RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SP01-R14

MSPS AND SMBS NEED REAL THREAT INTELLIGENCE

Hal Lonas

Chief Technology Officer
Webroot

Agenda

- The State of Threat Intelligence Today
- What “Real” Threat Intelligence Looks Like
- Why Small / Medium Businesses are Underserved
- How We Can Fix the Problem

THE STATE OF THREAT INTELLIGENCE

Threat Intelligence’s role in CyberSecurity

- CyberSecurity is really an *Information Problem:*
  - *If you knew that the website was bad – you wouldn’t click it.*
  - *If your firewall knew that the IP was bad, it wouldn’t accept the incoming connection.*
  - *If your mobile device knew that the free App was bad, it wouldn’t download and install it.*
  - *If you knew that the executable file was bad, you wouldn’t run it.*

Threat Intelligence Confusion

- Threat intelligence for threat researchers
  - Indicators of compromise
  - Tactics, techniques, procedures
  - Prevention, detection, remediation
  - Often meant to inform… *research*

… more Confusion

- Threat intelligence for machines
  - Machines = Devices (or software)
    - — A place where an action can be taken,
    - — Where a policy can be enforced
    - — Defines a “policy enforcement point”
  - Machine readable – often binary format
  - Various standards and orgs
    - — TAXII
    - — STIX
    - — OASIS

… more Confusion: Buzzwords and Marketing

- Intelligence can be derived from analysis of raw data
  - Threat Researcher Human analysis
  - Artificial Intelligence
    - Machine Learning is a subset of AI
- Actionable
  - Who or what is taking what action?
- Real Time
  - What does that mean?
- Contextual

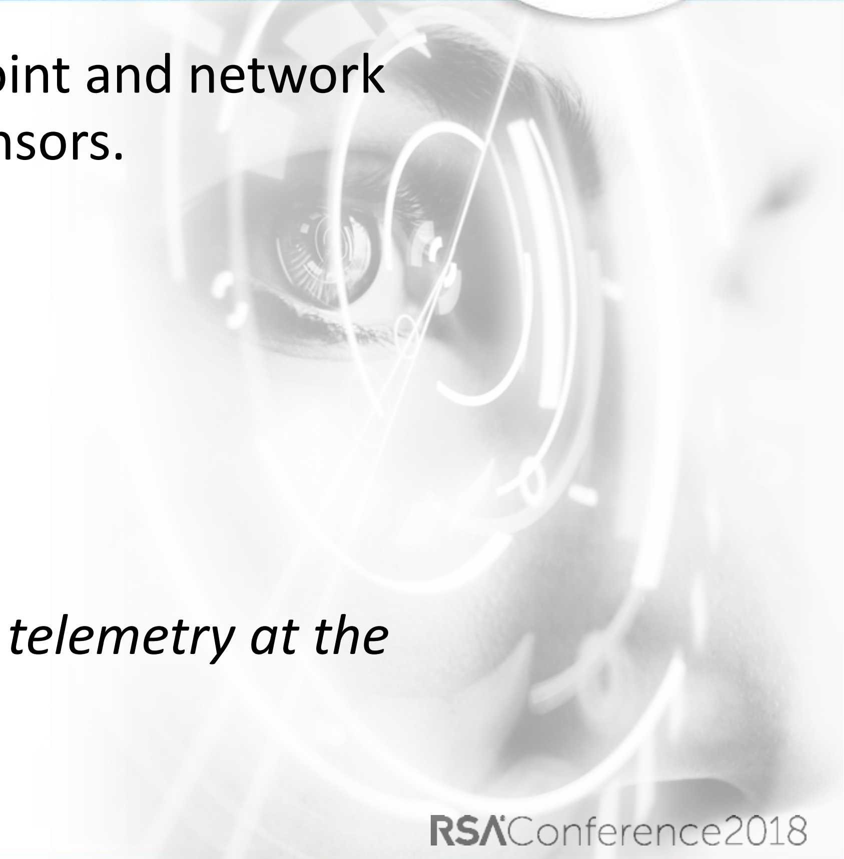
NEXT-GENERATION
SIMPLE COMPREHENSIVE OUTPACE
CLOUD-BASED
AUTOMATED
CLOUD
THREAT INTELLIGENCE SELF-LEARNING
INTEGRATED
NETWORKING
BRILLIANCE
PROACTIVE INNOVATIVE
ENDPOINT
EFFICI
CUTT
ELASTIC NEXT-GENERATION DWELL TIME
DETECT
OUTPACE
OUTPACE ELASTIC BUSINESS
LIGHTWEIGHT CLOUD-BASED PROTECTION DETECTION
FUT
DETECT
DYNAMIC
MITIGATE RISKS
BULLET-PROOF
BYOD
LEARN
ELASTIC INNOVATIVE NETWORKING MACHINE-LEARNING OUTPACE LEARNING
GLOBAL VISIBILITY
MACHI
FUTURE PROOF INTELLIGENCE-DRIVEN BULLET-PROOF
MITIGATE RISKS

