Summary for 2018 CAB Workshop

Pacha Chen

2018.11.15

Joseph Smith
Vince Koski
Eric Miller
Ben Adams
Eu Hsin*
Mike Heath
Paul Dumas

TEAM A

Imad Elimam
Greg Gabet
Chris Copeland
Tareq Allan
Dan Martin
Jonathan Maez
Sharon Pye*

TEAM B

Cecil Elie
Justin Knox
Albert Rivera
Leah Shaw*
Kevin Pimm

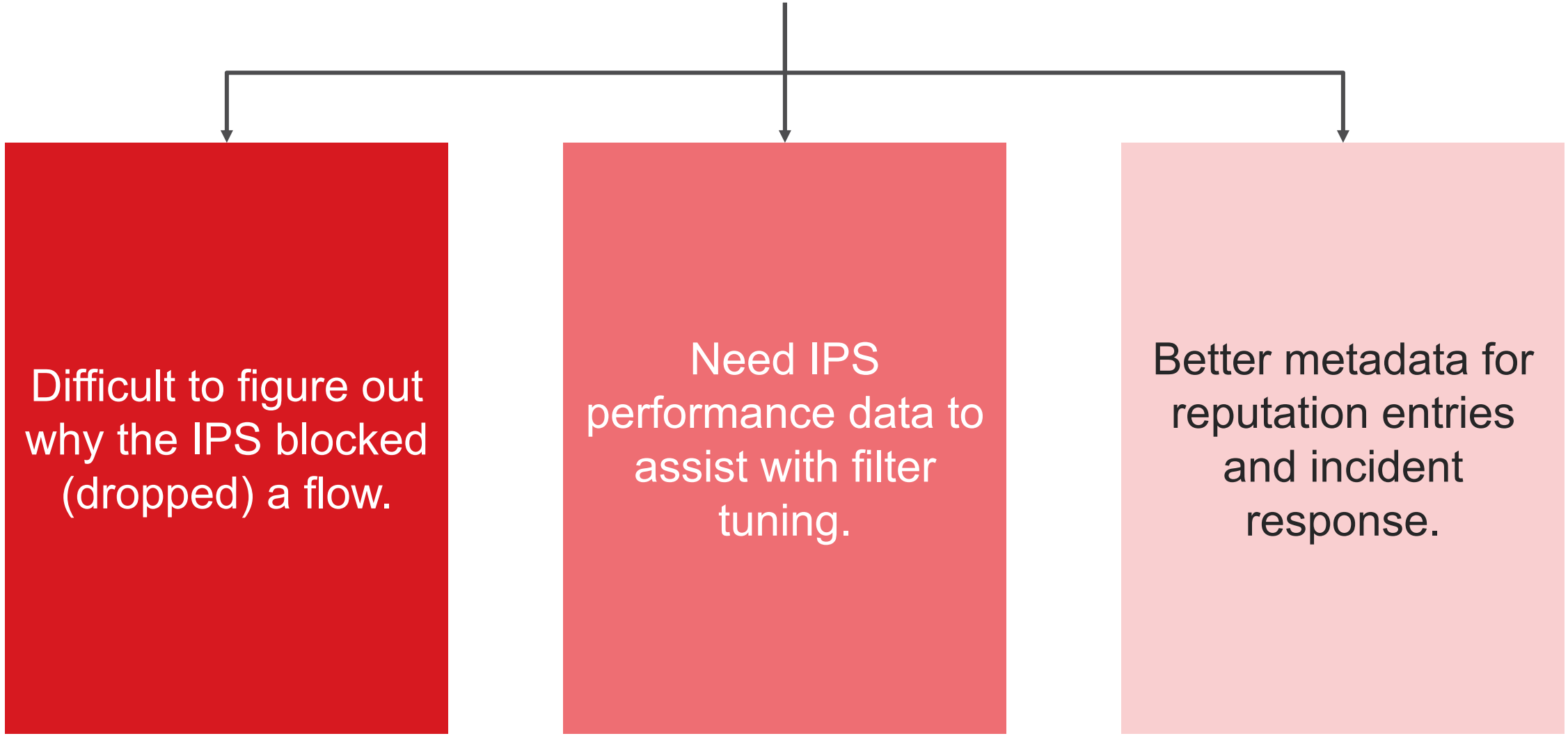
TEAM C

Perry Crabtree
Francisco Muniz
Brad Hutchins
Scott Rivers
Michael Lang*
Sarath Vemuri

TEAM D

2018 TippingPoint CAB User Experience Workshop

The most common pains mentioned by all groups



Difficult to figure out why the IPS blocked (dropped) a flow.

