Chapter 1: Introduction

Gonzalo De La Torre Parra, Ph.D.

Fall 2021

Network Security Management

- NSM is the collection, detection, and analysis of network security data. Information security has traditionally been divided into many different focus areas (Computer Network Defense [CND] per DoD 8500.2):
  - Protect: The protect domain focuses on securing systems to prevent exploitation and intrusion from occurring.
  - Detect: Detecting compromises that are actively occurring or have previously occurred. This includes network security monitoring and attack sense and warning.
  - Respond: Incident containment, network and host-based forensics, malware analysis, and incident reporting after a compromise has occurred.
  - Sustain. The final CND domain deals with the management of the people, processes, and technology associated with CND. This includes contracting, staffing and training, technology development and implementation, and support systems management.

Key NSM Terms

- Asset
- Threat
- Vulnerability
- Exploit
- Risk
- Anomaly: an observable occurrence in a system or network that is considered out of the ordinary. Anomalies generate alerts by detection tools such as an intrusion detection systems or log review applications.
- Incident: An incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices2. More simply stated, an incident means that something bad has happened, or is currently happening on your network.

What is Intrusion Detection?

- It is a component of network security management

- Characteristics
  - Vulnerability-Centric Defense: IDS is deployed with the goal of detecting the exploitation of vulnerabilities. Focuses on how the attacks take place.
  - Detection in Favor of Collection: Collecting data that is not tied to collection.
  - Mostly Signature-Based: relied on having knowledge of all known vulnerabilities and developing signatures for their detection.
  - Attempts to Fully Automate Analysis: Reduce the involvement by human analysts and attempt to automate post-detection analysis as much as possible.

Network Security Monitoring Network Security Monitoring

United States Information Operations (IO) doctrine3 mentions that a commander's IO capabilities should be used to accomplish the following:

- Destroy: To damage a system or entity so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.
- Disrupt: To break or interrupt the flow of information.
- Degrade: To reduce the effectiveness or efficiency of adversary command, control, or communication systems, and information collection efforts or means. IO can also degrade the morale of a unit, reduce the target's worth or value, or reduce the quality of adversary decisions and actions.
- Deny: To prevent the adversary from accessing and using critical information, systems, and services.
- Deceive: To cause a person to believe that which is not true. Seeking to mislead adversary decision makers by manipulating their perception of reality.
- Exploit: To gain access to adversary command and control systems to collect information or to plant false or misleading information.
- Influence: To cause others to behave in a manner favorable to friendly forces.

Cont…

- Protect: To take action to guard against espionage or capture of sensitive equipment and information.
- Detect: To discover or discern the existence, presence, or fact of an intrusion into information systems.
- Restore: To bring information and information systems back to their original state.
- Respond: To react quickly to an adversary's or others' IO attack or intrusion.

Characteristics of Network Security Monitoring

- Prevention eventually fails: A motivated attacker will always find his way in.
- Focus on Collection: Collecting all data is cost ineffective. You must have data to parse. It should be able to perform the same level of detection with less data.
- Cyclical process: IID is not a linear process (alert, validate, and respond). Attackers have become slow and methodical. Cyclical processes act based on:

- Threat-Centric Defense: Focuses on who performs the attack (Threat Actor) and why (Motivation). Requires extensive visibility into the network, collect data, and analyze it.

VULNERABILITY-CENTRIC VS. THREAT-CENTRIC DEFENSE

Table 1.1 Vulnerability-Centric vs. Threat-Centric Defense

Vulnerability Centric	Threat Centric
Relies on prevention	Knows that prevention eventually fails
Focus on detection	Focus on collection
Assumes universal view of all threats	Knows that threats use different tools, tactics, and procedures
Analyzes every attack in a vacuum	Combines intelligence from every attack
Heavy reliance on signature-based detection	Utilizes all-source data
Minimal ability to detect unknown threats	Stronger ability to detect adversarial activities beyond known signatures
Linear process	Cyclical process

Collection

- Collection occurs with a combination of hardware and software that are used to generate, organize, and store data for NSM detection and analysis.
- CAREFUL! Trash in → Trash out
- Data categories: Full Content Data, Session Data, Statistical
- Data, Packet String Data, and Alert Data.
- Effective collection requires a concerted effort from organizational leadership, the information security team, and network and systems administration groups.

