SSE MONTHLY TEAM UPDATES

NOTEWORTHY TEAM NEWS

JULY
2019

HOT THIS MONTH

- Introducing DSP
- Implementation of Executive Order 13873
- Robotics Process Automation (RPA)
- Data Loss Prevention (DLP)

PURPOSE

The purpose of the SSE Monthly Team Updates is to provide an inside view of what our SSE team is doing and how we are protecting Comcast and our staff from today's threats.

THE TEAM

The Security Solutions Engineering (SSE) team protects Comcast digital assets and intellectual properties from the ever-changing threat landscape to provide a secure business environment by delivering innovative security solutions, services and assurance. Our team is broken out into these core functions: Security Threat Engineering (STE), Design & Integration, Data Protection, Endpoint Security, Content and Data Engineering, and Security Development & Analytics (SDA).

Introducing DSP

Written By: Candra Cook Fried

What is DSP?

Cybercrime is a 500 billion dollar a year industry. The impact these incidents have cause severe consequences for affected businesses: loss of revenue, service interruption, and loss of costumer-relationships. Comcast's commercial customers deserve peace of mind in knowing their businesses can be protected, and DSP plays an integral role in this venture. We're excited to offer our wide range of network resources and to deliver competitive offerings to our customers.

DDoS Services Portal (DSP) is the solution that is replacing the former Security Dashboard, while interfacing with Arbor, DROM, CMS, My Account (CSP), Café and Remedy. DSP is being developed with our *2019 Comcast Business Goals & 2019 TPX Goals* in mind: driving growth, positioning ourselves for the future, committing to making the customer experience simple, consistent and digital, and delivering an innovative and reliable product experience.

This platform is built API-first – anything users can access from the web interface can be done programmatically (i.e. automation, simplification for users, and tie-in with broader security tools).

DSP will proactively monitor mid-market business customers for traffic and attacks. The platform will then alert customers when attack activity occurs, and mitigate the attacks to help minimize the impact to the business. Our platform will also orchestrate both the onboarding and maintenance of these commercial DDoS subscribers. Given that DSP draws in data from various existing Comcast platforms, it allows for a streamlined, speedy, and simplified customer experience.

