How do you deal with the sheer volume of security data

Peter Brecl, Director of Global Security Services

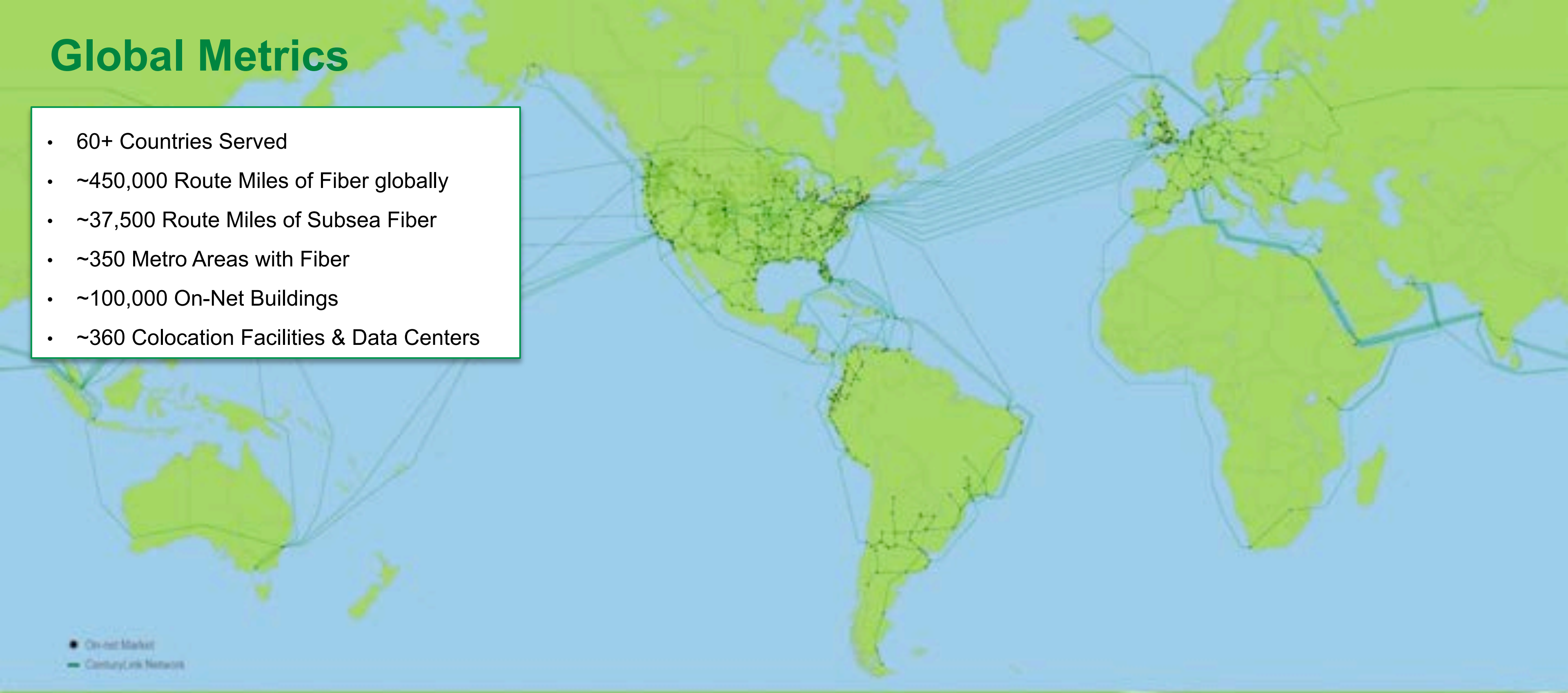
October 23, 2018

Services not available everywhere. Business customers only. CenturyLink may change or cancel services or substitute similar services at its sole discretion without notice. ©2018 CenturyLink.

