Continuous Risk Monitoring and Analysis

Dr. Lyron H. Andrews

ISO/IEC 42001 AIMS Lead Implementor
CISSP/CCSP/SSCP/CRISC/CISM/CCSK/CCZT

@drlyronandrews | www.profabula.com

Overview

Overview

- Describe the environment that supports monitoring and analysis
- Define the process of log management and how it integrates
- Demonstrate how monitoring tools are essential to success

Foundation for Monitoring

Do you recall what should precede monitoring and analysis in risk management?

Precursors to Monitoring

Maintain assessment

Communicate results

Determine risk

Determine magnitude of impact

Determine likelihood of occurrence

Identify vulnerabilities and existing conditions

Identify threat sources and events

Prepare for assessment

Risk Assessment Report

Tool for continuous communication

Key to maturation process

Maintains traceability of controls

Final step of risk assessment

Monitoring Terminology

Signature

False positive

False negative

True positive

True negative

Tuning

Promiscuous interface

Attacker Profile

Political

Greed

Revenge

Notoriety

Log Management

Log Policies and Procedures

Critical device determination

What data is collected

Where stored and for how long

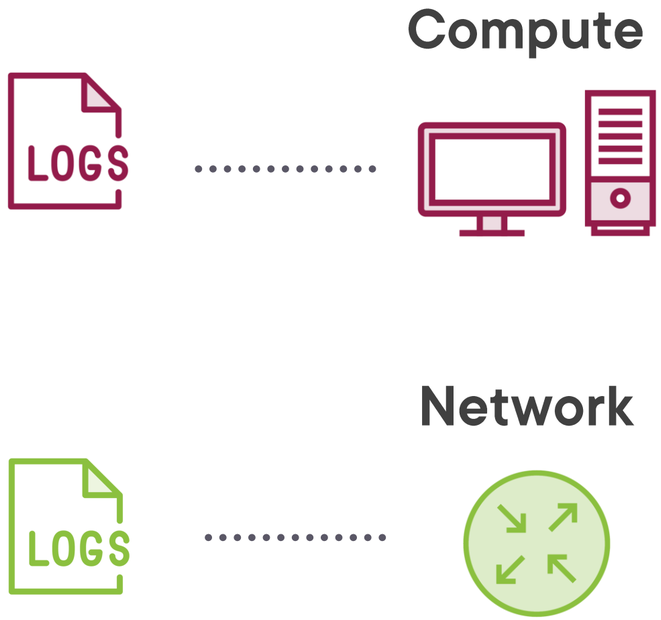
Integrity of logs for storage and transit

