Cyber Risk Meetup

DEV SEC OPS | CYBER RISK MEETUP

DEVSECOPS MELBOURNE

6pm to 6.30pm
Networking & Refreshments

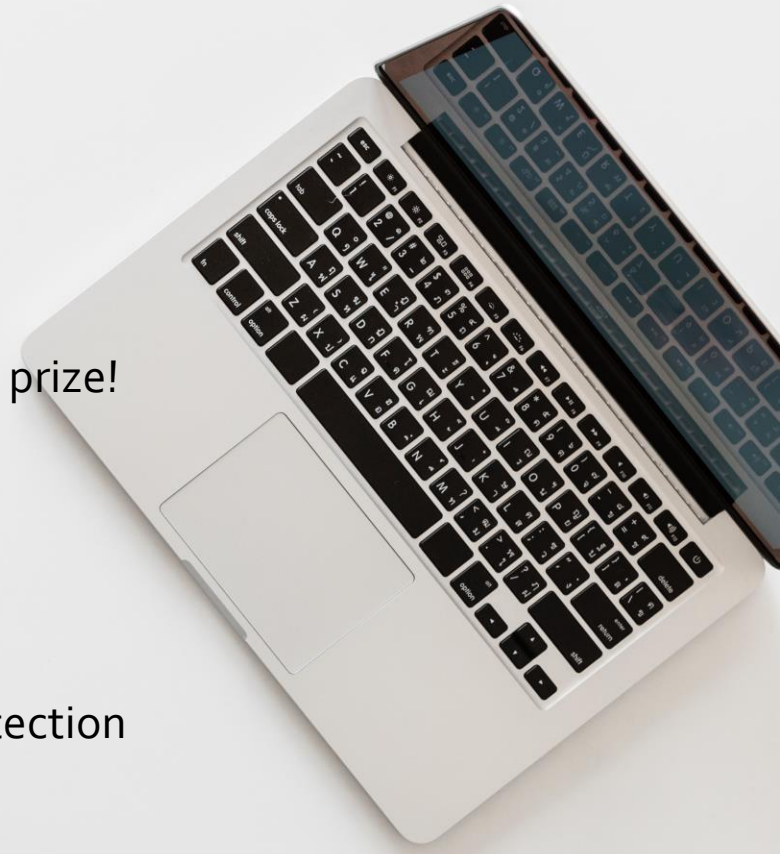
6.30pm to 6.35pm
Welcome opening and introduction

6.35pm to 6.45pm
10 mins Special on CISO Insights +
Opportunity to win an autographed Cyber Risk Leaders book prize!

6.45pm to 7.15pm
The Role of Cybersecurity in Scaling DevOps

7.15pm to 7.45pm
New Approaches to Achieve Automated AI-based Threat Protection

7.45pm to 8.30pm
Closing & the networking continues!



ORGANISER

HOST

Microsoft

SPONSOR

INTERNATIONAL PARTNER

Privasec

RED

RED TEAMING &
ADVANCED ETHICAL
HACKING

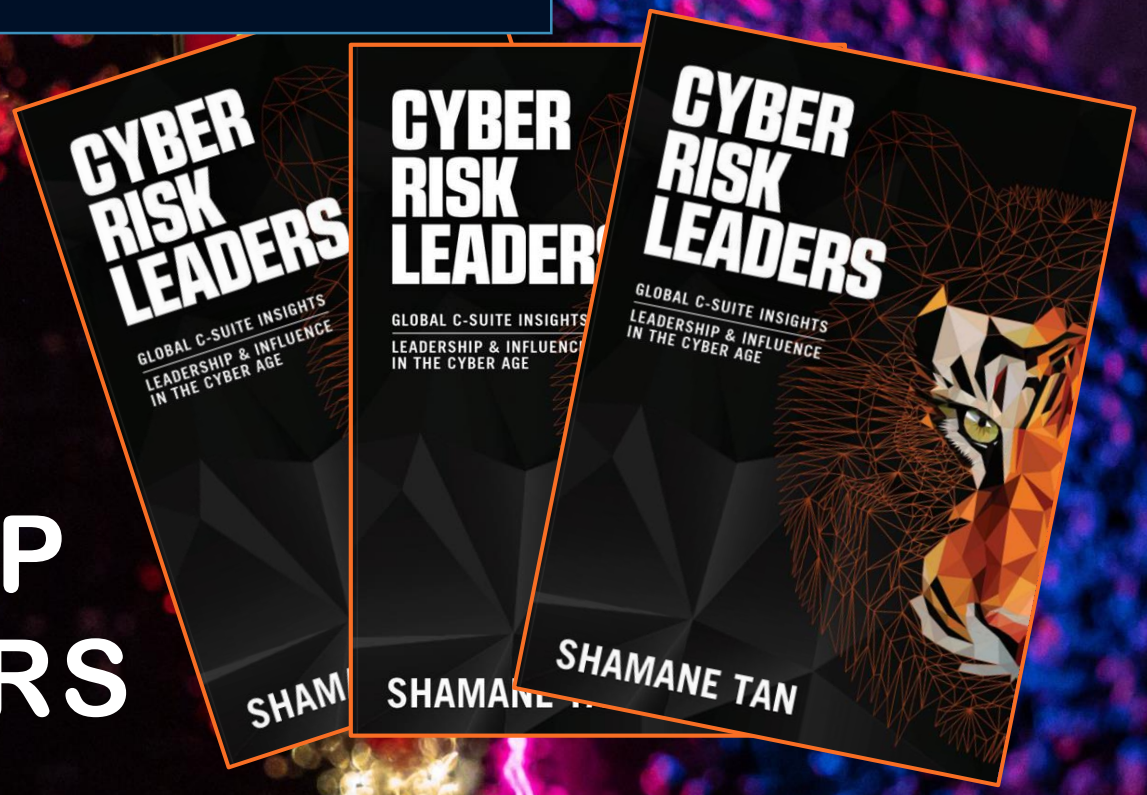
GRC

GOVERNANCE
AND INFORMATION
SECURITY PARTNERS

DRONE SEC

SECURITY
HACKING
HARDENING

PRIZE GIVEAWAY!