CenturyLink®

Global Metrics

- 60+ Countries Served
- ~450,000 Route Miles of Fiber globally
- ~37,500 Route Miles of Subsea Fiber
- ~350 Metro Areas with Fiber
- ~100,000 On-Net Buildings
- ~360 Colocation Facilities & Data Centers

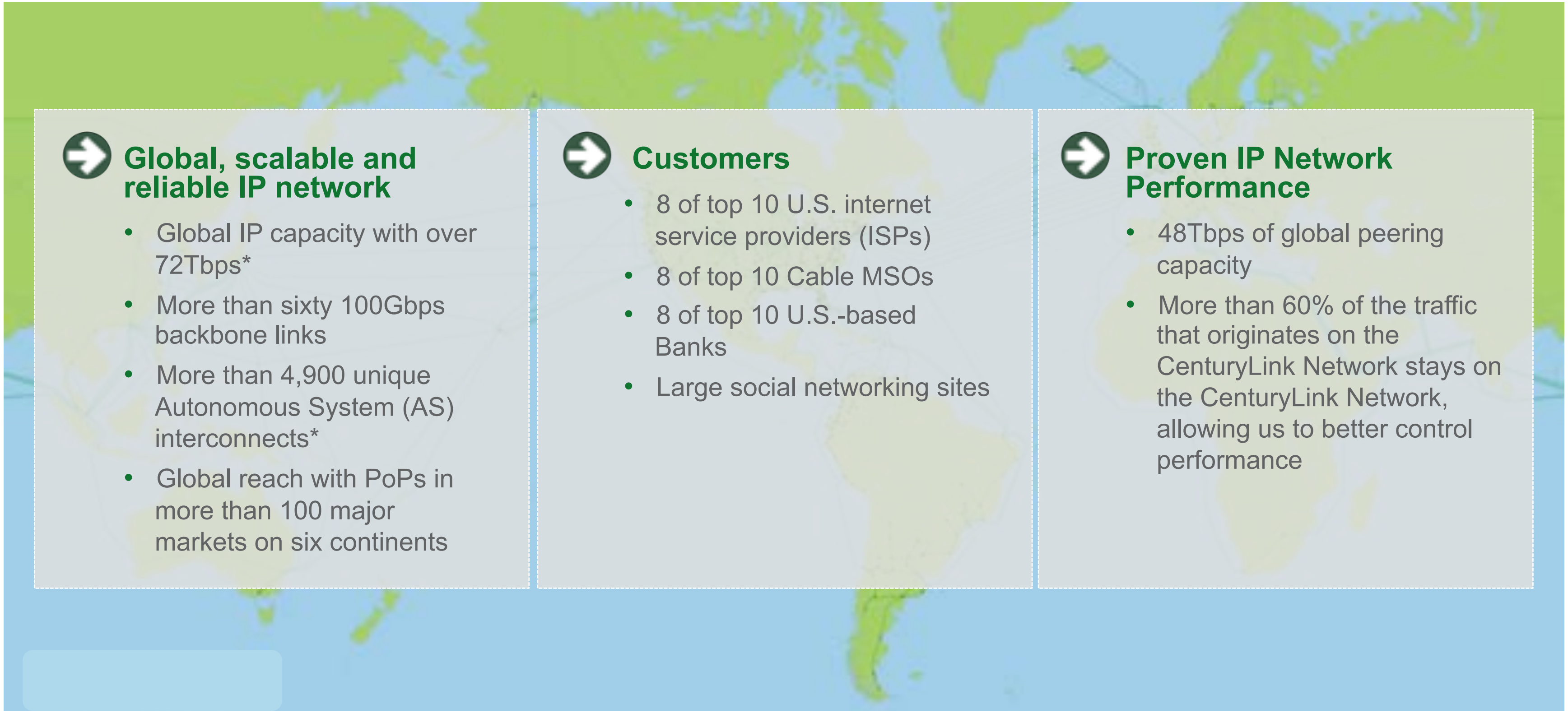


CenturyLink Global Network

CenturyLink®

Map information above is current as of March 2018. Information is subject to change. Contact CenturyLink for updates or details. CenturyLink's global network is made up of owned, leased access and IRU segments, which are not distinguished on this map. CenturyLink engages in region carriers to provide services in some markets.

