AmLight ExP
Americas Lightpaths Express & Protect

Internet2 Technology Exchange - Sep 21st, 2023

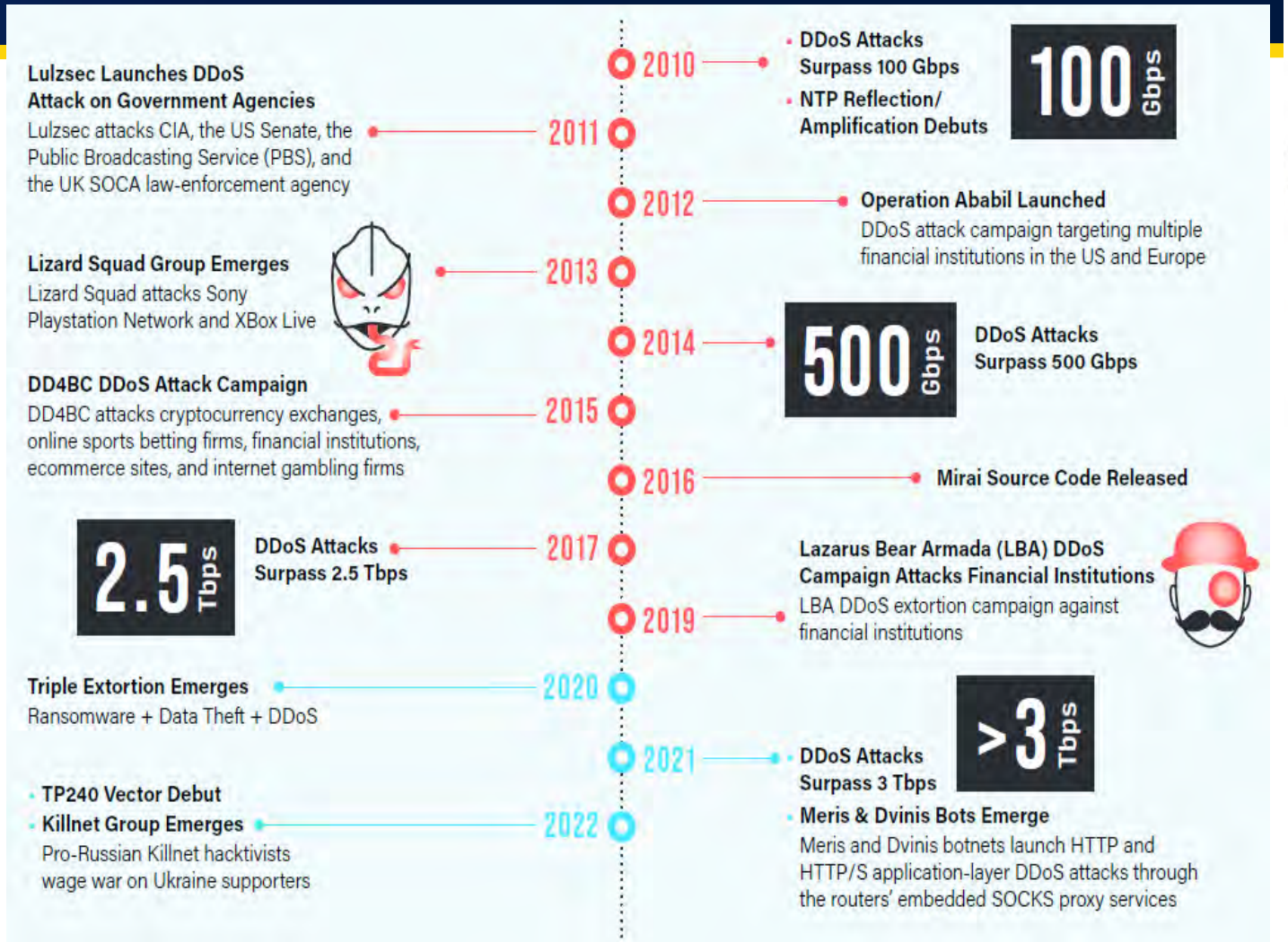
DDoS Detection/Mitigation @ AmLight

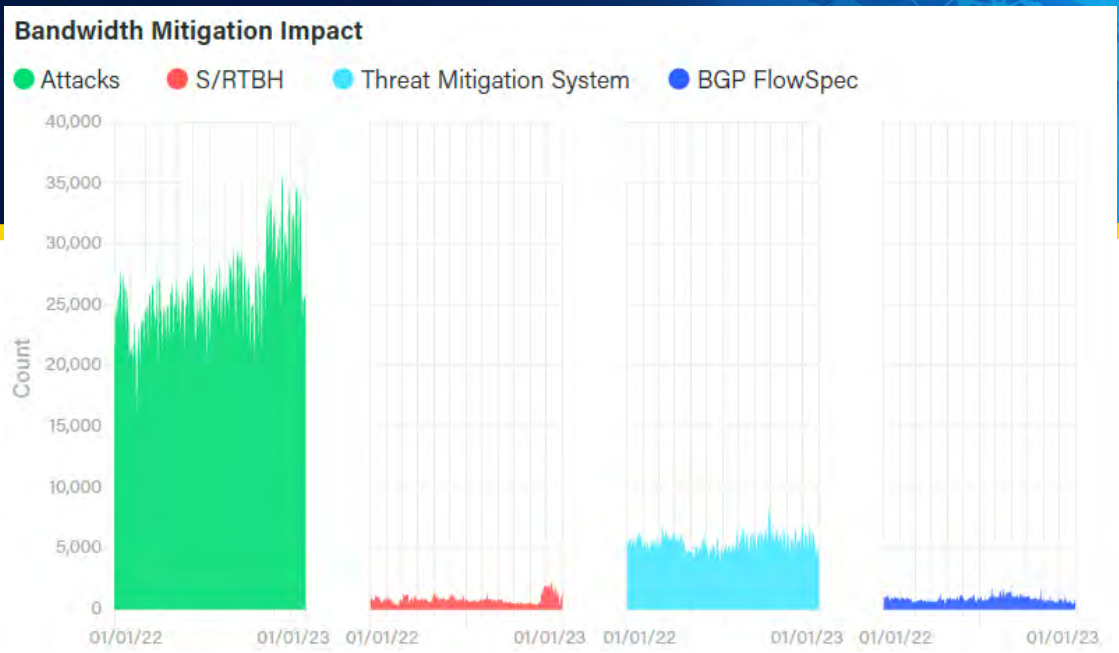
Renata Frez - Senior Network Engineer - RNP/AmLight

Overview

- Global DDoS Statistics
- Why do R&E networks need to be concerned about DDoS?
- Introduction to AmLight
- AmLight DDoS Detection/Mitigation Approach: 3 Tiers
- Tier 1 – The External/First Response – Pros/Cons
- Tier 2 – The Internal Response – Pros/Cons
- Tier 3 – The Community Response – Pros/Cons
- What Tier will we use in each situation?
- Tier 1 – DDoS Mitigation Report
- Tier 1 – Statistics
- Tier 2 – DDoS Detection Report
- Tier 2 – Statistics
- Challenges
- Future Work

Global DDoS Statistics [1]

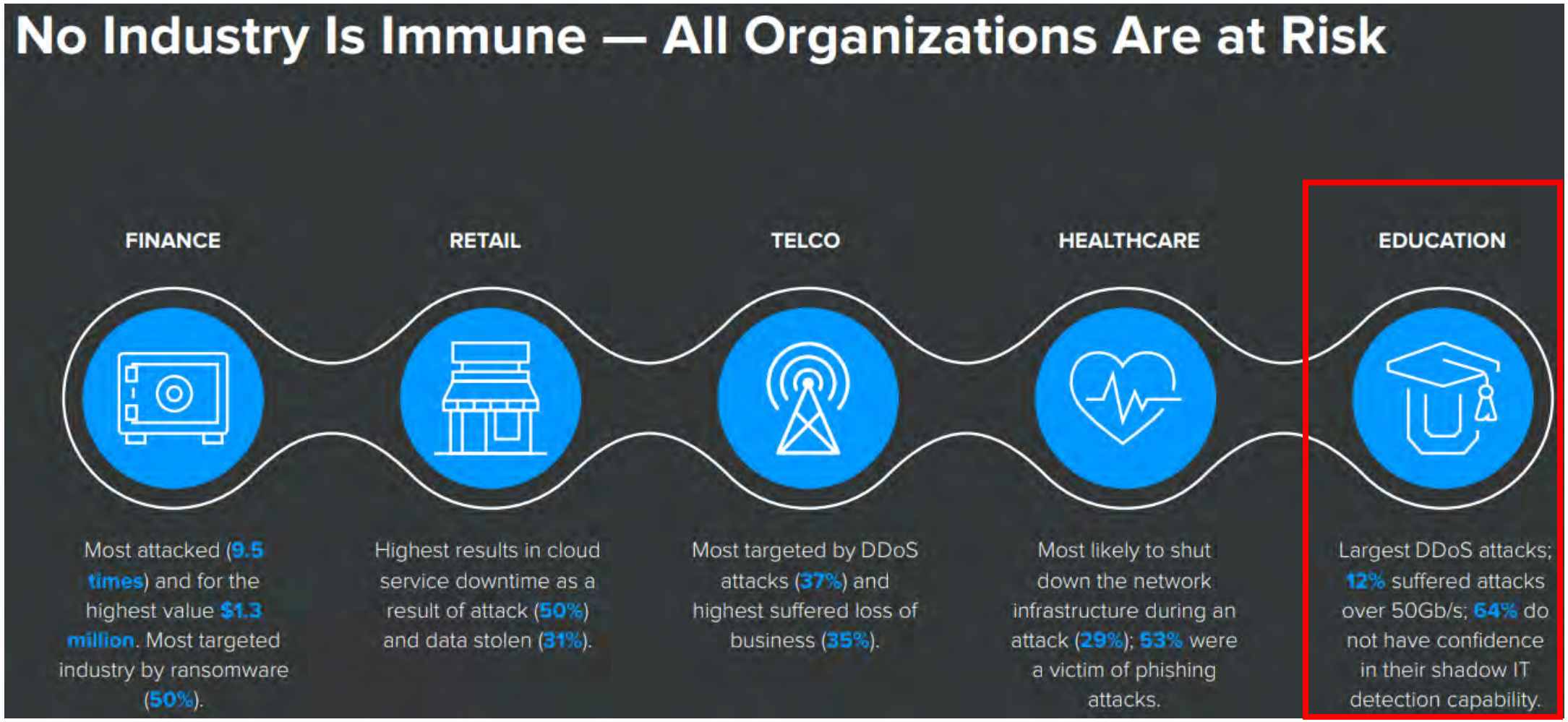




- Only 25% of customer alerts move into active mitigation.
- ISPs choose which alerts and traffic to mitigate balancing costs, capacity, and service disruption.