Collection Tasks

- Defining where the largest amount of risk exists in the organization
- Identifying threats to organizational goals
- Identifying relevant data sources
- Refining collection portions of data sources
- Configuring SPAN ports to collect packet data
- Building SAN storage for log retention
- Configuring data collection hardware and software

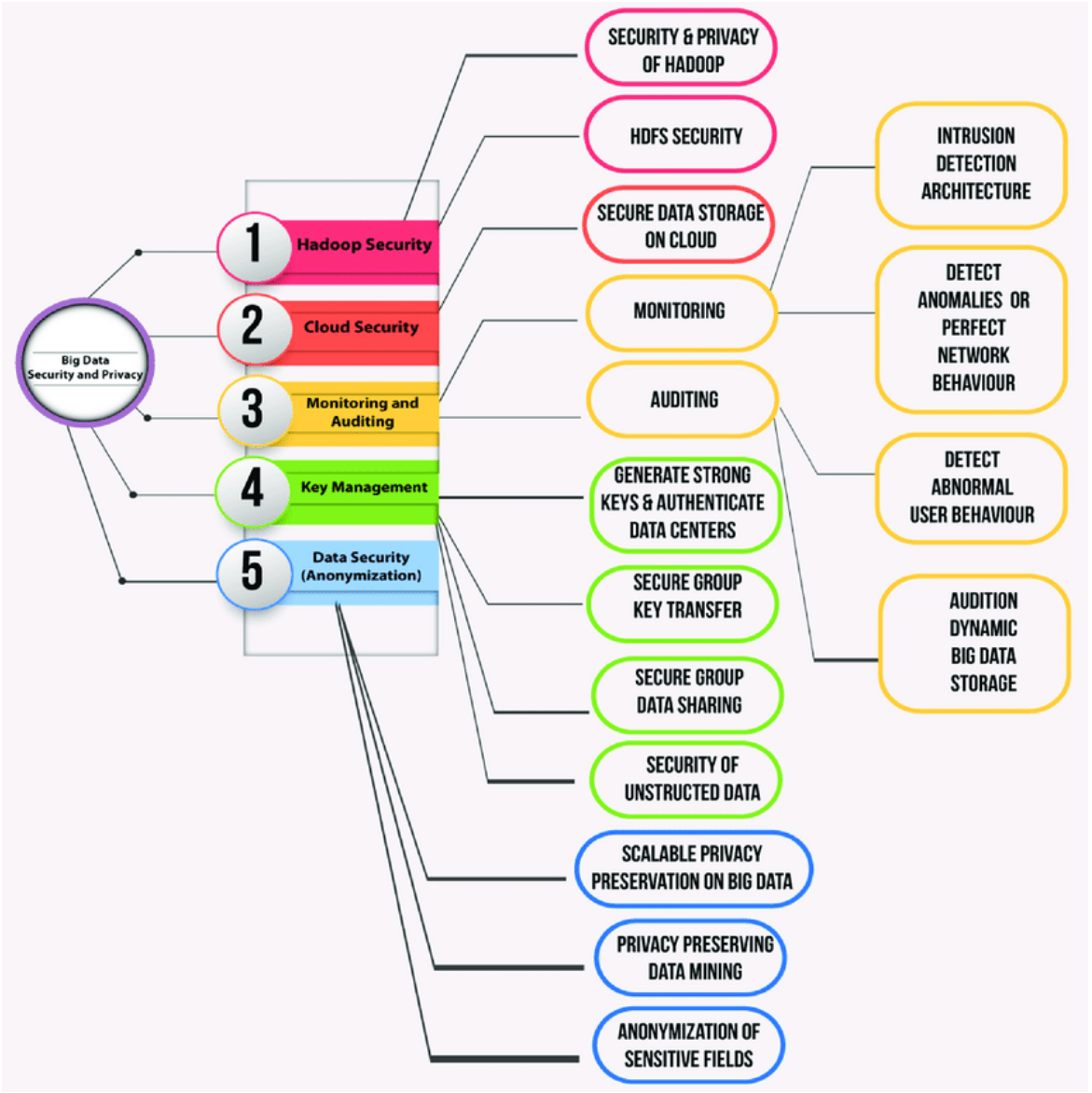
Detection

- Collected data is examined and alerts are generated based upon observed events and data that are unexpected.
- Network Intrusion Detection Systems (NIDS)
  - Snort IDS
  - Bro IDS → Zeek
- Host Based Intrusion Detection Systems (HIDS)
  - OSSEC
  - AIDE
  - McAfee HIPS
- Security Information and Event Management (SIEM) applications
  - Elastic SIEM
  - Make use of NIDS and HIDS to do detection

Analysis

- Interpretation of Collected Data and Interpretation
- Investigate other data sources
- Ways analysis can be performed:
  - Packet analysis
  - Network forensics
  - Host forensics
  - Malware analysis

Big Data Security



Challenges to NSM

- NSM is still immature science exiting within another immature science (Information Technology)
- Disparity in protocols (Written vs Applied)
- NSM lacks regulation: group of practitioners that often speak on different wavelengths.