Leverage The Power of Our Internet Services



Global, scalable and reliable IP network

- Global IP capacity with over 72Tbps*
- More than sixty 100Gbps backbone links
- More than 4,900 unique Autonomous System (AS) interconnects*
- Global reach with PoPs in more than 100 major markets on six continents

Customers

- 8 of top 10 U.S. internet service providers (ISPs)
- 8 of top 10 Cable MSOs
- 8 of top 10 U.S.-based Banks
- Large social networking sites

Proven IP Network Performance

- 48Tbps of global peering capacity
- More than 60% of the traffic that originates on the CenturyLink Network stays on the CenturyLink Network, allowing us to better control performance

* As of 5/31/2018

Cyber Threat Intelligence, Analysis & Defense – Creating a Safer Internet

CenturyLink

We **monitor**

~1.3 billion

Security events per day

We **collect**

~357 million

DNS queries per day

We **respond** to and

mitigate ~120

DDoS attacks a day

We **track** over

5,000 C2s

per day

We **monitor** over

114 billion

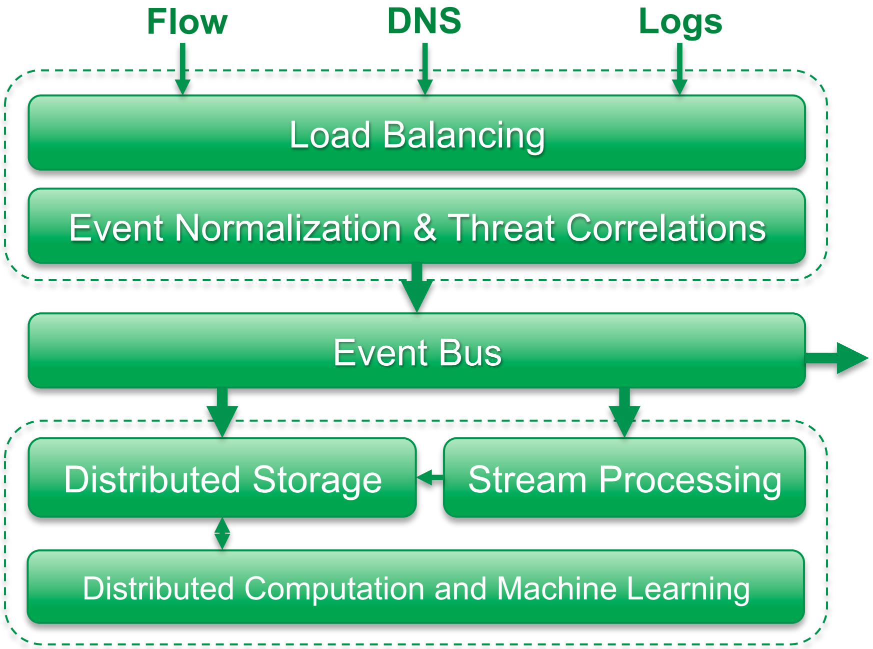
NetFlow sessions per day

We **identify** over

267 and **remove** **35**

new C2s a month

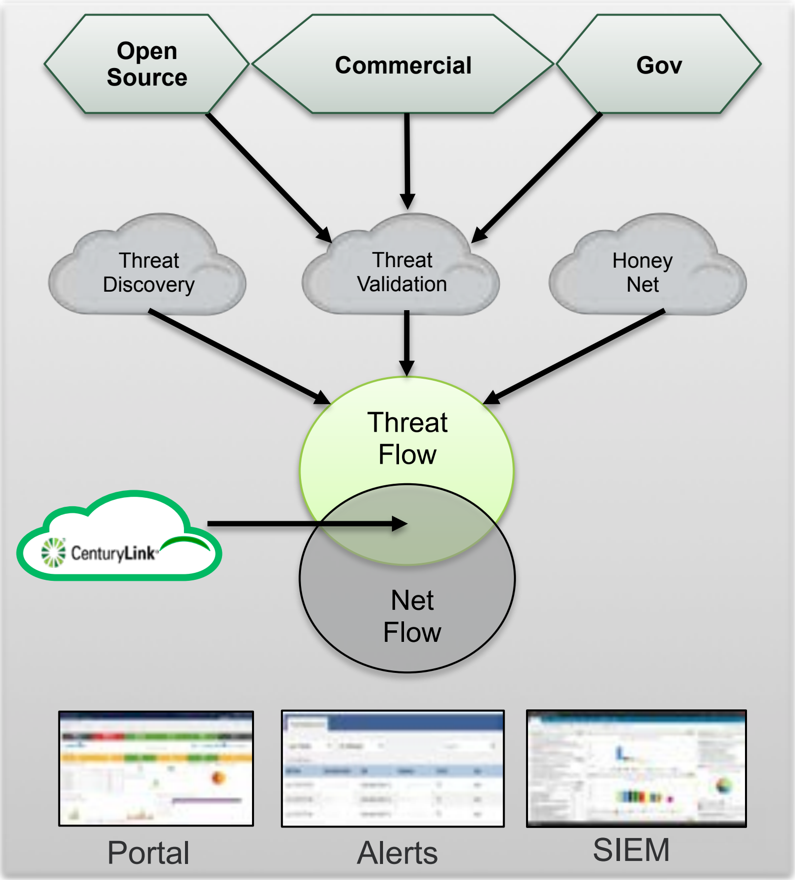
Processing Data at Large Scale


Flow
DNS
Logs
Load Balancing
Event Normalization & Threat Correlations
Event Bus
Distributed Storage
Stream Processing
