Ruling the Rules

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

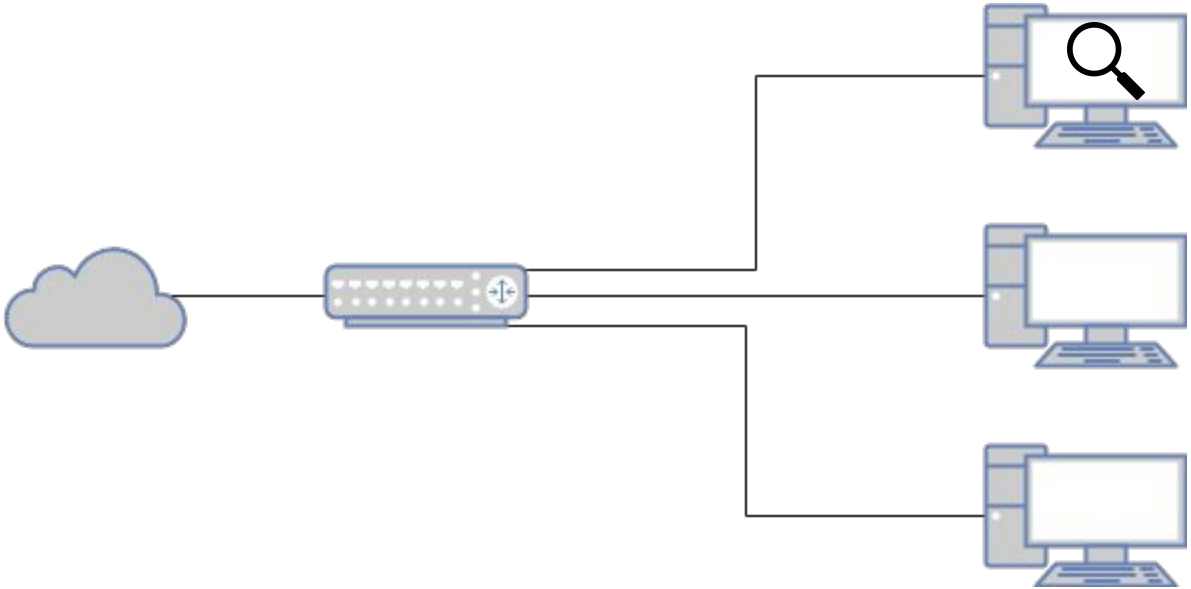
Mathew Vermeer, Michel van Eeten, Carlos Gañán