- Can't figure out why certain HTTP flows are getting blocked because of no entries in the block streams table or event logs. – B
- To rule out false positives, customers want to know:
  a) Reputation metadata
  b) The logic of Filters
  c) Packet/network metadata to what it actually found
  d) Meta data for flows that are in the IPS longer than a set threshold
  e) Meta data collection for dropped packets that did not match a filter
- With open source IDS (snort) they can see how a filter hits, They could do a trace, but that is expensive because it requires a profile distribution. - A

Annoying / Frustrating

TREND MICRO

Need IPS performance data to assist with filter tuning.

- Workaround: Automated by custom scripts to run on devices to gather the information / stats that are available on device and to use that to tune the policies. – A
- Graph out Rule stats (can only do that in CLI). - C
  - Want to chart over time on a per filter basis.
  - Want to know what matches up with bad filter performance.
- Would like to tweak policy and step away and don't have to worry about it. Tweak it based on traffic in network, what policy is catching. - C

Better metadata for reputation entries and incident response.

1

- Want to export it all in one big shot instead of small pieces. - C
- Having to pull in other tools to figure out what IPS is seeing. - C
- Want to add more meta data, define own tag and then use it. - C
  - Need more information about why a server is blocked by reputation entry so they can communicate with the owner of the server or their customer as to why it is blocked.
  - Is it everything at an IP address or is it one of many sites at that address? This type of info is needed.
- Use SPLUNK to pull data into single pane of glass. Helps with response time. - C

TREND MICRO

Better metadata for reputation entries and incident response.

2

- GoDaddy currently take advantage of msgParameters, but there still isn't enough information to understand why something got blocked. - A
- Would also like it to be more selective than just IP Address. - A
- Want to know *why* an IP address got that score. - A
- GoDaddy can't block anything below 100. - A