Distributed Computation and Machine Learning

Breaking down the problem

- Data ingestion, normalization, and correlation
- Buffering, stream processing, and persistence
- Distributed machine learning to identify emerging threats

Adaptive Threat Intelligence



Open Source

Commercial

Gov

Threat Discovery

Threat Validation

Honey Net

Threat Flow

CenturyLink

Net Flow

Portal

Alerts

SIEM

Threat Intel Resources

- Indicators of Compromise
- Continuous feed selection and evaluation

CenturyLink Threat Research Lab

- Original Threat Discovery and Validation
- Big Data Analytics / Machine Learning

Network is the Sensor

- CenturyLink Network Backbone Infrastructure
- 114+ Billion NetFlow Sessions Daily

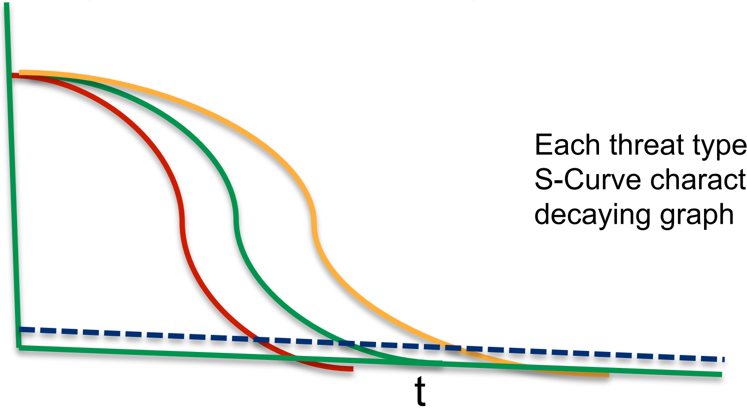
Active Data Correlation

- See threats in near real time
- Identify activity before it progresses to major security incidents

Risk Score

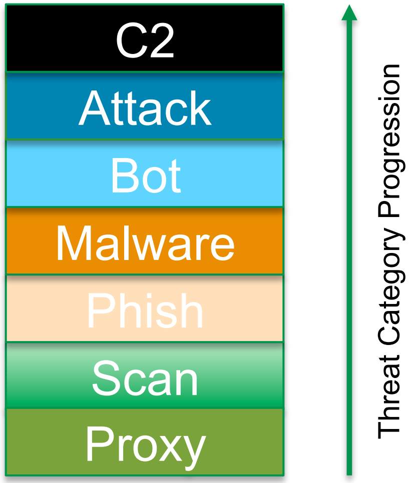
Factors that affect threat scores

- Source Score: Score reported by IOC source
- Source Confidence: Our confidence rating of source
- Category Weights: Threat categories progression
- Internal Validation: positive validation sets confidence factor to 100
- Positive Factors: De-risk score if CDN or Popular
- Event Update: Source changes score or removes threat from set
- Decay Factor: S-Curve decay over time