2022 ACM ASIACCS

TU Delft Delft University of Technology

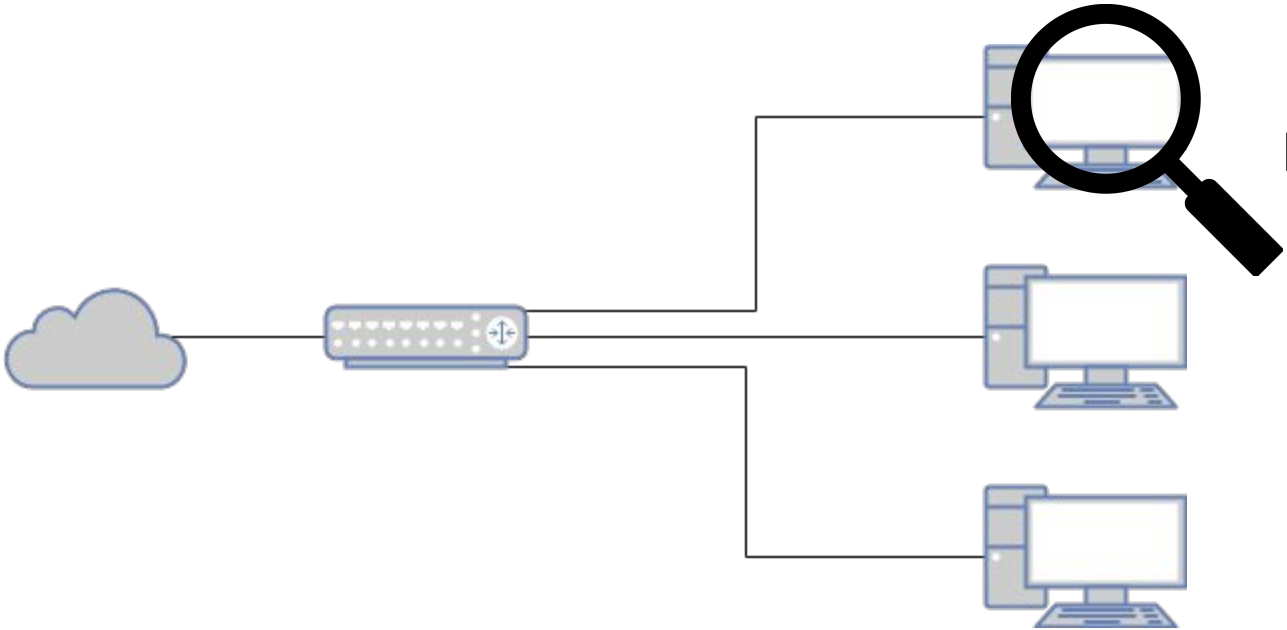

HACKERS LOOKING
AT ALL YOUR
EXPOSED DEVICES
imgflip.com

Intrusion detection systems (IDS)



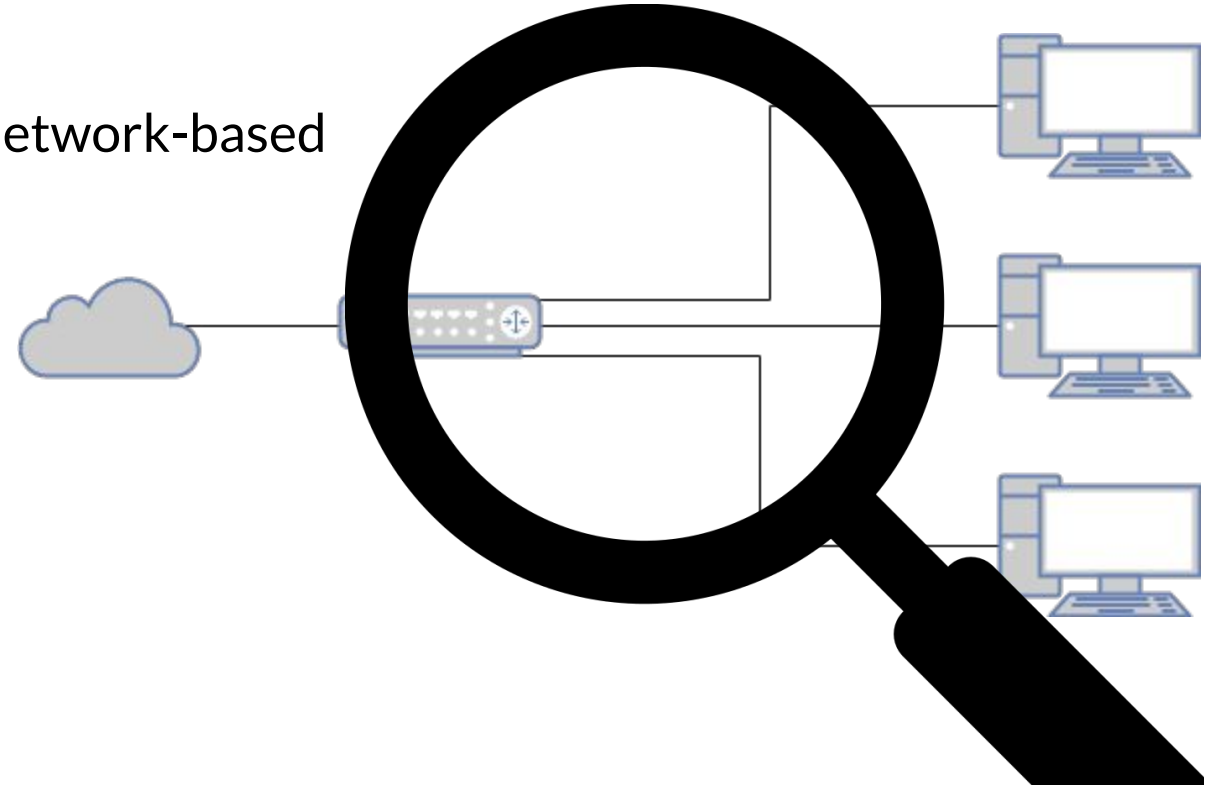
Application-based

Intrusion detection systems (IDS)