#CYBERRISKMEETUP
#CYBERRISKLEADERS

WWW.CYBERRISKMEETUP.COM

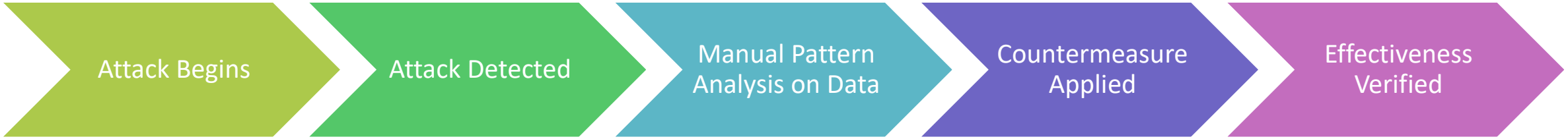
New Approaches to Achieve Automated AI-based Threat Protection

Tim Blombery – Sales Manager, ANZ

Reliable Security Always™

Reducing the Meantime to Mitigation

Manual DDoS Mitigation Workflow Takes Too Long



- Attack detected > minutes to hours
- Attack data is analyzed for patterns > first attempt
- Counter-measures are applied
- Verify for success > Try again if required

Problems with the DDoS Mitigation Workflow

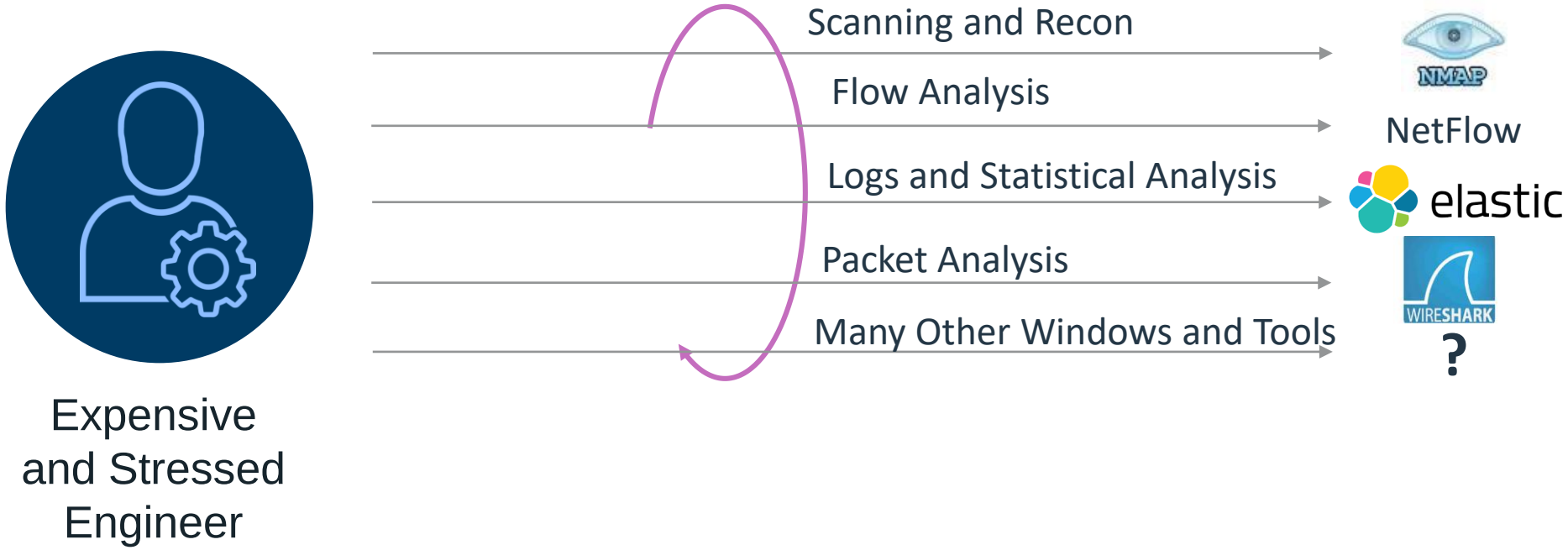
It takes far too long to detect the attack

Manual pattern analysis is costly and takes too long

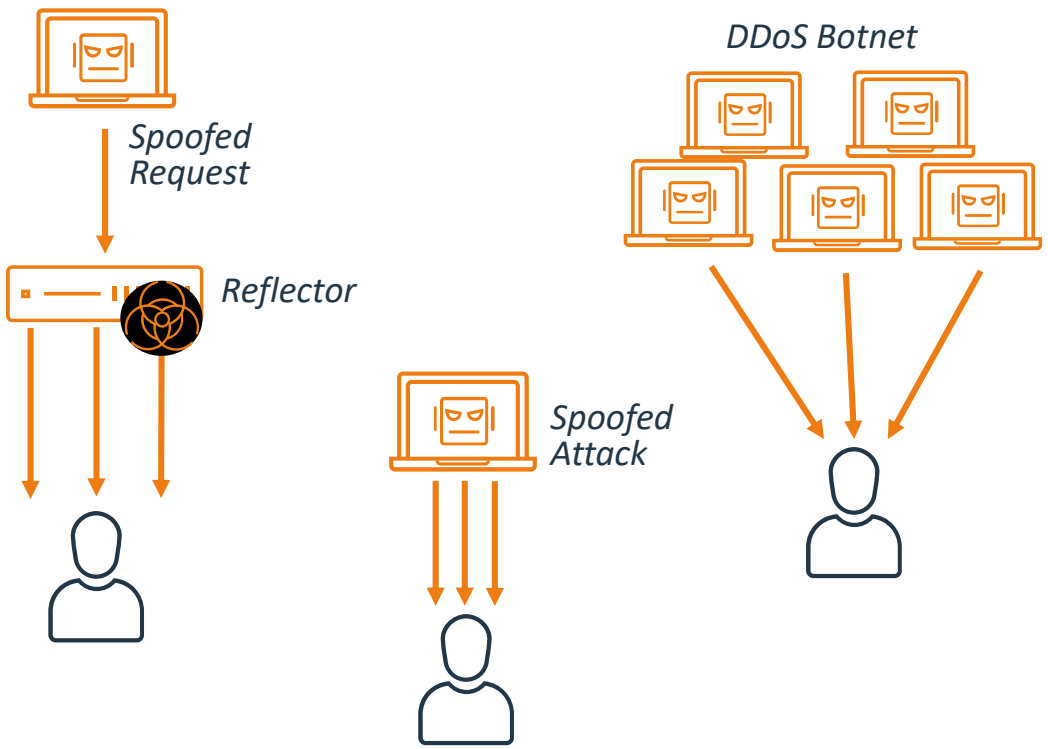
Too much trial and error occurs before the mitigation is successful