Each threat type gets its own S-Curve characteristics decaying graph

t = time



C2

Attack

Bot

Malware

Phish

Scan

Proxy

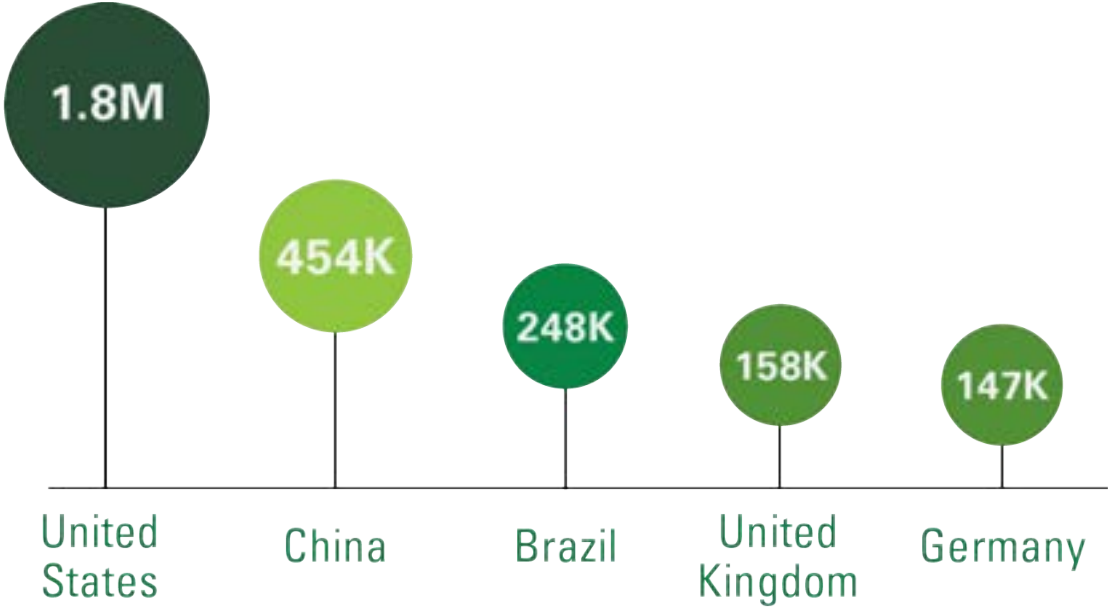
Threat Category Progression

CenturyLink

CenturyLink Threat Report

Top 5 Bot Hosting Countries

Daily Average



Source: CenturyLink 2018 Threat Report
https://lookbook.centurylink.com/threat-report/2018threatreport

Who is Attacking, and Using Which Strategies?

CenturyLink

C2s by Country of Origin

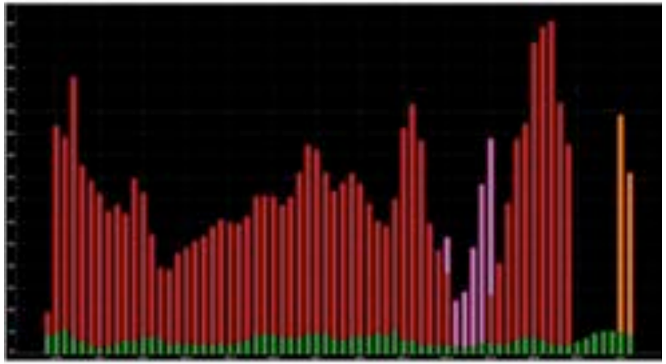
1. United States
2. Russia
3. Ukraine
4. China
5. Germany
6. Netherlands
7. France
8. United Kingdom
9. Brazil
10. Canada

6
8
3
2
10
1
5
7
4
9

Examples of Hunting for Threats in the Network

Original Command & Control (C2) and Bot Discovery

- Use network as a sensor
- Identify C2 traffic
- Categorize the botnet
- C2 validation
- Reverse trace the compromised bots communication with the validated C2
- Inform other security services about the applicable bots (e.g. DDoS Mitigation)



Source: Cisco Talos Group. RED/PINK/ORANGE – Attacker. GREEN – Rest of Internet

Classification “Shortcuts”