WHAT “REAL” THREAT INTELLIGENCE LOOKS LIKE

What Real Threat Intelligence *Isn't*

- Sandboxes
  - Not representative of reality (VMs), can't simulate enough variety
  - Malware can spot artificial environments
  - Too slow to wait, can't be inline
  - Times out at some point - Can't catch APTs
- Crawlers
  - Can't replace humans – limited in user agent, arguments, ads, geos
  - Can't get to unlinked or orphaned URLs – email spears for example
- Honeypots
  - Network attacks can spot artificial lures
- A combination of feeds, lists, or unverified sources
  - False positives, stale or incomplete lists
  - Crowdsourcing isn't accurate or timely

What Real Threat Intelligence Should Be



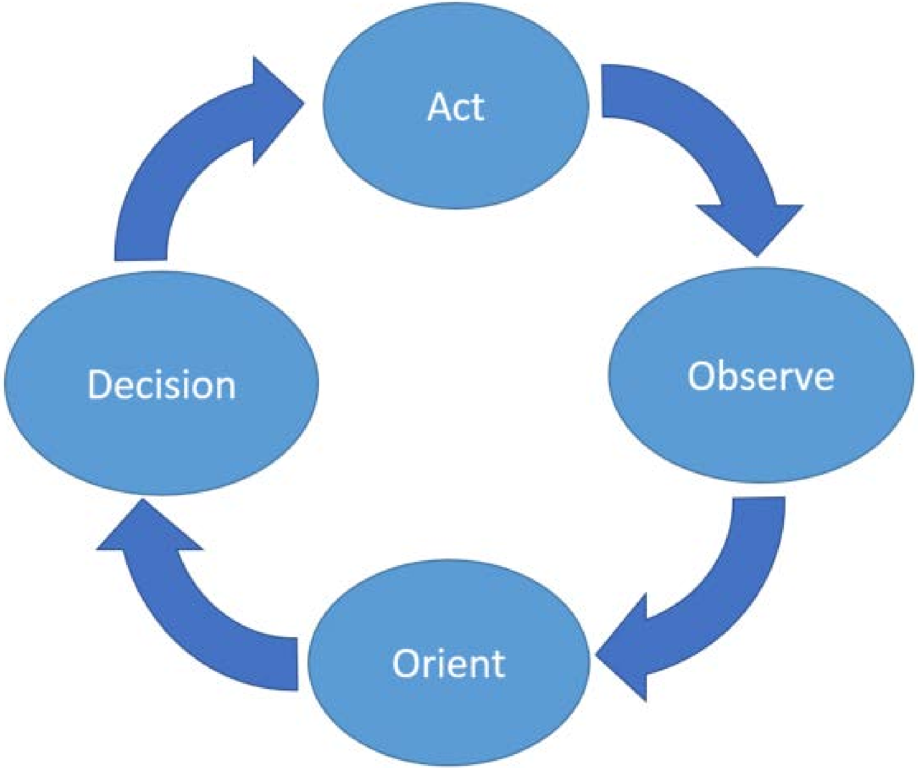
Source is everything: Products and endpoint and network data are high fidelity threat telemetry sensors.

