PARTNER BRIEF

FARSIGHT SECURITY

Microsoft Sentinel and Farsight Security / DNSDB

Threat indicator enrichment in Microsoft's Sentinel SIEM

DNS enrichment can be invaluable to threat hunters and analysts, who must often make quick decisions about suspicious traffic flows. Integrating Farsight Security's DNSDB with Microsoft Sentinel adds important context around domain and IP indicators seen in the protected environment.

Integration Benefits

With the supported logic apps, an investigator can answer questions such as "where did this domain previously resolve," or "what other domains share hosting with this domain or IP?" Such information can be extremely valuable when trying to correlate events that may otherwise show no relationship to each other. For example, a traffic flow to an domain or IP address that is not currently associated with a malicious domain, but where that domain or IP did previously reside, could be an indication of harmful activity such as command and control callbacks, malware downloader traffic, or other threats. You can see this by running the **DNSDB_Historical_Address** playbook for domain indicators or **DNSDB_Historical_Hosts** playbook for IP indicators. Likewise, if your DNS logs contain lookups for other domains that you know to be co-hosted with a known-bad domain, then you may have threat traffic to investigate. The **DNSDB_Co_Located_Hosts** playbook enables this. Or if you are enriching an IP address, use the **DNSDB_CO_Located_IP_Address** playbook to identify all the IPs that are co-located.

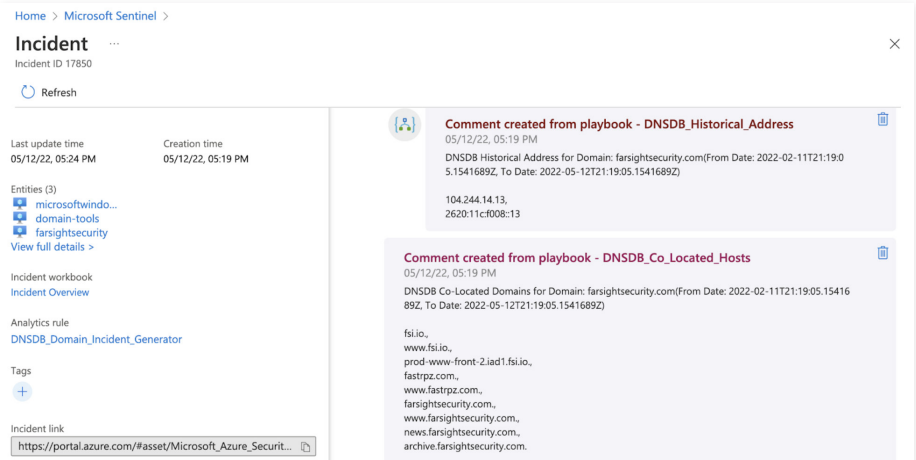


Image 1: Indicators with domain evidence gain additional context showing co-located domains or historical IP addresses for that domain

Available Actions

- Adds DNS enrichment details to Sentinel Incidents containing domains or IP addresses, which gives investigators more context and can help lead to the discovery of correlated infrastructure not yet observed or flagged in the protected environment
- Can show first time a threat (represented by a hostile asset) is seen in the environment

Typical users of the integration

- Threat hunters and network defenders
- SOC analysts
- Incident responders

Integration Use Cases

Threat Hunting

By developing a more complete picture of the assets adversaries use in campaigns, threat hunters working within Sentinel can identify patterns of infrastructure use, allowing them to anticipate future moves by adversaries. This can enable blocking or alerting on emerging campaigns before they cause further harm.