Who has access

Logging Eco System

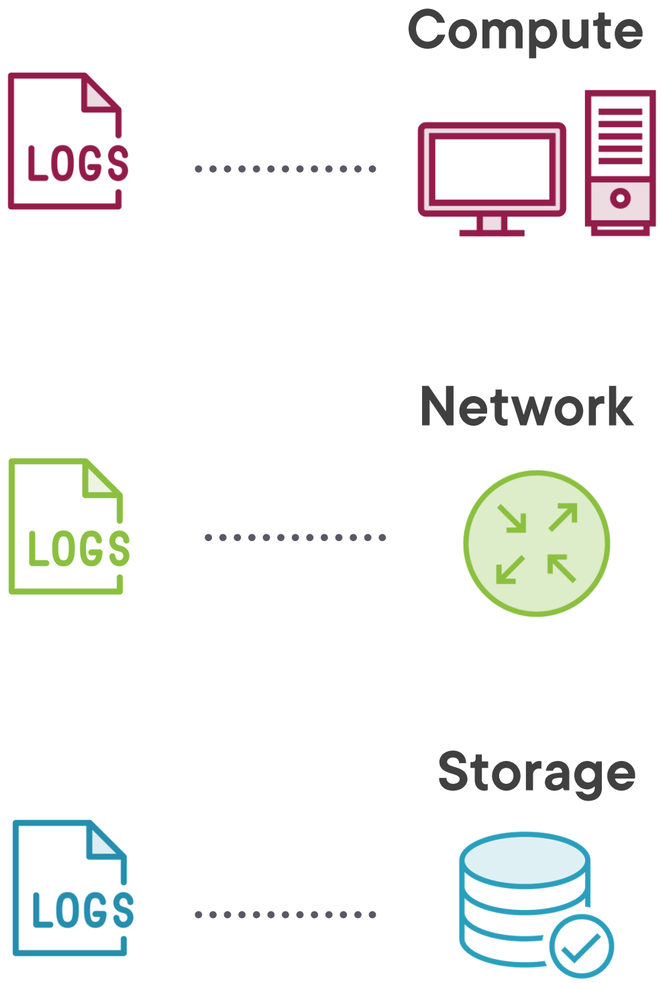
syslog, rsyslog, or syslog-ng

Logging Eco System

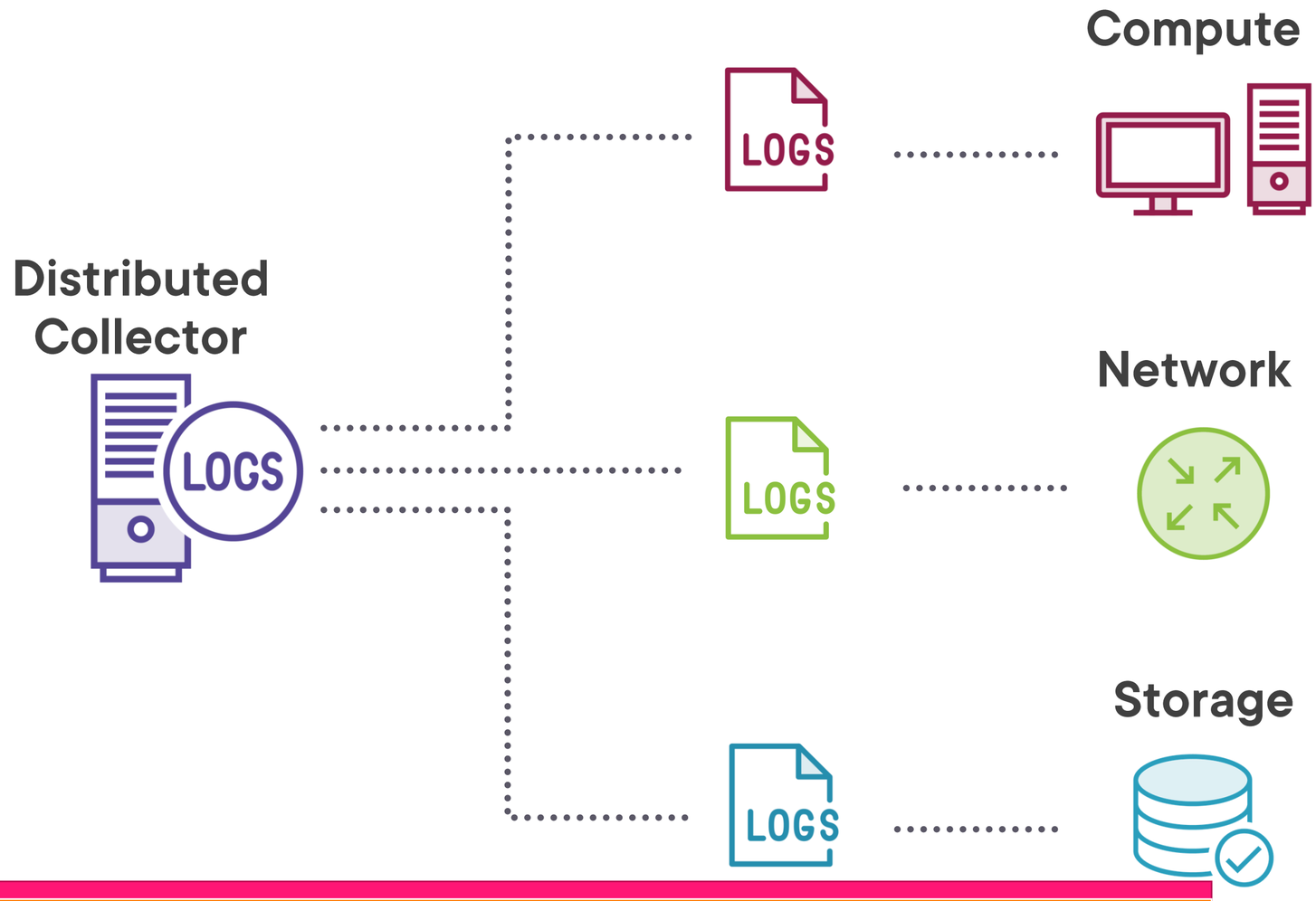


IP Flow, NetFlow, and sFlow, and IPFix

Logging Eco System



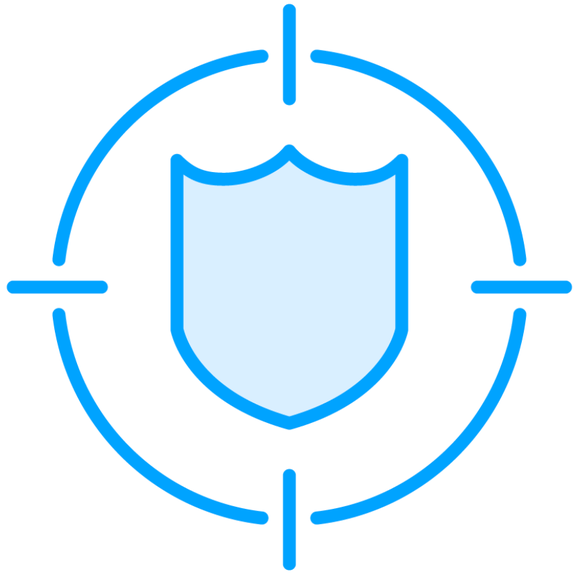
Logging Eco System



Logging Eco System

Analyzing Data

Indicators of Compromise



- Mismatched port-application request
- Inordinately oversized HTML responses
- Inordinate number of requests for the same file
- Dramatic increase in database reads