- Real products
- Real machines
- Real people

Difficult to provide protection and gather telemetry at the same time.

What Real Threat Intelligence Should Be (cont.)

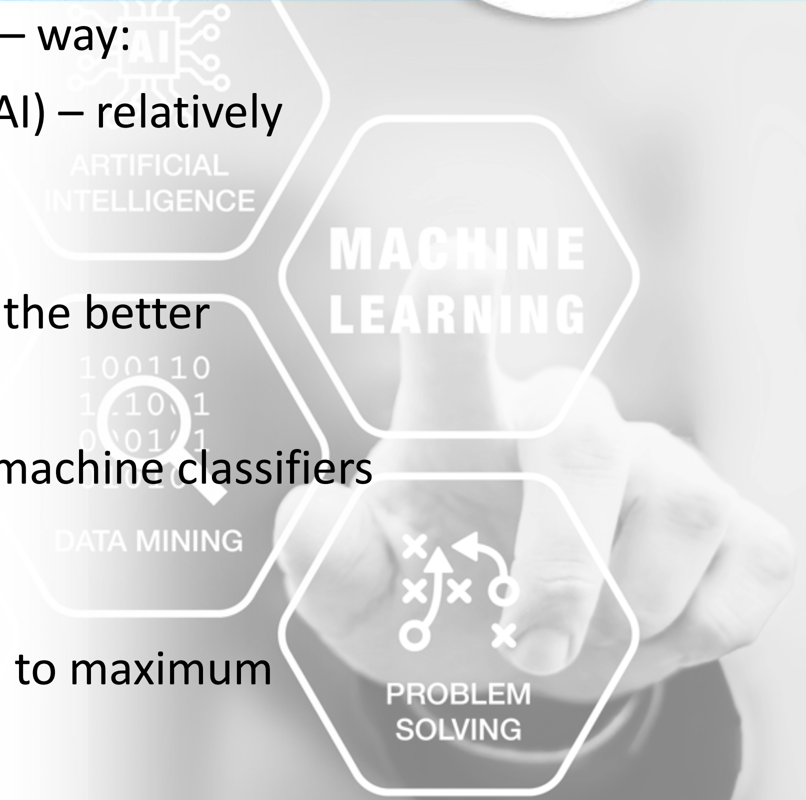
- Gather telemetry and observations in real time
  - Observe, orient, decide, act (OODA)
    - — Fast feedback loops are vital
  - Shorten time from observation to action to seconds.
  - Only a machine (automation) can do that.
- Challenges
  - Terabytes of data, several hundred billion behaviors per day



Converting raw data to Real Threat Intelligence

Machine learning is currently the best – and only – way:

- ML is a special subset of artificial intelligence (AI) – relatively modest in scope
- Fed by threat telemetry from real products
- Historical perspective on data – the more data the better
- Trained and refined by threat researchers
- Human skill and experience incorporated into machine classifiers that never get tired, need breaks, etc.
- Best algorithms for a low signal to noise ratio
- Doesn’t replace humans; uses their knowledge to maximum advantage