Reference: NETSCOUT 5th Anniversary DDoS Threat Intelligence Report – Findings from 2nd half 2022

Global DDoS Statistics [2]



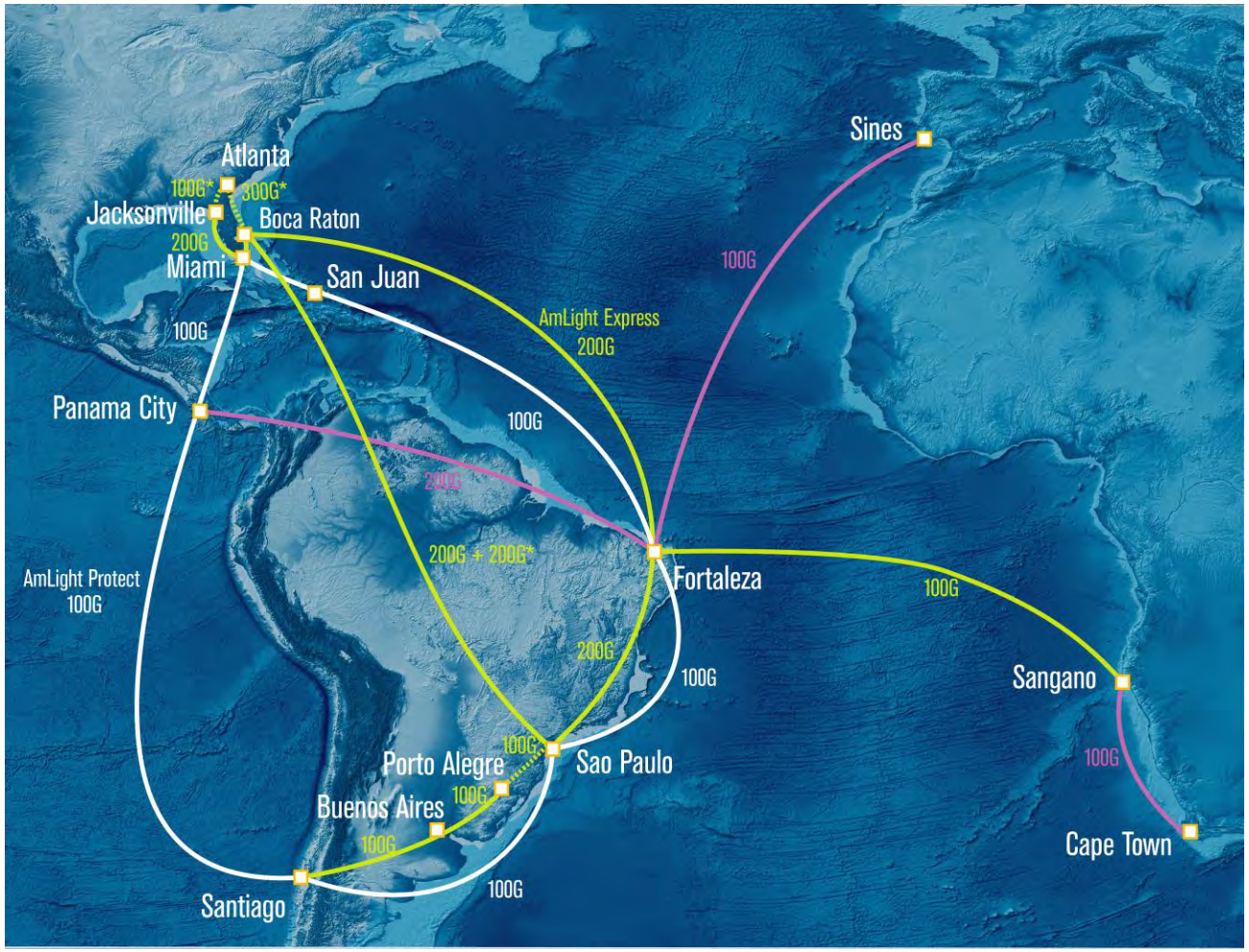
Reference: IDC efficient iP - 2022 Global DNS Threat Report

Why do R&E networks need to be concerned about DDoS?

- Commodity services to some institutions are only provided by R&E networks.
- Online classes and remote work increased commodity traffic.
- A DDoS attack could congest R&E Commodity links and affect all connectors.
- Even small attacks can completely block communication with some institutions.
- While the DDoS attack could have a massive impact on an environment, it could carry an even more significant threat: **Ransom DDoS attacks**.
  - An RDDoS attack uses the well-known DDoS attack, but the objective of the criminals is to extort an organization.

Introduction to AmLight [1]

- AmLight Express and Protect (AmLight-ExP) (NSF IRNC program).
- NAPs: USA(3), Brazil(2), Chile, Puerto Rico, Panama, and South Africa.
- Academic connections:
  - 600Gbps of Academic upstream capacity between the U.S. and Latin America, and 100Gbps to Africa.
- Commodity connections:
  - 2 Upstreams: NTT and TISparkle.
  - 2 Peerings: Equinix and FL-IX.



Introduction to AmLight [2]

- Academic exchange point built to enable collaboration between Latin America, Africa, and the United States.
- Supported by NSF, OAC, and the IRNC program through 2021-2025 award #OAC-2029283.
- Partnerships with R&E networks in the US, Latin America, the Caribbean, and Africa, built through layers of trust and openness, sharing:
  - Infrastructure resources
  - Human Resources

AmLight ExP
Americas Lightpaths Express & Protect
(NSF Award # OAC-2029283)

NSF

AMLIGHT

FIU
FLORIDA INTERNATIONAL UNIVERSITY

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

ansp

rednesp

Red CLARA

RedCLARA
Ciencia y Educación en Red

AURA

TENET
Tertiary Education and Research Network of South Africa

SANReN
South African National Research Network

FLR
Florida Lambdarail
Network Operations Center
University of Florida

INTERNET2

Evaluating DDoS Detection/Mitigation Solutions

- Questions done before choosing our tools:
  - Is it provided by one of our Upstreams?
  - Does the tool support Detection and/or Mitigation?
  - Is it cloud-based or requires on-premises devices?
  - What kind of mitigation does it support?
  - Does the mitigation happen internally or externally?
  - Does the mitigation can be triggered manually and automatically?

AmLight DDoS Detection/Mitigation Approach: 3 Tiers

Tier 1

DPS MAX

- Tool provided by NTT, one of our Upstreams.
- External detection and mitigation.

Tier 2

Kentik

- A cloud-based tool that communicates with our internal Routers.
- External detection and Internal mitigation. (Mitigation under deployment)

Tier 3

Unwanted Traffic Removal Service (UTRS)

- A free peer-to-peer defense against DDoS provided by Team Cymru. (Under deployment).
- Internal detection and External mitigation.

Tier 1 – The External/First Response - Pros

- It executes a traffic cleaning. Since it runs outside our environment, an attack does not affect our link.
  - The mitigation can be started automatically or manually.
  - It doesn't require much knowledge about DDoS by the Network Engineers.
  - No on-premises devices are required.

Figure Reference: https://www.psychz.net/client/blog/en/serious-new-ddos-attack-method-surfaces-threatens-internet-providers-businesses.html

Tier 1 – The External/First Response - Cons

- Available on only one Upstream.
- For small but long attacks, the cost could exceed the benefits. In this case, the mitigation could be handled internally.
- The threshold customization is not straightforward. It requires acting from our provider.
- It is hard to find a good balance for the thresholds.
  - Decreasing the thresholds could lead to unexpected costs.

Tier 2 – The Internal Response - Pros

- Addresses the pitfalls from Tier 1.
- It's a Cloud-based solution.
  - It creates a database using Netflow samples, SNMP counters, and BGP information. Uses AI to create a baseline.
- Easy customization of a policy (detection and mitigation).
- It pushes instructions using BGP FlowSpec to our internal routers.
- The instruction can be directed to the destination IP or to only some signatures, like Destination Port, Protocol, TCP Type, etc.