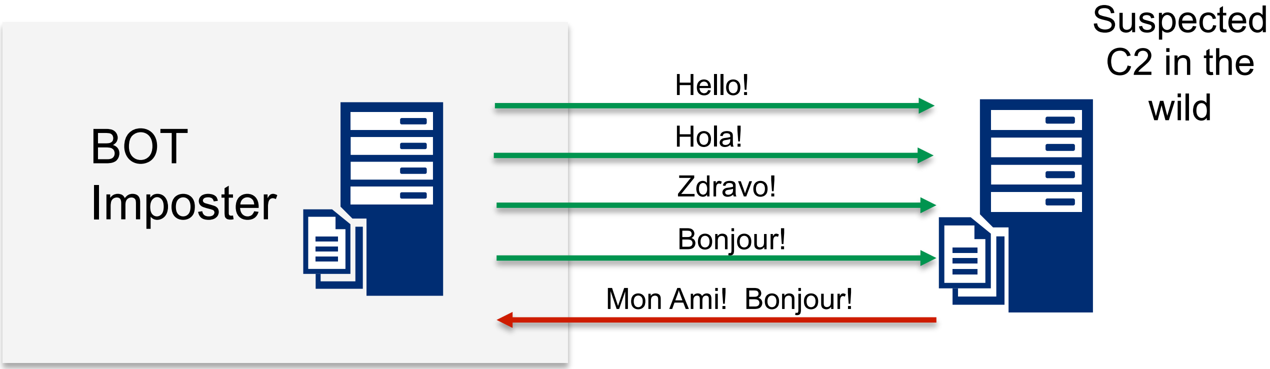
“You don’t need a weatherman to know which way the wind blows” --Bob Dylan

Examples:

- C2: a node in contact with several hundred infected bot hosts, is likely a command and control (C2) server

- Port Scanner: a node that sends requests to many ports on the same IP address (an repeats the behavior with new IPs), is likely a port scanner

Validation Example – C2



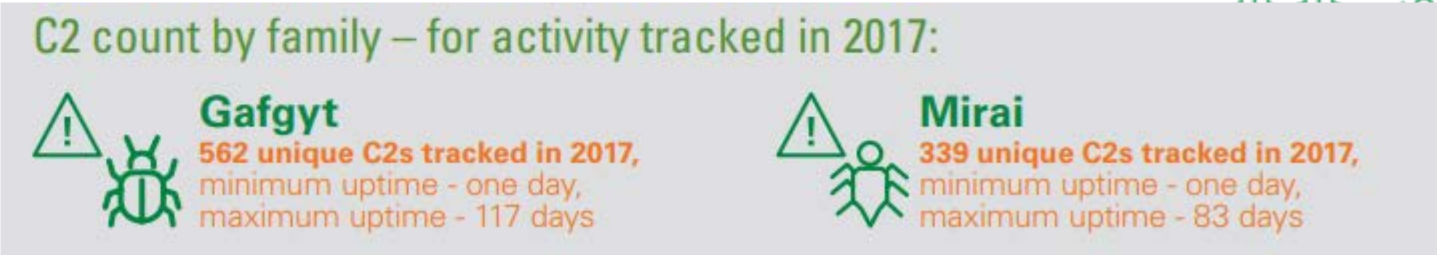
Machine Learning - validation can feed back into the ML algorithms.

Example:

- Several sample sets find 10 classifiers as good candidates (call them C1 thru C10)
- Observation: Each time classifiers C1 thru C10 show up together from Random Forrest processing, validation always indicates C4 is the correct selection
- This gets “feedback” as a shortcut: “Check C4 first”

C2 Tracking and Takedown

- Utilize the network visibility to track C2 communication
- Disrupt communication between the C2 and compromised machines
- Track and disrupt communication of reemerging or backup C2 controls trying to regain control of the bots
- CenturyLink tracks over 5000 botnets and takes down 35 per month



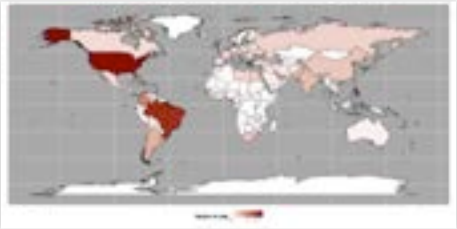
C2 count by family – for activity tracked in 2017:

Gafgyt
562 unique C2s tracked in 2017,
minimum uptime - one day,
maximum uptime - 117 days

Mirai
339 unique C2s tracked in 2017,
minimum uptime - one day,
maximum uptime - 83 days

DDoS Botnet Detection and Mitigation

- Source intelligence from the network
- DDoS attacks often use spoofed source IPs
- Discover DDoS botnet communication
- Mitigate the attack at the botnet layer before redirecting the traffic for mitigation to the scrubbing centers
- Detect new type of attacks before they are used against business



Global Distribution of Mirai Bots

Source: CenturyLink Threat Research Labs

[How 1.5 million connected cameras were hijacked to make an unprecedented botnet]
Motherboard, September 29th, 2016

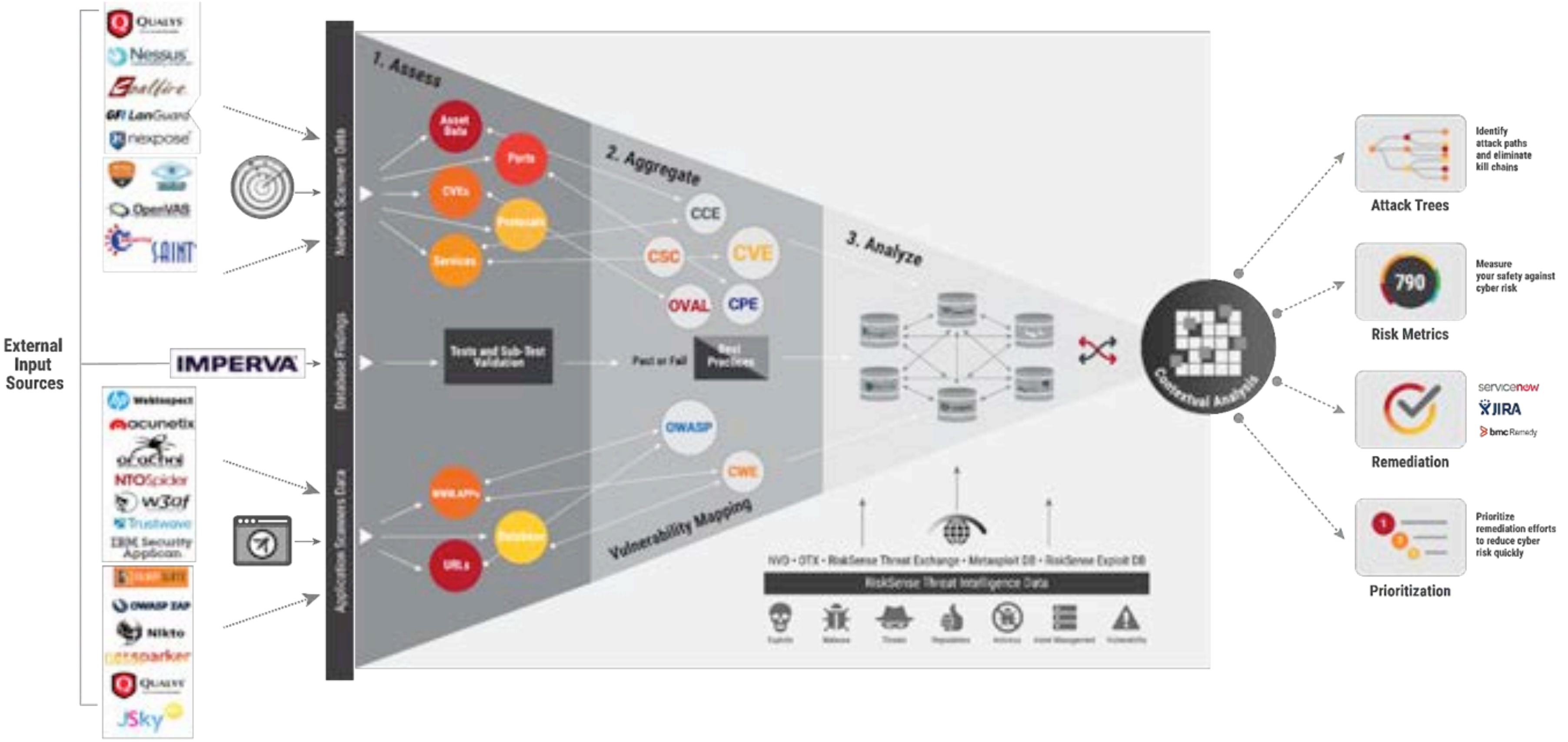
[Hackers Release Botnet Code, Raising Specter of More Attacks]
WSJ, October 5th, 2016