Other pain points mentioned by few groups

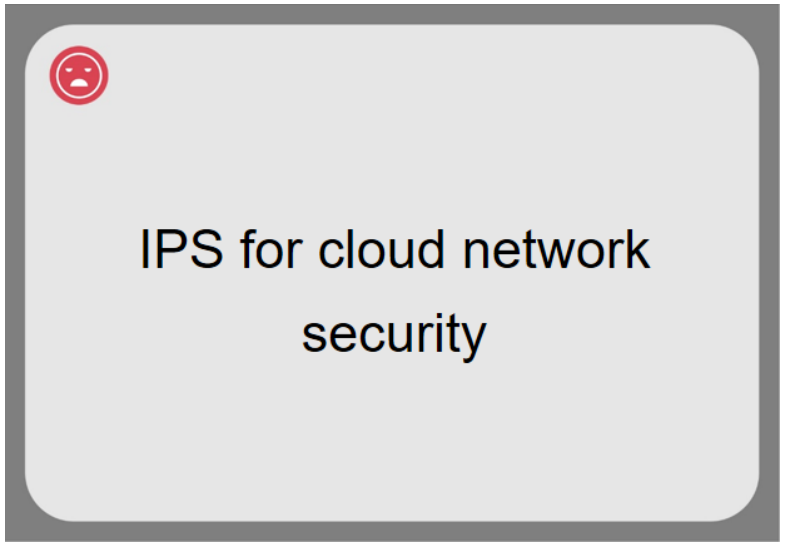
IPS for cloud network security

Configure multiple active directory servers on SMS

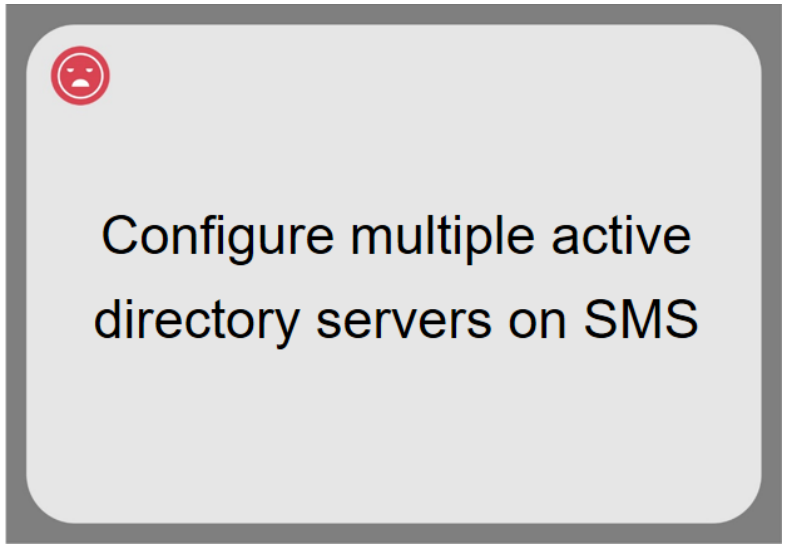
Scheduled distribution for Malware DV

IPS inspection with encrypted traffic

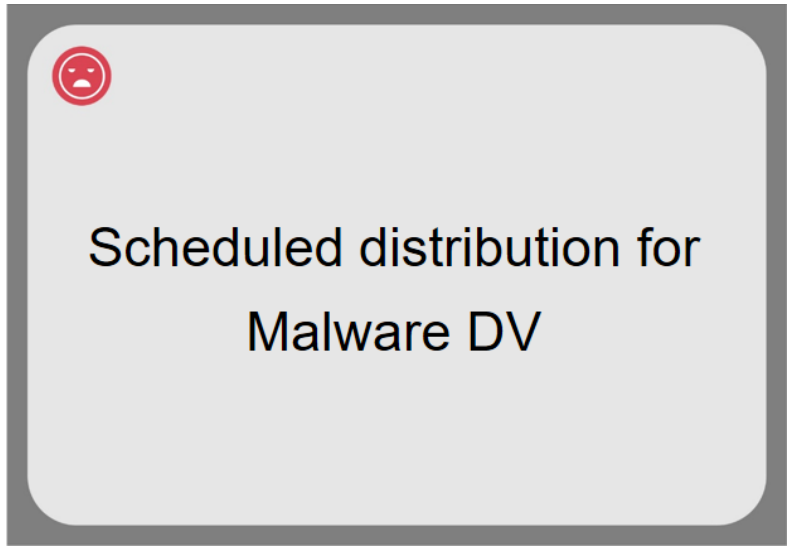
Notifications on traffic management filters



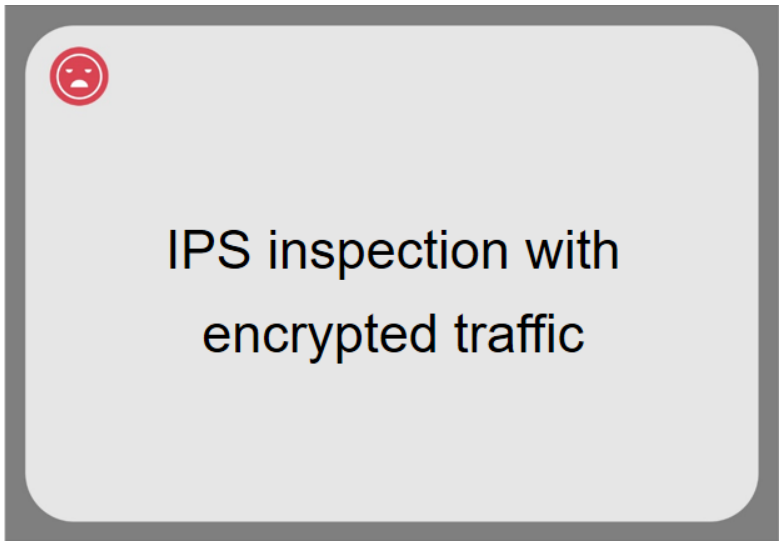
- Baked into protection in cloud solution, looking at AWS.
  - Want same level of security w/cloud as in premise. Only want to manage one set of rules. Don't want to dump data into something
  - Want to be able to add IPS in front of the 3rd party vendor offerings in the cloud. - C
- V-TPS places in front of each server; It was difficult to setup the test to compare to other products (such as DS), vTPS is below competitors offering (like Palo Alto). - A
- Went with Symantec HIPS solution and says it is painfully underdeveloped and slow. - B



