

Ruling the Rules

Quantifying the Evolution of Rulesets, Alerts and Incidents in Network Intrusion Detection

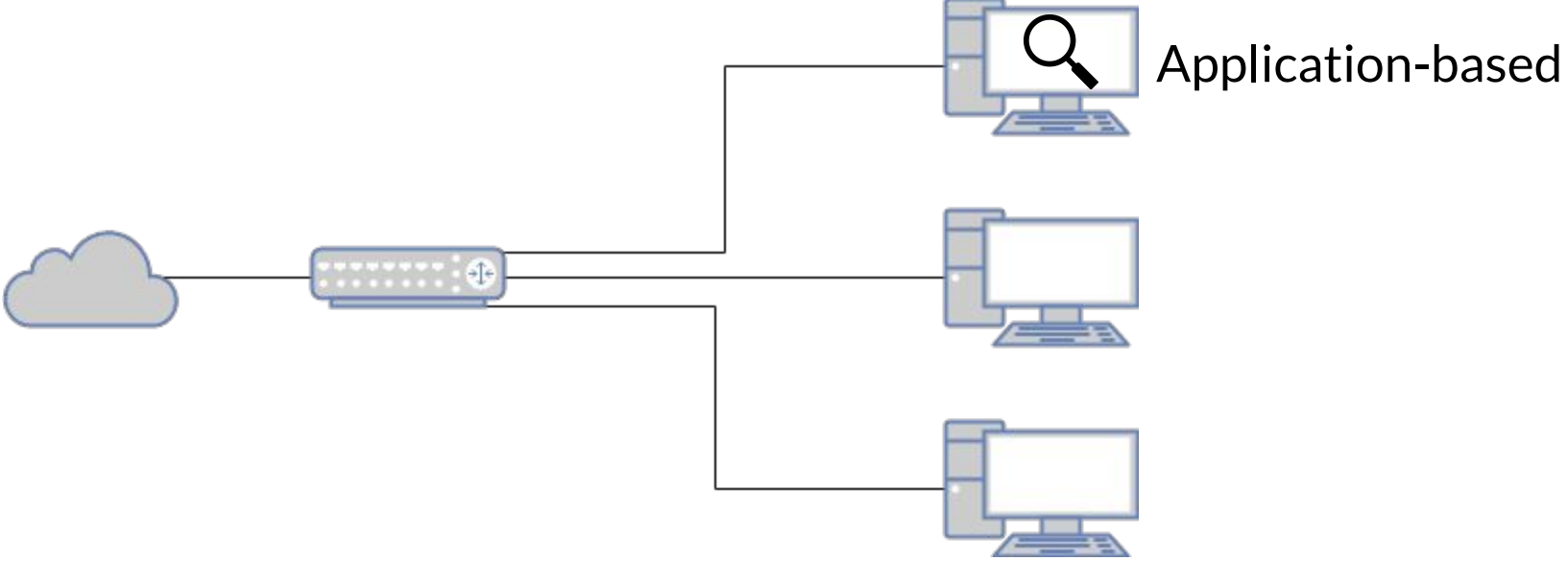
Mathew Vermeer, Michel van Eeten, Carlos Gañán