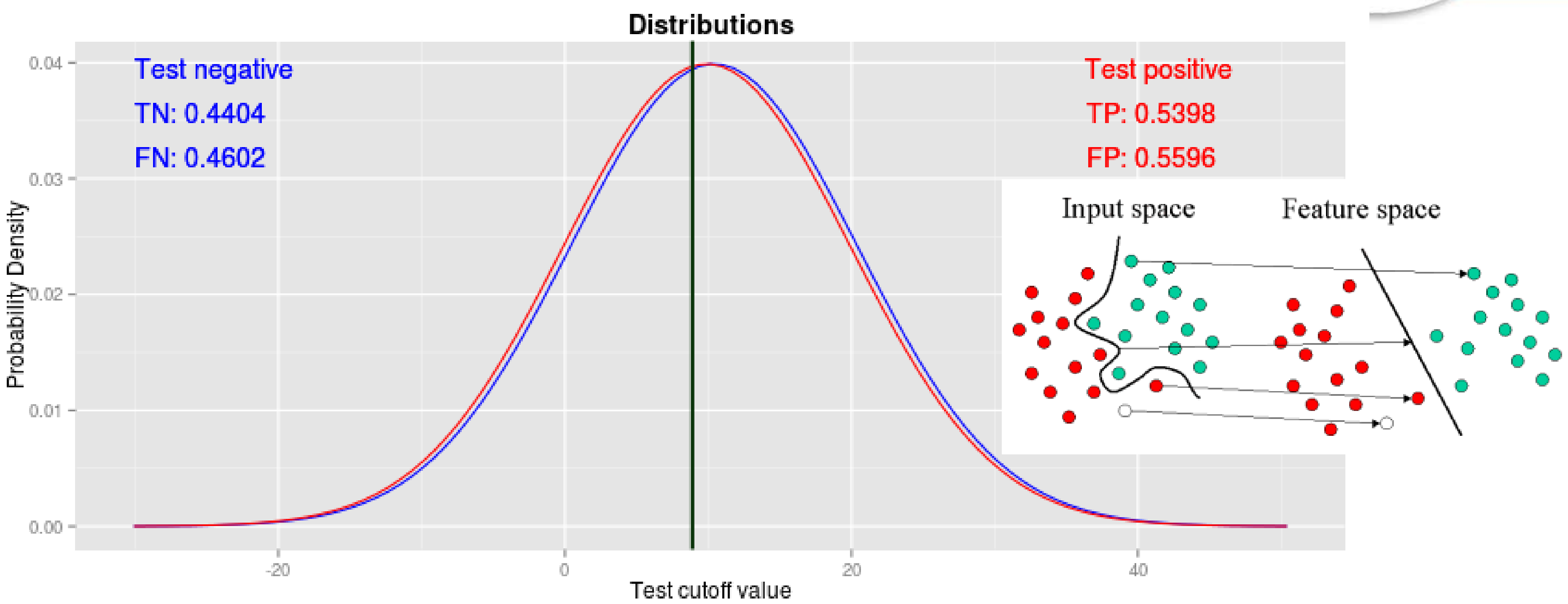
Real Threat Intelligence based on Machine Learning

No “silver bullet”

- MED, DL, algorithms
- Fast Math, performance, C code, Linux
- Infrastructure for Scale
- Real People / Real Products
- 100 Million Features
- 10 years experience, world class talent
- Active Learning
- Active Feedback
- Score granularity
- Classifier Reputation
- Sources of data
- Time from discovery to publish
- Contextual Analysis
- NoSQL and Fast Data
- Partners and Customers protected every day
- 6th generation
- Training compute power
- TR and WA teams train models