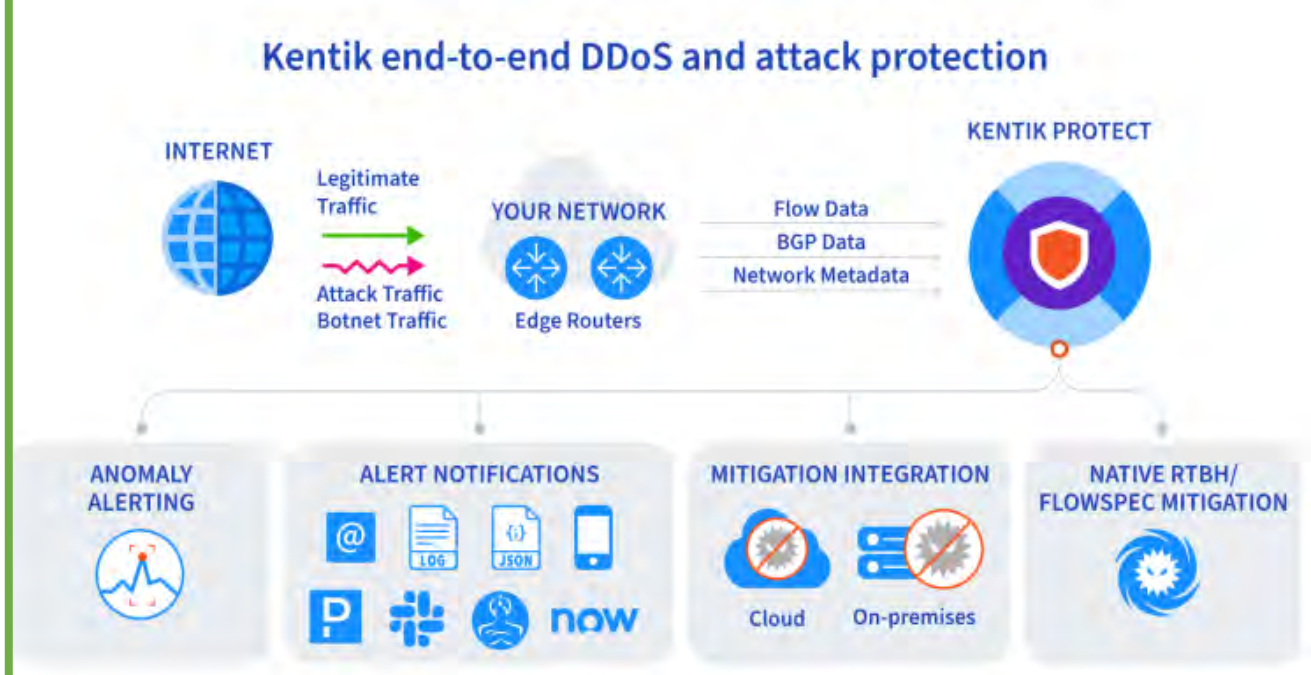


Figure Reference:
https://www.kentik.com/blog/secure-your-network-against-attacks-prevent-detect-mitigate-cyberthreats/

Tier 2 – The Internal Response - Cons

- The mitigation occurs inside the AmLight network. The malicious traffic could impact our links.
  - For more significant attacks, our links can be congested and affect the connection with the Cloud-based tool.
- Due to the higher number of customizable signatures to detect an attack, Tier 2 adds a new layer of complexity.
- The BGP FlowSpec, chosen by the AmLight team as the mitigation approach, doesn't clean the malicious traffic, i.e., the traffic will be dropped or limited, "contributing" to the attackers (for the greater good).

Tier 3 – The Community Response - Pros

- UTRS 2.0: No-cost tool provided by Team Cymru to the Internet community. "You help your neighbor, and they help you."
  - It has 1,300+ network operators around the world.
- Validates an attack announcement sent by an operator before sending it to others.
- The attack announcement triggers a response from the community, blocking the traffic to the destination of the attack and mitigating it closer to the source.

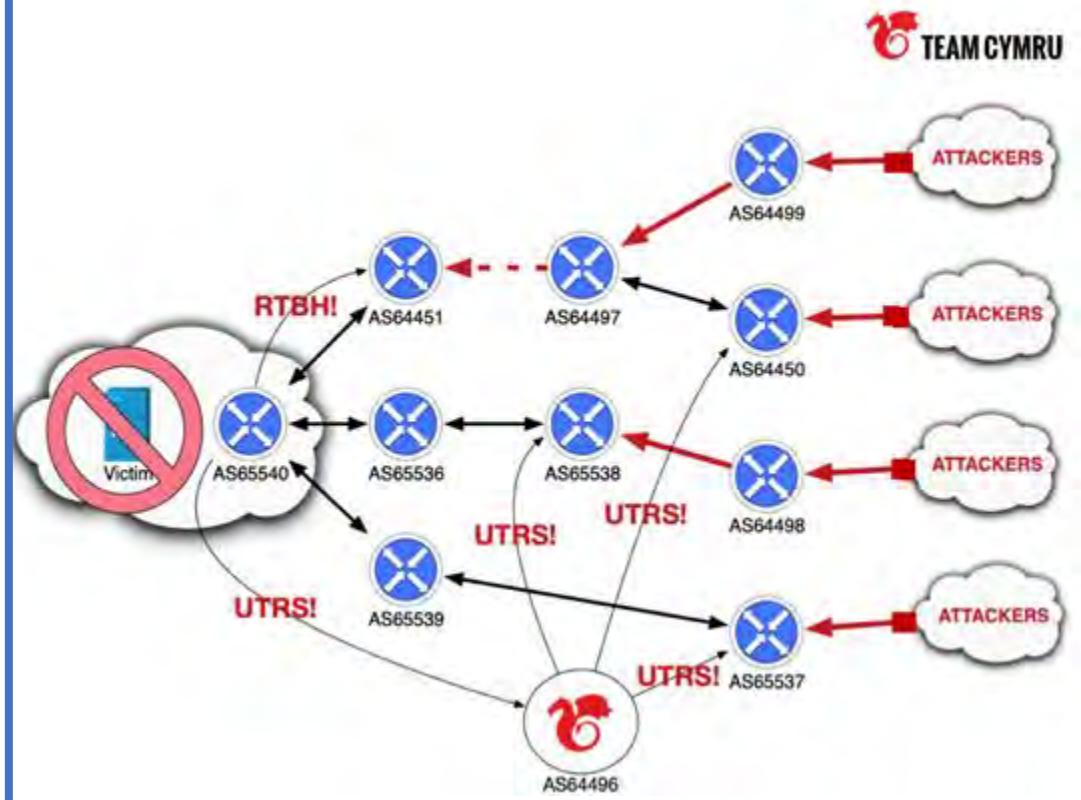


Figure Reference: Team Cymru - UKNOF47 - https://indico.uknof.org.uk/event/53/contributions/774/attachments/1002/1449/NimbusTM%20Presentation.pdf

Tier 3 – The Community Response - Cons

- The detection must be done internally, and an announcement must be made to the community.
- Since it is not an automatic process, some time is required to automate the functions and ensure no false positives will be announced.
- The mitigation will occur on the Internet community, so all the traffic to the destined host will be dropped, sacrificing the host to keep the infrastructure running.
- Only protects the prefixes that belong to our ASN. It doesn't protect our connectors.

What Tier will we use in each situation?

Tier 1

- Large/Medium attacks.
  - Attacks destined for a host that can't face downtime.
  - Situations where the malicious traffic has to be cleaned.

Tier 2

- Medium/Small attacks.
  - More specific policies.
  - Attacks destined for a host where the partial/total traffic can be blocked for "the greater good".

Tier 3

- Large/Medium/Small attacks.
  - Since it is a new solution, it requires testing to automate the detection process.
  - Attacks destined for a host where the whole traffic can be blocked.

Tier 1 – DDoS Mitigation Report

Mitigation Details

Print

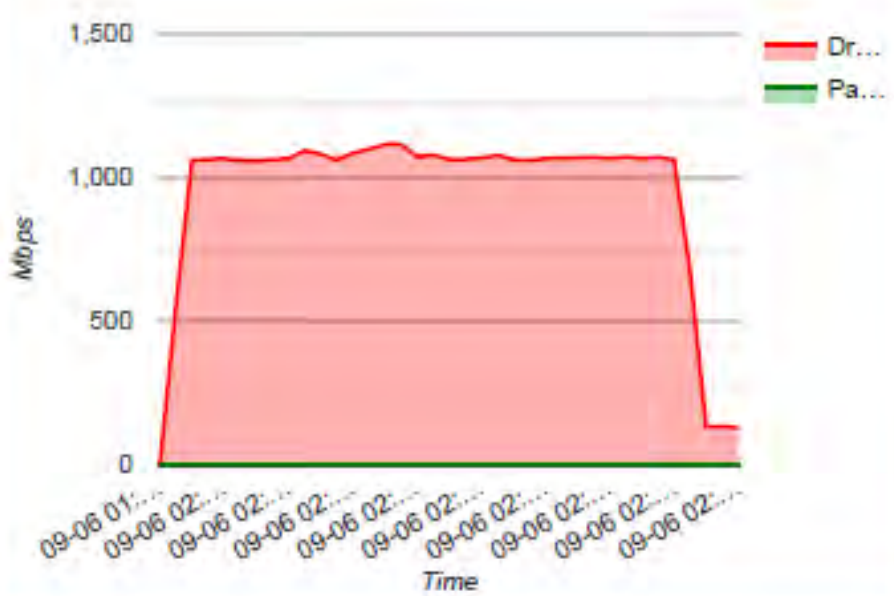
tms-93373 - Alert 5291495 IPv4 Auto-Mitigation

Mitigation ID:	tms-93373
Name:	Alert 5291495 IPv4 Auto-Mitigation
Managed Object:	[redacted]
IP version:	4
Prefix:	[redacted]
Start Time (UTC):	06-Sep-23 01:56:56
Stop Time (UTC):	06-Sep-23 02:33:40
Alert ID:	5291495

