The Security Perimeter of 2019: what will be your first and last line of defense?

Kirill Kasavchenko, CTO Office EMEA
kirill.kasavchenko@netscout.com
The brief history of enterprise security perimeter

Internet Router

- DDoS
- IDPS
- IPS
- NGFW
- End Points

SIEM
Threat hunting: from prevention to detection

Internet Router

DDoS

IDPS

NGFW

Sandbox, Etc. …

EDR

End Points

SIEM

 Threat Intelligence Feeds

UEBA

Security Analytics
Scale is the problem

3M* indicators

Hundreds of thousands entries in IP Reputation System*

- Obtained from companies public documents or newsroom
Whitelists for curated Threat Intelligence

Top 1M websites

Cisco Umbrella

1M of most queried domains
TIP: Threat Intelligence Platform

DDoS

IDPS

NGFW

Sandbox, Etc. ...

End Points

Threat Intelligence Feeds

TIP

SIEM
Where IoCs should be applied?

- TIG
- IDPS
- NGFW
- Sandbox, Etc. ...
- End Points
- SIEM
- Threat Intelligence Feeds
Wait a moment… Another device at my perimeter?

- The average enterprise uses **75 security products** to secure their network.

- 74% of survey respondents said their organizations select best-of-breed security technologies **but only if they are designed for broader integration**. "Integration is the new best of breed." - Jon Oltsik is an ESG senior principal analyst

What about on-premise DDoS Defense?

- Stateless, high performance blocking of all types of inbound DDoS attacks
  - volumetric attacks
  - state exhaustion attacks
  - application layer DDoS attacks, reconnaissance, Geo-location, known bad IoCs.

- Takes load off downstream stateful devices (e.g. NGFW) making them more effective.
Netscout AED: Combining DDoS and TIG
The first line of defense

- DDoS
- AED
- Reputation-based blocking
- IDPS
- Firewall
- Sandbox, Etc. …
- End Points

Threat Intelligence Feeds:
- DDoS mitigation
- Stateless Network Perimeter Enforcement (GeoIP, known bad IoCs)
- Protecting & Augmenting NGFW Threat Prevention

SIEM

TIP
The last line of defense

End Points

IDPS  Firewall  AED  Reputation-based blocking  DDoS

Outbound Threat Communication

SIEM

Stop incident before it becomes a breach

Stop outbound malicious communication

Threat Intelligence Feeds

TIP

COPYRIGHT © 2018 NETSCOUT SYSTEMS, INC. | PUBLIC
From a single alert...
... to threat consolidation and analysis...

What should I hunt?

Where should I hunt?
... to Contextual Threat Intelligence

Additional details (e.g. malware hash values) can be used by other security tools to hunt inside an organization.

Look to be trending up in ATLAS
Global view on a local incident

Attack pervasiveness throughout AED ecosystem
Netscout AED as a VNF

- Support of major hypervisors
- Cloud-init for Day0 configuration
- REST API for Day1/Day2 operations
- Ansible playbooks
- Integration with Cisco NFVIS and other orchestrators
Learn details of Arbor-Cisco collaboration

NETSCOUT.

EVOLVED ARBOR-CISCO SOLUTIONS IN THE DDoS SPACE

Speaker: Jorge Escobar, Solutions Architect, WW Strategic Alliances

JANUARY 31, 2019

Session ID: BRKPAR-2777
Date/Time: Thursday, 16:00
Location: Innovation Showcase Theatre
Netscout AED: the first and last line of defense

First Line of Defense:
• protects availability and performance of network and service from DDoS;
• takes pressure off downstream security stack.

Last Line of Defense:
- detects and stops missed IoCs before the data breach occurs.

Integrated into security workflows:
- Continuously armed with highly curated ATLAS Threat Intelligence and 3rd party IoCs via STIX & TAXII
- Automatically obtains additional context related to blocked IoCs enabling security teams to hunt using other tools
Thank You.

kirill.kasavchenko@netscout.com

www.netscout.com