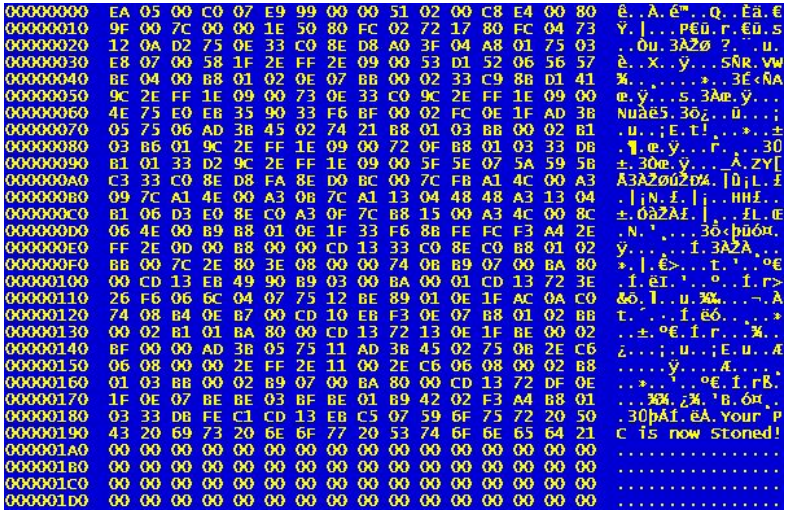


Intrusion detection systems (IDS)

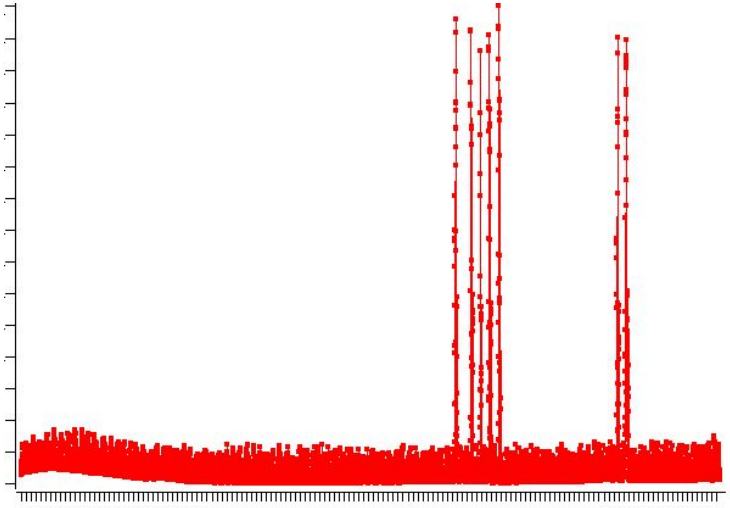
Network-based



Network intrusion detection systems (NIDS)