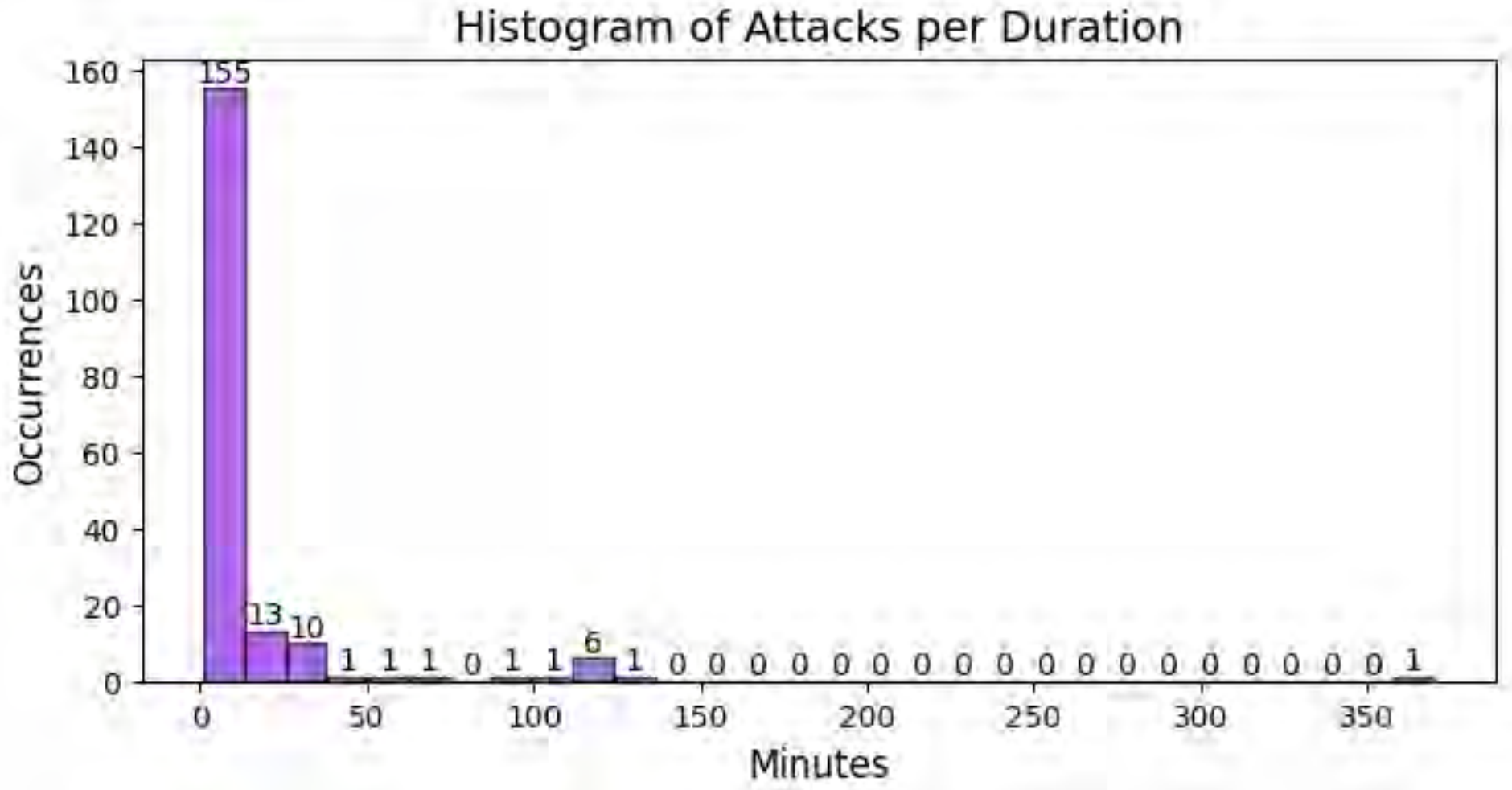
Countermeasures

	Status	Countermeasure
+	OFF	Zombie Detection
+	ON	IPv4 Black/White List
+	OFF	DNS Scoping
+	ON	TCP SYN Authentication
+	ON	TCP Connection Reset
+	OFF	TCP Connection Limiting
+	OFF	IP Location Filter List
+	ON	UDP Reflection/Amplification Protection
+	ON	SIP Malformed
+	ON	DNS Regular Expression