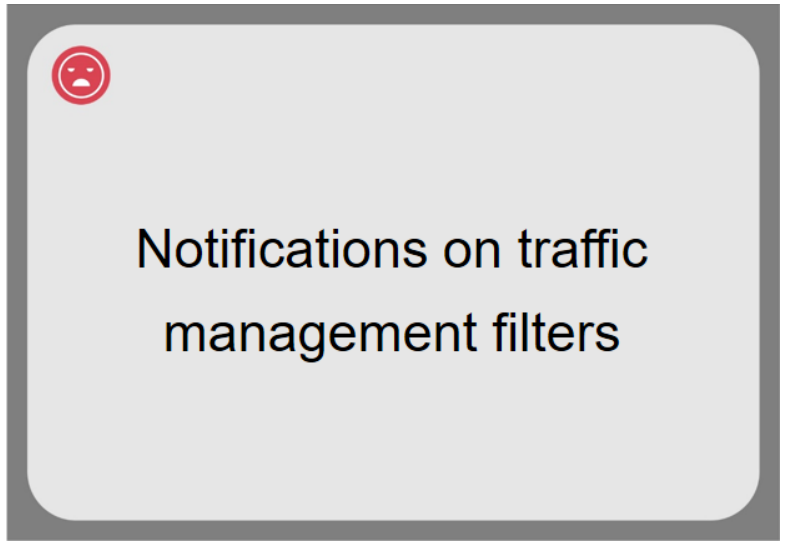
- Need to be able to configure more than one active directory (AAA) server (up to 3 but 2 would suffice). - B
- Alabama Power has 10 Domain Controllers but could get by with 2 or 3. - B



- Inconsistent
  - Can schedule prime DV updates. RepDV is sealed for protection. It’s confusing. Every week doing late night work. In perfect world, scheduling would be done in one place. - C
- Frustrating
  - Can't delete malware DV. Multiple DVs and updates w/ distribution is a nightmare and has caused problems. - C
  - Full profile push takes four hours to 6 NX's: (4) 7500's and (2) 6200's) - C
- Not only schedule them but if it fails, auto restart it after a set amount of time. - B
- Malware DV is not cost effective. A lot of false positives and some filters are too old, that malware isn't around anymore (Eric). - A



- 50%-70% of network traffic are encrypted. – All
- SSL traffic that can be trusted causes the Trust table to overflow. - A
- Certificate management is important. Over 40k certificates in GoDaddy. Would like to see integration with HSM (Hardware Security Module). - A
- Looking at 3rd party SSL decryption, which is the best solution now. - A
- Eventually they'll need the decryption and re-encryption to be on the same box. - A
- Our SSL support is not viable for larger customers. - A



- Had to take 12 packet captures to prove the problem wasn't caused by IPS. - C
- Being able to know why something dropped would be wonderful. Silent drops are a problem (manual response with quarantine). - C
- Want at least a counter for traffic management rules that is **time based**. E.g., How many hits in the last 30 days. - B
- Need to add description field to bypass rules.- B
- Audit point for Lincoln financial because they can't identify what the rule was originally for. - B

Emerging Needs

1. Decrypt SSL traffic is needed

- Increased SSL inspection throughput.
  - Increased throughput also requires an equally fast device to process the traffic, i.e. the capacity of the device should not slow down the traffic.
- Ease of HSM Management.
  - Certificates storage and management; interacting with other license management; e.g. AWS interacts with other cert. management
    - e.g. BlueCoat; Both parties need to have traffic going through and have the certificates verified and updated within 5 minutes

Team A

1. Decrypt SSL traffic is needed

- The group was not pleased when they bought a 40G box and had to pay extra for an SSL license just to have the box inspect traffic at 2G.
- In order for this to be scalable, the SMS has to be able to **integrate with an HSM** so that once a new certificate is added to the HSM, the SMS can quickly push that certificate to the devices.
  - Otherwise the IPS administrator must get notified a new certificate was added and he must import that onto the SMS and get it pushed to the device.
  - In a customer environment, days, weeks, or months can go by before the cert is added to the SMS and SSL traffic is getting inspected.