Monitoring Systems

Two Basic Monitoring Capabilities

Real-time

Ease of technical means of vulnerability

Non-real-time

Direct consequence of successful exploit

Monitoring Categories

Intrusion Prevention/Detection
Network and host-based

Data Loss Prevention
Cloud and non-cloud

Data Loss Prevention

Features

Discovery and Classification

Monitoring

Enforcement

Architecture

Endpoint

Network

Storage

NIDS

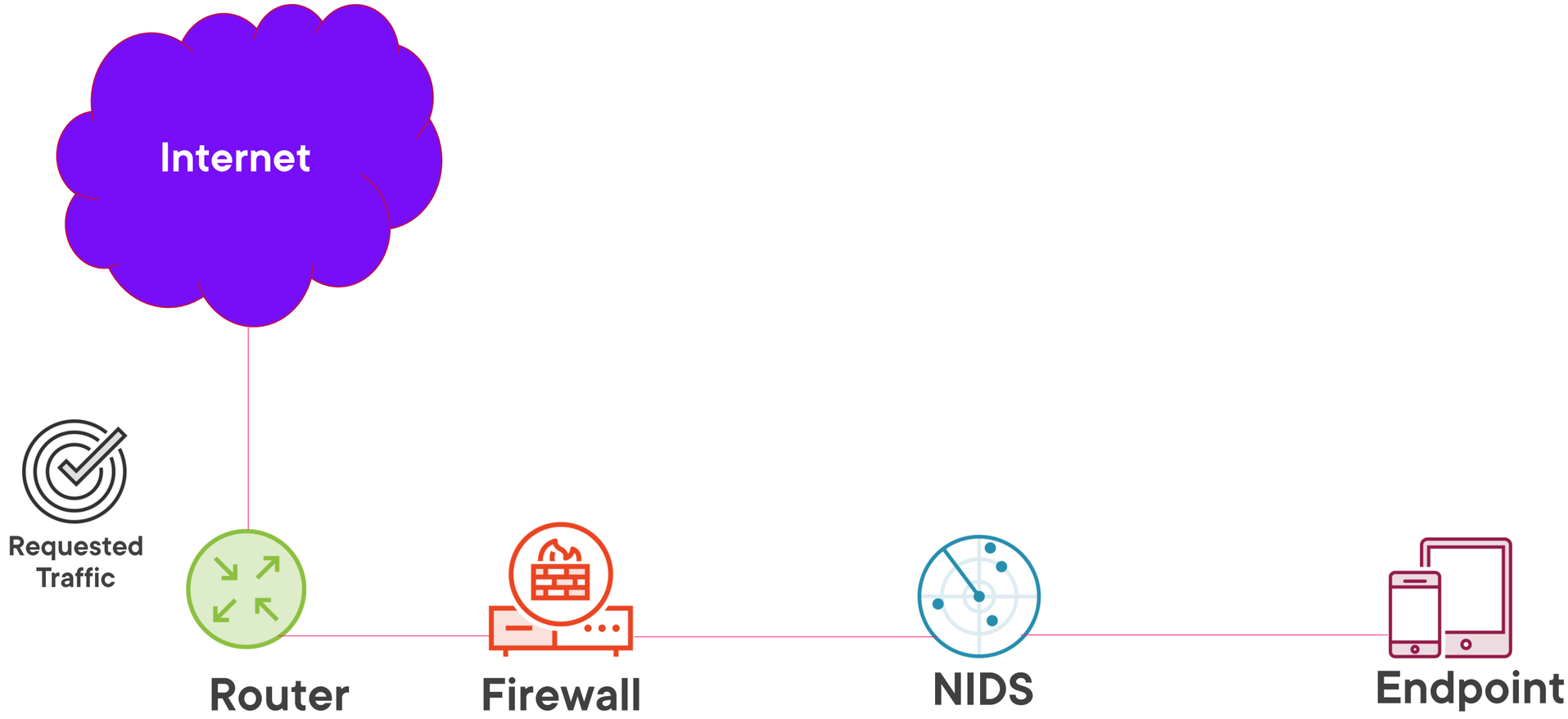
HIDS

NIPS

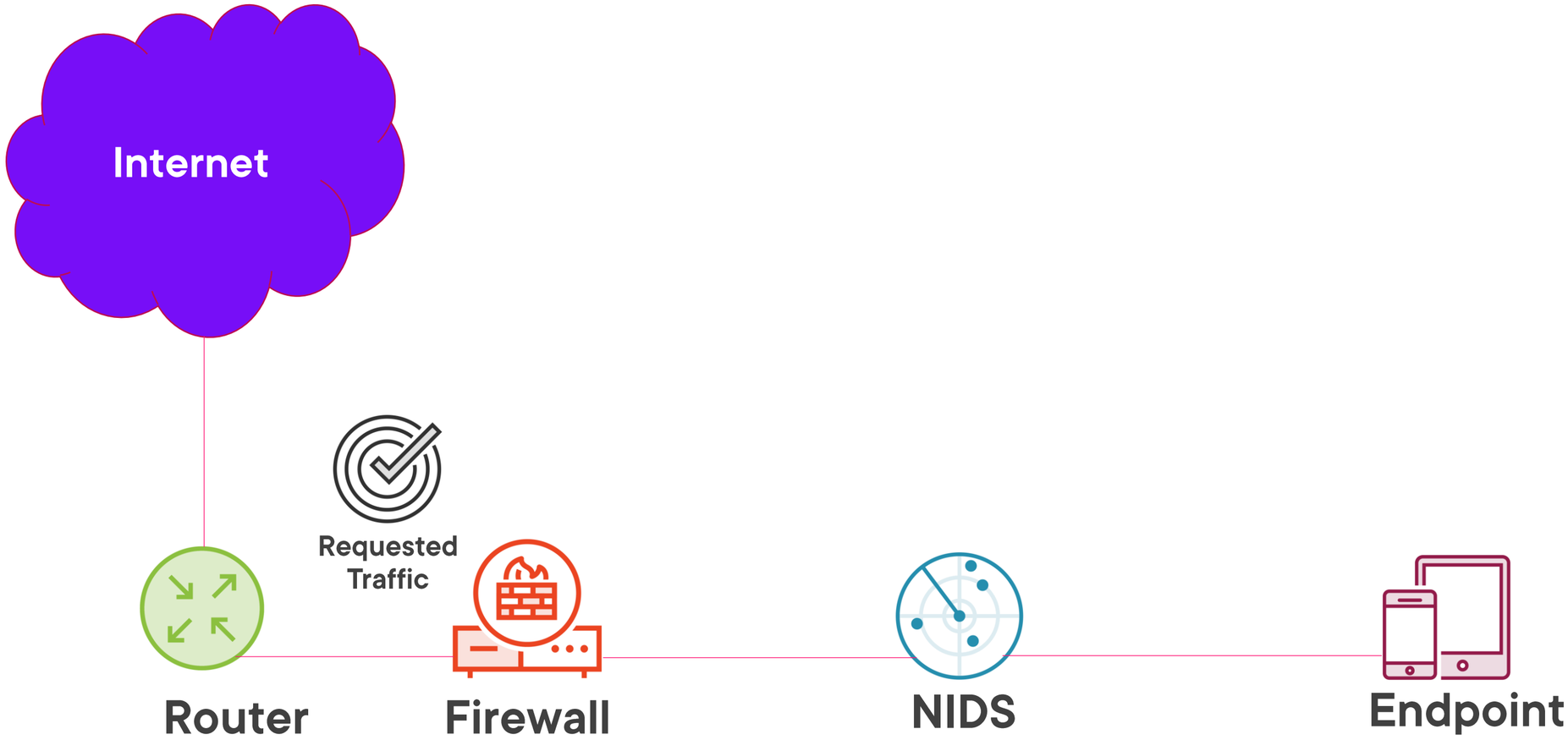
HIPS

Intrusion Detection and Prevention Systems

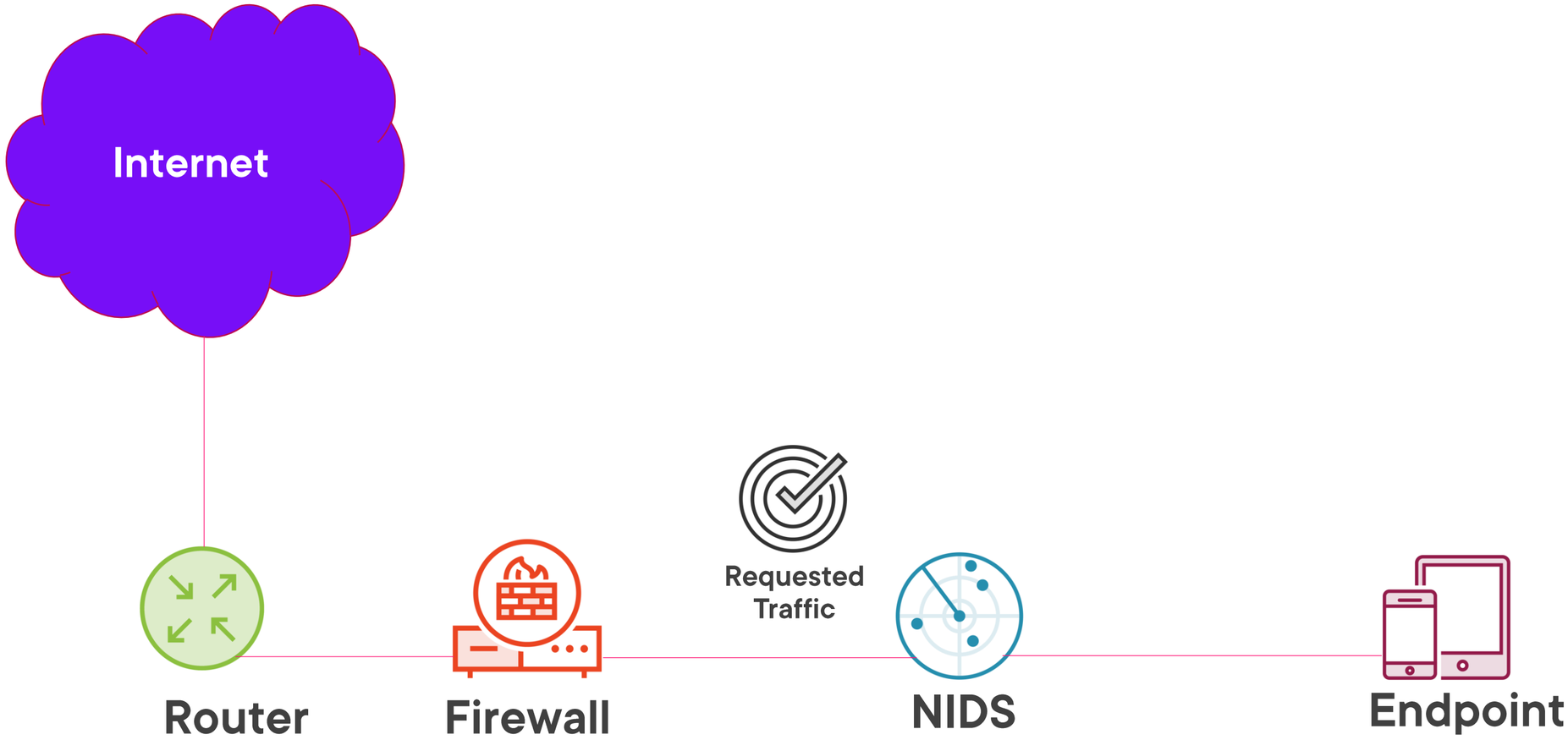
Intrusion Detection System



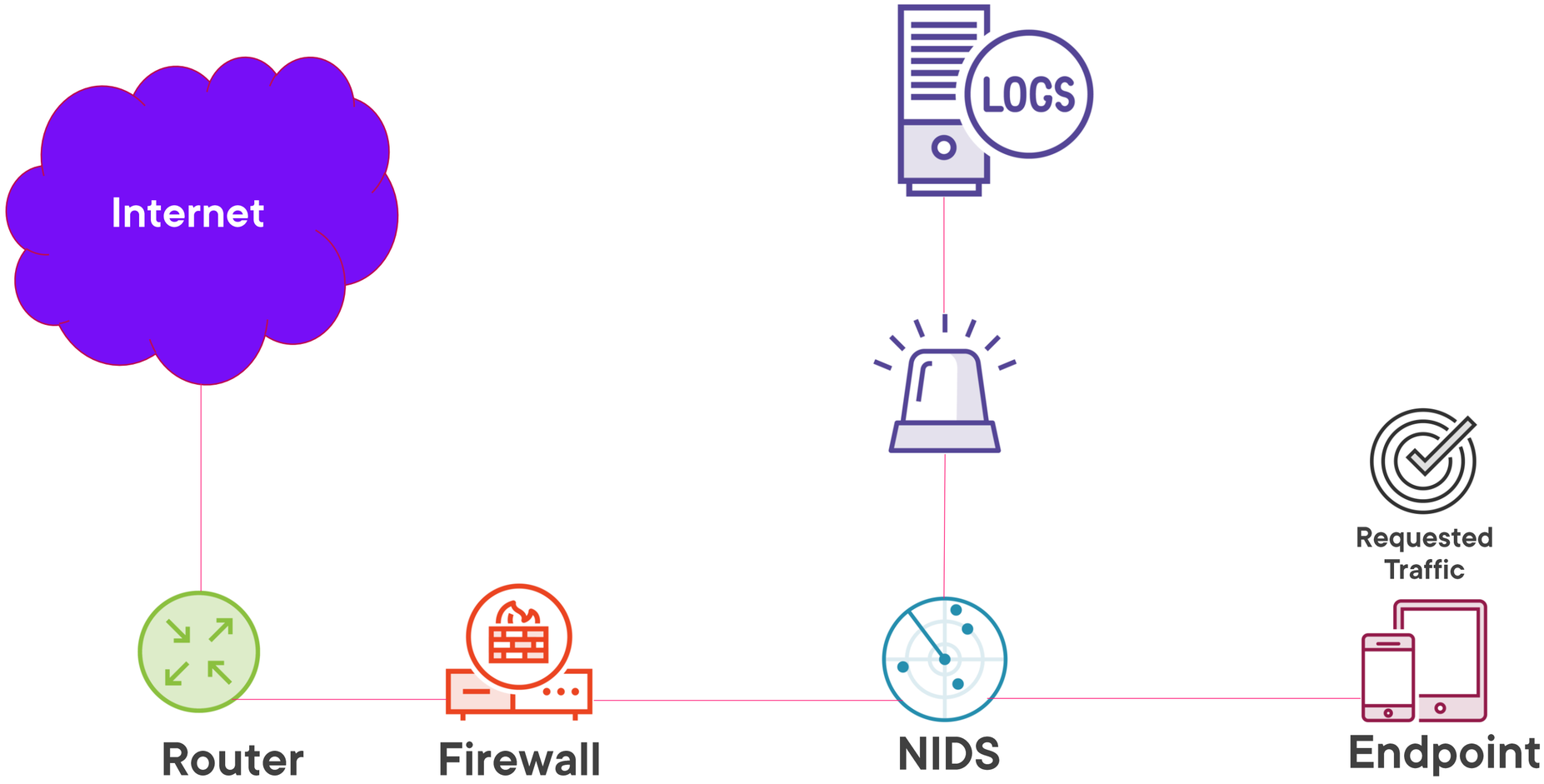