Signature-based

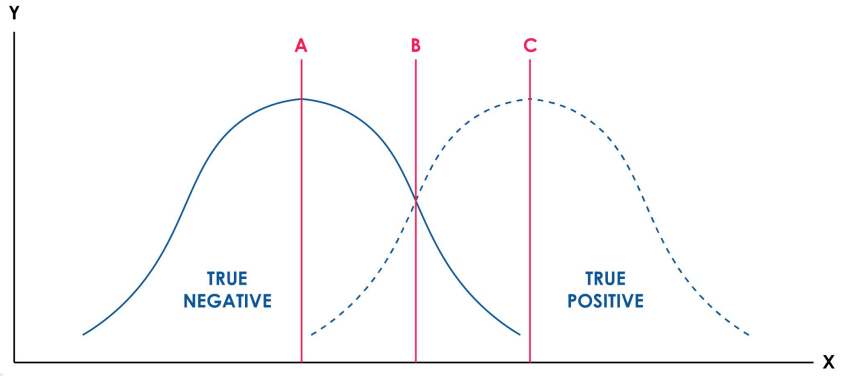


Anomaly-based


SECURITY
COMMUNITY
ANOMALY-BASED
NIDS
SIGNATURE-BASED
NIDS
imgflip.com

The NIDS black box

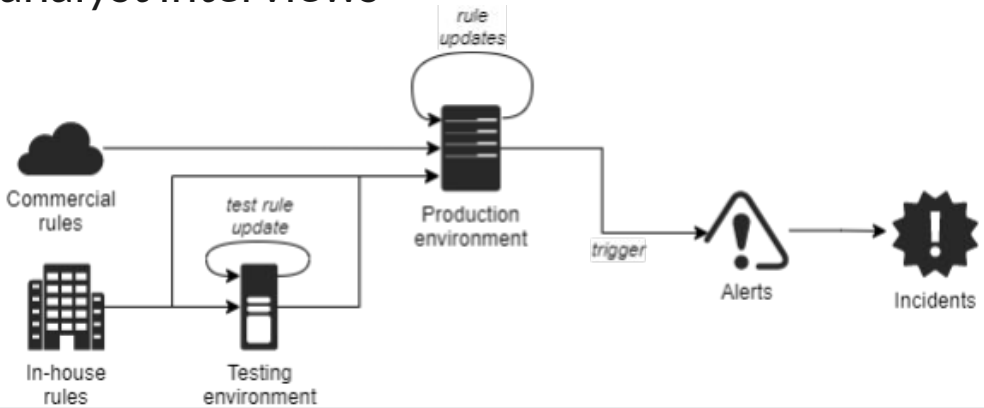
- Not as straightforward as it seems.
  - Why do they work?
  - What role do the rulesets play?
  - How do security professionals keep them working effectively?
- Critical tradeoff: Maximize intrusion detection vs minimize number of alerts.



https://www.publichealthnotes.com/sensitivity-vs-specificity-10-important-differences/

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



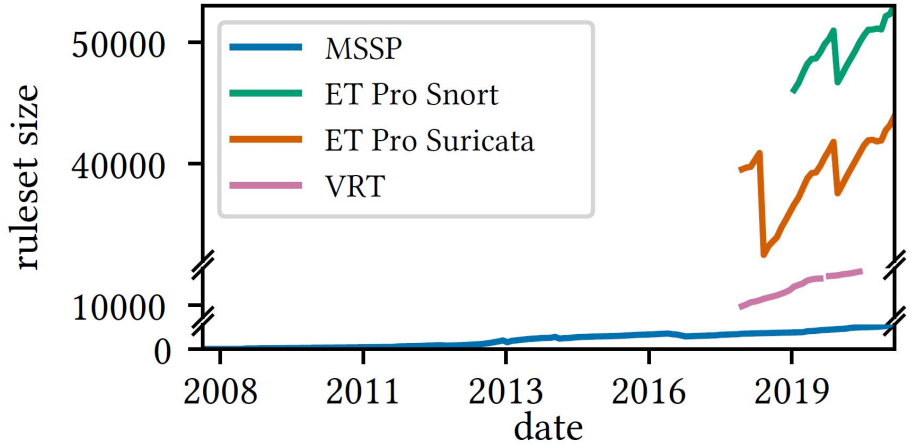
Methodology

- 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.