Team A

2. All of your infrastructure are in the cloud

- IPS in the cloud with guaranteed inspection of data
  - Guaranteed delivery path through the IPS; agent on the device or talking to API.
- Flexible cloud solution to meet the needs of regulations or compliance
  - Cloud solution must be flexible enough to meet the regulations, HIPAA, PCI GLB, etc.
- Security stack in every endpoint
  - A way to control egress/ingress in network in the cloud; antivirus; anti-malware.
  - Need the entire security stack baked into every endpoint, servers and VDI, such as HIPS, Anti-Virus, DLP, Endpoint protection

Team B, C

Solution 1 – Unmasking TPS

TEAM A

Unmasking TPS

Problem Statement

Growing SSL encrypted traffic leads security provider in a blind.

Growing SSL encrypted traffic leads security provider in a blind. Full line speed inspection rate on SSL streams with no impact to performance, and the solution is easily managed and cloud ready.

Target Group

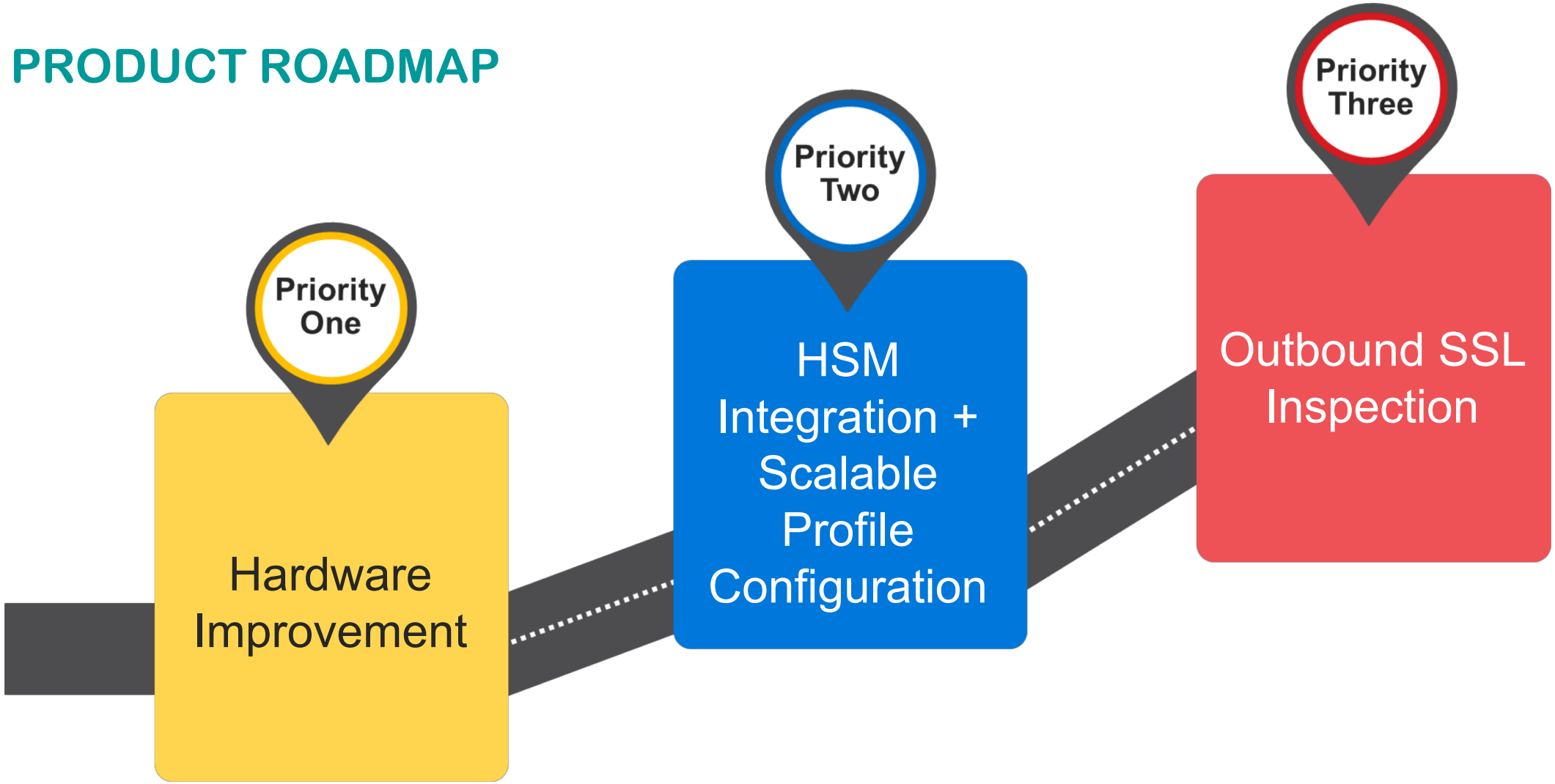
- Imperva users
- Load balancer users
- SSL site manager
- network provider