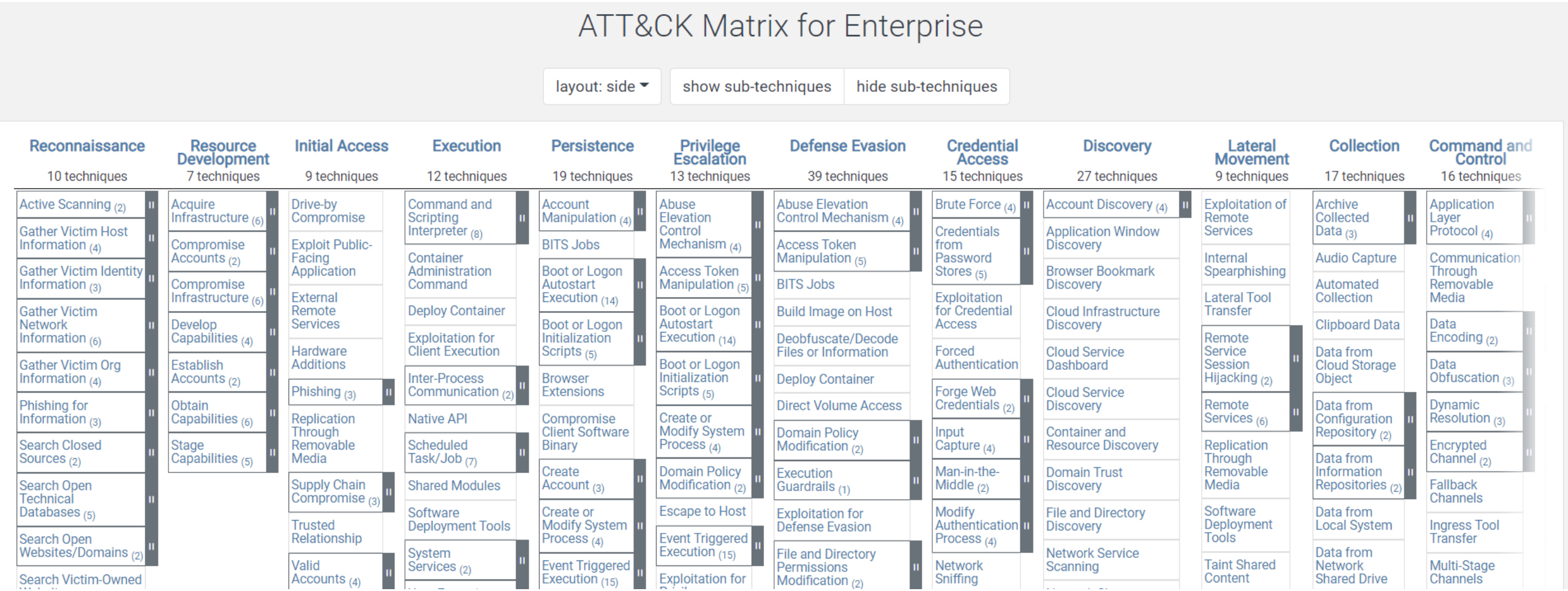
The Analyst – Baseline Skills

- Threat-Centric Security, NSM, and the NSM Cycle
- TCP/IP Protocols
- Common Application Layer Protocols
- Packet Analysis
- Windows Architecture
- Linux Architecture
- Basic Data Parsing (BASH, Grep, SED, AWK, etc)
- IDS Usage (Snort, Suricata, etc.)
- Indicators of Compromise and IDS Signature Tuning
- Open Source Intelligence Gathering
- Basic Analytic Diagnostic Methods
- Basic Malware Analysis

Specializations – Offensive Tactics

- Attempt to gain access to attack the network in the same way an adversary would.
  - Penetration testing
  - Security Assessment