Tracking Beyond the Compromised Machine

- Detect attacking IP communication to the business asset
- Track attacking IP to Command & Control infrastructure
- Look for sources instructing the C2 to execute commands

```
COPYFILE(PATH,SO,FALSE);
UNSIGNED CHAR PATHTOFILE[20] = "TROJAN.BMP.EXE";

REGOPENKEYEX(HKEY_LOCAL_MACHINE,"SOFTWARE\\...",0,KEY_SET_VALUE,&HKEY );
REGSETVALUEEX(HKEY, "SECURITYMANAGER",0,REG_SZ,PATHTOFILE,SIZEOF(PATHTOFILE));
REGCLOSEKEY(HKEY);

WHILE(1==1)

HWIN = FINDWINDOW(NULL,"TASK MANAGER");
SENDMESSAGE(HWIN,WM_CLOSE,(LPARAM)0,(WPARAM)0);

HWIN = FINDWINDOW(NULL,"REGISTRY EDITOR");
SENDMESSAGE(HWIN,WM_CLOSE,(LPARAM)0,(WPARAM)0);

HWIN = FINDWINDOW(NULL,"COMMAND PROMPT");
SENDMESSAGE(HWIN,WM_CLOSE,(LPARAM)0,(WPARAM)0);

HWIN = FINDWINDOW(NULL,"CLOSE PROGRAM");
SENDMESSAGE(HWIN,WM_CLOSE,(LPARAM)0,(WPARAM)0);
```

Holistic View of Cyber Risk

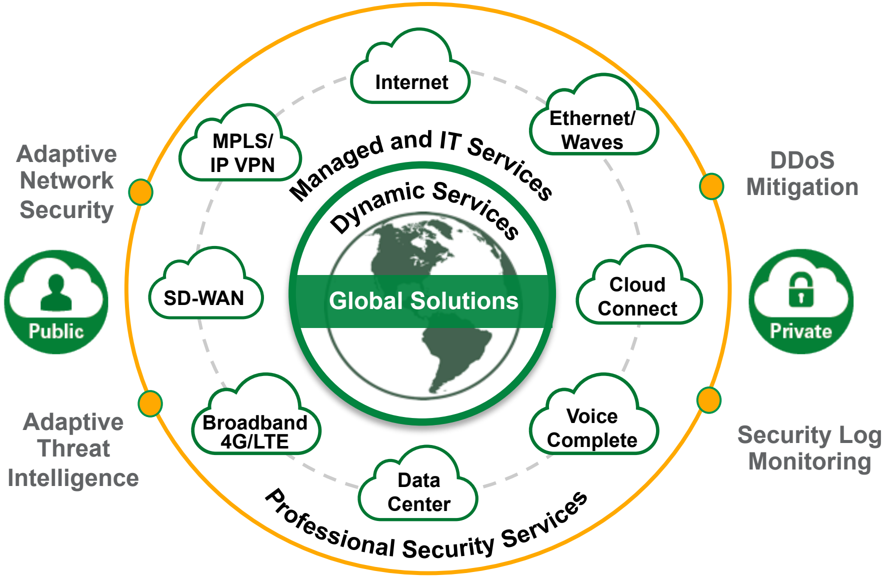


CenturyLink Adaptive Networking and IT Solutions

Evolve Your Infrastructure as Your Business Transforms

CenturyLink

Networking | Hybrid IT and Cloud | Security | Voice and Unified Communications | Managed and IT Services



CenturyLink®

Your link to what's next™