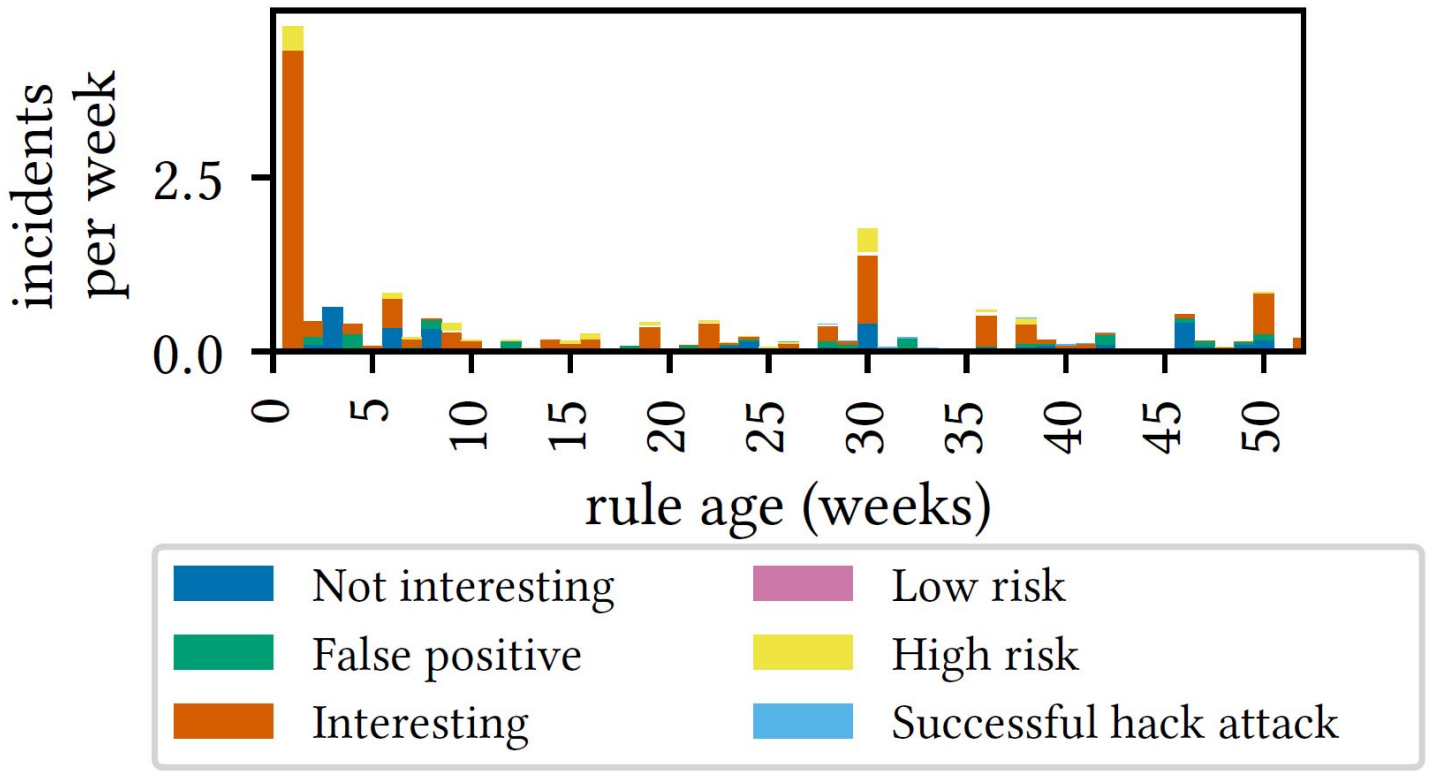
Results

Custom ruleset important for proper functioning of NIDS

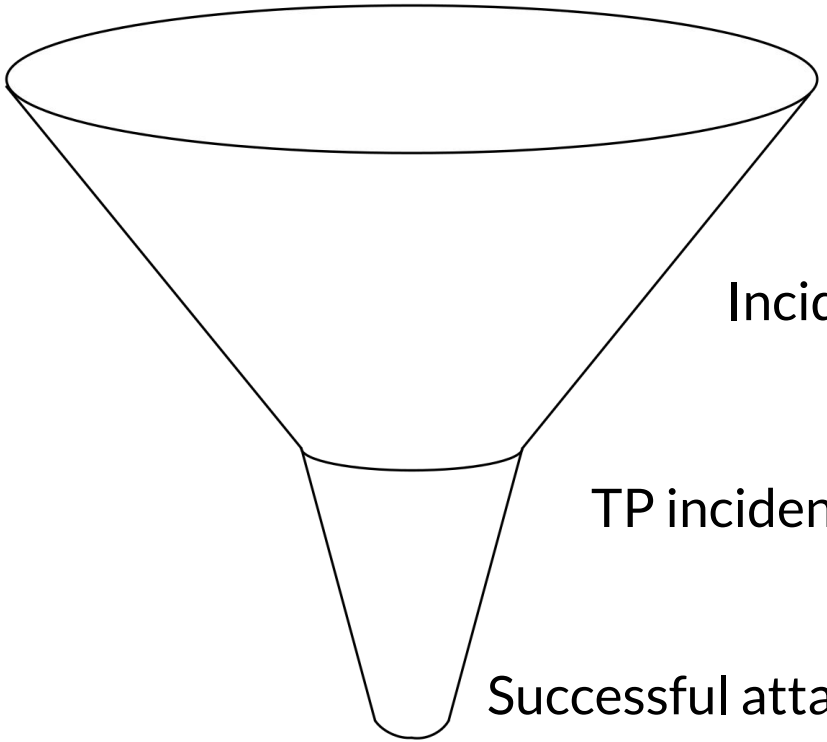
- Precision of MSSP ruleset higher than commercial rulesets.
- MSSP ruleset much smaller than commercial rulesets, but present in **27%** of all true positive incidents.
- Complementary to commercial rulesets, validated by interviews.



Newest rules produce most incidents