2022 ACM ASIACCS

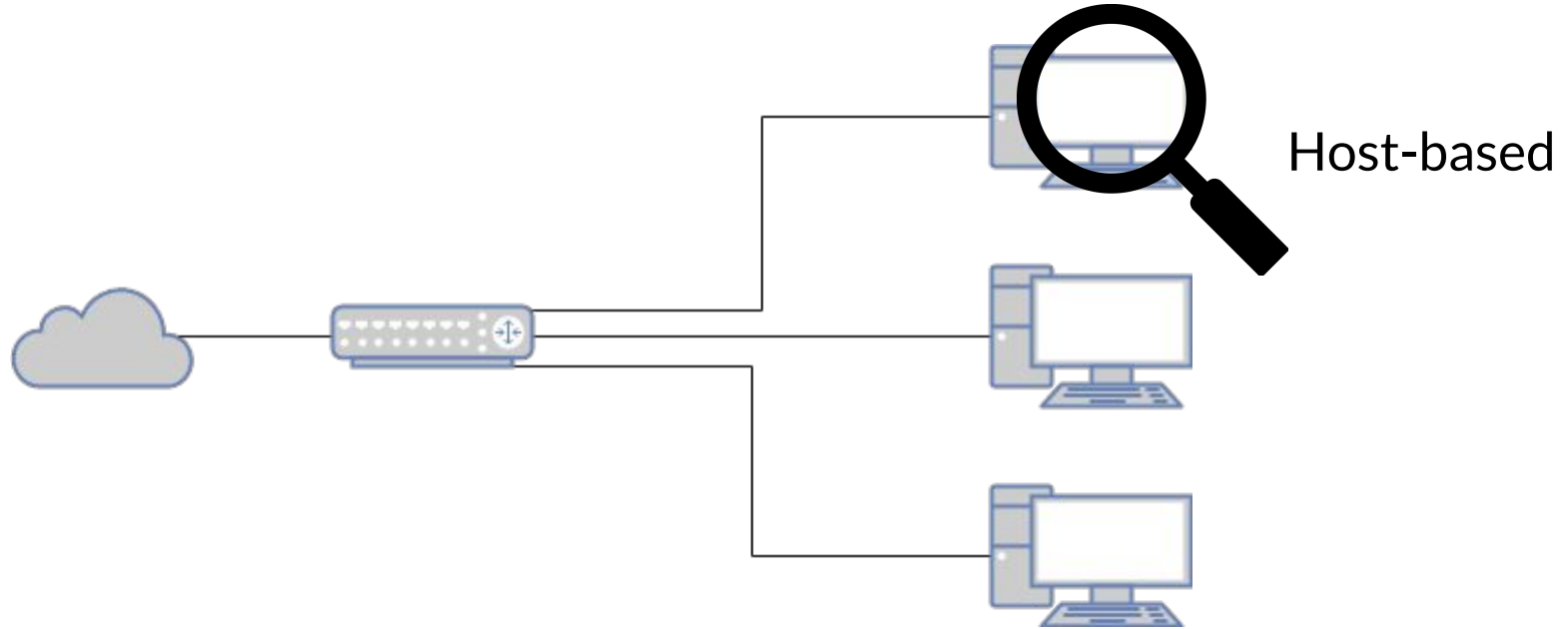
HACKERS LOOKING

**AT ALL YOUR
