Offense Informs Defense

- Enterprises are under constant attack
- Monitoring systems alert to suspicious events that SoC analysts review
- Countless analysts across the world respond to the same or similar attacks
- Aggregating these indicators and the analyst's results to share with the community is a profoundly effective mechanism to enhance detection and accelerate response.

THREATSTREAM®

Threat Intelligence

Definition: Threat intelligence is 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.

Common (Tactical) Threat Intelligence Indicators:

- IP Addresses
- Domain Names
- URLs
- File Hashes/MD5s
- Email Addresses

Fog of More

Network:
- IDS: (Bro, Suricata, Snort)
- SiLK /NetFlow
- DLP
- Network Forenics: Netwitness, nPulse, Solera
- Moloch
- Google Stenographer
- NGFWs
- FireEye EX

Logs:
- SIEM (Splunk, ArcSight)
- Proxy/Secure Web Gateway
- Access
- VPN
- Syslog
- AD

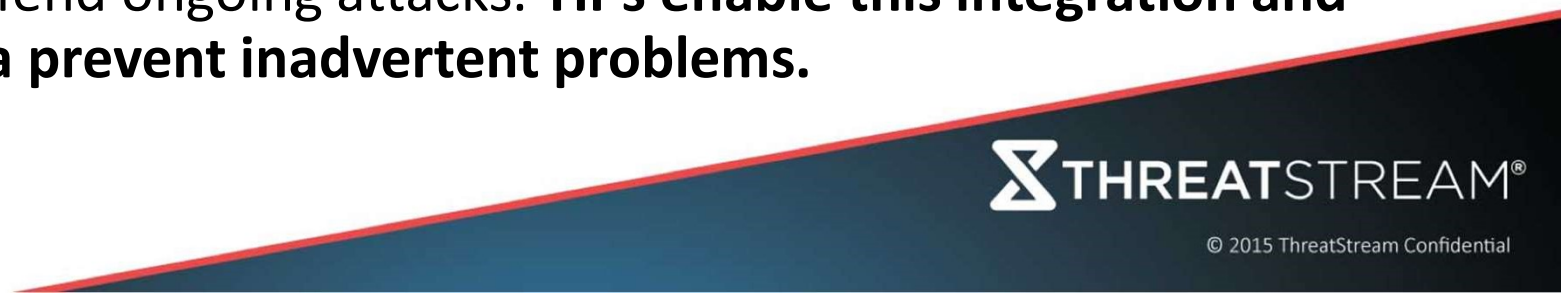
Host:
- Antivirus
- CarbonBlack
- PowerShell
- MiR
- Tanium
- RSA ECAT
- OSquery
- Grr
- OSXCollector
- RedCloak
- CounterTack
- SysMon
- AutoRunSC

Overwhelmed Analyst

THREATSTREAM®

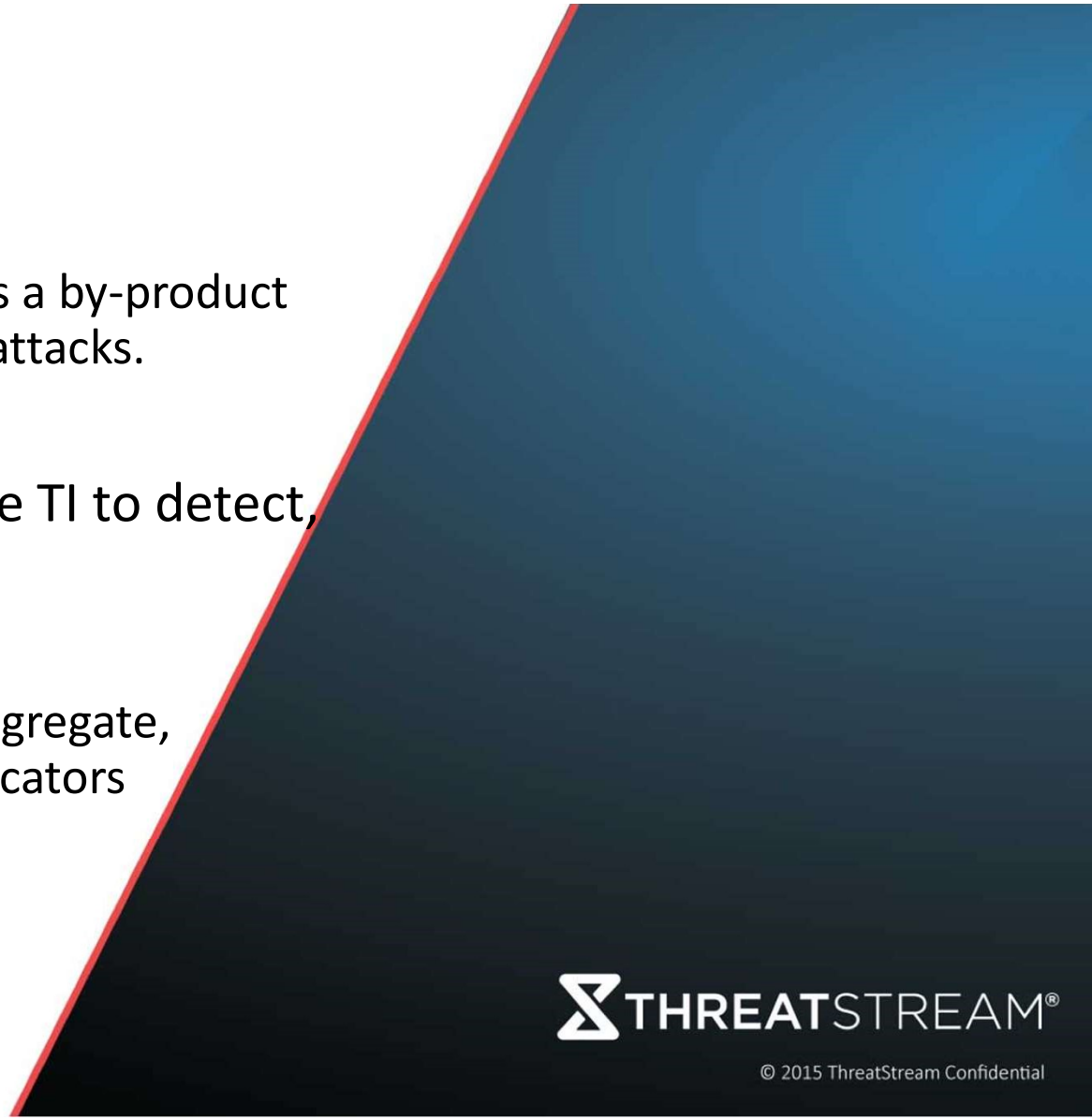
Threat Intelligence Platforms

- TIPs are systems that aggregate, normalize, retain, and distribute TI.
- Actors re-use infrastructure and TTP for cost savings and because they (usually) can.
- Sharing TI within trusted groups (especially within industry verticals) is an effective strategy to efficiently detect attacks, **but this has to be balanced against the fog of more.**
- Automated integration/operationalization of TI is critical to effectively detect and defend ongoing attacks. **TIPs enable this integration and clean the data prevent inadvertent problems.**



Conclusions

- Large amounts of threat intelligence is a by-product of security operations in response to attacks.
- SOC defenders commonly leverage TI to detect, triage, and respond to attacks.
- Threat Intelligence Platforms (TIPs) aggregate, normalize, and distribute cleaned indicators suited for automated ingestion and correlation which speeds blocking, detection, and response.



Contact

Matthew Wollenweber

Sr. Research Engineer

www.threatstream.com

info@threatstream.com

@ThreatStream