intigrityShield

Threat Intelligence (TI)

Add global context to accelerate detection and elimination/containment of threats

According to SANS 2022 Cyber Threat Intelligence Survey

A key strategy and process must be in place to automate the use of threat intelligence and this capability must be available to all SOC, incident response (IR) and threat hunting team members. “In this regard, the first result is that only 46% of respondents integrate their threat intelligence within their defense and response systems. This is not great, as we would all hope to see a much higher number, but the good news is that this represents a significant increase from the 41% of last year. Organizations integrate CTI information into defense and response systems most commonly via CTI platform (67% of respondents), followed by intelligence service providers (59%) and vendor APIs (45%). Again, this shows that vendors currently play an important role in making such integration happen.”

The results of the survey highlights the important role that intigrityshield aiSecure™ TI360 provides in automating and adding real-time enrichment for teams. Threat intelligence enrichment is a key aspect of empowering teams within the organization with transparent IOCs/Threat Interdictors enabling proactive threat detection, threat hunting, forensic reporting and insights for IR teams.

Threat Intelligence and its effective uses

Use of threat intelligence to enrich logs, flows and event data to create the IOCs is daunting task for any SOC team. The traditional way of humans doing reviewing and applying threat intelligence does not work in today’s digital world that has massive amounts of data that hide IOCs and zero-day threats.

It is critical for SOC teams to have access to a wide range of threat intelligence sources, which are used to enrich data in real-time in-memory and generate the IOC’s, a far better method that the legacy way of trying to do manual rule-based enrichment.

intigrityshield aiSecure TI360 (Threat Intelligence)

intigrityshield's approach has always focused on the incorporation of real-time enrichment based on wide range of threat intelligence feeds to give customers a transparent view of what is happening around the world in the cybersecurity domain and known threats exposers.

aiSecure TI360 includes a variety of threat feed sources, which are curated by intigrityshield. intigrityshield aiSecure TI360 builds the intelligence from more than five hundred billion global event feeds ingested every day by intigrityshield as well as specialized threat intelligences feeds from trusted sources like governments, open source, and alliances of industry associations.

aiSecure TI360 Capabilites

1. Host Names and Public IPs: Enables protection against known hostnames and IPs that are sources of threats such as APTs, bots, compromised host/domains, exploit kits, malicious name servers and blacklisted IPs.

2. Anti-malware: This set enables protection against hostnames that contain known malicious threats that can act on or take control of your system, such as malware command and control (C&C), malware download and active phishing sites.

3. Ransomware: The ransomware set enables protection against hostnames that contain malware that restricts access to the computer system that it infects and demands a ransom for removal of the restriction. Some forms of ransomware encrypt files on the system's hard drive. Others may simply lock the system and display messages intended to coerce the user into paying.

4. Known Bots: Known Bots IPs or those using reserved IPs. Numbers Authority (IANA) or a delegated Regional Internet Registry (RIR). The areas of unallocated address space are called "bogon space." Many ISPs and end-user firewalls filter and block bogons because they have no legitimate use, and usually are the result of accidental or malicious misconfiguration.

5. DHS (IP, Host Names and Domains)
This feed is normalized and ingested to give customers another set of high velocity threat feeds. It is not fully validated by either DHS or intigrityshield because its purpose is to to enable customers as soon as data becomes available so that speed is of the essence here, not the velocity.
DHS Automated Indicator Sharing Terms of Use available: www.us-cert.gov/ais. and must be handled in accordance with the Terms of Use. Prior to further distributing the AIS data, you may be required to sign and submit the Terms of Use available at: www.us cert.gov/ais. Please email ncciccustomerservice@hq.dhs.gov for additional information.

6. Blacklisted & Exploit IPs: The blacklisted IP set enables protection against known malicious or compromised IP addresses. These are known to host threats that can act on or control a system by way of C&C malware downloads and active phishing sites. Exploit IPs contain malicious programs used to execute "drive-by download" attacks to infected users with malware. These exploit kits target vulnerabilities in the user's machine (usually due to unpatched versions of Java, Adobe Reader, Adobe Flash, Internet Explorer and other applications) to load malware onto the victim's computer.

7. Bot IPs: This set enables protection against self-propagating malware designed to infect a host and connect back to a C&C center. Bots are typically used for log keystrokes, gather passwords, capture and analyze packets, gather financial information, launch DoS attacks, relay spam and open back doors on the infected host.

8. Malware DGA hostnames: Domain generation algorithms (DGA) appear in various families of malware used to periodically generate many domain names that can act as rendezvous points with their C&C servers. Examples include Ramnit, WannaCry, Conficker etc.

9. Tor Exit Node IPs: Tor Exit Nodes are the gateways where encrypted Tor traffic hits the Internet. This means an exit node can monitor Tor traffic (after it leaves the onion network). The Tor network is designed to make it difficult to determine its traffic source.