EXPOSED DEVICES**

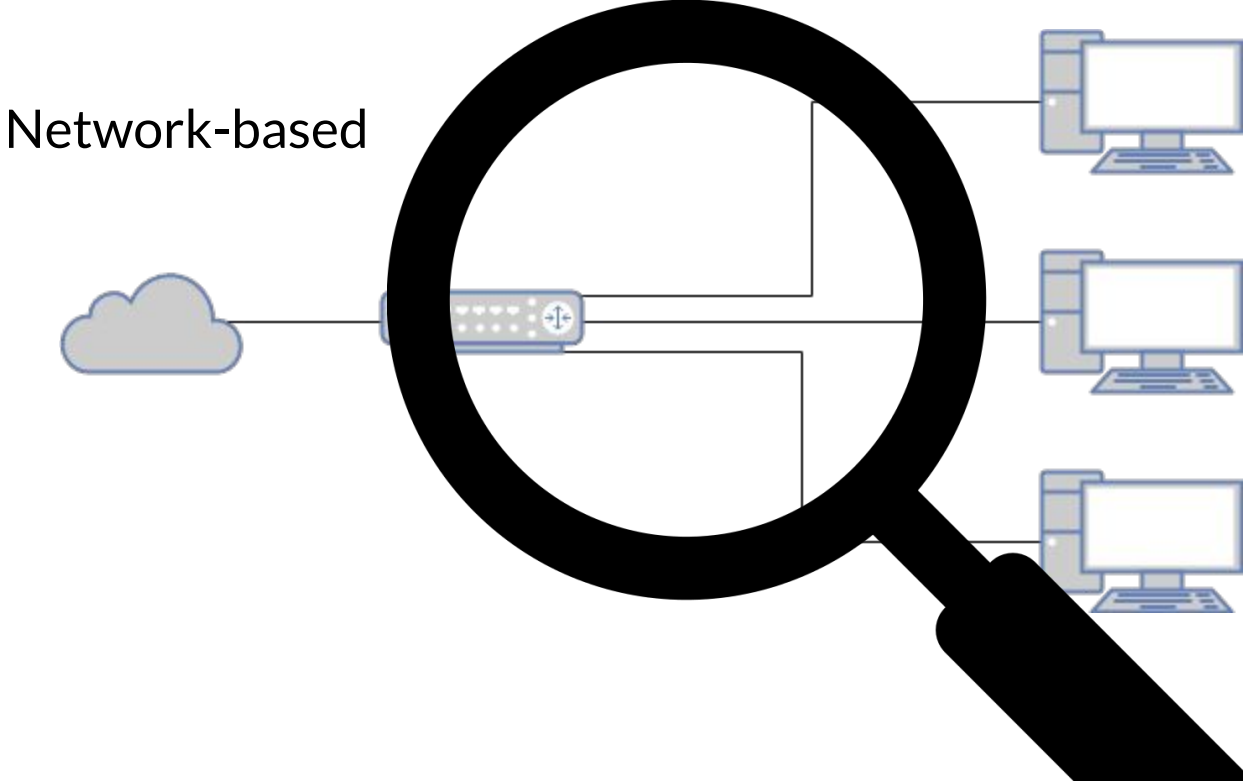
Intrusion detection systems (IDS)