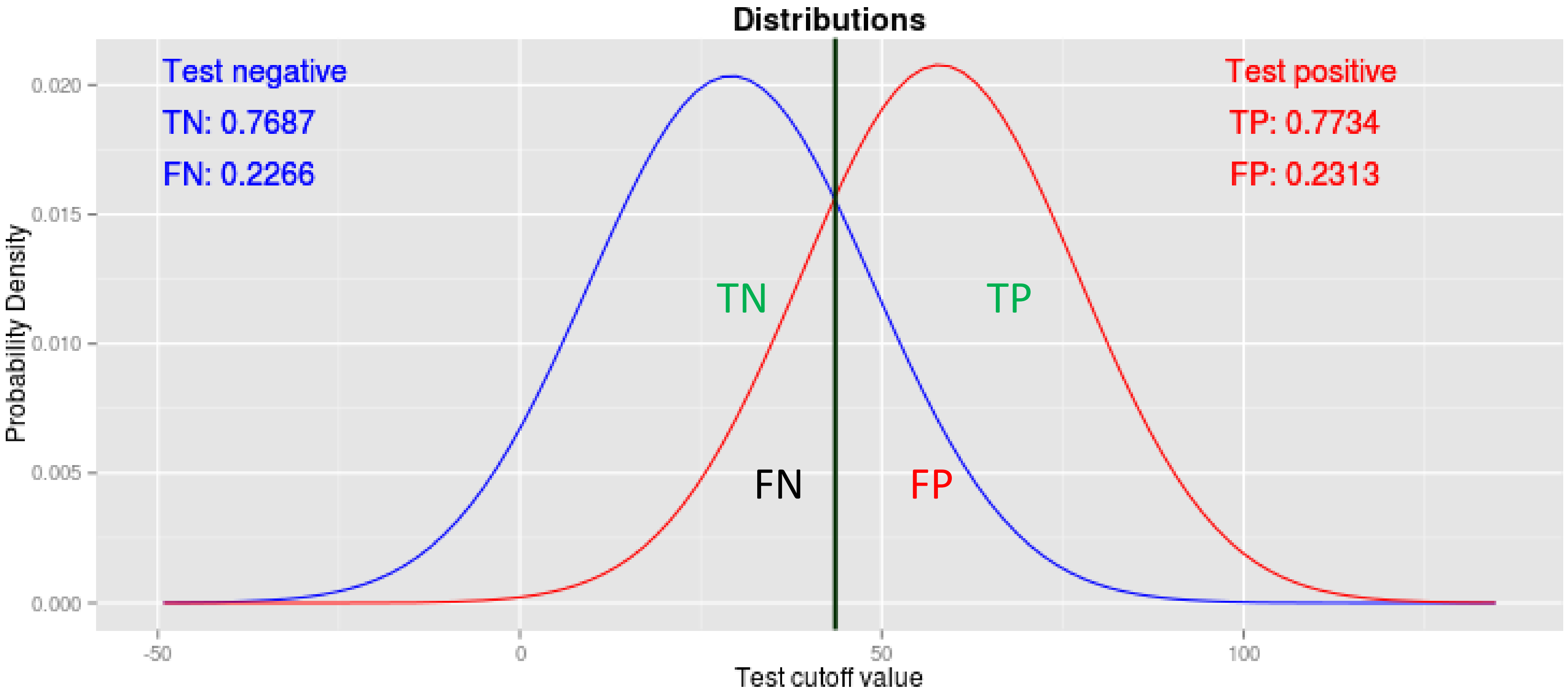
WEBROOT
Smarter Cybersecurity

How do you measure your ML model Receiver Operating Characteristic (ROC)

