

# 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.

## 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.

## 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

# Introducing DSP (continued)

**Customer Profile**  
ALL CUSTOMERS | CUSTOMER A

**CONTACT INFORMATION**

Primary Contact  
Address: 13101 Bonus Pay Central, CO 80112  
Contact Name: Trank King  
Email: trank.king@comcast.com  
Phone: 303-795-4442  
Website: [Empty]  
Available After 5pm:  Yes  No

Billing Contact  
Contact Name: Trank King  
Email: trank.king@comcast.com  
Phone: 303-795-4442

Technical Contact  
Contact Name: Trank King  
Email: trank.king@comcast.com  
Phone: 303-795-4442

**STATUS**  
0 ATTACKS  
View Attack History

**PAYMENT STATUS**  
Plan: [Dropdown]  
\*All plans based on regulated markets. See Pricing Model for more info.

**Circuits**

Subnets	UMs	GRE Tunnels
52.225.47.129/27, 88.85.15.129	10.10.0.0/16, 10.10.1.0/24	68.85.15.129
		68.85.15.130
		68.85.15.131

**Customer Details**

Account Number: 19789657  
Managed Object: 1204 ETOA Customer A @19789657

**DDoS Services Portal**  
The power of DDoS, at your fingertips

Navigation: New Customer | View Customers | View Circuits | Manage GRE Tunnels

Total Alerts: There are 172 active threats

**Welcome to the DDoS Services Portal**

Distributed Denial of Service (DDoS) attacks cost businesses billions of dollars each year. These attacks can knock a business or web site offline in seconds by flooding their internet circuit with a large volume of unwanted network traffic. The traffic is typically distributed, coming from a wide range of sources - typically malware-infected devices (collectively referred to as a "botnet"). While the impact in terms of lost revenue is very high, the cost of carrying out such an attack is quite low and can be purchased on the dark web. The duration, number, and volume of these attacks rises every day. Businesses and web sites are at ever-increasing risk of being knocked off-line, unless they subscribe to Comcast DDoS protection.

With Comcast DDoS protection, customers can share in the benefit of the wide range of network resources that we have deployed in an effort to help stem the flow of malicious traffic. Comcast DDoS protection blocks malicious attacks so that normal traffic can flow normally, even under heavy load.

Comcast DDoS protection is made possible by a sophisticated landscape of network software and infrastructure. Protecting business assets involves a complex series of configuration steps that would be quite daunting if it weren't for the help of the DDoS Services Portal.

The DDoS Services portal (DSP) plays a key role in automating many of the steps involved in onboarding customers and configuring DDoS protection for those customers. While DSP gathers data from some sources, it makes DDoS data available to other applications as well. The DSP API provides a rich set of features that enable tools like MyAccount, Café, Einstein, and Customer Timeline to gather detailed information about attacks and services provided to stem those attacks.

The DDoS Services Portal is designed by the Comcast Cybersecurity Development team (CCS\_SDA\_DEV@comcast.com) and is used by a wide range of users, including CSA, commercial support teams, and indirectly by Café, Einstein 360, as well as subscribers to the service via the MyAccount portal.

**Chart #1**  
500 HIGH | 28 MEDIUM | 2 LOW

**Chart #2**  
4000 DDoS Attacks | 28 HIGH | 2 MEDIUM | 2 LOW

**Chart #3**  
234.08 PPS | 500 HIGH | 28 MEDIUM | 2 LOW

**Chart #4**  
183.24 MBps | 500 HIGH | 28 MEDIUM | 2 LOW

COMCAST CYBERSECURITY | Security Development and Analytics | #sda-dev-support | tps\_sda\_dev@comcast.com | Submit Feedback

**New Customer**

Use this form to sign up a new customer.

**SEARCH ACCOUNT NUMBER**

Account Number: 123456  
Next

**CHOOSE CIRCUIT**

Select	Name	EvcID	UM
<input type="radio"/>	Customer A	20 VLKP02048-CBCL	22-KFQ5-006191-CBCL
<input checked="" type="radio"/>	Customer A	12 VLKP02048-CBCL	22-KFQ5-006204-CBCL
<input type="radio"/>	Customer A	28 VLKP02048-CBCL	25-KFQ5-006009-CBCL

Next

**CHOOSE GRE TUNNEL**

Select	IP Address	Description	Region
<input type="radio"/>	68.85.15.129	sample description text	sample region
<input type="radio"/>	68.85.15.130	sample description text	sample region
<input type="radio"/>	68.85.15.131	sample description text	sample region

Next

**DDoS Services Portal**  
The power of DDoS, at your fingertips

Navigation: New Customer | View Customers | View Circuits | Manage GRE Tunnels

Total Alerts: There are 172 active threats

**Welcome to the DDoS Services Portal**

Distributed Denial of Service (DDoS) attacks cost businesses billions of dollars each year. These attacks can knock a business or web site offline in seconds by flooding their internet circuit with a large volume of unwanted network traffic. The traffic is typically distributed, coming from a wide range of sources - typically malware-infected devices (collectively referred to as a "botnet"). While the impact in terms of lost revenue is very high, the cost of carrying out such an attack is quite low and can be purchased on the dark web. The duration, number, and volume of these attacks rises every day. Businesses and web sites are at ever-increasing risk of being knocked off-line, unless they subscribe to Comcast DDoS protection.

With Comcast DDoS protection, customers can share in the benefit of the wide range of network resources that we have deployed in an effort to help stem the flow of malicious traffic. Comcast DDoS protection blocks malicious attacks so that normal traffic can flow normally, even under heavy load.

Comcast DDoS protection is made possible by a sophisticated landscape of network software and infrastructure. Protecting business assets involves a complex series of configuration steps that would be quite daunting if it weren't for the help of the DDoS Services Portal.

The DDoS Services portal (DSP) plays a key role in automating many of the steps involved in onboarding customers and configuring DDoS protection for those customers. While DSP gathers data from some sources, it makes DDoS data available to other applications as well. The DSP API provides a rich set of features that enable tools like MyAccount, Café, Einstein, and Customer Timeline to gather detailed information about attacks and services provided to stem those attacks.

The DDoS Services Portal is designed by the Comcast Cybersecurity Development team (CCS\_SDA\_DEV@comcast.com) and is used by a wide range of users, including CSA, commercial support teams, and indirectly by Café, Einstein 360, as well as subscribers to the service via the MyAccount portal.

**Chart #1**  
500 HIGH | 28 MEDIUM | 2 LOW

**Chart #2**  
4000 DDoS Attacks | 28 HIGH | 2 MEDIUM | 2 LOW

**Chart #3**  
234.08 PPS | 500 HIGH | 28 MEDIUM | 2 LOW

COMCAST CYBERSECURITY | Security Development and Analytics | #sda-dev-support | tps\_sda\_dev@comcast.com | Submit Feedback

# 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](mailto:sample_email@comcast.com).