Intrusion detection systems (IDS)



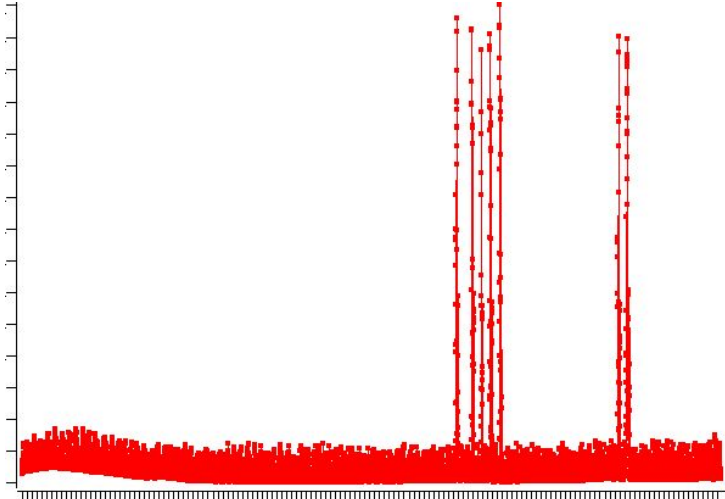
Intrusion detection systems (IDS)



Network intrusion detection systems (NIDS)

```
00000000 EA 05 00 C0 07 E9 99 00 00 51 02 00 C8 E4 00 80 é . A. é" . q. . éä. é
00000010 9F 00 7C 00 00 1E 50 80 FC 02 72 17 80 FC 04 73 Y. | . . pëü. r. ëü. s
00000020 12 0A D2 75 0E 33 C0 8E D8 A0 3F 04 A8 01 75 03 . . ou. 3AZ0 ? . . u.
00000030 E8 07 00 58 1F 2E FF 2E 09 00 53 D1 52 06 56 57 è. . x. . y. . . SNR. VW
00000040 BE 04 00 B8 01 02 0E 07 BB 00 02 33 C9 8B D1 41 % . . . . . * . . 3E < NA
00000050 9C 2E FF 1E 09 00 73 0E 33 C0 9C 2E FF 1E 09 00 e. y. . . s. 3Am. y. .
00000060 4E 75 E0 EB 35 90 33 F6 BF 00 02 FC 0E 1F AD 3B Nuàè5. 30z. . ü. . ;
00000070 05 75 06 AD 3B 45 02 74 21 B8 01 03 BB 00 02 B1 . . u. ; E. t! . . . * . ±
00000080 03 B6 01 9C 2E FF 1E 09 00 72 0F B8 01 03 33 DB ¶ . e. y. . . r. . . . 30
00000090 B1 01 33 D2 9C 2E FF 1E 09 00 5F 5E 07 5A 59 5B ±. 30e. y. . . A. ZY[
000000A0 C3 33 C0 8E D8 FA 8E D0 BC 00 7C FB A1 4C 00 A3 A3A200204. |D;L. I
000000B0 09 7C A1 4E 00 A3 0B 7C A1 13 04 48 48 A3 13 04 | . | N. . i. | . | . HHf. .
000000C0 B1 06 D3 E0 8E C0 A3 0F 7C B8 15 00 A3 4C 00 8C ±. 0àZAf. | . . . fL. e
000000D0 06 4E 00 B9 B8 01 0E 1F 33 F6 8B FE FC F3 A4 2E . N. ' . . . 36. pùóµ.
000000E0 FF 2E 0D 00 B8 00 00 CD 13 33 C0 8E C0 B8 01 02 y. . . . . I. 3A2A. .
000000F0 BB 00 7C 2E 80 3E 08 00 00 74 0B B9 07 00 BA 80 * . | . é > . . . t. ' . °é
00000100 00 CD 13 EB 49 80 B9 03 00 BA 00 01 CD 13 72 3E . i. éL. ' . °. . i. r>
00000110 26 F6 06 6C 04 07 75 12 BE 89 01 0E 1F AC 0A C0 èó. l. . u. %µ. . . . . À
00000120 74 08 B4 0E B7 80 CD 10 EB F3 0E 07 B8 01 02 BB t. . . . . i. éó. . . . *
00000130 00 02 B1 01 BA 80 00 CD 13 72 13 0E 1F BE 00 02 . . . ±. °é. i. r. . . %µ.
00000140 BF 00 00 AD 3B 05 75 11 AD 3B 45 02 75 0B 2E C6 z. . . ; . u. ; E. u. A
00000150 06 08 00 00 2E FF 2E 11 00 2E C6 06 08 00 02 B8 . . . . . y. . . . A. . . .
00000160 01 03 B8 00 02 B9 07 00 BA 80 00 CD 13 72 DF 0E . . . * . . . °é. i. rB.
00000170 1F 0E 07 BE BE 03 BF BE 01 B9 42 02 F3 A4 B8 01 . . %µ. zµ. 'B. óµ.
00000180 03 33 DB FE C1 CD 13 EB C5 07 59 6F 75 72 20 50 . 30pAf. éA. your P
00000190 43 20 69 73 20 6E 6F 77 20 53 74 6F 6E 65 64 21 c is now Stoned!
000001A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . .
000001B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . .
000001C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . .
000001D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 . . . . .
```