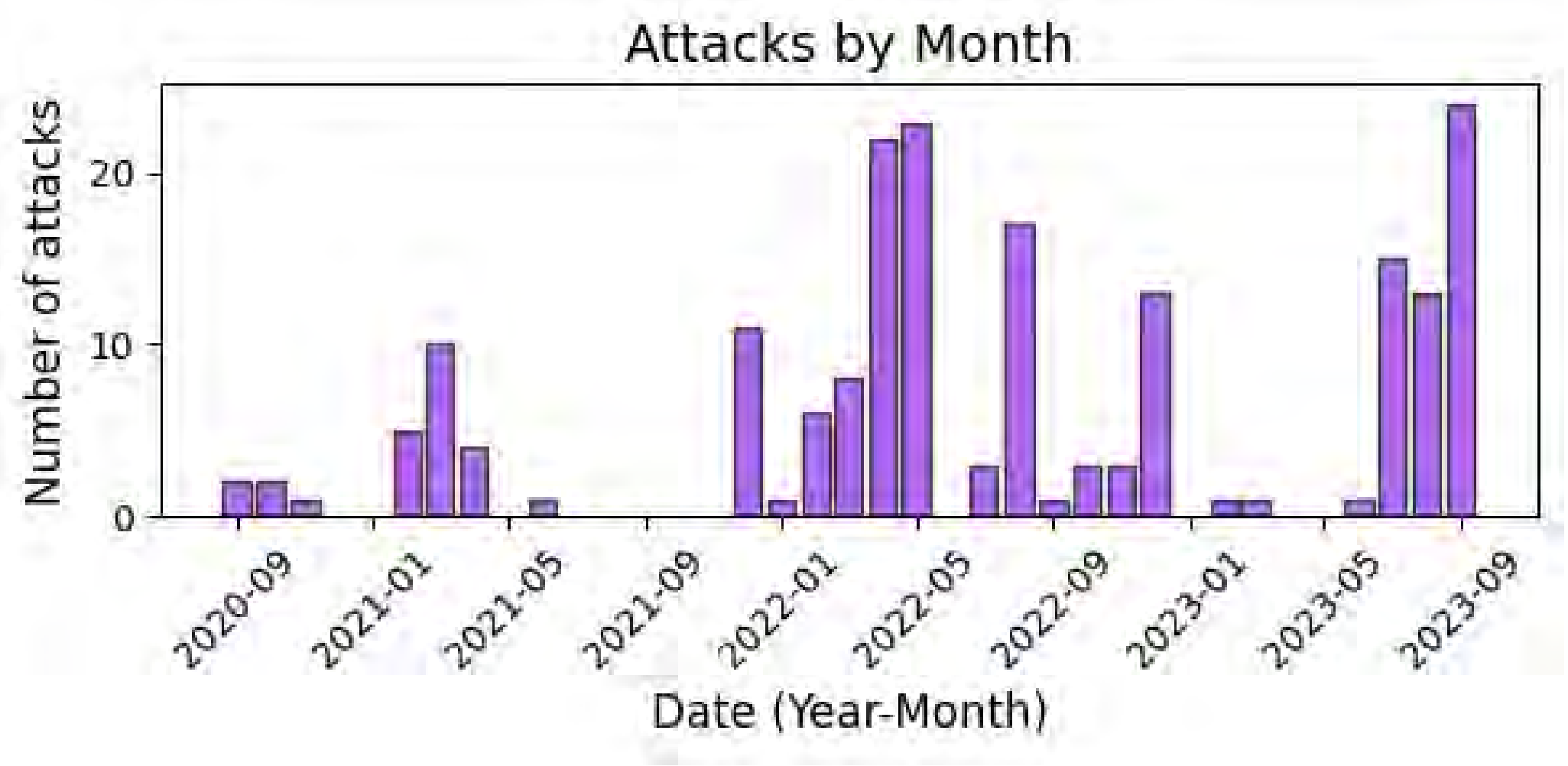
Drop/Pass Mbps



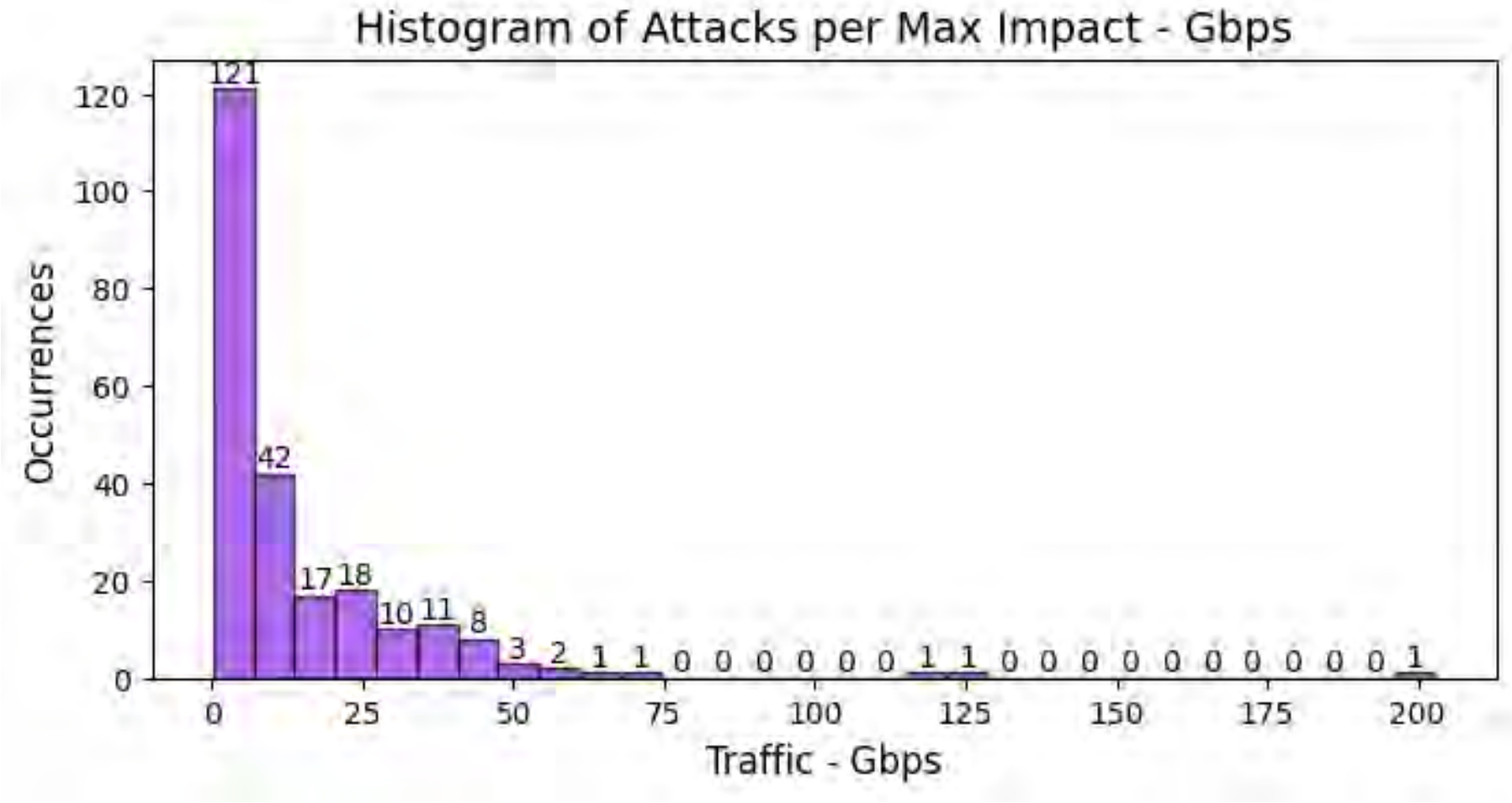
Tier 1 – Statistics [1]



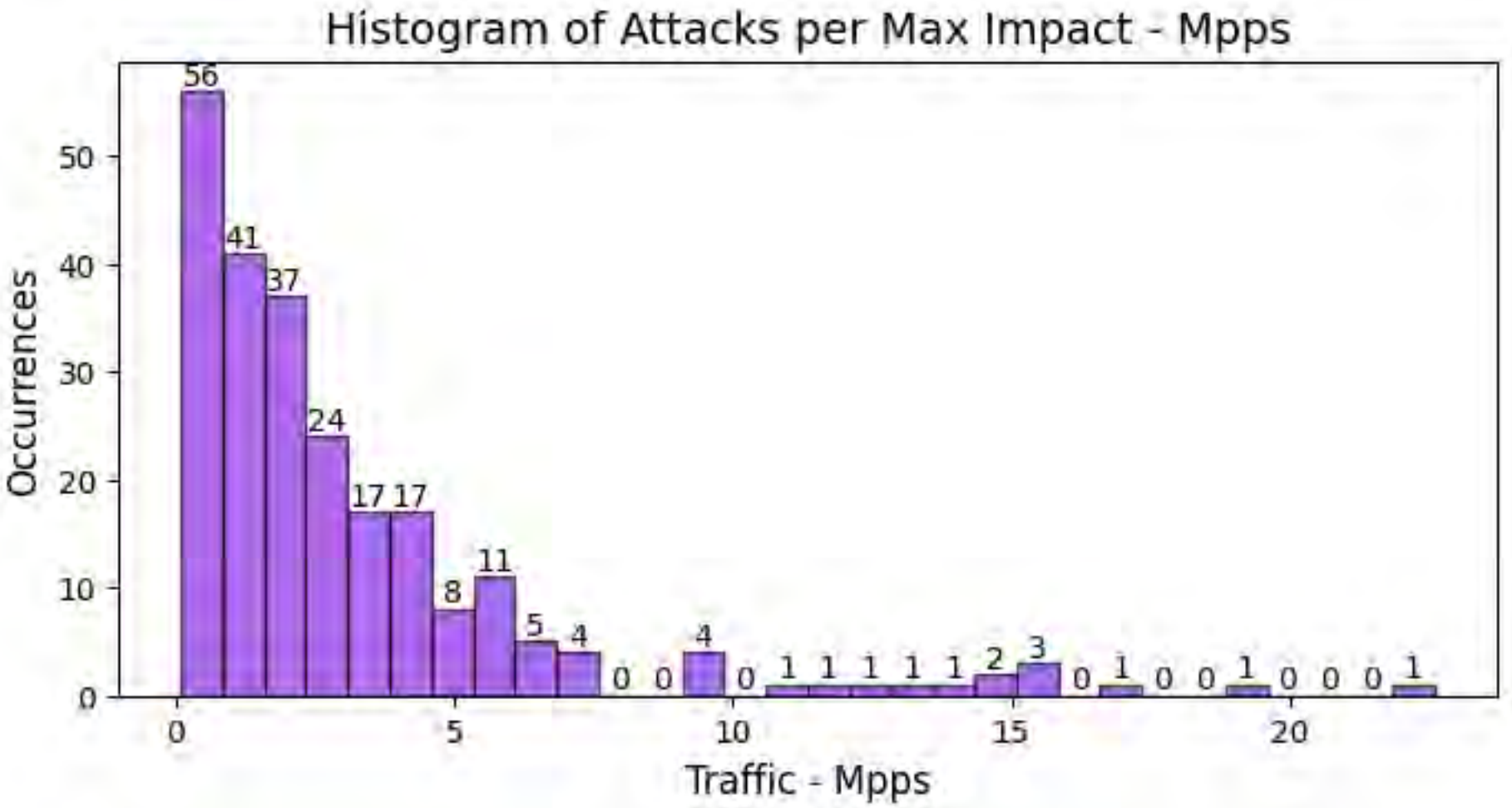
Tier 1 – Statistics [2]



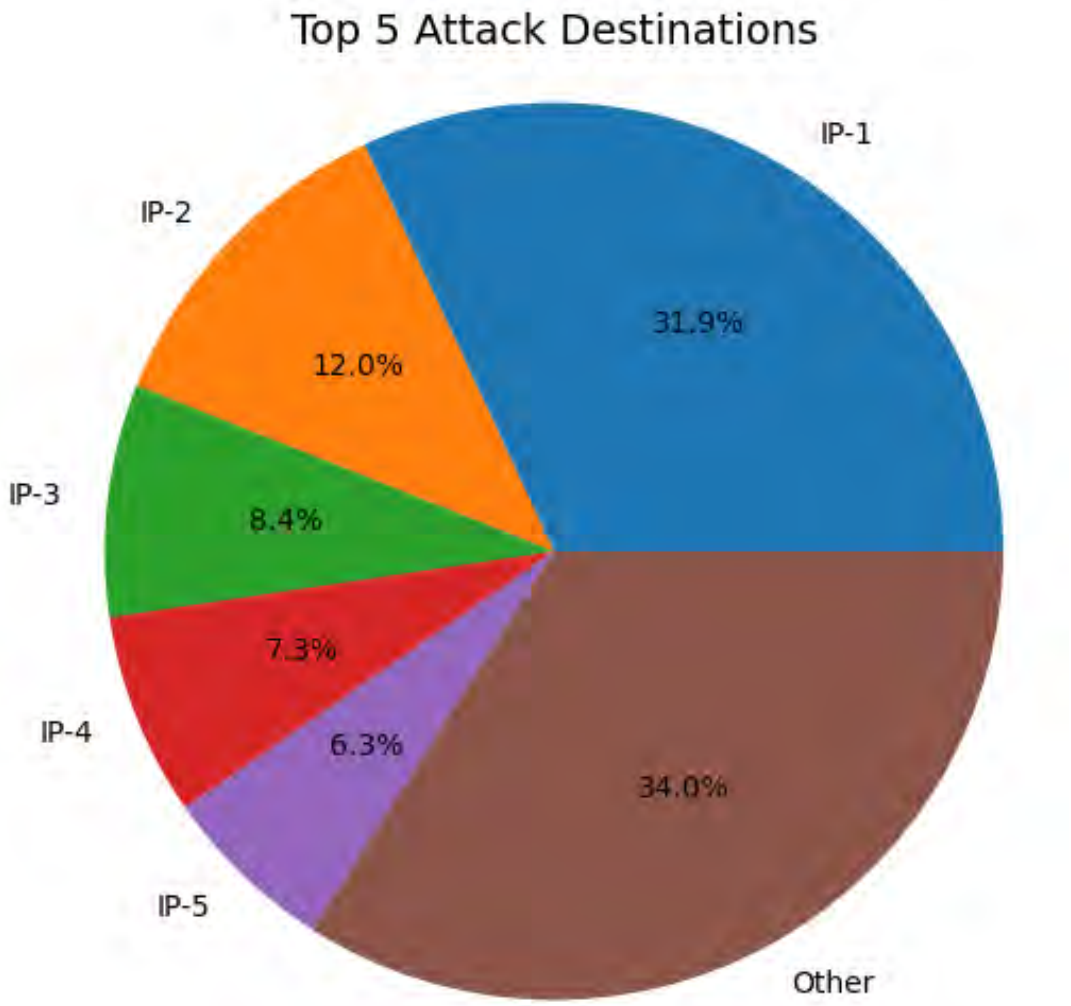
Tier 1 – Statistics [3]