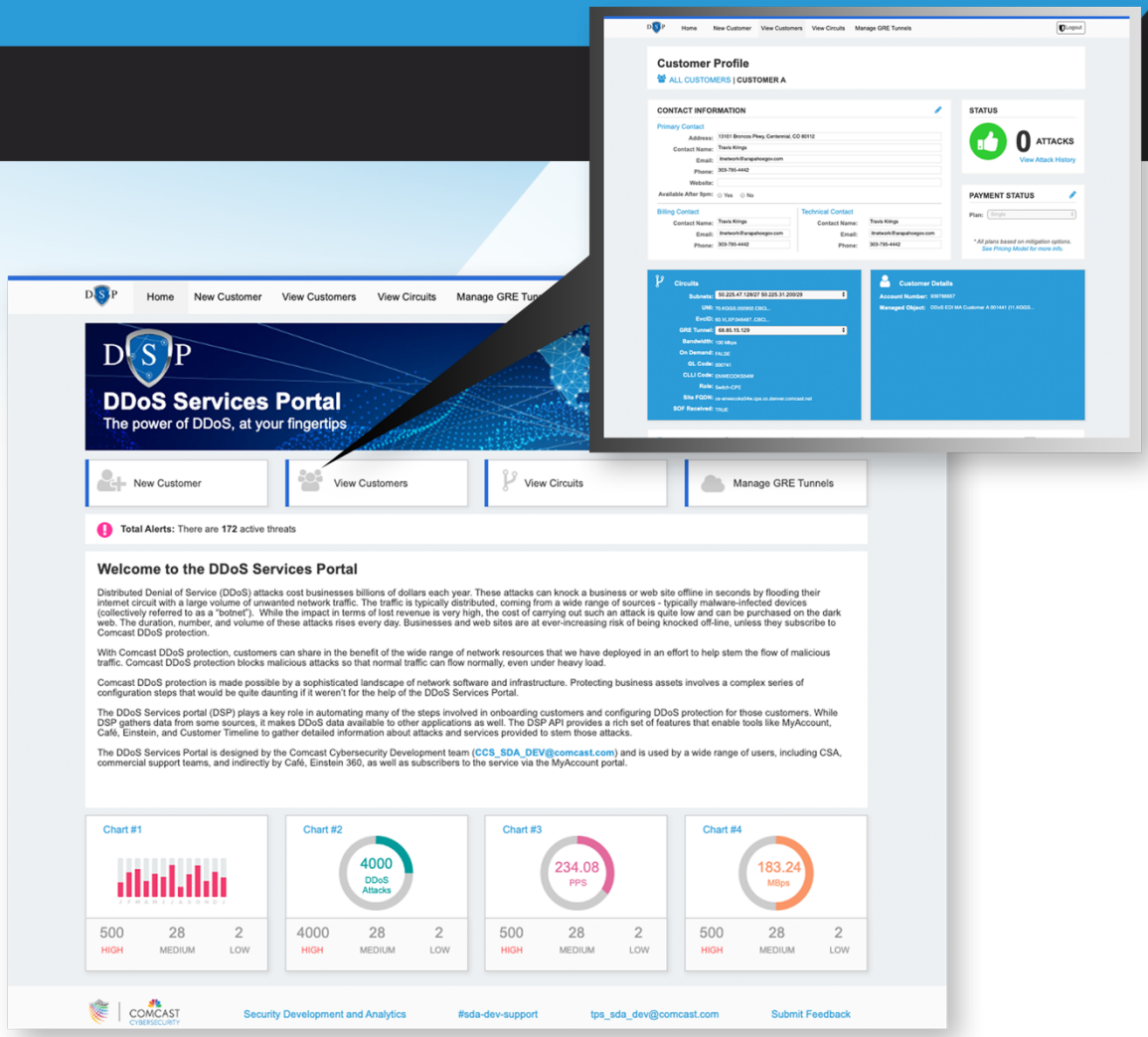
HIGHLIGHTS

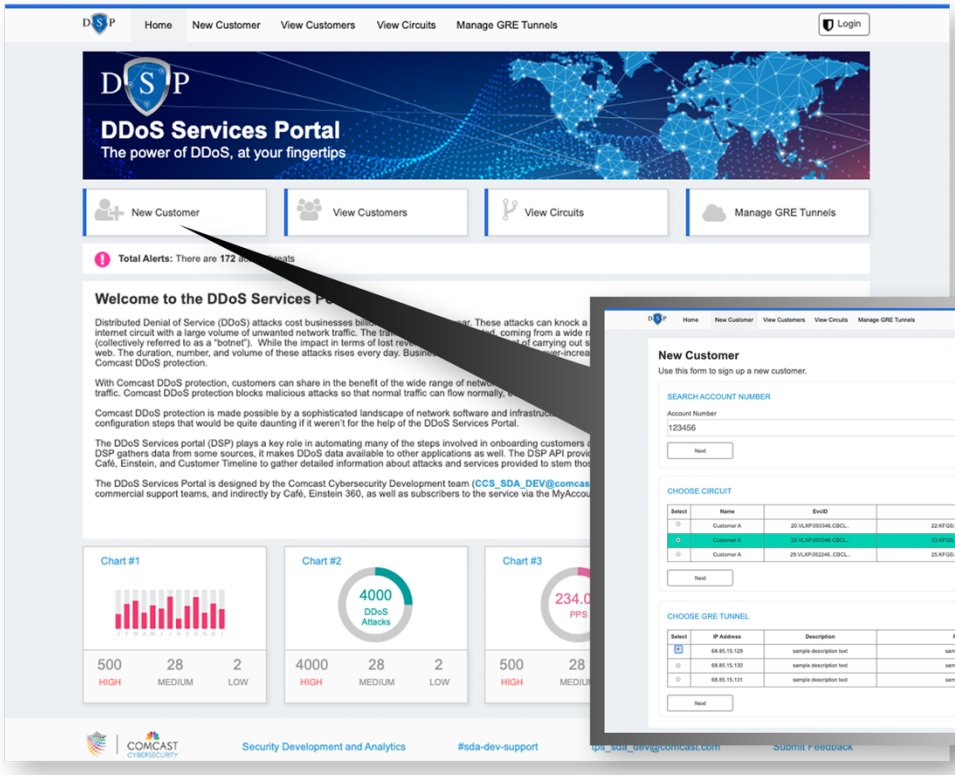
- Cybercrime is on the rise and growing everyday
- DSP now being offered to Comcast subscribers to protect businesses in the event of cyber-threats
- DSP is made possible by a sophisticated landscape of network software and infrastructure
- Notable features include:
  - Live data feeds to SIEM & CSOC
  - Support for fully automated incident response
  - Mitigation sync to Arbor
  - Automatic population of customer info

All Hands On Deck

The Security Development & Analytics team has been in lockstep with several contributors to design and develop DSP effectively: Commercial SOC, Einstein 360, Comcast University, CSA, Security Dashboard super-users, and many more. This open channel of communication helps us to ensure that we create a simplified platform that has ease of use, access to the latest data in real-time, automation of customer data, and constant feedback for our support staff who will be providing training through Comcast University.

Introducing DSP (continued)





Introducing DSP (continued)

Features & Delivery

Our development team is working hard to perfect DSP features according to schedule. Such features include (but are not limited to):

- Recording notes and customer attributes (i.e. Account Number, Address, Circuits)
- Documenting customer contacts (primary, billing, technical and other pertinent contacts)
- The automatic population of customer information from external systems such as DROM
- Mitigation synchronization to Arbor
- Updating, Modifying and Canceling services associated with existing customers
- Integration of: Arbor, DROM, CMS, MyAccount, Café and Remedy
- Notifying customers (ie. under attack, attack mitigated)
- Reporting
- Live data feeds to SIEM and CSOC
- Support for fully automated incident response

The slated production release is for **September 2019**. For additional information, please feel free to reach out to our development team: sample_email@comcast.com.