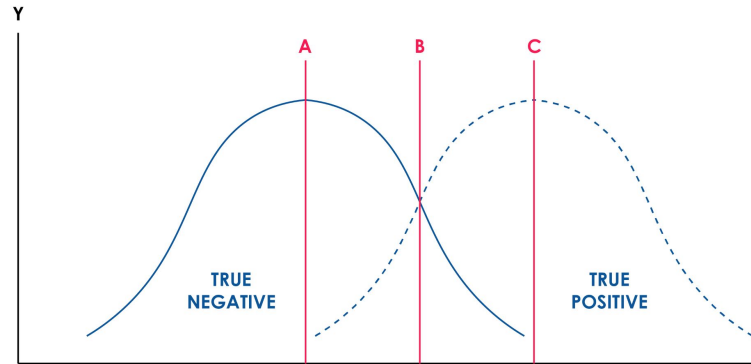
Signature-based



Anomaly-based

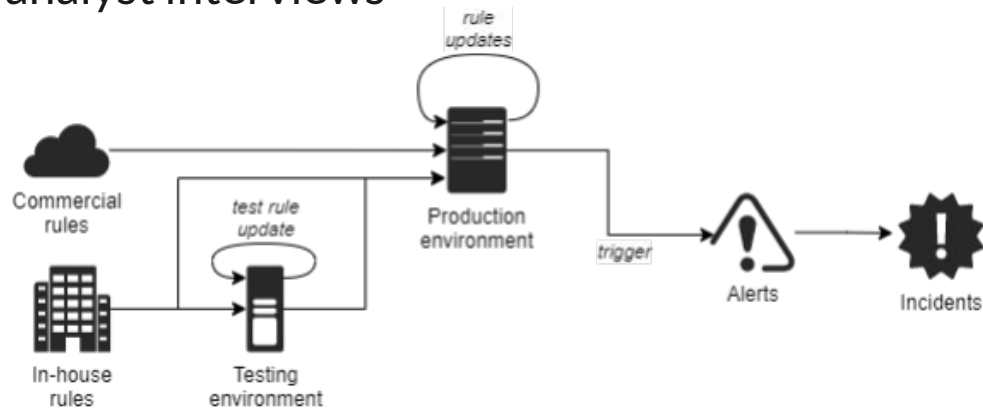
The NIDS black box

- Not as straightforward as it seems.
 - Why do they work?
 - What role do the rulesets play?
 - How do security professionals keep them working effectively?
- Critical tradeoff: Maximize intrusion detection vs minimize number of alerts.



Methodology

- Partnered with managed security service provider (MSSP).
 - MSSP in-house NIDS ruleset
 - Three commercial NIDS rulesets (ET Pro Snort & Suricata, VRT)
 - Alerts & incidents over time
 - Security analyst interviews



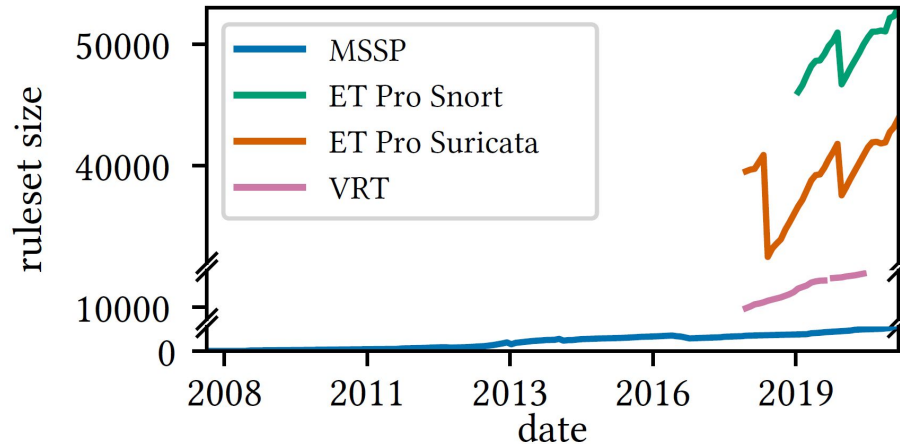
Methodology

- Create tool to track ruleset evolution in git repo.
 - Track new rules, updated rules & deleted rules.
- Calculate many different statistics that shed light upon ruleset management processes and organizational security.
- Interview security analysts to cross-validate the insights.