High collateral damage due to trial and error

Attack Forensics During Wartime



Rapidly Detecting Greed and Automation is the Key



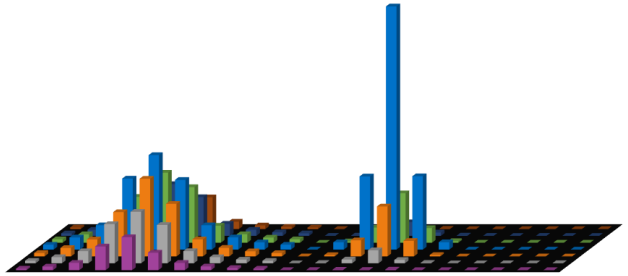
- Greedy Sources
  - High volume (packets, bandwidth, connections)
  - Smaller number of sources with extremely high output
- Suspiciously high number of sources
  - Flood of packets seemingly coming from every source on the Internet
  - Small number of packets from each SPOOFED source
- Normal seeming sources which when acting in an automated group are greedy
  - Grouping is harder for a human to understand
  - More complex in nature
  - Sourced from large numbers of REAL sources

The ZAP Solution – Wartime Learning and Mitigation

DDoS Weapons Intelligence

- *Potential Attackers*
- *Stresser/Booter Attacks*
- *DDoS Malware Reversing*
- *Code Analysis*
- *Social Data Sources*

Behavioral Heuristics



- *Packets per Second*
- *Bits per Second*
- *Connections per Second*
- *Concurrent Sessions*
- *Layer 3 and Layer 4*

Pattern Recognition

Machine Learning-Based Pattern Recognition

- *Advanced Statistical Techniques Pinpoint Anomalous*
- *Rapid Feature Selection*
- *Unsupervised Machine Learning*

Automatically Learning From Each Other

Zero-day Automated Protection (ZAP): Training with Weapons Intelligence

Monitoring Weapons to Train Mitigation Systems

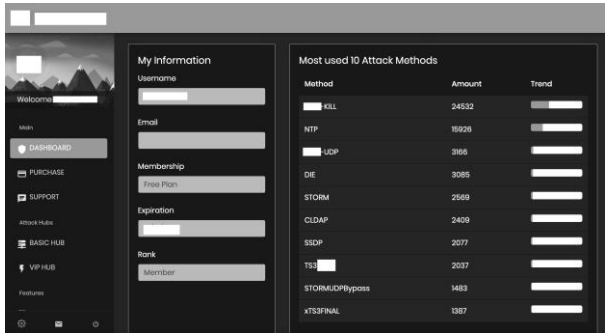
DDoS Weapons Intelligence

- *Potential Attackers*
- *Stresser/Booter Attacks*
- *DDoS Malware Reversing*
- *Code Analysis*
- *Social Data Sources*

- Monitoring potential attackers
  - Amplifiers, drones, other
- Stresser/Booter traffic patterns
- Reverse engineering DDoS focused malware
- Attack code analysis
- Social data monitoring

Be Aware of Your Opponents Weapons

- Knowing where your opponents' weapons are important in any combat
- DDoS protection is no different



New photographic evidence has emerged of "significant" Chinese military defences on artificial islands in the South China Sea, a think tank reports.

Intelligence on Attack Methods is Essential

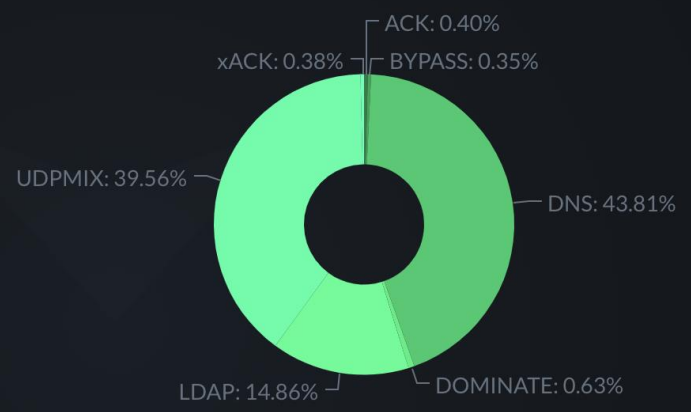
Most used 10 Attack Methods

Method	Amount	Trend
[redacted]-KILL	24532	
NTP	15926	
[redacted]-UDP	3166	
DIE	3085	
STORM	2569	
CLDAP	2409	
SSDP	2077	
TS3[redacted]	2037	
STORMUDPBypass	1483	
xTS3FINAL	1387	

