Overcoming threat fatigue

Using threat intelligence intelligently

Bryn Norton
Director solutions Architecture and Security – EMEA
Map information above is current as of April 2017. 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.
Why CenturyLink, a network company?

Global scale and reach

- **We monitor** ~1.3 billion Security events per day
- **We respond** to and **mitigate** ~120 DDoS attacks a day

- **We identify** over 267 and **remove** 35 new C2s a month
- **We monitor** over 114 billion NetFlow sessions per day

- **We track** over 5,000 C2s per day
- **We collect** ~357 million DNS queries per day
Malicious Traffic
By Country of Origin
1 United States
2 Russia
3 China
4 Brazil
5 Ukraine
6 Germany
7 France
8 Netherlands
9 Turkey
10 United Kingdom

CenturyLink tracked an Average 195,000 threats per day, impacting 104 million unique targets.
See more, stop more.
Top 5 Bot Hosting Countries – Daily Average

- **United States**: 1.8 million unique bots per day
- **China**: 454 thousand unique bots per day
- **Germany**: 147 thousand unique bots per day
- **Brazil**: 248 thousand unique bots per day
- **United Kingdom**: 158 thousand unique bots per day

Map information above is current as of April 2017. Information is subject to change. Contact CenturyLink for updates or details. CenturyLink’s global network is made up of owned, leased access and IPU segments, which are not distinguished on this map. CenturyLink engages in region carriers to provide services in some markets.
Pressure
To stop threats, you first have to see them coming

G.I.G.O.
What is ‘Truly’ actionable

Cloud
How do you secure your journey to the cloud

Data Growth
AI is driving the expansion of Data Clusters as it become Mainstream

Digital Transformation
Evolve or Die Disrupt vs. Disrupted

Breaches\(^1\)
58% breached
Majority Known vulnerabilities

Population\(^1\)
Over 54% now on the Internet
Users have Grown 1052\(^2\)

Dispersed World
Enablement from collaboration
Mobile devices

Supply Chain\(^1\)
Over 36% now on the Internet
Hijack of Legitimate Service

1: Top Cybersecurity Threats in 2018
https://www.forrester.com/report/Top+Cybersecurity+Threats+In+2018-_a-RS137206
2: www.internetworldstats.com
**Approach**
To stop threats, you first have to see them coming

**Respond**
You are already breached

- Public traded, need to report on material risk
- The treatment of data has matured for instance GDPR
- Dev Opps on the Journey

**Assess**
The ‘Edge’ the impact of IoT

- Shelf ware
- Actionable Data – tied to your business
- Where does you data live, the impact of the ‘Cloud’

**Protect**
The basics (not been done well)

- To much focus on prevent 10% of IT budgets
- What are you protecting

**Predict**
Attacks are not sophisticated

- Inherent vulnerabilities for instance Spectre and Meltdown
- Knowledge based authentication has had its day
Customer experienced frequent malware compromises within their network, despite a large security equipment investment.

Experienced a high-profile event that resulted in significant financial and reputational damage. Internal resource struggling to manage the volume of information from multiple existing threat feeds.

ROOT CAUSE ANALYSIS
Through analysis of the data it was identified that the root cause of the malware compromises was due to transient temporary workforce.
An ageing network perimeter, lack of internal security expertise, ineffective employee education and outdated process & procedure resulted in a high-tech leader in their field struggling to protect core intellectual property.

The volume of noise had reached a point where known security events were being ignored.

**ACTIONABLE THREAT INTELLIGENCE**

Effective threat scoring based on 3rd party feeds, tuned through intelligence gathered from our backbone by CenturyLink Threat Labs reducing the 'noise'.

**RELEASE OF INVESTMENT**

Clear identification of the current external risk profile helped facilitate release of investment to replace legacy infrastructure.

**ACCESS TO EXPERTISE**

CenturyLink 24/7 SOC augmenting in-house resource.

**TECHNICAL AGNOSTIC**

As all CenturyLink security services are network agnostic service benefit would continue throughout and beyond any infrastructure transformation.
Key takeaways
Using threat intelligence intelligently

- Make sure your intelligence in actionable, source effective partners to manage change and cut through the noise.
- Identify the data – Let this be your focus
- Build controls around that data
- Building applications in containers
- Think about your supply chain
- Key element of your digital ecosystem – don’t view as an inhibitor
Overcoming threat fatigue

Using threat intelligence intelligently

Bryn Norton
Director solutions Architecture and Security – EMEA