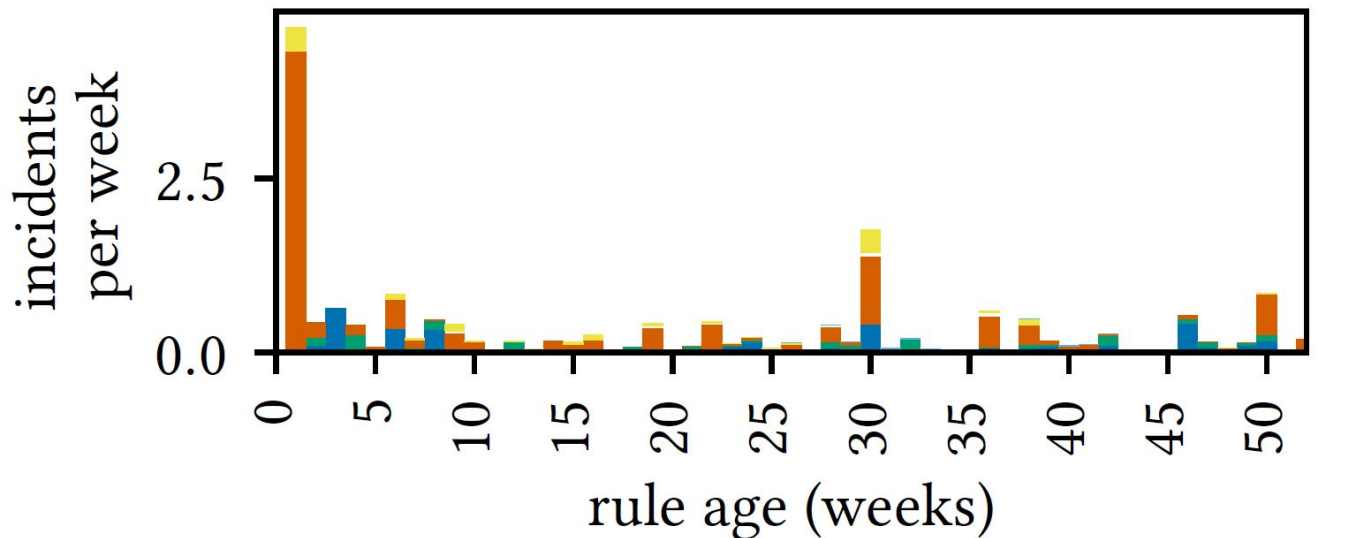
Results

Custom ruleset important for proper functioning of NIDS

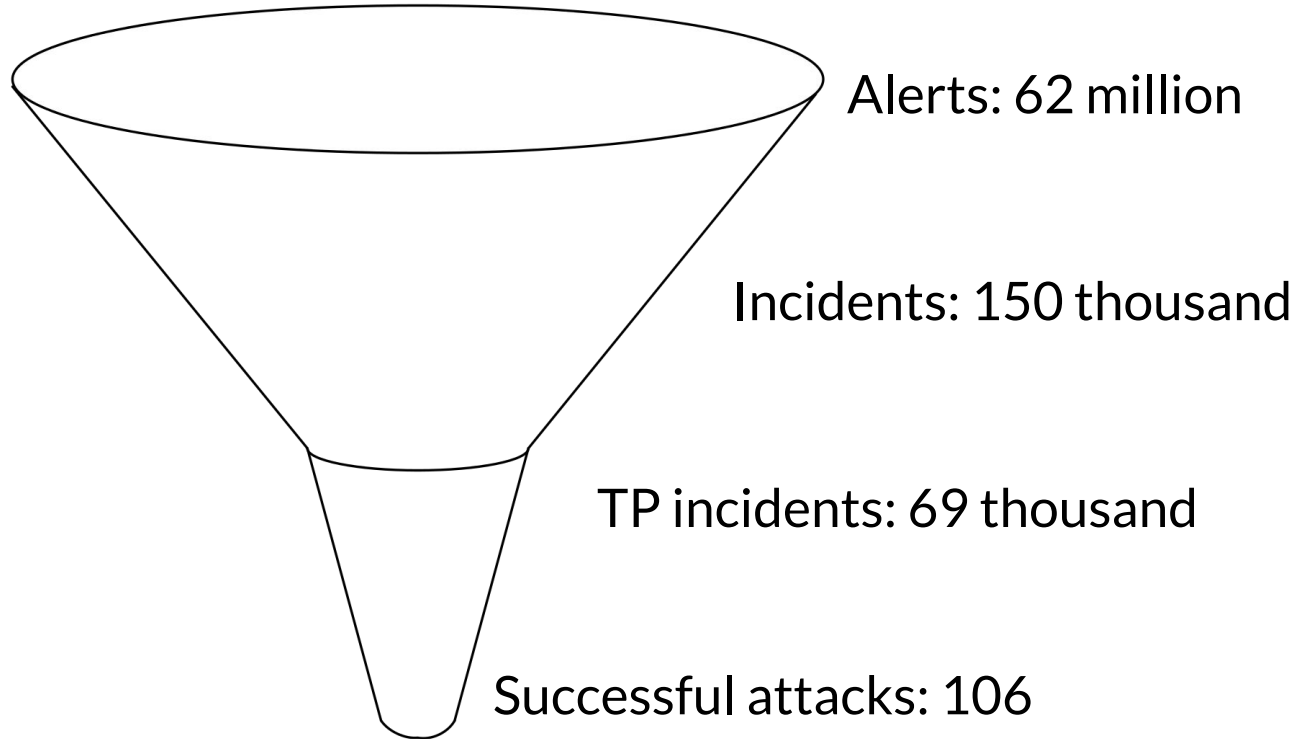
- Precision of MSSP ruleset higher than commercial rulesets.
- MSSP ruleset much smaller than commercial rulesets, but present in **27%** of all true positive incidents.
- Complementary to commercial rulesets, validated by interviews.



