Designing a Comprehensive IDS Strategy for a Zero Trust Architecture Environment

FERMILAB-POSTER-24-0157-STUDENT

Lucas D'Antonio - Purdue University Northwest, Under the Mentorship of Jason Ormes & Jeny Teheran
Security and Emergency Management Division, Cybersecurity Team, Fermi National Accelerator Laboratory, Batavia, Illinois 60510

Intrusion Detection, Network Detection and Response

An Intrusion Detection System or IDS, is a passive security mechanism designed to inform on malicious network traffic. IDSs are often used in tandem with a Network Detection and Response system (NDR), which monitors all network traffic and logs interesting or unusual activity. These systems supplement active protection mechanisms such as firewalls or Intrusion Prevention Systems. Patterns of known or suspected malicious activity can generate alerts to inform users about attack attempts on their network, prompting them to respond. These alerts can be processed by event management services and trigger blocking countermeasures against the offending party from accessing an organization's resources. IDSs and NDRs can either monitor inbound and outbound communications (North/South) or intranet traffic (East/West). Having monitoring in both directions is a prerequisite for achieving comprehensive network coverage.

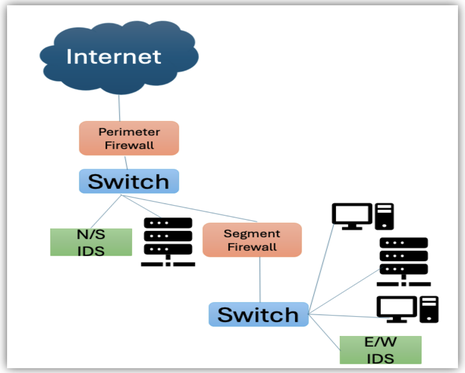

Figure 1: Topography of a simple network with North/South and East/West Intrusion Detection System coverage.

Requirements for a ZTA Deployment

Zero Trust Architecture or ZTA is a cybersecurity model for enterprises to structure their networked resources around to maintain total security externally and internally. In a Zero Trust environment, no part of the network is considered "trustworthy" and thus should be scrutinized and monitored extensively as is done in traditional "Trust But Verify" schemes at the network's perimeter. In this way, Zero Trust Architecture is a superior model for securing access to networked resources at the enterprise level. Fermilab, in pursuit of a better security posture, has decided to embrace this model of architecture for its network. Attaining this goal requires tremendous infrastructural, policy, and procedural adjustments that will affect all the lab's personnel and resources.

Intrusion Detection Infrastructure Improvements

At Fermilab, the current IDS infrastructure exists to support perimeter security, where traffic is only inspected at the entry points of the network. While this helps to mitigate many forms of attack and data exfiltration, this IDS solution is inadequate to detect internal threats to the organization, and does not provide robust, heuristic analysis of the traffic at the lab. Working with the expertise of the cybersecurity team, I have proposed a plan to augment Fermilab's IDS capabilities to inspect East-West network traffic in addition to existing North-South traffic monitoring, alongside the rollout of an NDR platform. Under my proposal, Increased internal network coverage will enable many new insights into network traffic be made available to the cybersecurity team. By increasing internal coverage, less information will be obfuscated at the application layer, permitting granular analysis by the IDS/NDR not currently possible.

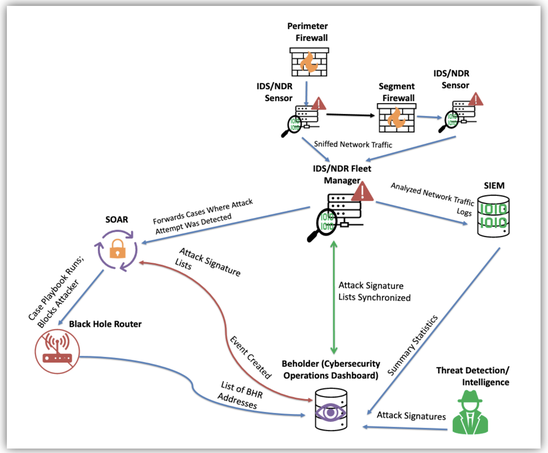

Figure 2: Overview of the proposed IDS deployment and its workflows. Only relevant relationships are depicted.