99.8% of TP incidents detected before becoming successful attack



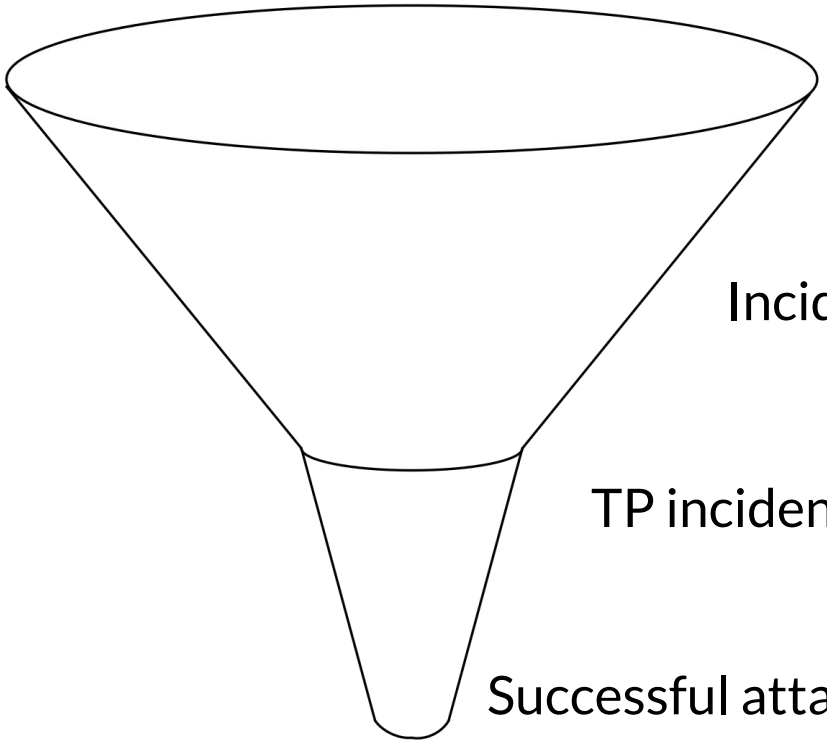
Alerts: 62 million

Incidents: 150 thousand

TP incidents: 69 thousand

Successful attacks: 106

99.8% of TP incidents detected before becoming successful attack



Alerts: 62 million

Incidents: 150 thousand

TP incidents: 69 thousand

Successful attacks: 106

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?