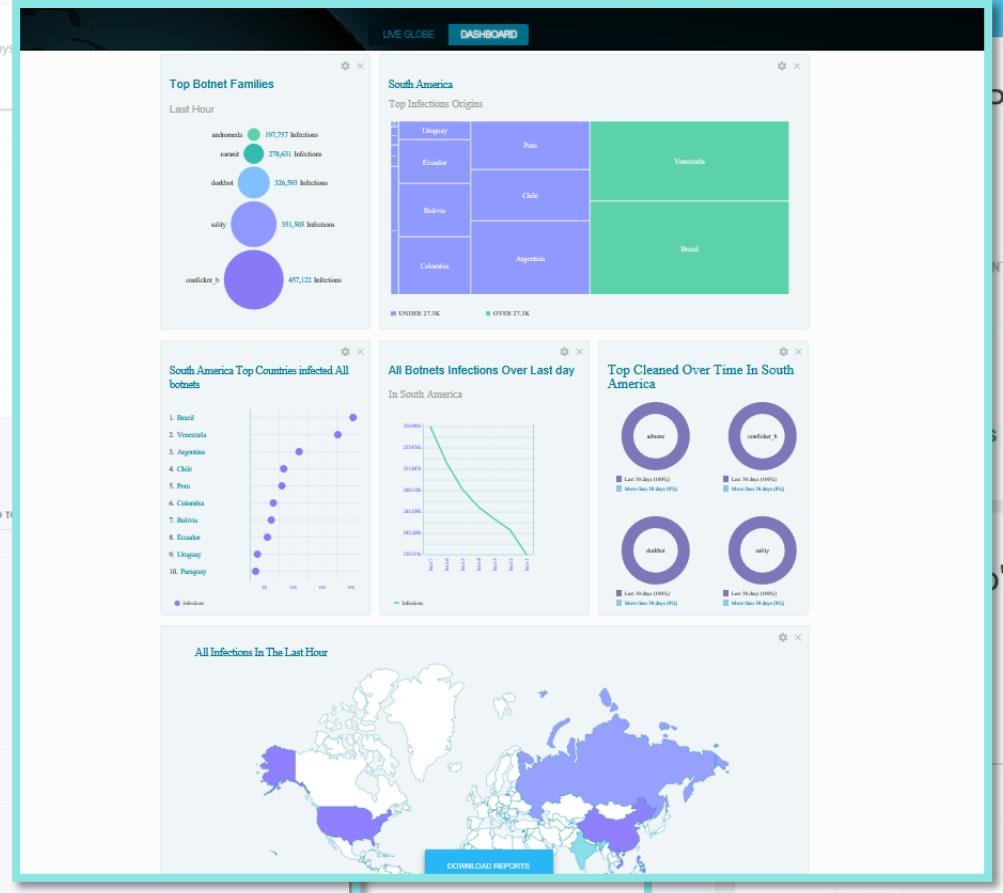


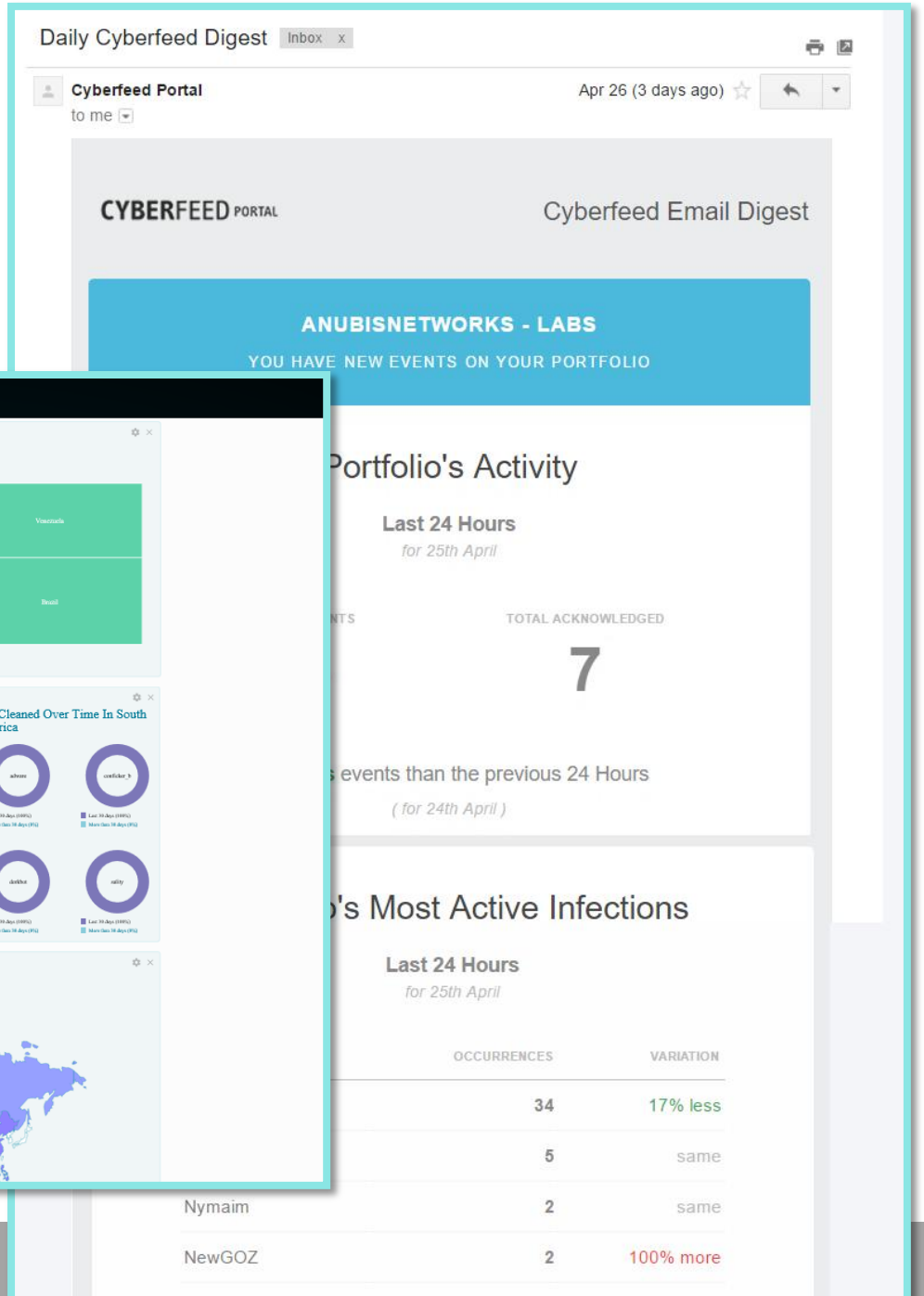
Cyberfeed Live Analytics



Reporting & Monitoring







Cyberfeed - Inteligência

Infection detection

- Detection of infected systems communicating with Command & Control servers
- Metadata from real-time communications between machines compromised and C&C servers

Social awareness

- Detection of sensitive information leaked in open social media platforms
- Monitoring of live posts in social websites in open and dark web

Compromised systems

- Malware analysis of files and websites
- Correlation between infected systems (file, email, web) and infection campaigns

Email ecosystem

- Identification of messages being flagged as SPAM and brand abuse campaigns
- Information about URI shortener services, with shortened URI translation
- IP Reputation for an IP Address or domain


anubisnetworks™
a BITSIGHT company
Obrigado!
Tecnologias Focadas
Respostas Direcionadas
Confiança
• Malware Campaigns
• Forensics
• Scope global
Situational Awareness & Response
• Real-time
• Accuracy
• Monitoring
• Reporting
• Incident Handling

Backup Slides