Threat Intelligence and Layered Security in the ~~Target Breach~~ Equifax Era

Ted Gruenloh
Chief Operating Officer
Sentinel IPS

@tedgruenloh
@sentinelips

*

New-School Layered Security

"Prepare to be breached."
Shift from preventative to detective? Sort of.

- ✓ The perimeter is disappearing: Blame The Cloud™, mobile devices, SDWANs, etc.
- ✓ Pick your vector: External vulnerabilities, phishing, vendor software, CPUs(!)
- ✓ On the Edge: TIG, IPS, Firewalls/UTMs, Vulnerability Scanning, Penetration Testing
- ✓ Endpoints: Anti-virus, AI and Machine Learning, Patching, Software Updates
- ✓ In Between: IDS, NSM Products, Web Proxies, SPAM Filters, Sandboxes, DNS tools
- ✓ Effective Security == Protection + Visibility

So, where does Threat Intelligence fit in?
All of the above!

What is Threat Intelligence?

… Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

- Rob McMillan, Gartner

Imagination is more important than knowledge.

- Albert Einstein, Really Smart Guy

No, really. What is Threat Intelligence?

IDS/IPS Event Feedback Loop

Universities
ISPs and Carriers
IDS/IPS Customer base

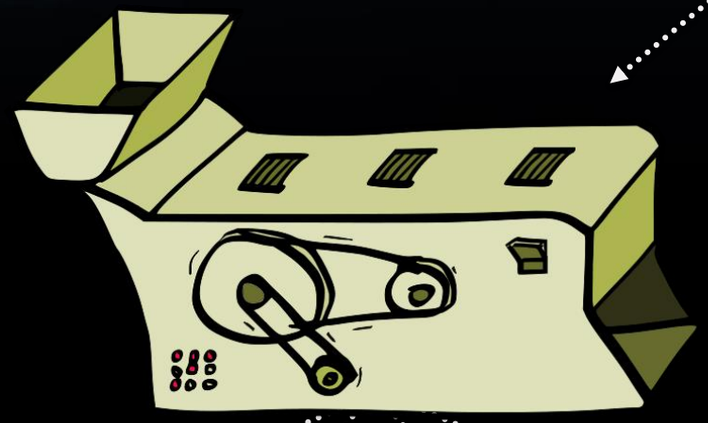
Malware Exchanges & Sources

Malware Exchange (major NetSec vendors)
VirusTotal.com
VirusShare.com

Sandnets

Pcaps

Data Engine
(Pcap analysis and data correlation)



SENTINEL INTRUSION PREVENTION SYSTEMS

EMERGING THREATS

criticalstack

This is Threat Intelligence.

IDS/IPS Rulesets

IP and Domain Reputation Lists

IOCs and TTPs (“Context”)

Other Proprietary Information

OK. What does Threat Intelligence look like?

Old School/Grass Roots: Lists of IPs and/or URLs
Could be as simple as a text file of IP addresses, or domains associated with bad actors and command & control servers