  - Network reconnaissance, software and service exploitation, backdoors, malware usage, and data exfiltration techniques.

Mitre – Cyber Kill Chain



Specializations – Defensive Tactics

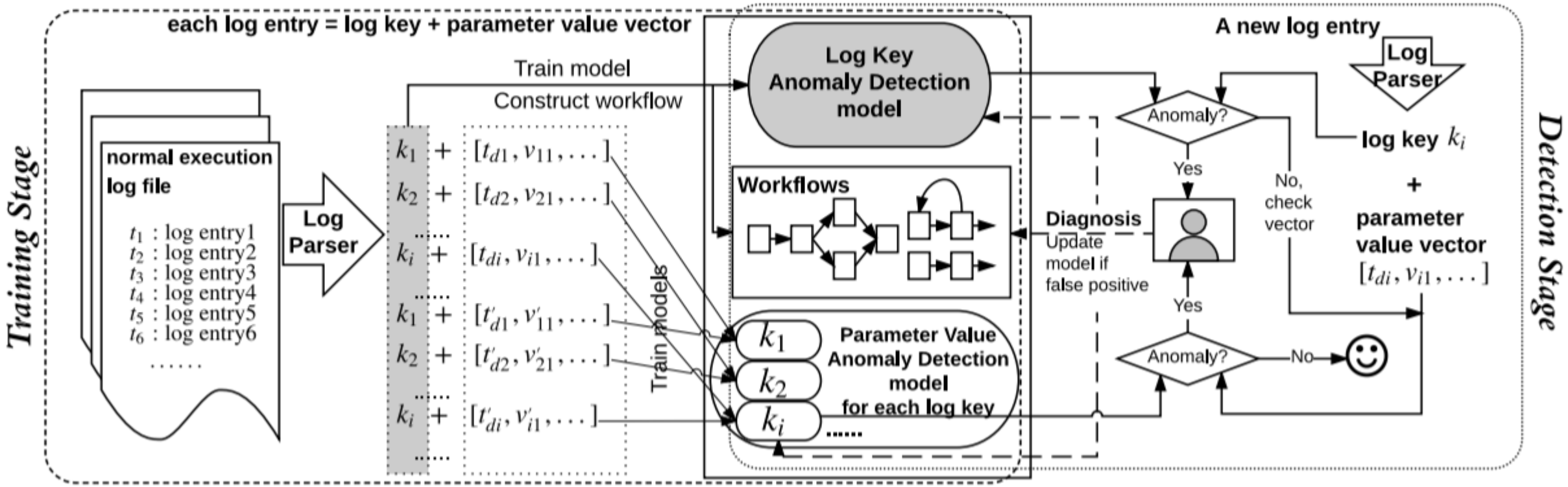
- Master of detection and analysis
- Conceptualizing new development tools and analytic methods.
- New tools and research related to network defense, and to evaluate those tools for use within the organization's NSM program.
- Detailed knowledge of network communications,

Specializations - Programming

- Develop custom detection and analysis solutions for an NSM team
- Expert in parsing datasets
- Very strong understanding of the Linux BASH environment
- Literate in Python, PERL, C++, Java