#millennialsolution
#xrayglasses
#guyinhoodies

TREND MICRO

Unmasking TPS

PRODUCT ROADMAP



Solution 2 – Traffic Flow Lost + Found

TEAM B

Traffic Flow Lost + Found

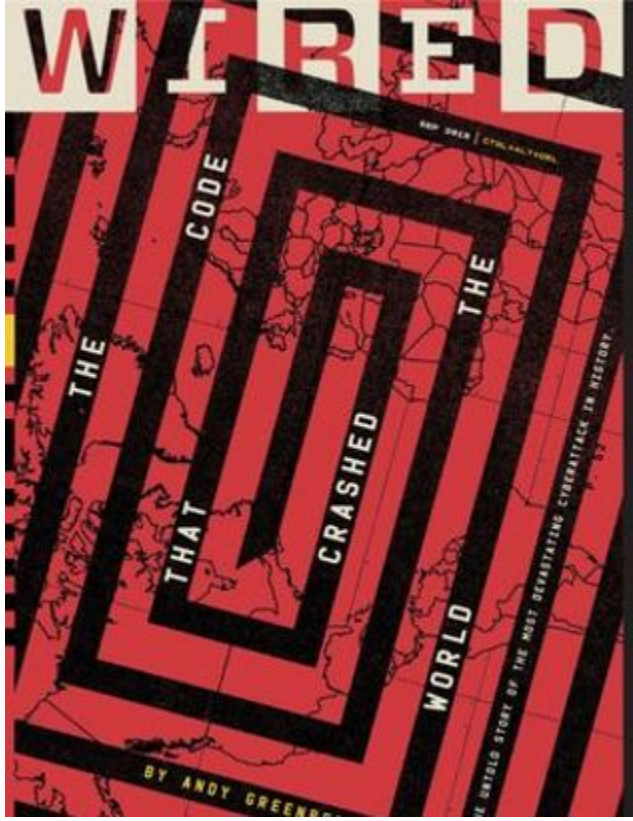
No More Lost Traffic

Problem Statement

Difficult to figure out why the IPS blocked a flow.

Solution Briefing

1. Meta data analysis + notification
2. Collection for dropped packets when they don't match
3. Visibility of unidentified blocks



Target Group

- IPS Admin
- SOC/NOC Admin
- Data Center / Infrastructure Admin

#TrafficFound
#NOMOREDINGOS
#rollrideyall

TREND MICRO

Solution 3 – IPS Deep View

TEAM C

IPS Deep View

RELEASING THE INSIDE INFORMATION

Problem Statement

Need IPS performance data to assist with filter tuning. Ease of IPS tuning and reduce support calls.

Solution Briefing

1. Collect data from the IPS via rule stats, etc.
2. Make data present on SMS per device
3. Aggregate the data further to correlate with protocols, filters, etc.
4. Expose data via SMS API
5. Present the data in real-time views

Target Group

- Security Engineers
- Security Admins

#IPSDeepView
#ipsdview
#interinfo
#IPSinnerinfo2020

TREND MICRO

Solution 4 – Enterprise Manager

TEAM D

Enterprise Manager

One Manager To Rule Them All

Problem Statement

No single pane of glass.

Solution Briefing

1. Decentralized for autonomy and performance
2. Centralization for oversight and control
3. Multi-national
4. Faster distribution

Workshop Feedback

Feedback to the workshop

- Kahoot game is good
- Set expectations at the beginning of workshop, no promises, etc.
- Set specific scenarios, for example, is the innovation for power users or others?
- “Task” card, people don’t really follow
- Some customers like 2017 CAB (more focused) better; others like 2018 one better (more open/game)
- 2 separate roles, Facilitator and Note Taker
- Good to have 1 team share the learning/conclusion with other teams, etc.
- Using a Chime/Bell, etc. for team reminders
- Small community to share and to learn others’ pains, etc.
- Planning shall be done much earlier, etc.