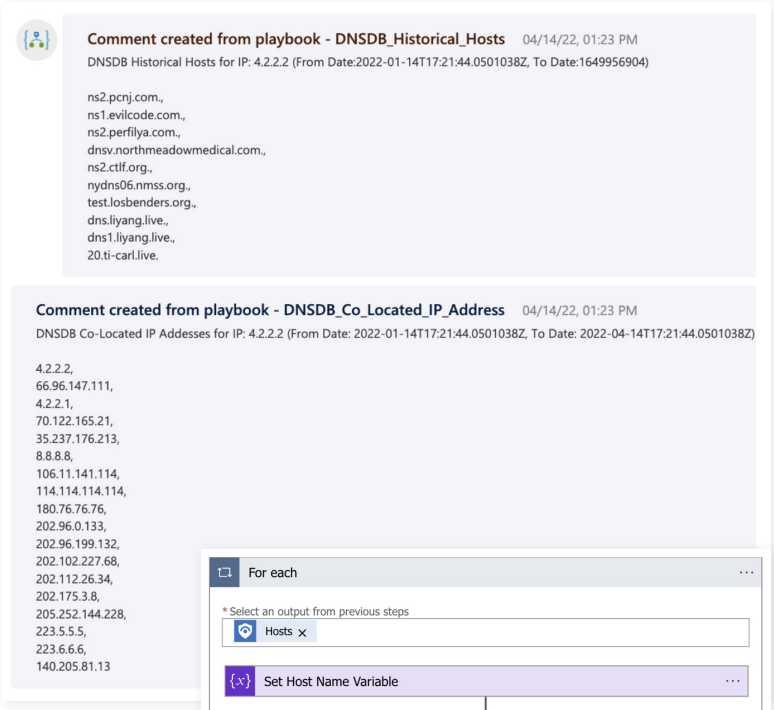
Incident Response

Forensics and incident response investigators can expose entire networks, gain an outside-in view of adversary assets to detect any suspicious or hostile activities, and take measures to defend against malicious attacks on the systems.

Network Defense

Pinpointing traffic flows to IP addresses or DNS lookups for domains known to be suspicious or hostile can help network defenders develop alerting or blocking rules to identify or stop threats such as malware, phishing, ransomware, and any other threat that relies on connections to adversary infrastructure.

Image 2: Playbooks provide additional context to IP indicators, providing historical hosts and co-located IP addresses associated with an IP address based on Farsight intelligence



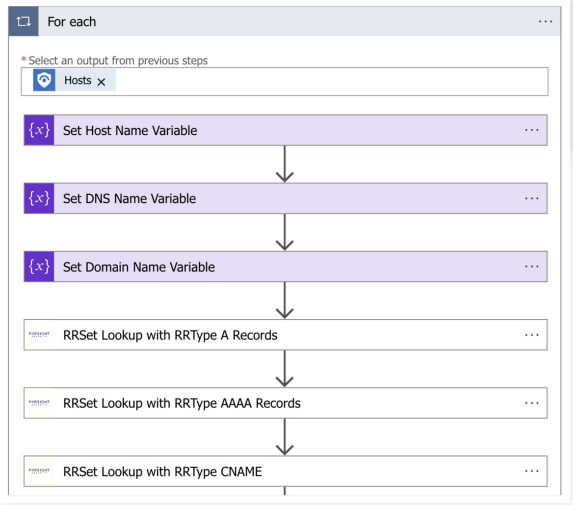


Image 3: Fine-tune your DNSDB searches with fully customizable playbooks

About Microsoft Sentinel

Microsoft Sentinel is your birds-eye view across the enterprise, allowing you to see and stop threats before they cause harm with SIEM reinvented for a modern world.Put the cloud and large-scale intelligence from decades of Microsoft security experience to work. Make your threat detection and response smarter and faster with artificial intelligence (AI). Eliminate security infrastructure setup and maintenance, and elastically scale to meet your security needs—while reducing costs as much as 48 percent compared to traditional SIEMs (source: https://aka.ms/sentinel-tei-report)

About FSI/DNSDB

Farsight Security (now part of DomainTools) DNSDB is the world's largest DNS intelligence database that provides a fact-based view of the configuration of the global Internet infrastructure. DNSDB leverages Farsight's Security Information Exchange (SIE) data-sharing platform and is engineered and operated by leading DNS experts. Farsight collects, filters, and verifies Passive DNS data from its global sensor array. DNSDB is the highest-quality and most comprehensive DNS intelligence data service of its kind.

+1-206-838-9020

info@farsightsecurity.com www.farsightsecurity.com
Farsight Security, 2101 4th Ave, Suite 1150, Seattle, WA 98121