Attack statistics

Commonly used methods

Attack methods usage in comparison



Online users
253

Total users
411311

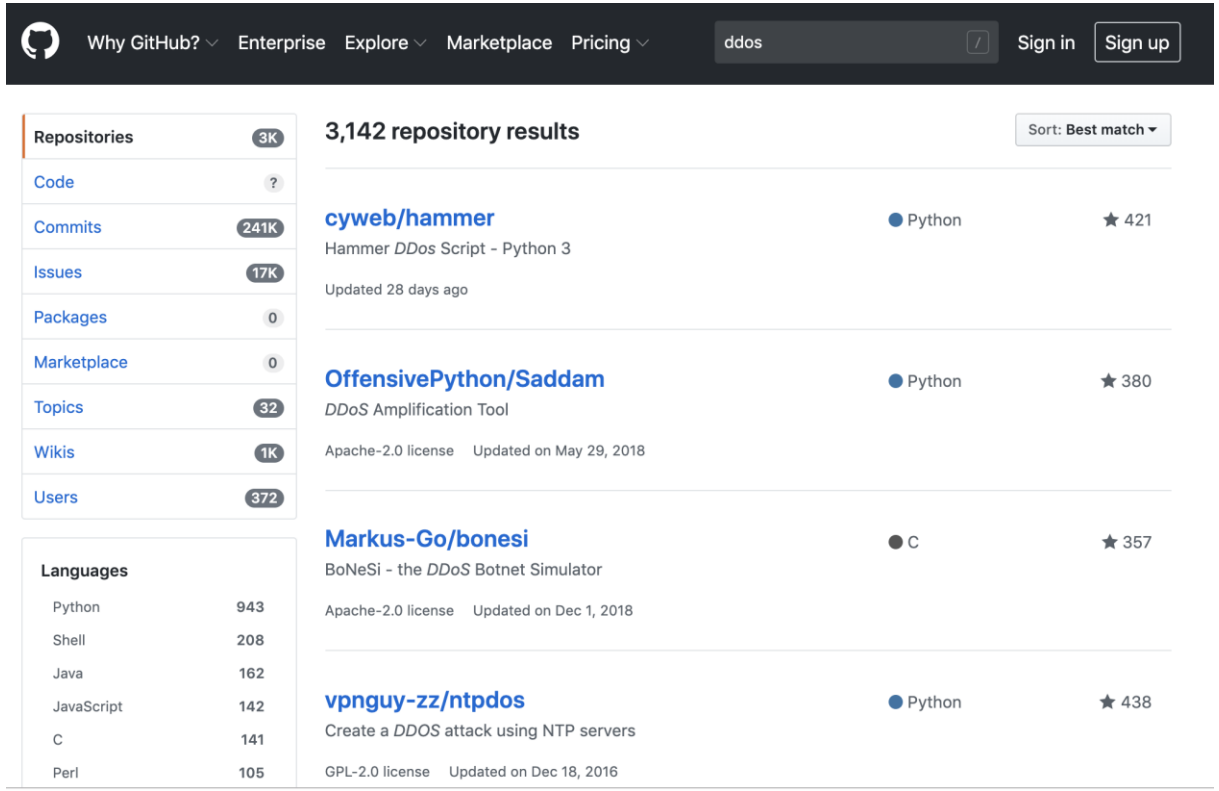
Running attacks
93

Total attacks
6665981

Hello [redacted], Your attack power is highly limited, you should upgrade to launch stronger attacks with up to 225x more power packages are starting from 3 USD for 2 days.

Upgrade now!

DDoS Weapon Code Collaboration

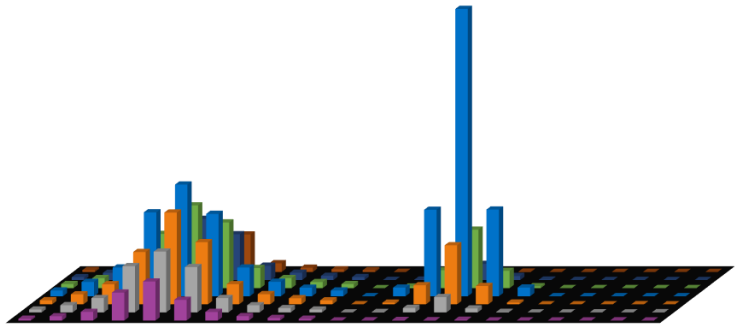


- Sharing Mirai Source on Github has given birth to 8 out of the top 10 binaries we received in the past 30 days
- Github alone has thousands of DDoS related repos. Some of which contain attack code
- Attackers and defenders share code with similar functionality but for different reasons
- Even lists of IP addresses which can be used for an amplification attack are openly shared.

Rapidly Learning Behavior at Wartime

The ZAP Approach to Behavioral Heuristics

Behavioral Heuristics



- *Packets per Second*
- *Bits per Second*
- *Connections per Second*
- *Concurrent Sessions*
- *Layer 3 and Layer 4*

- Tracks various characteristics for every source and destination observed by TPS in real-time.
- Sources are categorized into dynamically created usage bands for each indicator that is tracked.
- This allows us to apply policy directly to each categorized band or to extract an even deeper understand through our ML logic