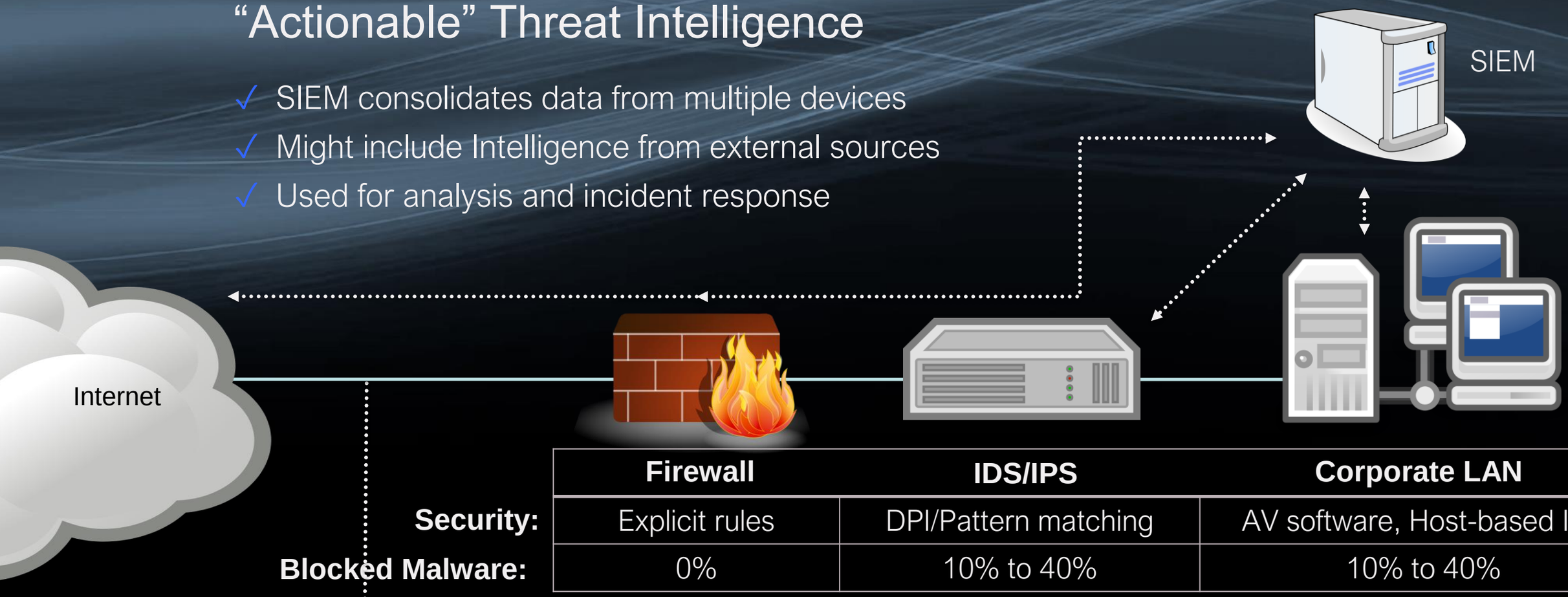
New School: STIX and TAXII
Comes from DHS, and designed and maintained by MITRE. Provides a common markup language and method of exchange for threat intelligence data. Many ISACs and private companies provide their threat intelligence in STIX. (Other formats include OTX and CIF, among others.)

```
<stix:STIX_Header>
   <stix:Title>Example watchlist that contains IP information.</stix:Title>
   <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators - Watchlist</stix:Package_Intent>
</stix:STIX_Header>
<stix:Indicators>
   <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-33fe3b22-0201-47cf-85d0-97c02164528d">
      <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">IP Watchlist</indicator:Type>
      <indicator:Description>Sample IP Address Indicator for this watchlist. This contains one indicator with a set of three IP addresses.</indicator:Description>
      <indicator:Observable  id="example:Observable-1c798262-a4cd-434d-a958-884d6980c459">
         <cybox:Object id="example:Object-1980ce43-8e03-490b-863a-ea404d12242e">
            <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
               <AddressObject:Address_Value condition="Equals" apply_condition="ANY">10.0.0.0##comma##10.0.0.1##comma##10.0.0.2</AddressObject:Address_Value>
            </cybox:Properties>
         </cybox:Object>
      </indicator:Observable>
   </stix:Indicator>
</stix:Indicators>
```

Threat Intelligence and Layered Security

“Actionable” Threat Intelligence

- ✓ SIEM consolidates data from multiple devices
- ✓ Might include Intelligence from external sources
- ✓ Used for analysis and incident response



	Firewall	IDS/IPS	Corporate LAN
Security:	Explicit rules	DPI/Pattern matching	AV software, Host-based IPS
Blocked Malware:	0%	10% to 40%	10% to 40%

“Active” Threat Intelligence

- ✓ Malicious IP and/or Domain intelligence
- ✓ Pushed out to security devices regularly
- ✓ Collaboration of InfoSec community
- ✓ e.g., ransomware C2 servers

BLOCKED MALWARE AND RANSOMWARE

~85%

MALICIOUS SCANS, PROBES, EXPLOITS

~70%

Publicly Shared Threat Intelligence

The Who.

A sampling of NetSec organizations that provide free Threat Intelligence.

http://hailataxii.com

http://iplists.firehol.org/

https://criticalstack.com/

http://rules.emergingthreats.net

Open Threat Exchange

CI Army list at http://cinsarmy.com

http://shadowserver.org
and https://www.abuse.ch

Center for Internet Security

http://dshield.org
(SANS Internet Storm Center)

Publicly Shared Threat Intelligence

The How.

Here's how we do it.

open source firewalls, curl, python urllib, etc.

CINS Lists
("Active" Threat Intelligence)
CINSarmy.com

And in conclusion…

Layered security still makes sense as a network security strategy, and its diversity produces better threat intelligence. And, active threat intelligence can dramatically improve a network's protection from malware and other attacks.

Questions?

SENTINEL
INTRUSION PREVENTION SYSTEMS™

Ted Gruenloh
Chief Operating Officer
(972) 991-5005
tedg@sentinelips.com

http://www.sentinelips.com/free

@tedgruenloh
@sentinelips

Ted Gruenloh