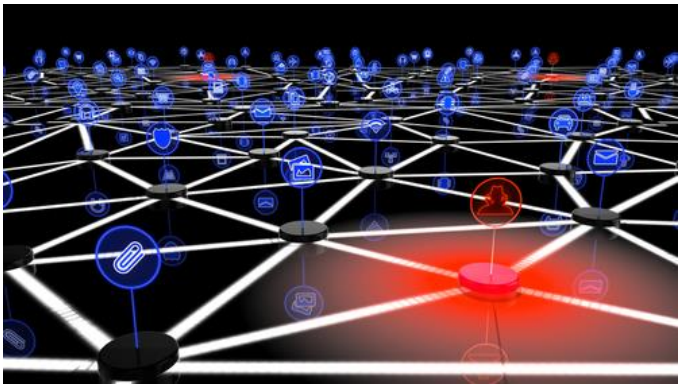
Internet of Things Auditor

safe connect by impulse



- ***Do you know which IOT devices are on your network?***
- ***Do you know the security posture of your IoT devices?***
- ***How do you know if your IOT devices are vulnerable to Denial of Service attacks?***

These are among the questions raised by the extremely large and unusual distributed denial-of-service (DDoS) attacks experienced recently. Internet security blog KrebsOnSecurity was taken offline in September 2016.[1] In addition, Dyn, a company that manages crucial parts of the Internet's infrastructure, was under attack several times on October 21, 2016. Sites affected by the DDoS attack on Dyn included Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud and The New York Times.[2]

The attacks appear to have relied on hundreds of thousands of internet-connected devices like cameras, baby monitors and home routers that have been infected, without their owners' knowledge, with software that allows hackers to command them to flood a target with overwhelming traffic.

Security researchers have long warned that the increasing number of devices being hooked up to the internet, the so-called Internet of Things (IoT), would present an enormous security issue. And these assaults are only a glimpse of how those devices can be used for online attacks.

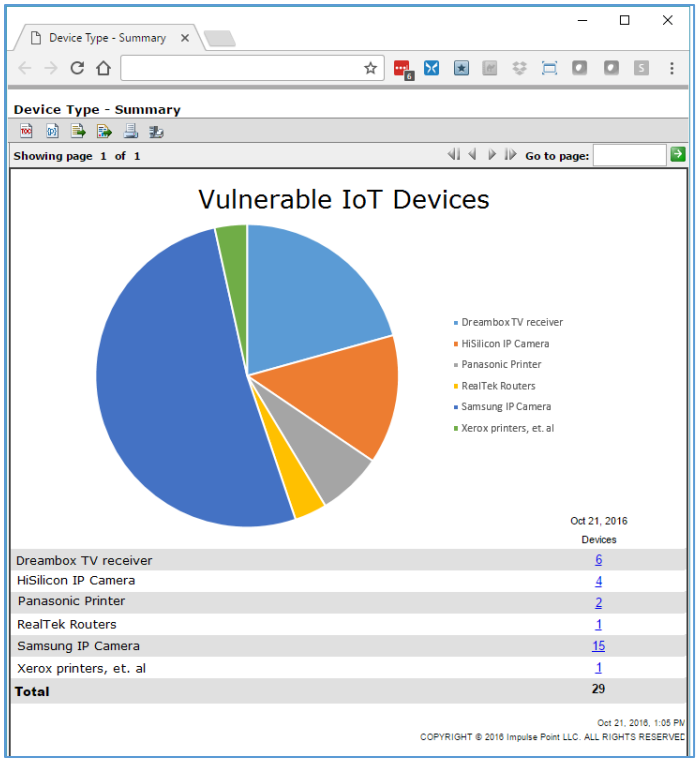
Impulse | Experience the Freedom

Impulse is the leading provider of Contextual Intelligence and Network Security Orchestration in support of BYOD and IoT enabled enterprises. Impulse securely and efficiently automates BYOD by combining our real-time, context-aware and simplified access control architecture, remote cloud-managed support services, and customer-centric business philosophy to enable customer freedom. Our customers know this as the Impulse Experience. Visit www.Impulse.com

Internet of Things (IoT) Auditor

SafeConnect's IoT auditor passively discovers all devices on your network including those that are browser compatible such as those listed above.

- Passively discovers IoT, mobile, and traditional devices on your network identifying them by device type, IP Address, MAC address, and optionally even the user identity and location.
- Easy to deploy and configure simply by pointing the information your network devices already generate to the IoT Auditor (e.g. Netflow). The Auditor starts to passively discover the IoT, mobile, and traditional devices on your network.
- Visual view of all devices currently and historically using your network.
- See and search devices by type, location, and other key attributes.
- See when each device came on and left the network.
- Easily see when a new type of device (never seen on your network before) joins.



1 https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

2 http://mobile.nytimes.com/2016/10/22/business/internet-problems-attack.html?referer=https