ZAP Behavioral Solution – Memcache Amplification Attack

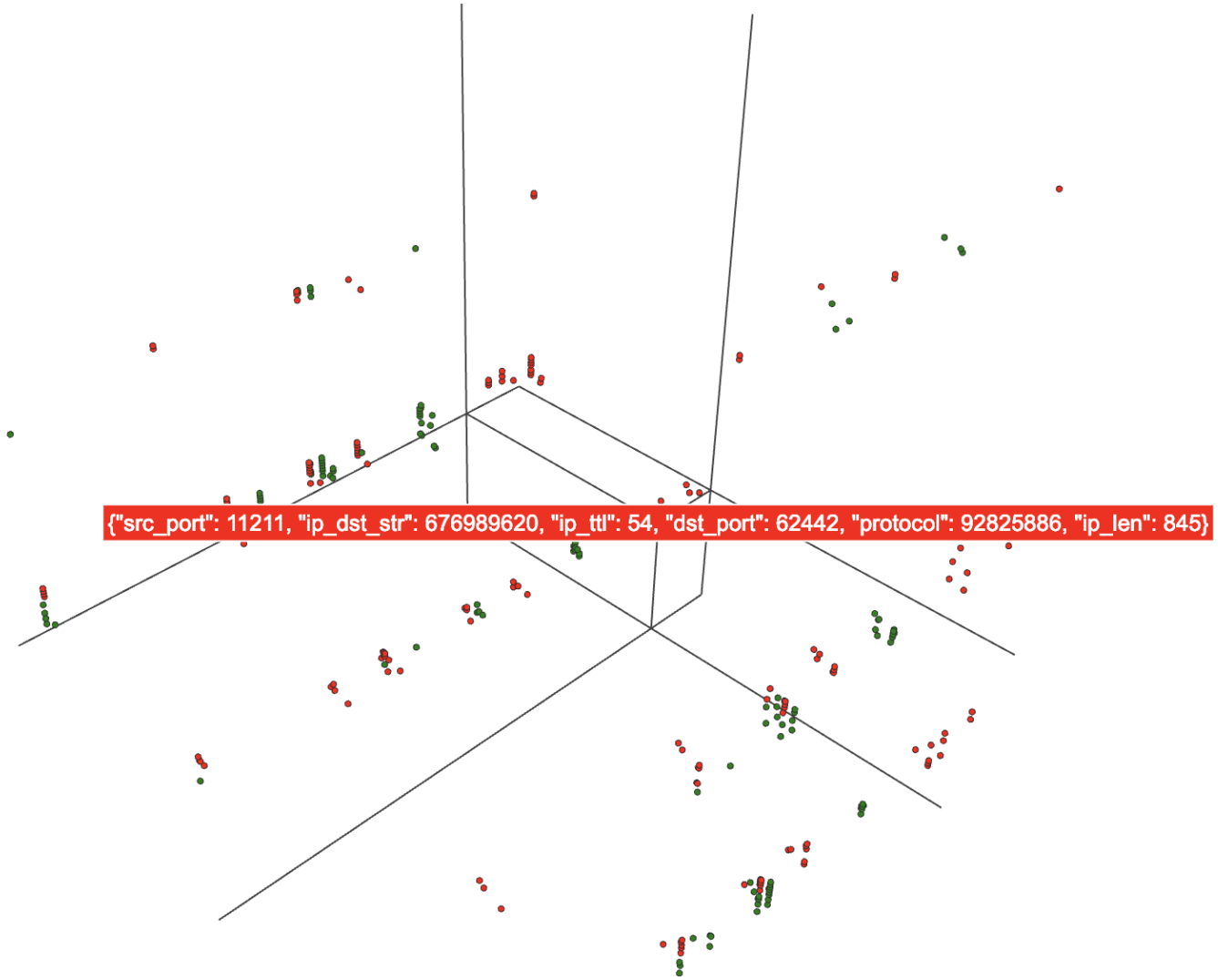
Packet Volume Per Source

UDP Source Port 11211

IP Destination 1.1.1.1

Many Source IP Addresses

Small number of sources create the bulk of the attack



Finding the Pattern in the Attack

The ZAP Approach to Pattern Recognition

Pattern Recognition

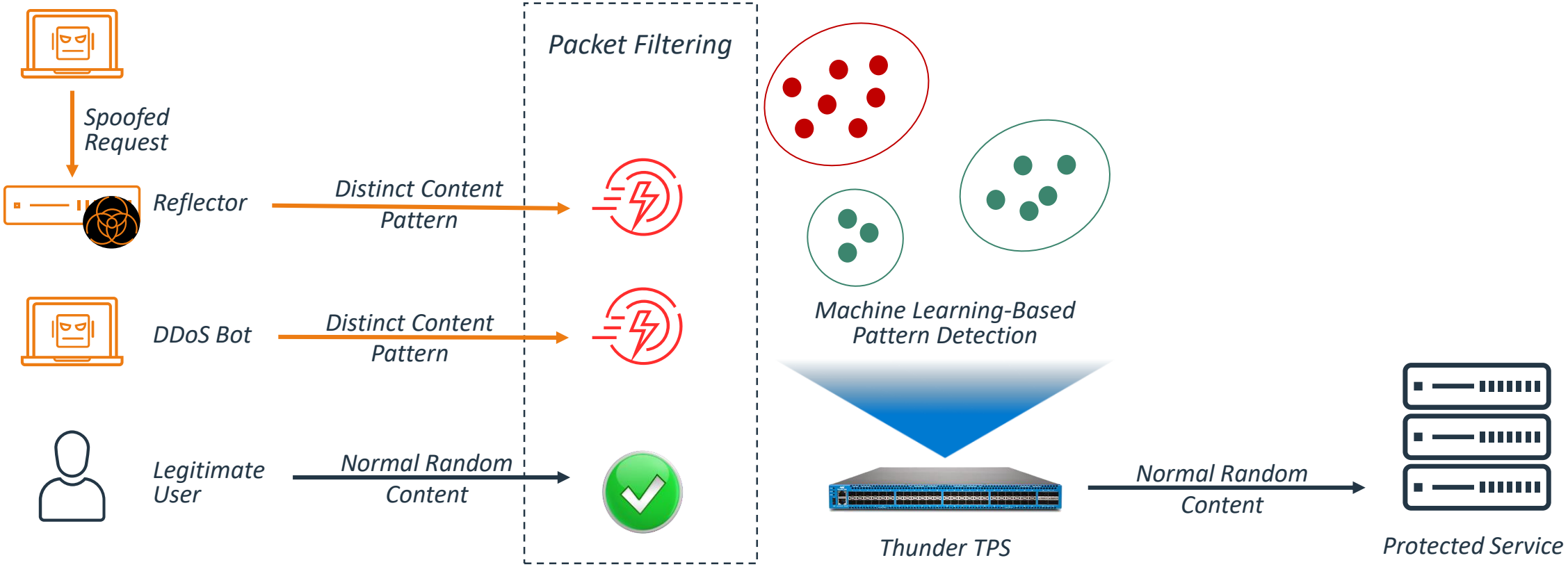
0100010110001111

Machine Learning-Based Pattern Recognition

- *Advanced Statistical Techniques Pinpoint Behavioral Anomalies*
- *Rapid Feature Selection*
- *Unsupervised Machine Learning*