Once analyzed, logs of all activity captured by the IDS/NDR will flow into the lab's SIEM solution, where further manipulation and reference to the logged traffic will occur. Patterns of known malicious network activity or otherwise anomalous behavior, no matter where it is in the network, will now be forwarded to the Security Orchestration and Response (SOAR) solution for automatic remediation. Detailed playbooks, written in accord with site policy, have been proposed to handle many scenarios commonly encountered. This will serve to prevent data exfiltration from the organization, as well as prevent unauthorized access to or abuse of resources both externally and within Fermilab's network. Once the IDS appliances are operating in their respective zones, communication between IDSs will be necessary to facilitate the use of these additional security appliances. This will be accomplished by leveraging an internal tool developed by the cybersecurity team: Beholder.

Role of Beholder in IDS and ZTA Enhancement

A crucial part of my proposed IDS deployment strategy involves the in-house developed cybersecurity engine, Beholder. Initially a series of scripts to automate scans of devices on the network, Beholder has evolved into a centralized web service with extensive responsibilities. These include coordinating network traffic flows, triggering blocking mechanisms, remediating phishing attempts, and tracking end devices. Beholder is an event driven application where, upon receiving an alert on any of its IDS triggers, creates an event that triggers black hole routing for the offender's address. This block remains in place until reviewed and removed by the security team.

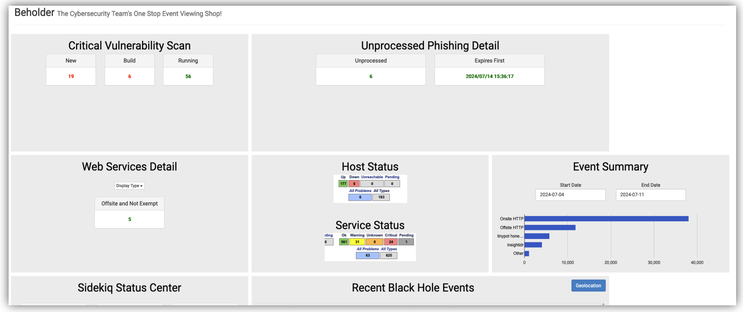

Figure 3: Beholder Dashboard. In addition to its planned role in augmenting laboratory IDS capabilities, Beholder combines several cybersecurity operational efforts such as detecting policy violations, identifying phishing attempts, and tracking system statuses through scans.

Beholder will be heavily involved in the lab's IDS strategy going forward. The existing, event driven nature of Beholder can easily be adapted to accommodate the new network sniffing feeds into its environment. New vectors of attack will be automatically shared with Beholder through intelligence sharing services Fermilab participates in. This will further speed up incident response to novel attack forms. Overall, my proposal will enable Fermilab's cybersecurity team to better automate remediation of many forms of malicious or anomalous behaviors across the entire lab's network by providing previously unprecedented monitoring of network traffic at the lab. This will play an important role in reaching Fermilab's goal of a Zero Trust Architecture for the entire lab. Furthermore, my proposal could easily be adapted for organizations with similar infrastructural considerations and challenges.

This work was produced by Fermi Research Alliance, LLC under Contract No. DE-AC02-07CH11359 with the U.S. Department of Energy. Publisher acknowledges the U.S. Government license to provide public access under the DOE Public Access Plan.

This research was supported in part by the U.S. Department of Energy (DOE), Omni Technology Alliance Internship Program. The program is championed by the DOE's Office of Chief Information Officer (OCIO) and represents a partnership with the leadership of the Office of Economic Impact and Diversity, the Office of Science, the Office of Nuclear Energy, and the National Nuclear Security Agency. The program is administered by the Oak Ridge Institute for Science and Education