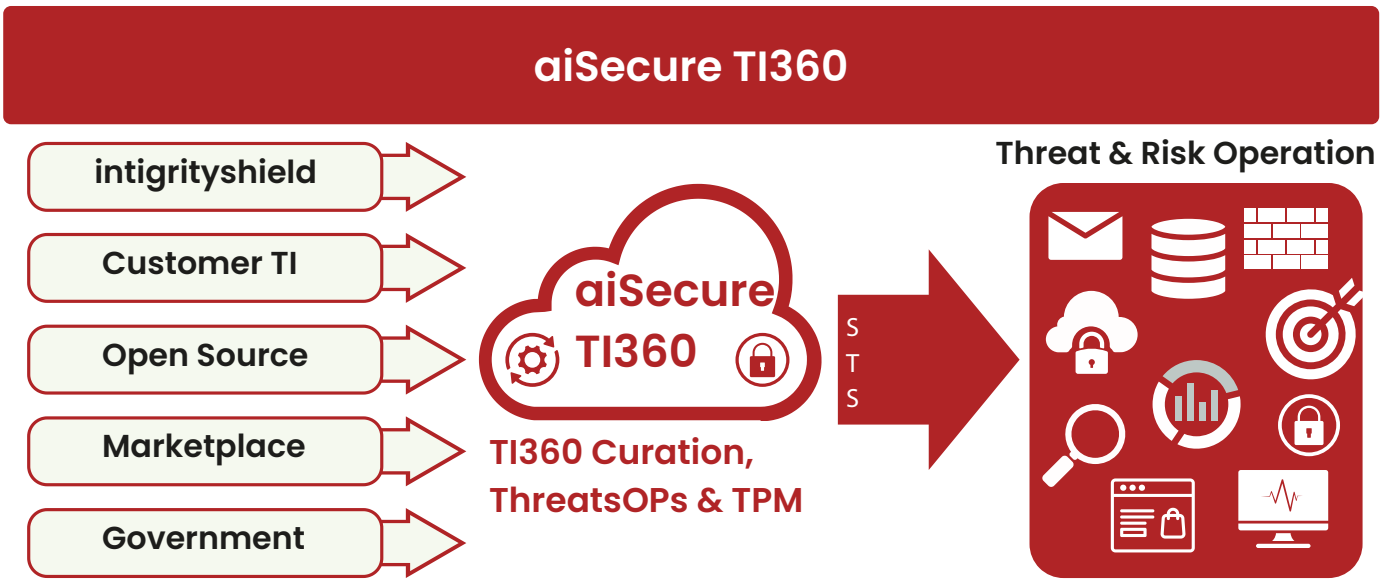
10. Extended TTL feeds: These feeds expand the base, anti-malware, ransomware, exploit kits and TOR Exit Node feeds that contain recently expired threats with an extended time-to-live (TTL) applied. Extended TTL may cause few false positive but might be worth in certain sector and their risk profile.

11. Suspicious Domains: These are domains that are known to be suspicious and used by attackers to launch attacks.

12. Suspicious Lookalikes: These are suspicious domains with the additional factor of appearing to impersonate a trusted domain, which is a common technique used in 'phishing threat activity.

13. Suspicious Newly Observed Emergent Domains: These are suspicious domains that have demonstrated a significant uptick in traffic globally among our customers, which may indicate that this domain is now part of an active campaign

aiSecurity TI360: Primary Threat Categories				
• Host Names and Public IPs • Anti-malware • Ransomware	• Known Bots • DHS (IP, Host Names and Domains) • Suspicious Lookalikes	• Blacklisted & Exploit IPs • Bot IPs • Suspicious Newly Observed Emergent Domains	• Malware DGA hostnames • Tor Exit Node IPs	• Extended TTL feeds • Suspicious Domains



intigrityshield aiSecure TI360: Threat Intelligence for a Proactive Defense

Threat intelligence is retrospective in nature, and the release of indicators often arrives long after the first attacks take place. It's primary value is in recording the well know bad.

intigrityshield TI360 includes protection via a proactive, low regret model that enables threats to be blocked before they are validated. intigrityshield TI360 threat intelligence feeds help identify IPs, Domains, URIs and Hashes based on it's own behavior analysis of hundreds of billions of telemetries processed each day and it's behavior and then adds TI to deliver proactive detection.

intigrityshield aiSIEM Platform STIX/TAXII APIs for any Standard 3rd Party Feed

intigrityshield aiSIEM Platform supports the industry standard interface to enable customers to ingest and use any third party feeds using STIX and TAXII APIs.

Some intigrityshield customers have ingested threat feeds from Recorded Future, Cisco, Palo Alto, Crowdstrike, FireEye, and more. Customers are not limited to any TI platform, all of them can be ingested.

Learn more about Intigrityshield aiSecurity TI360

Schedule a Demo