Specializations - Programming

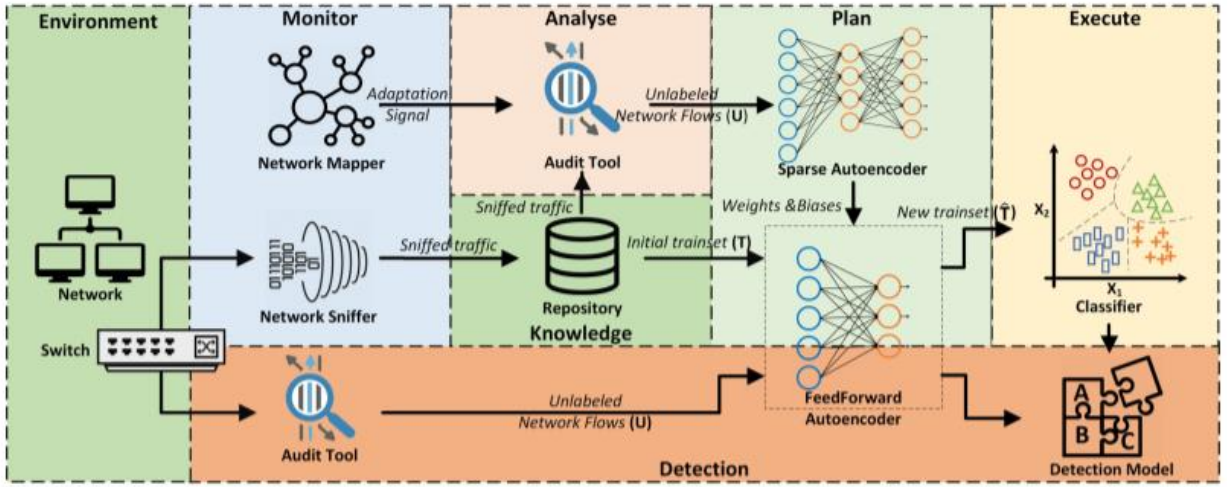
- Host-Based IDS



Du, Min, et al. "Deeplog: Anomaly detection and diagnosis from system logs through deep learning." *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 2017.

Specializations - Programming

- Network-Based IDS



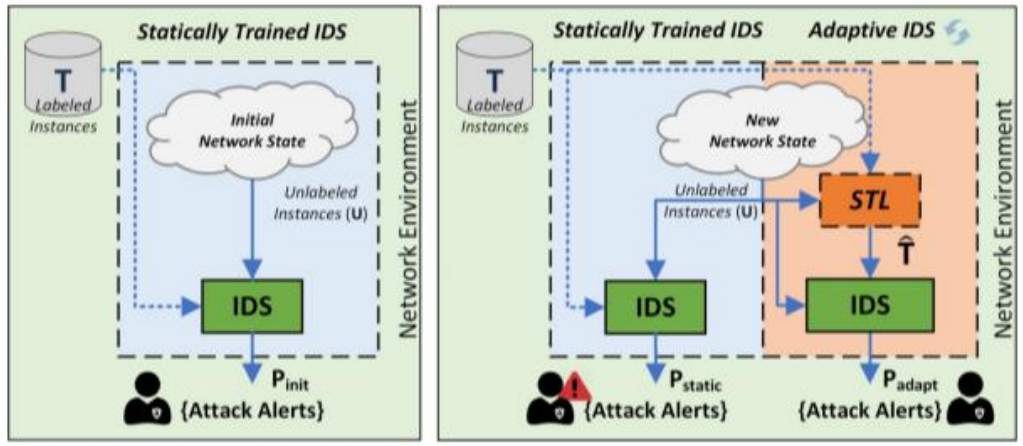


FIGURE 3. In the initial network state, a statically trained IDS can achieve an acceptable performance P_{init} (left). In new network states, the adaptive IDS has the ability to sustain an acceptable performance in contrast to the statically trained IDS. The goal of our methodology is to improve the efficiency of the IDS so that $P_{adapt} > P_{static}$ (right).

Papamartzivanos, Dimitrios, Félix Gómez Mármol, and Georgios Kambourakis. "Introducing deep learning self-adaptive misuse network intrusion detection systems." IEEE Access 7 (2019): 13546-13560.