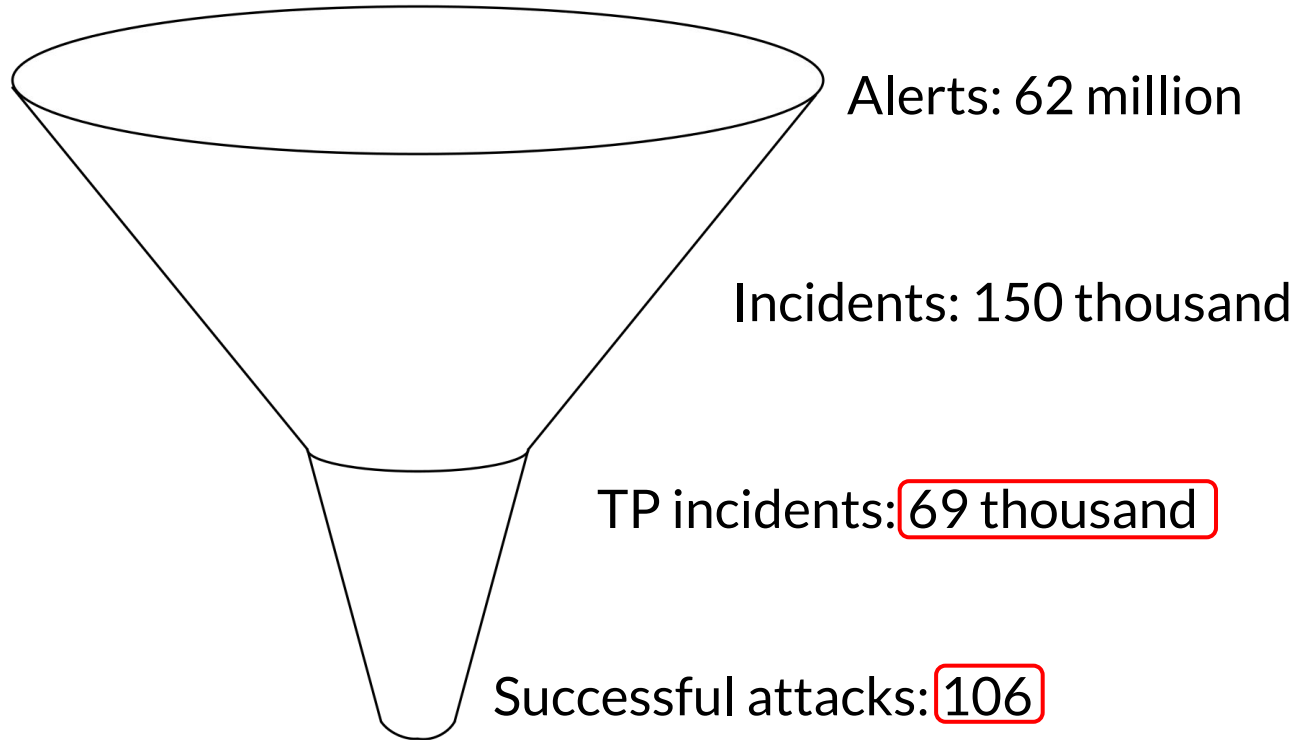
Newest rules produce most incidents



99.8% of TP incidents detected before becoming successful attack



99.8% of TP incidents detected before becoming successful attack



Wrapping up

- Custom ruleset important for the proper functioning of an NIDS.
 - Importance of keeping up to date with threat landscape: newest rules responsible for most incidents.
 - Detects & prevents 99.8% of all TP incidents.
-
- Signature-based systems are still effective.
 - Future work still needed to compare to different (N)IDS approaches.
 - Archaic and obsolete or indispensable to security?