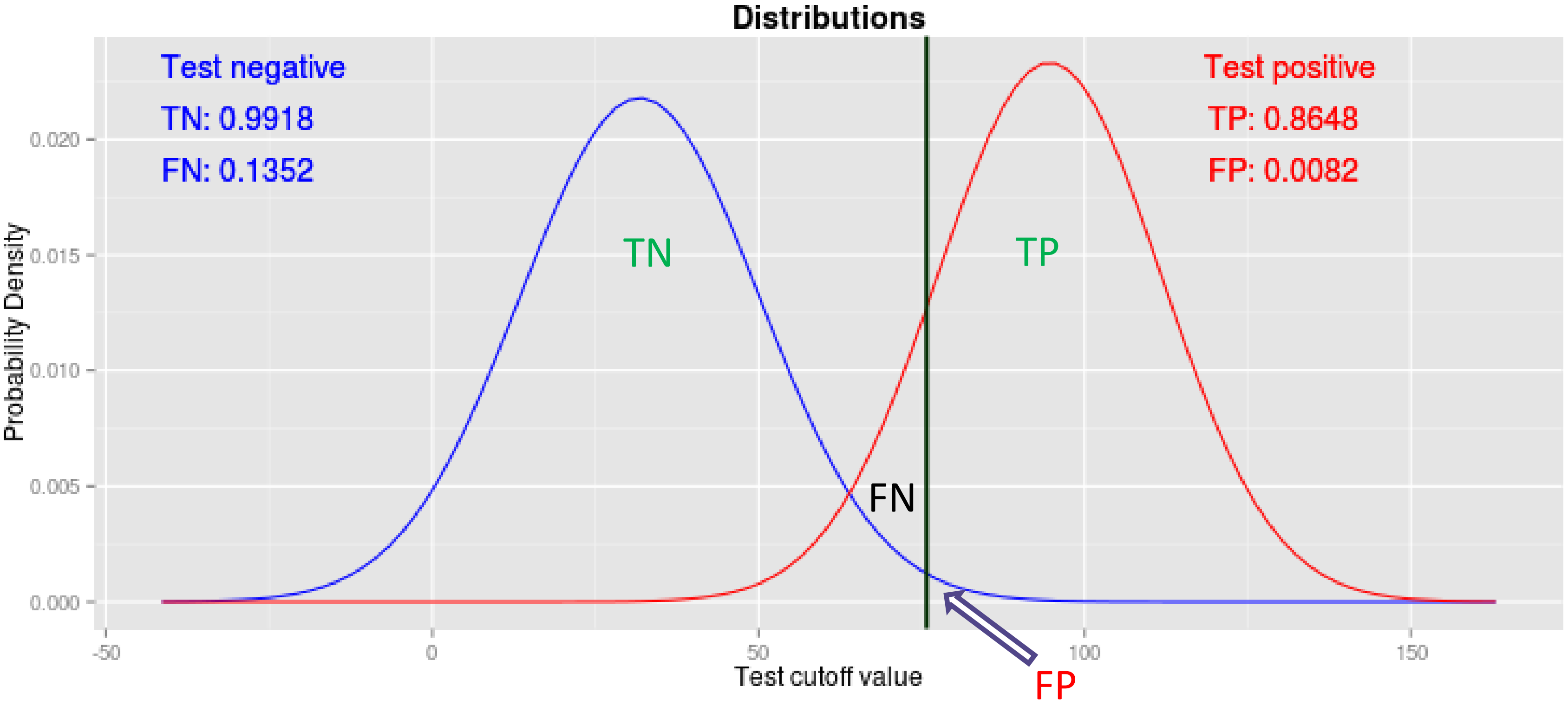


Object is to define a mathematical space and plane to separate (classify) objects