Tier 1 – Statistics [4]



Tier 1 – Statistics [5]



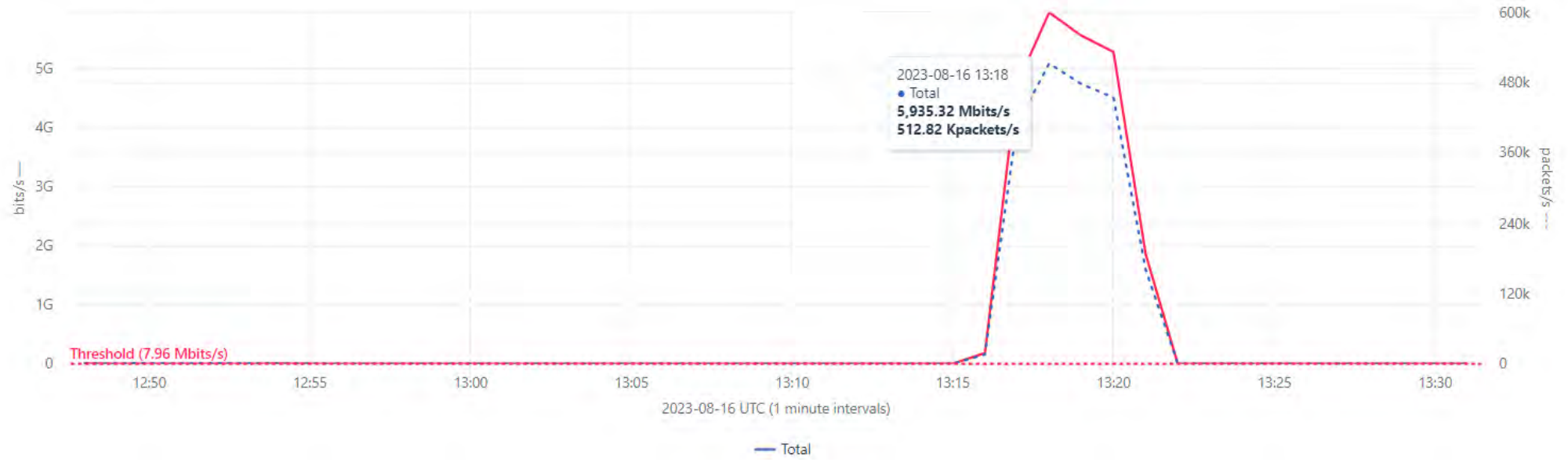
Tier 2 – DDoS Detection Report

DDoS: Amplification Reflection Attack

Reflection attacks exploit unsecured networks and unauthenticated, connectionless services that reply to requests without validating that the host in the source address field of the IP header is truly making the request. Amplification at... **Show More**

Src Port	Dest IP/CIDR			
53	[redacted]	**5.33** Gbits/s	**461.14** Kpackets/s	**7k** Unique Src IPs
		5.32 Gbits/s above threshold		6k Unique Src IPs above threshold

Alert | Ingress Interfaces | Traffic Patterns | Source Countries | Source Services | Packet Size Distribution