Specializations - Programming

- Heavily involved with collection processes such as configuring IDS and moving data around so that it may be properly ingested by various detection software packages

- An in-depth knowledge of both
- Windows and Linux platforms is the basis for the specialization, along with an adept
- understanding of data and log collection

Specializations – Malware Analyst

- Basic malware sandboxing in order to extract indicators
- High level of malware analysis: knowledge of both dynamic and static analysis.

Specializations – Host-Based Forensics

- Gains intelligence from an asset that has been compromised by doing a forensic analysis of the host.

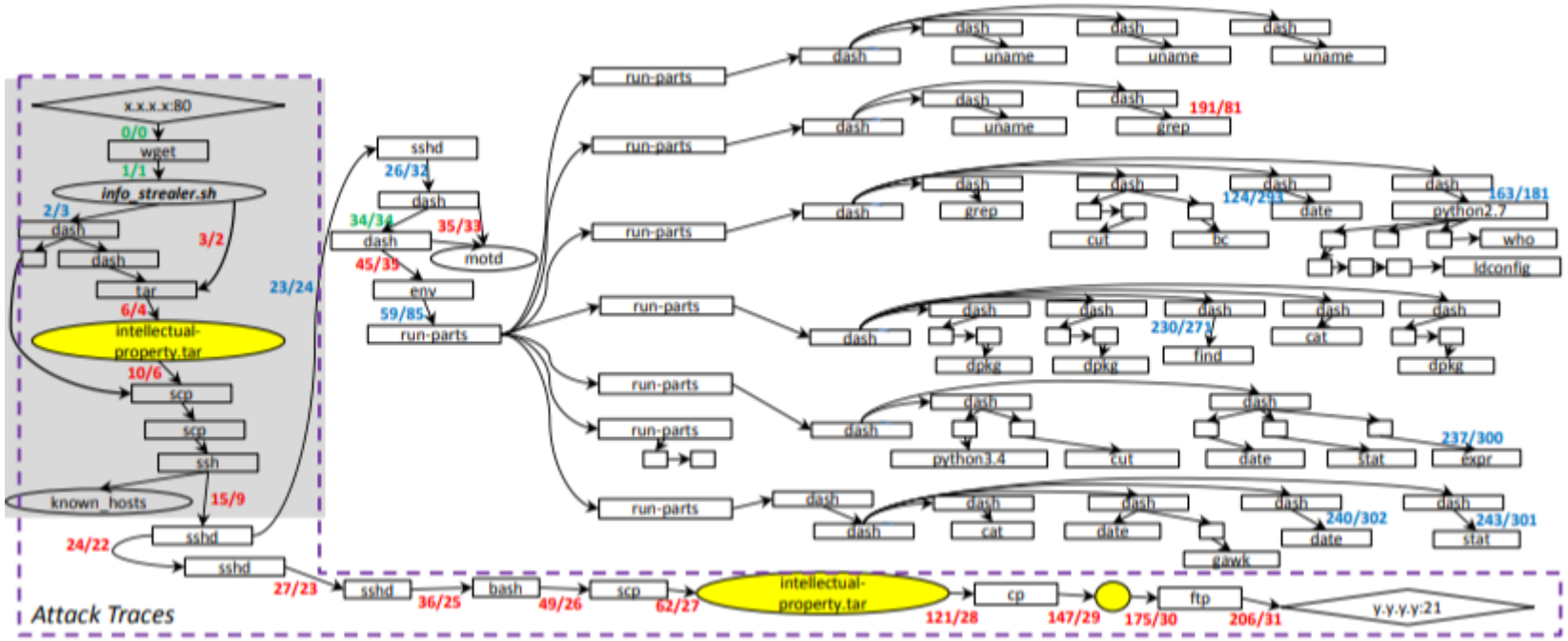


Fig. 5: Reduced Version of Forward Tracking Graph for Motivating Example.

Before Next Class

- Create a Security Onion VM using Virtual Box and Vagrant
- Page 19 in your book and tutorials