- DDoS patterns are ephemeral in nature
- Filtering attacks through Machine Learning requires proper feature selection through complex mathematics
- Clustering of features at attack time allows us to understand the automated qualities of the attack itself

ZAP Pattern Recognition Overview



Zero-day Automated Protection Workflow

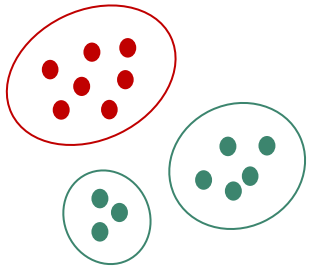
Attack Behavior

- *Source/Dest Learning*
- *PPS/CPS/Conn*
- *Active Weapon Behavior*

Identify Features of Attack Vector

- *Packet Field Values*
- *Rapid Stats Analysis*
- *Active Weapon Behavior*

Unsupervised Machine Learning



Filter Creation and Testing

- *Filter Creation*
- *Iterative offline testing*

Automatic Blocking

- *Inline Filtering*

IOT Sourced Syn-Ack Flood Cluster Visualization

Packet Volume Per Source

50k Sources

TCP Flags SYN and ACK

TCP Source Port 8080 and 8443

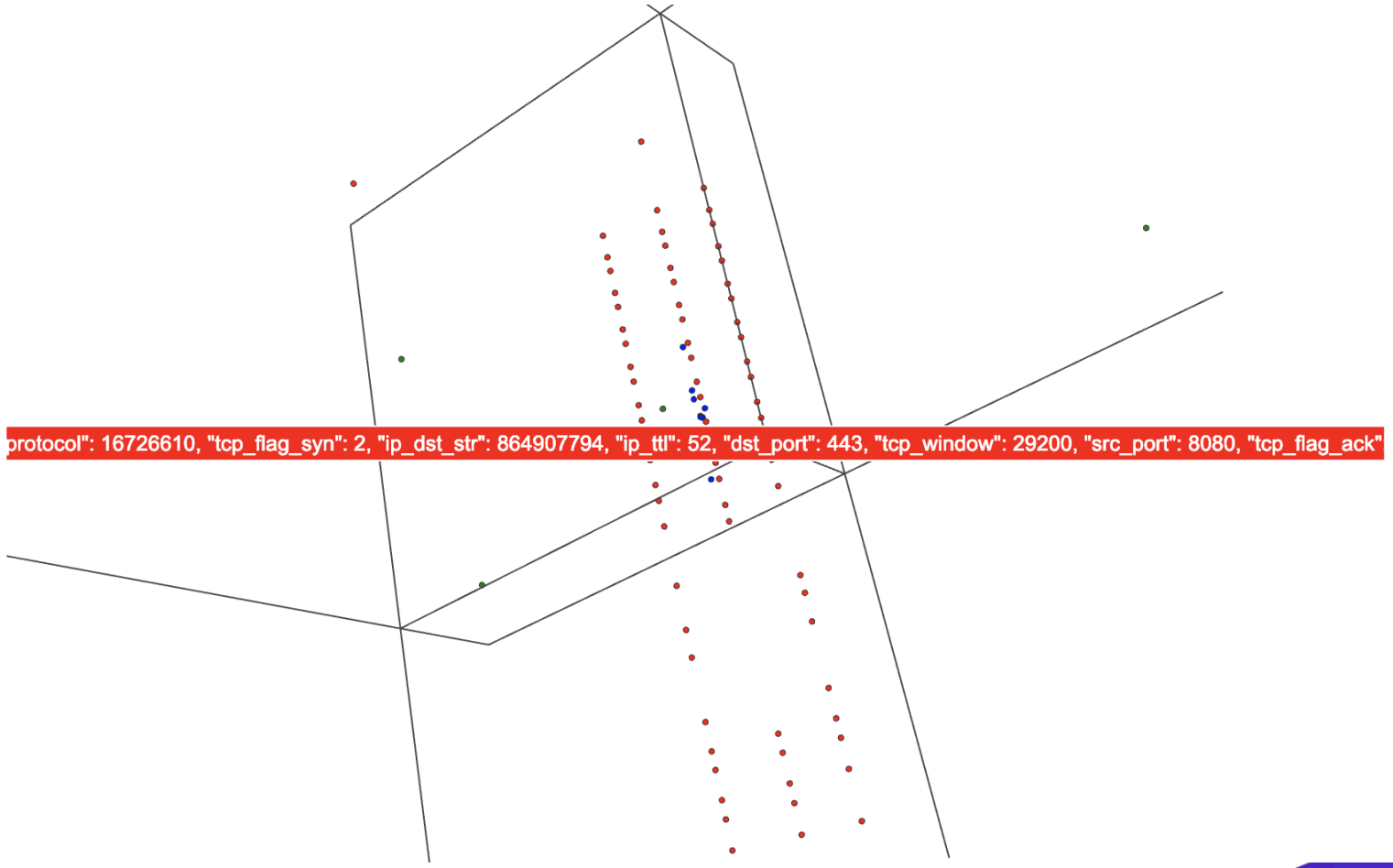
IP Destination 1.1.1.1

IP TTL Range 45 to 55

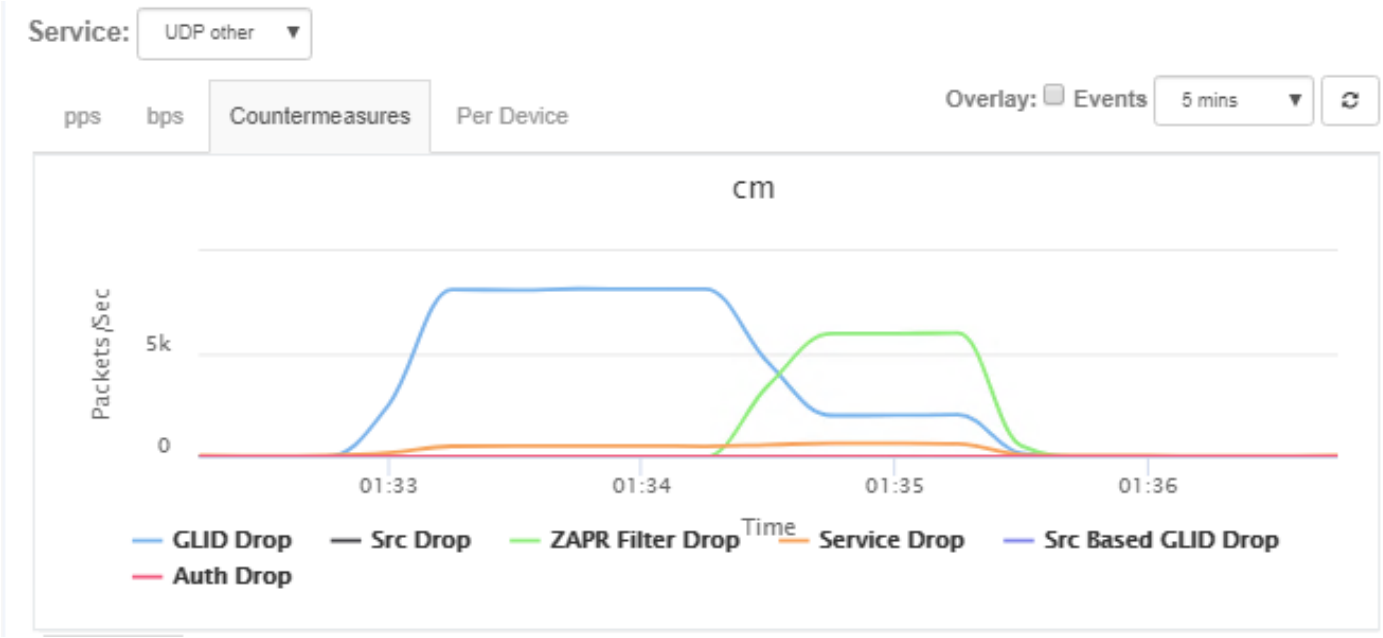
TCP Dest Port 443

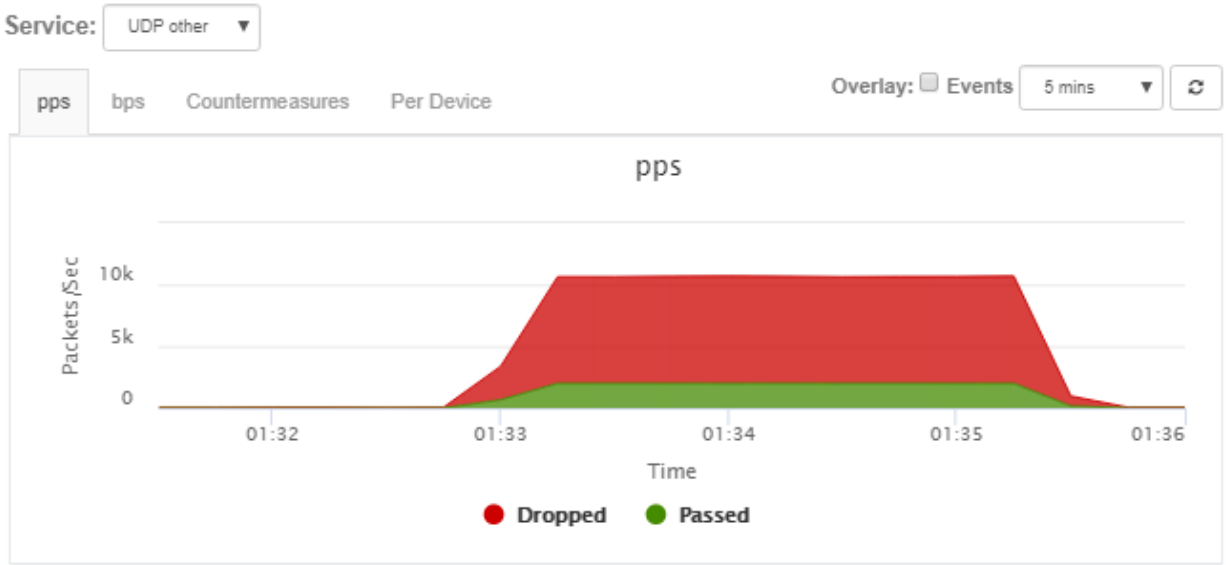
TCP Window Size 29200

IP Len 38 to 46

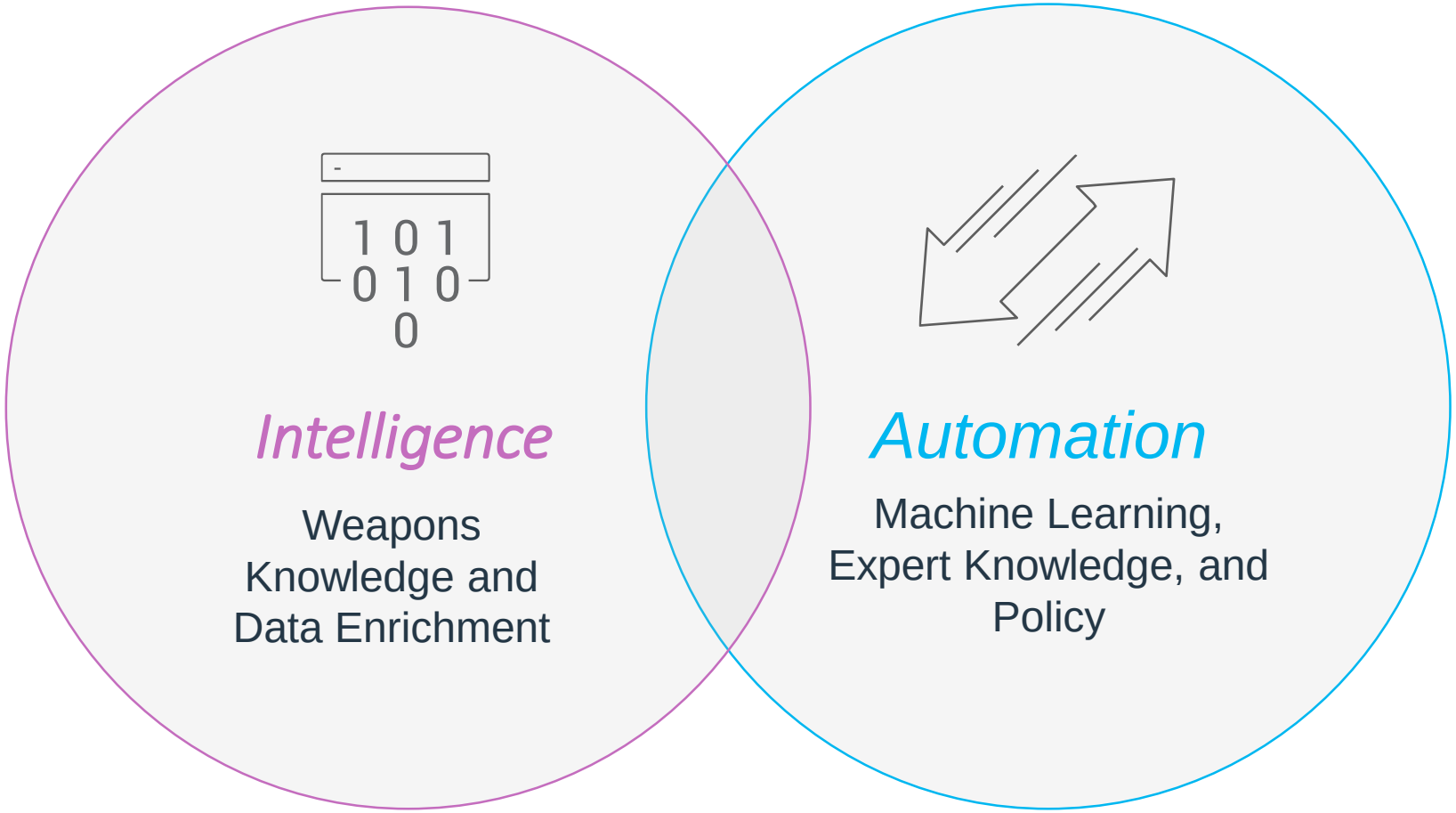


What Does This Look Like In Practice?





Summary: New Attacks Need New Approaches



About A10 Networks

Who is A10 in DDoS Defense

6500
A10 CUSTOMERS

160+
DDOS PROTECTION

80% SWITCHED
20% NEW

70% SP
30% ENT

75+ *Tbps Deployed*

DETECTION
Thunder TPS

MITIGATION
Thunder TPS

MANAGEMENT
aGalaxy

Flow-based detection & inline packet-based detection

Industry performance leader

Zero touch Automation

A10 SECURITY AT UNPRECEDENTED SCALE

135,000,000 USERS

6,000,000 ORGANIZATIONS

48,000,000 USERS

Thank You

Reliable Security Always™

Thunder TPS Appliance Family

1 Gbps to 500 Gbps