Severity
Major

Alert Start Time
2023-08-16 13:18

Event End Time
2023-08-16 13:22

Alert End Time
2023-08-16 13:32

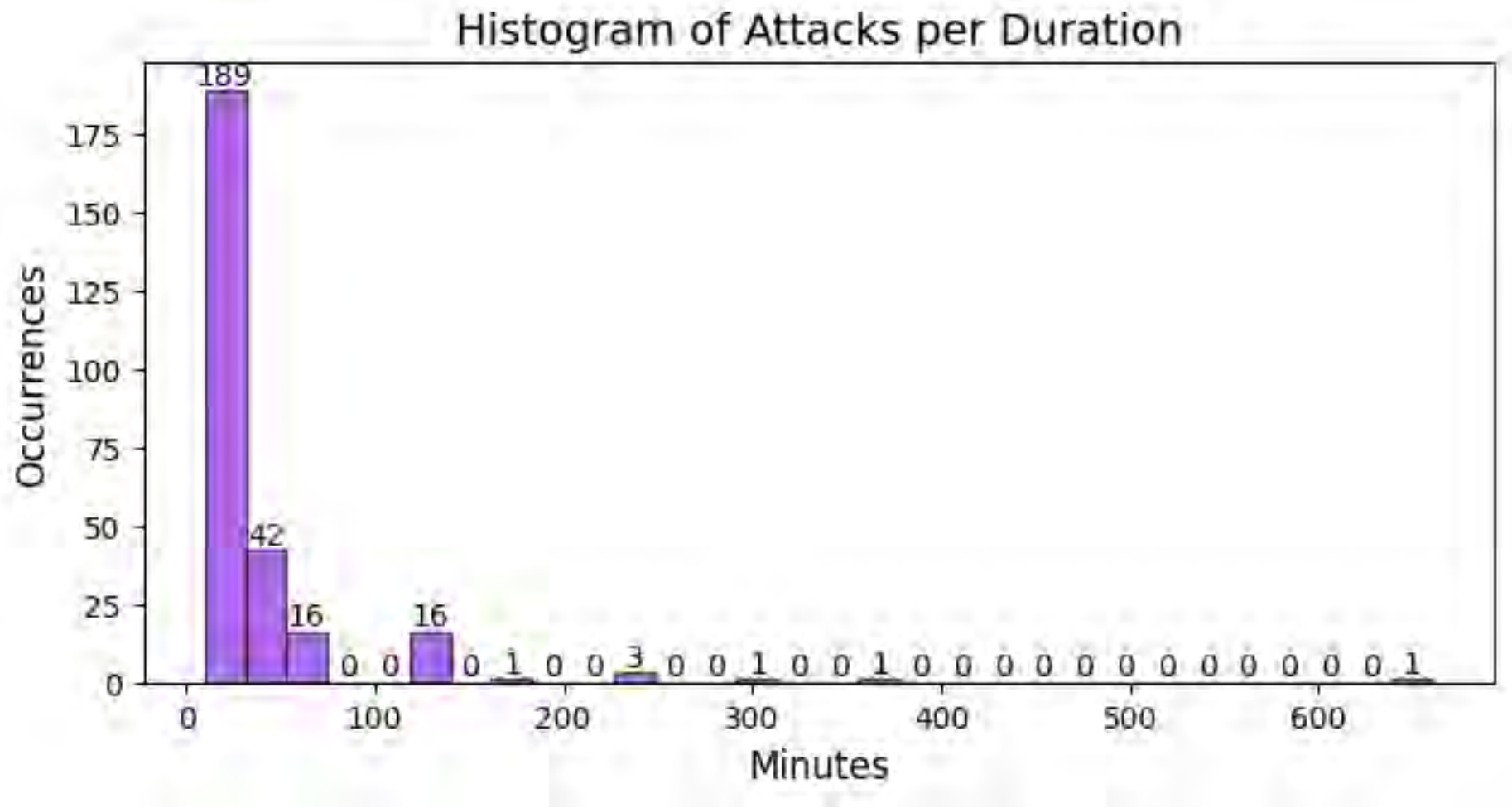
Status
Cleared

Alert ID
284995754

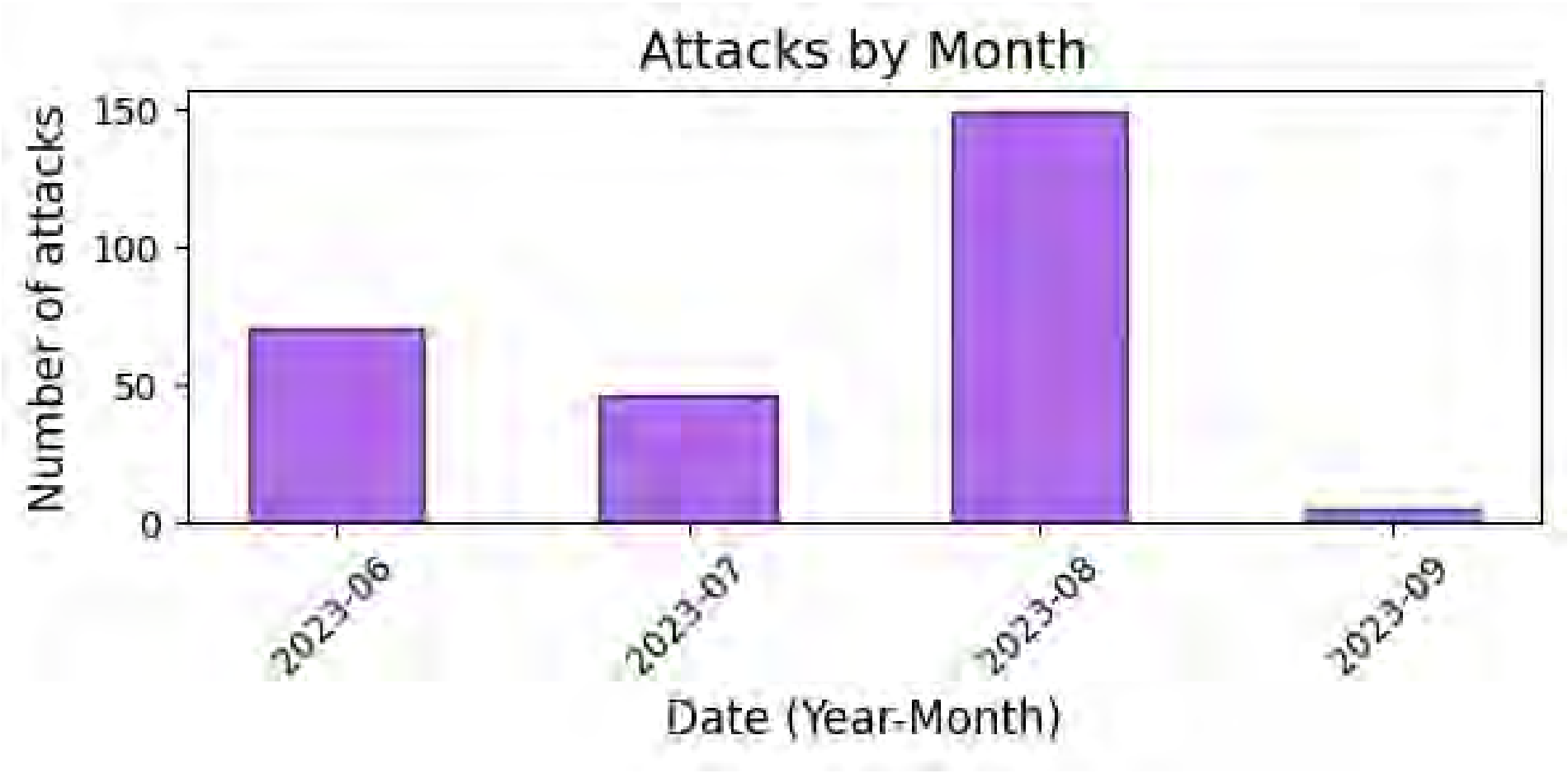
Policy
DDoS: Amplification Reflection Attack

Frequency
This alert has happened roughly 2x per day in the last 30 days
Show all Occurrences

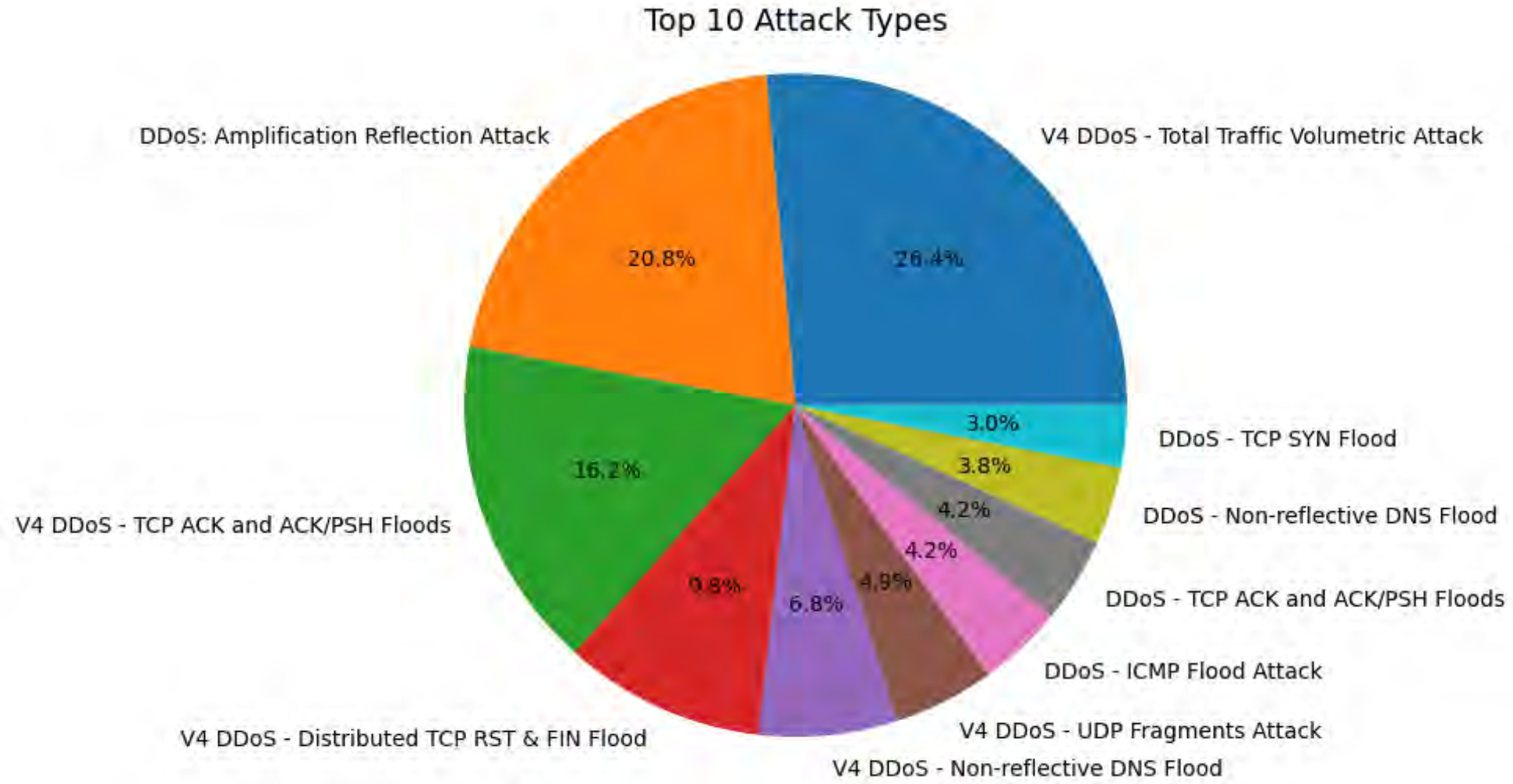
Tier 2 – Statistics [1]



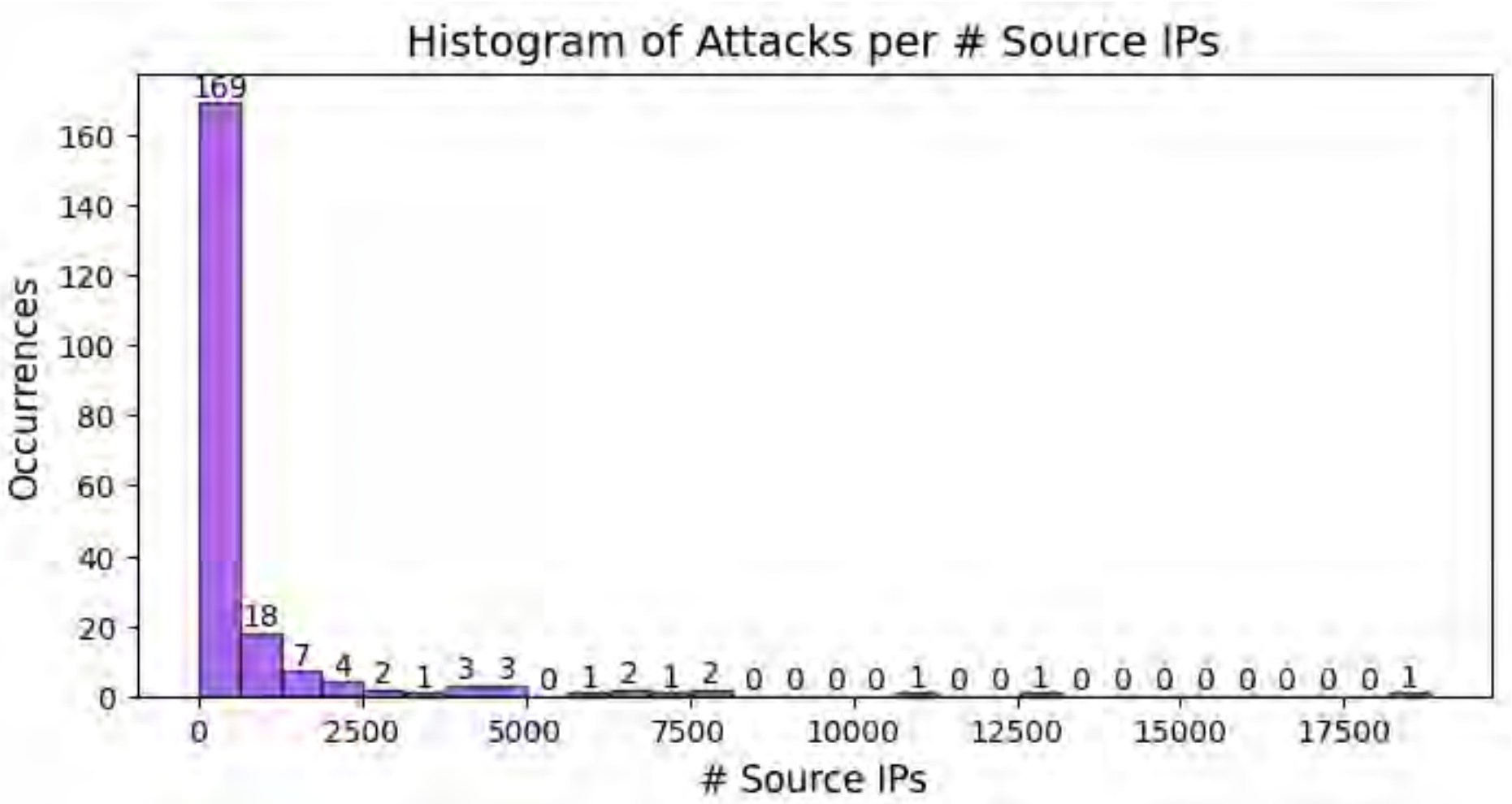
Tier 2 – Statistics [2]