Intrusion Detection System



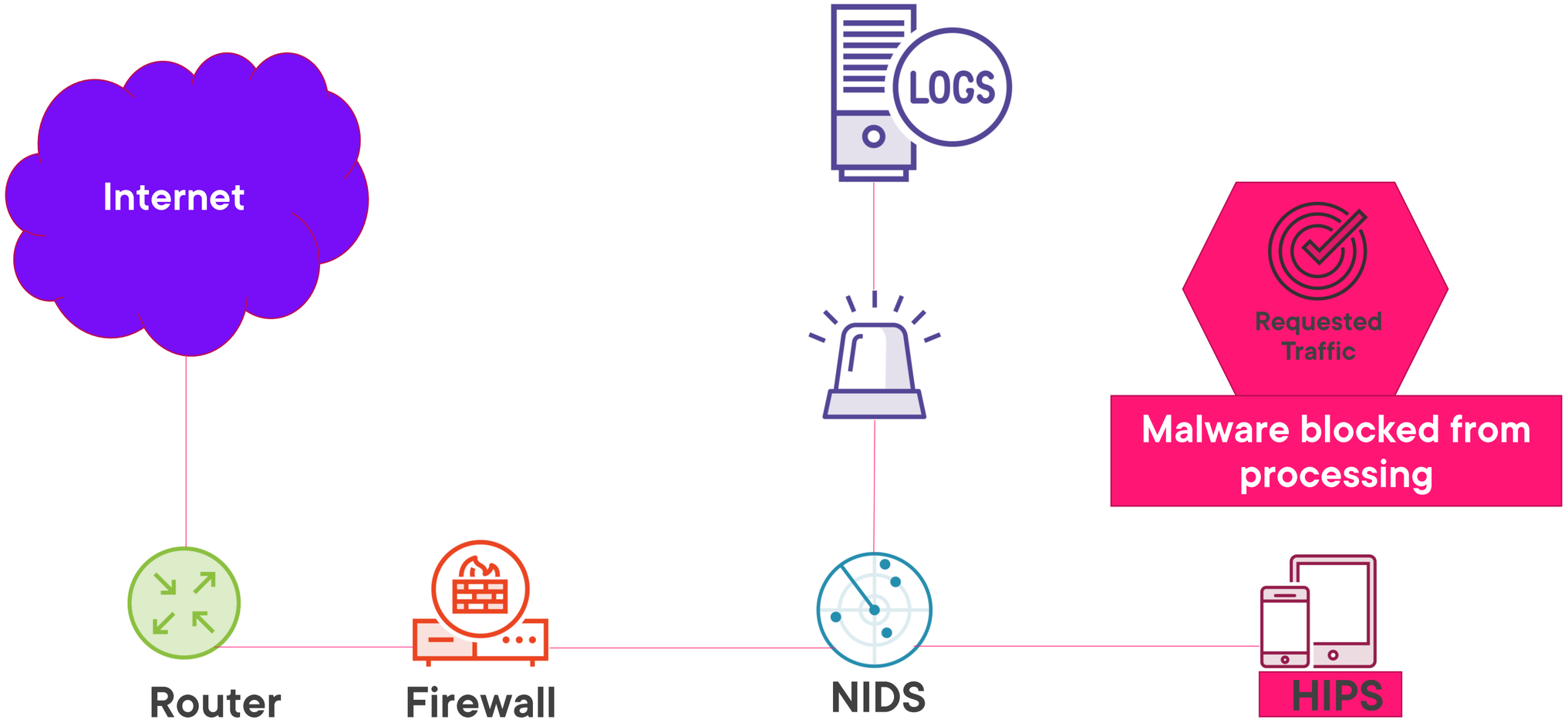
Intrusion Detection System



Intrusion Detection System



Intrusion Detection and Prevention Systems



Continuous monitoring and analysis needs continuous auditing.

Communicate Audit Findings

Continuous audit necessary

Provides assurance to management

Data visualization tools helpful

Course Summary

Summary

- What in your organization needs the greatest attention in the risk management lifecycle?
- How do you ensure that your IT risk management practices are aligned with your business?
- What will be the first area you address upon completion of this course?