Improvement…



Really good…

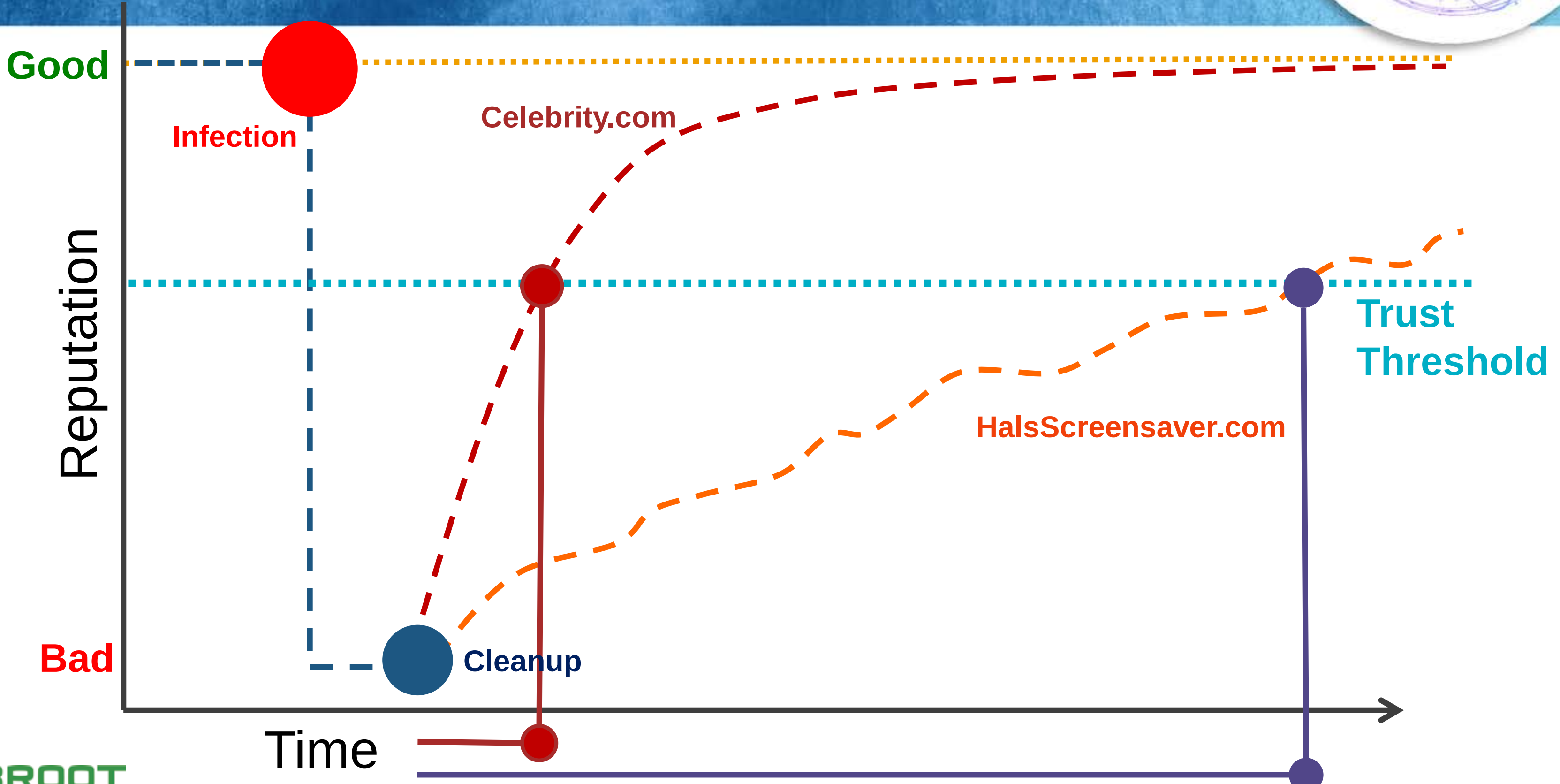

Distributions
Test negative
TN: 0.9918
FN: 0.1352
Test positive
TP: 0.8648
FP: 0.0082
TN
TP
FN
FP
Probability Density
0.020
0.015
0.010
0.005
0.000
-50
0
50
100
150
Test cutoff value

Contextual Threat Intelligence

Threats don’t operate in isolation. Contextual intelligence must:

- Analyze relationships between internet “objects” (URLs, IPs, apps, files)
- Fixup discontinuities
  - For example, a bad file can’t come from a good URL
- Determine likelihood of future risk based on connections to malicious objects
- Provide relationship context and risk categorization in a consumable format
- Reputation can be based on “distance from bad”

Reputation Over Time – Real Threat Intelligence



Decisive Threat Intelligence

- Enables human administrators to create automated security policies.
- Enables machines to automatically allow or block according to policies.
- Enables time-of-need security decision-making.
    - For example, real time anti phishing based on content downloaded to browser.

