SAND2018-7822D

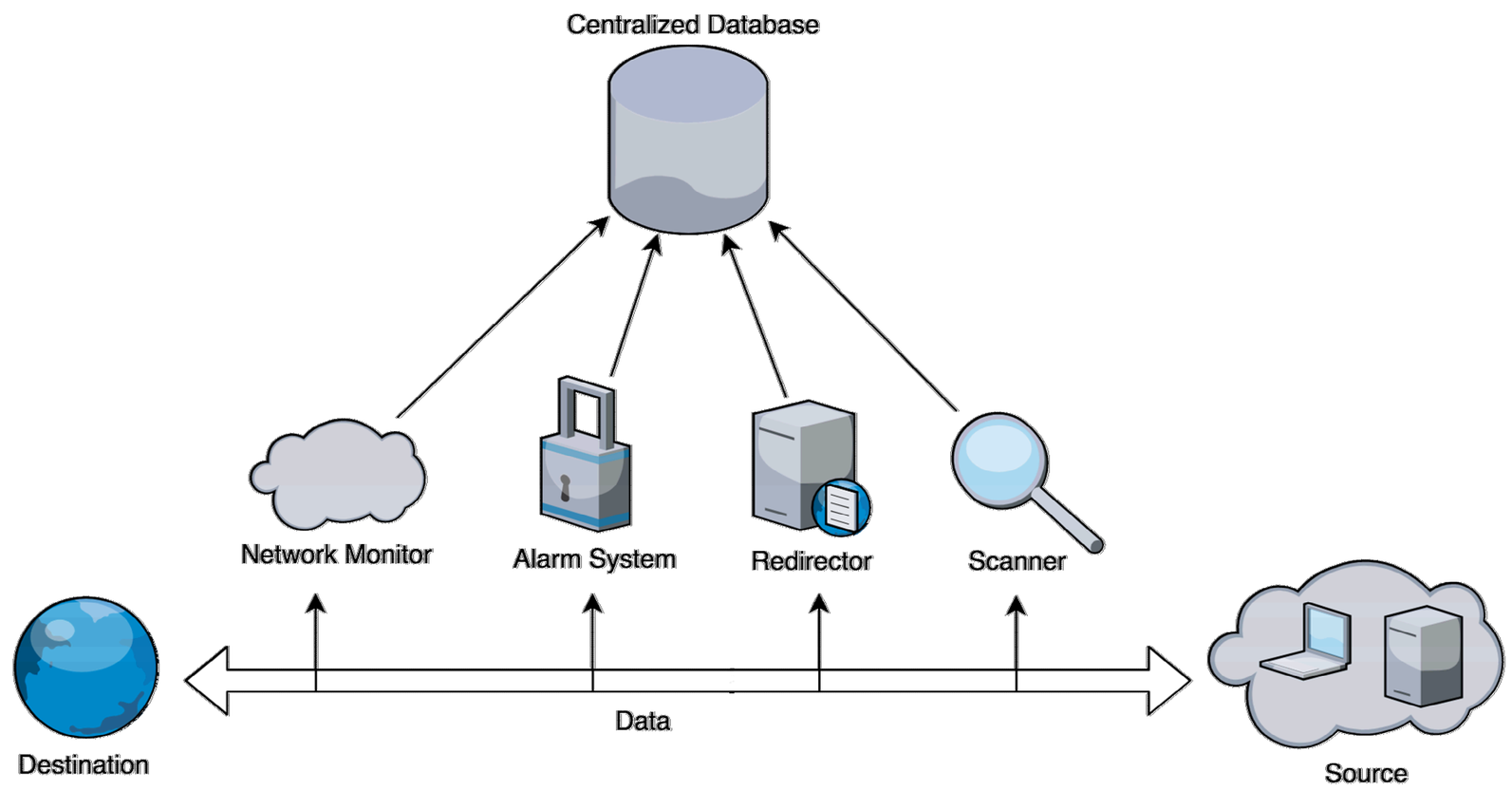
Virtualized Integrated Network Monitoring System

Nolan Bonnie, Kyle Ebding, Christopher Harrell, Abhiram Kothapalli, Sam Sabetan, Guy Watson

With the rise of malicious network traffic in complex enterprise networks, the need for automated detection is rising. Our monitoring system mimics a complex integrated network and has the ability to block cyber attacks from compromising critical infrastructure. With the addition of a centralized database, we also have the capability to use historical data and threat information to protect assets in future attacks.

Our system analyses network traffic before it reaches it's destination. It logs pertinent data, scans hosts and redirects or blocks known bad websites – all in a single, virtualized container.

Our system is not a catch-all defense implementation, cybersecurity professionals believe in in-depth analysis. This system is a tool to that eases analysis required in threat hunting. The system is designed to be an additional tool to other threat detection and prevention platforms.



Centralized Database: Unstructured data containing variable formats is constantly streamed real-time from our security systems. In order to meet the challenge of data retention and efficient information extraction, we implemented a MySQL Database. MySQL is a relational database that enables us to aggregate and correlate our data sources across multiple tables. The database allows us to build in functions to accept and correct data formats and also develop effective and timely queries to extract relevant information. We provide procedures and queries that an analyst can leverage to pivot the stored tables gathering information on a particular event.

Intrusion Detection System: An IDS is a device that monitors network traffic for suspicious activity by matching it against predefined rules setup by an analyst. Using the Snort IDS, our system, using only a listen-only connection, collects data passing through the network. The sensors setup by an analyst generate metrics on network flow and alerts the necessary personnel when suspicious data is seen. The metrics collected are useful for differentiating the different types of traffic seen. The alerts let us correlate events and run in depth analysis on data collected from the entire system.

Domain Name System: DNS is the main naming convention used on the internet for accessing different hosts. Each domain name corresponds to an IP address, which is how a network router knows where to route your request. Our system includes a DNS interceptor that will look at all DNS requests and see if there is a request to a bad website. If we have no matches in our database, the request is allowed to go out to the internet. If we do find a match in our database, our system will either block the request (and notify the user of the blocked request), or redirect the request to a safe version of that website. The primary use for this is to prevent malware installed on enterprise networks from communicating with malicious Internet domains. If a malicious piece of software, or malware, realizes it has no network access, it will most likely deactivate. With our DNS redirector attached to a centralized database, we have the ability to look back at all DNS requests and determine when and if a website was compromised and view all previous requests to that website.

Vulnerability and Email Scanning: With email vulnerability scanning, we have the added ability to search incoming and outgoing email attachments for malicious software. Emails are scanned before being delivered to the recipient. If an infected email is detected, we have the ability to quarantine or redirect them for further analysis. Additionally, incorporating enterprise security solutions, such as the Nessus Vulnerability Scanner, we can match our network traffic against rules and vulnerabilities which have been discovered outside our system – creating a collaboration between other enterprises that use our system.

Impact: Our solution to fighting malware that has been discovered in an enterprise allows for a clean roll-out and ease of use for a security analyst. Incorporating a centralized database that stores metrics and historical data gives the analyst a large dataset for tracking down malicious behavior on a network. Our system, combined with other enterprise solutions, will lower the risk of known malicious software infiltrating a network and give security analysts a easier and useful tool to defend their enterprise.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND No. _____