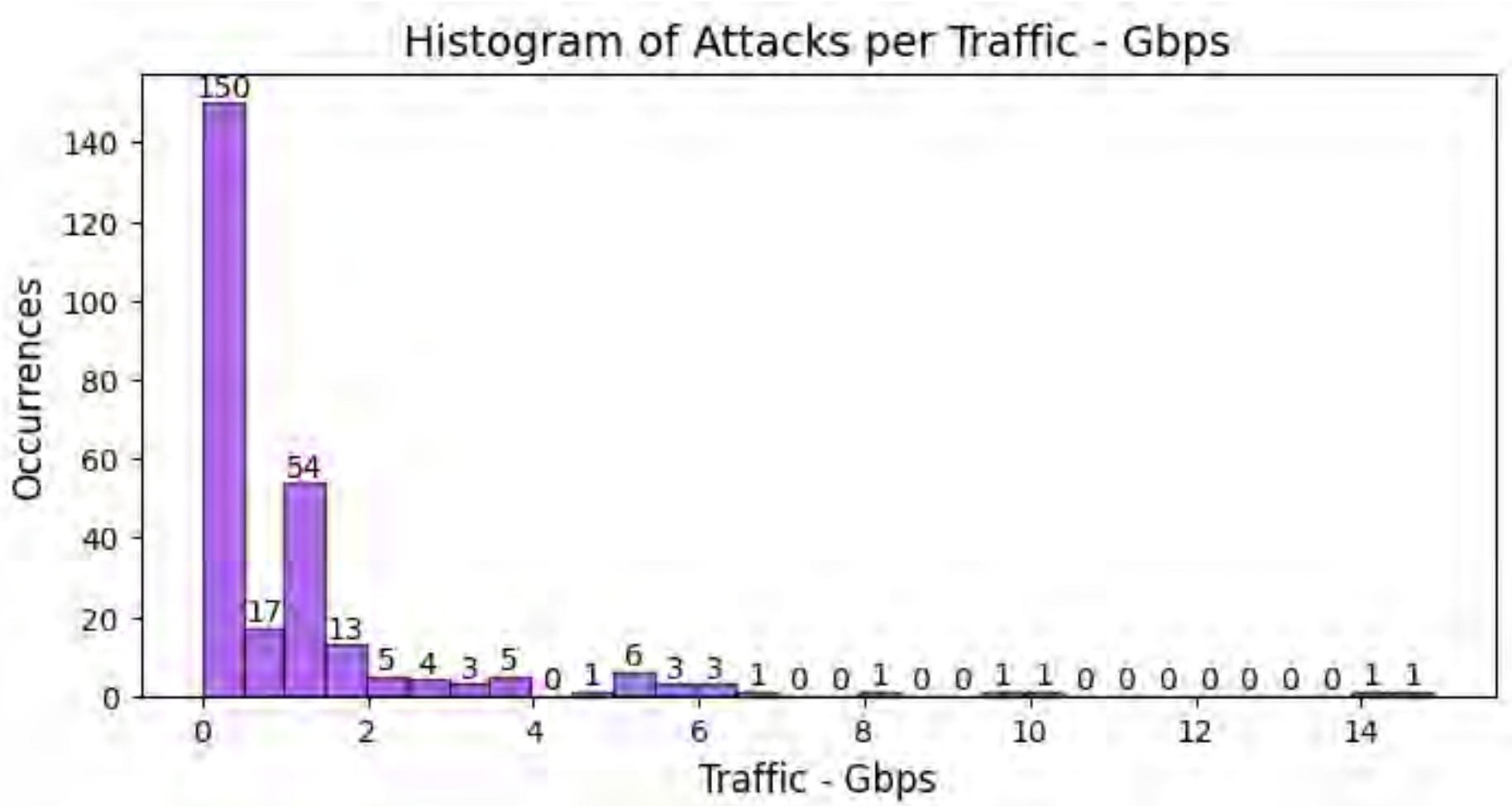
Tier 2 – Statistics [3]



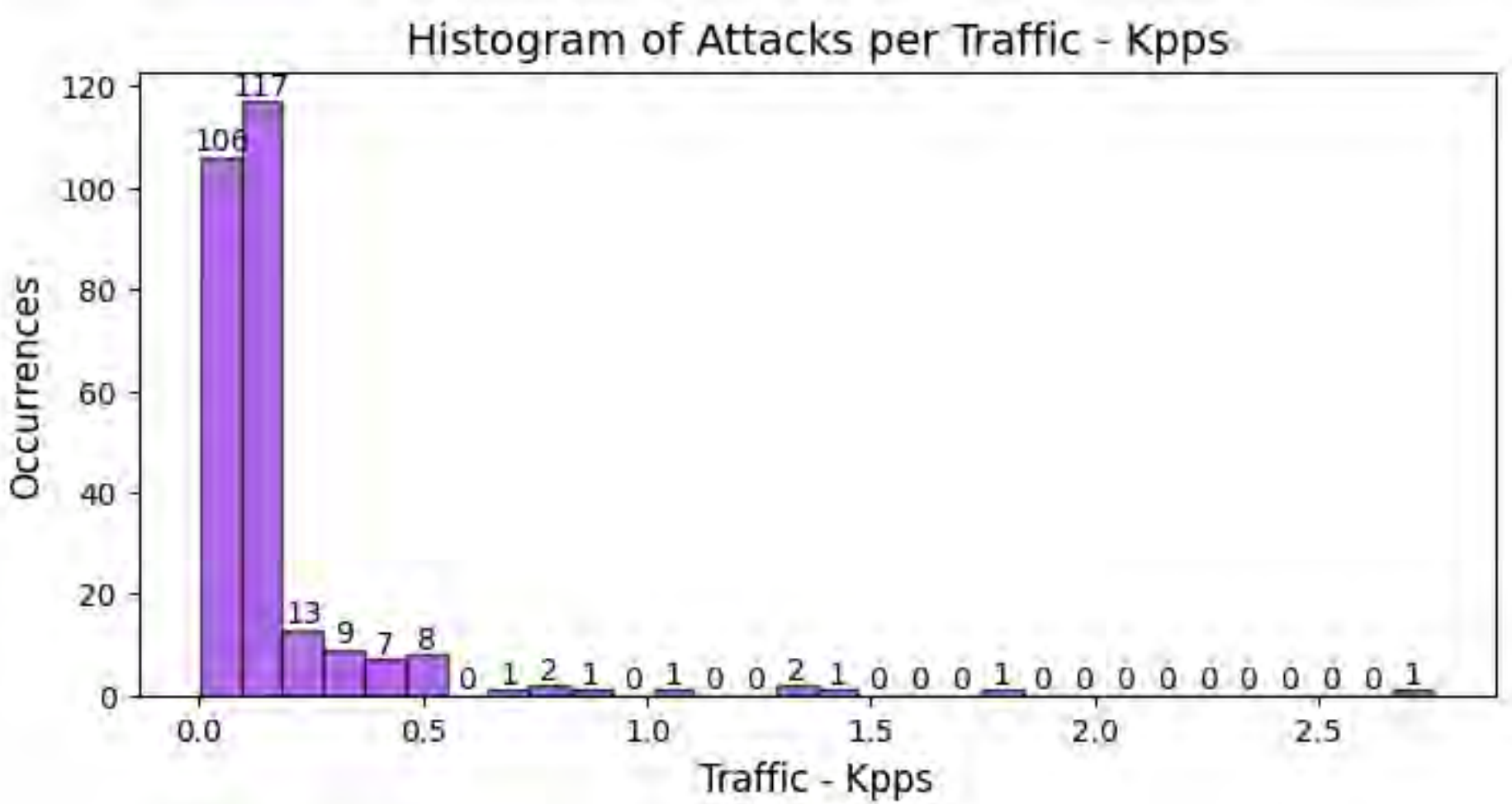
Tier 2 – Statistics [4]



Tier 2 – Statistics [5]



Tier 2 – Statistics [6]



Challenges [1]

- How will we merge the 3-tier proposal without causing any issues to the connectors and avoiding increasing costs?

- What are the optimal thresholds for each connector and type of attack?
  - High diversity on the connectors links' capacity.
  - Not all the connectors and institutions have a security device on their side.

- Science traffic can be deceiving! Some experiments have similar signatures as those of a DDoS attack. For example:
  - High throughput could come from different servers during a data transfer.
  - New security features testing.
  - Sparse traffic.

Challenges [2]

- How can we avoid false positives, especially when using AI to create the baseline?
- How can we ensure we can block all the traffic to a destined host without causing more issues to the destination?
  - Some attacks are destined for critical services, such as DNS, VPN, Firewall, etc.
  - If we block all the traffic, “we will help the attacker.”

Challenges [3]

- How can we engage the community to help us?
  - How the attack notification will take place?
  - Will we start mitigation automatically or wait for the connectors to give us a “good to go”?
  - Since most institutions are not connected directly to the AmLight network, how can we engage those partners?

- Tier-2, Kentik, enables tenants.
  - Our connectors could analyze their information and ask us to build a policy as they wish.

Future Work

- Enable Tier-2 for mitigation using BGP FlowSpec.
- Implement Tier-3.
- Enable DNS inspection.
- Engage our community to gather more information about our connectors' needs.

DDoS Detection/Mitigation @ AmLight

Renata Frez - Senior Network Engineer - RNP/AmLight