WHY SMBS ARE UNDERSERVED

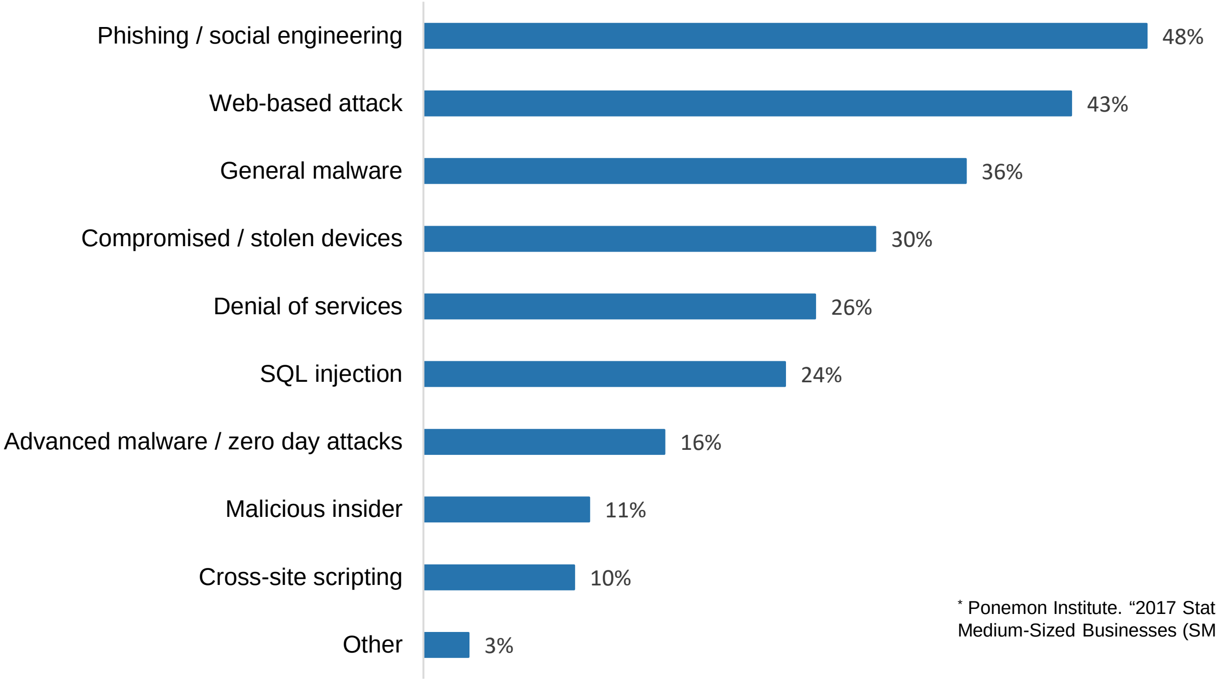
(some definitions)

❖SMB = *Small / Medium Business (100 - 1000 employees)*

❖MSP = *Managed Service Provider*

SMBs Under Siege

Attacks Faced by Small and Medium-sized Businesses*



* Ponemon Institute. “2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)”

SMB Challenges

- The market doesn’t serve SMBs
  - Products and services focus on enterprises
  - It’s hard to make money selling to SMBs
- SMBs have less time and fewer resources
  - No threat researchers, SOCs, NOCs, spare personnel
- SMBs are easy targets
  - Hacking, ransomware, BYOD, untrained users

❖ SOC = *Security Operations Center*

❖ NOC = *Network Operations Center*

HOW WE CAN FIX THE PROBLEM

CyberSecurity is an Information Problem

- Endpoints and networks need real-time anti-phishing and anti-malware
- Users wouldn’t click links or run apps if they knew they were at risk
- 90% of successful network breaches are caused by user error*
- Businesses need ongoing, relevant security awareness training for end users

* Verizon. “2017 Data Breach Investigations Report.”

What We Can Do for SMBs

- More than ever SMBs rely on MSPs for security expertise. We can:
  - Arm MSPs and their clients with enterprise grade security, services, and reports
  - Create security products for MSPs and SMBs that use real threat intelligence
  - Enable greater automation and less dependency on human resources
  - Provide security awareness training for end users

Problems		Solutions
MSPs and SMBs are ill-equipped to deal with security problems	→	Arm MSPs to act as security experts
Poor handling of today’s threats: phishing, polymorphic, APTs	→	Build protections against modern threats into the products
ML / AI hype has confused security decision-makers	→	Demystify, use ML to create decisive threat intelligence
End users continue to be a weak link and exploitable	→	Security awareness training to help end users avoid common attacks
Endpoint security is a mess: legacy, overhyped, poor efficacy	→	Cut through the hype and deliver lightweight EP, with cloud security based on ML
IoT problems are emerging	→	Network security products like DNS can protect ALL devices on the network
Cybercriminals focus on SMBs	→	Arm SMBs (through MSPs) with enterprise-grade security products tailored for their unique needs

Next Steps

- Understand what real threat intelligence is (and isn’t)
- Understand decisive threat intelligence
- Understand what decisive threat intelligence can do for businesses of all sizes—especially the underserved SMB