Entry Level / CPE

Thunder 3040
10 Gbps Scrubbing

Thunder 1040
5 Gbps Scrubbing,
HW bypass option

vThunder TPS
1 to 5 Gbps Scrubbing,
100Gbps SR-IOV*

** Coming soon*

Mid-Range

Thunder 5845
100 Gbps Scrubbing,
100 GbE ports

Thunder 4435
38 Gbps Scrubbing

High-End

Thunder 14045
500 Gbps Blocking*, 300 Gbps
Scrubbing, 100 GbE ports

Thunder 7445
500 Gbps Blocking*, 220 Gbps
Scrubbing,
100 GbE ports

aGalaxy TPS
Management

aGalaxy 5000
Manage 25 TPS devices

aGalaxy-VM
Manage 10 TPS
devices

High performance Security & Policy Engine (SPE)
with Flexible Traffic Accelerator (FTA)

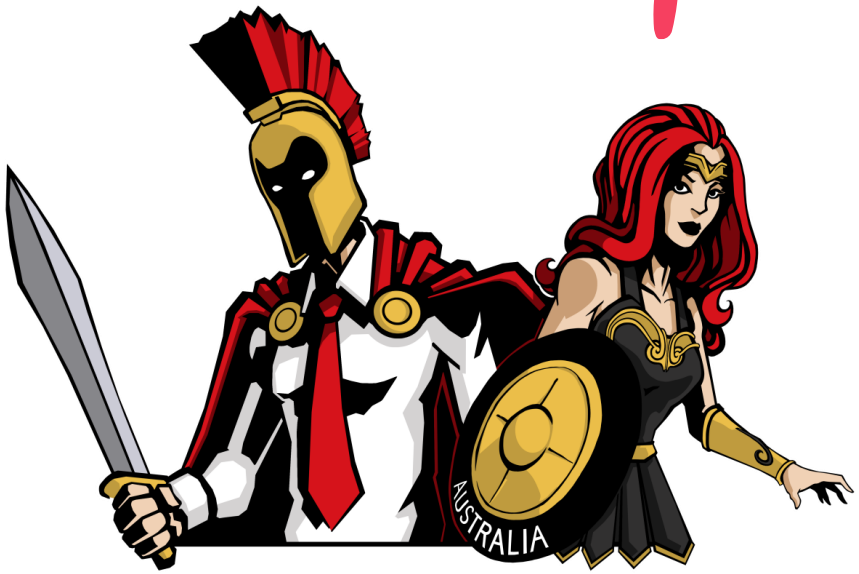
SCAN TO DOWNLOAD YOUR COPY

Thunder TPS Datasheet

IDG DDoS Report: Evolving Strategies for Handling Today's Complex and Costly Threats

The State of DDoS Weapons Report

Meetup



CYBER RISK MEETUP

WWW.CYBERRISKMEETUP.COM