PRACTIONER'S Mini Notebook

Series | Cybersecurity

Volume I

NAND RESEARCH

Introduction & Taxonomy

Field Guide

Content Preview

- Landscape Introduction
- A Taxonomy

Version 1.0: 07Oct2025

Table of Content

Landscape Intro

Cybersecurity has rapidly become a cornerstone of IT operations. With digital transformation accelerating and the sophistication of cyber threats on the rise, organizations now face unprecedented risks to their data, applications, networks, and cloud infrastructures. Regulatory pressures and consumer expectations around data privacy only heighten the urgency to implement robust security measures. As a result, cybersecurity is no longer an isolated discipline—it's an integral part of virtually every layer of enterprise IT.

Yet the cybersecurity market can appear incredibly complex and fragmented, with new tools and acronyms (XDR, CSPM, DLP, SOAR, etc.) seeming to emerge every week. Each category promises to solve a specific set of security challenges, but they frequently overlap or interact in ways that can be difficult to understand.

For many IT practitioners — whether they're systems administrators, network engineers, DevOps leads, or CIOs — this creates confusion about which solutions map to their specific needs, who should be responsible for deploying them, and how they fit into a broader defense strategy.

To navigate this complexity, it's helpful to have a clear taxonomy or mental map of key cybersecurity segments and the teams that typically implement them. By breaking down the major security functions (e.g., endpoint protection, network security, cloud security, application security, etc.) and exploring how they relate to one another, IT practitioners can align solutions with their organization's unique threat landscape.

This primer will walk through these segments, highlight the primary tools and practices involved, and indicate how responsibilities might be shared among IT teams—helping you chart a more cohesive, effective security posture for your enterprise.

A Taxonomy

To help IT practitioners navigate the array of cybersecurity tools, services, and approaches, it's useful to segment the market into functional domains. Each domain corresponds to a set of objectives—such as securing endpoints, protecting data, or responding to incidents—and typically involves a collection of technologies and processes.

While acronyms like **CSPM**, **XDR**, **SIEM**, and **DLP** refer to individual capabilities or platforms, they often form part of a layered or integrated defense strategy. The key is understanding how these categories map to an organization's specific threat landscape and compliance requirements.

Below is a practical taxonomy that outlines these domains, highlights key solution categories, and shows which IT teams are often responsible for their implementation and ongoing management.

Area	Categories	Responsible Teams
Endpoint & Extended Detection /Response	**EPP:** Endpoint Protection Platforms **EDR:** Endpoint Detection & Response **XDR:** Extended Detection & Response	IT operations (for endpoint management), security operations center (SOC) analysts (for alert triage and incident response), and desktop support teams (for agent deployments and policy enforcement).
Network & Perimeter Security	**NGFW:** Next-Generation Firewall **IDS/IPS:** Intrusion Detection/Prevention Systems **WAF:** Web Application Firewall **SASE:** Secure Access Service Edge	Network engineers, security architects, and IT infrastructure teams typically oversee deployment and configuration. The SOC team may leverage logs from these devices for threat hunting and incident analysis.
Cloud Security	**CSPM:** Cloud Security Posture Management **CWPP:** Cloud Workload Protection Platform **CASB:** Cloud Access Security Broker **CNAPP:** Cloud-Native Application Protection Platform	Cloud architects and DevOps teams typically set up and maintain cloud workloads, while cloud security specialists ensure policy enforcement, auditing, and monitoring.
Application Security	**SAST:** Static Application Security Testing **DAST:** Dynamic Application Security Testing **IAST:** Interactive Application Security Testing **RASP:** Runtime Application Self-Protection	Application developers, DevOps engineers, and dedicated AppSec teams. Collaboration with QA testers is vital to ensure vulnerabilities are caught early.
Identity & Access Management (IAM)	**MFA/SSO:** Multi-Factor Authentication and Single Sign-On **PAM:** Privileged Access Management **IGA:** Identity Governance & Administration **Zero Trust**	IAM specialists, corporate IT identity teams, and security architects. The SOC may receive alerts for anomalous authentication attempts or privilege escalations.
Data Security	**DLP:** Data Loss Prevention	Database administrators, storage teams, and security architects. Data governance and compliance managers also play key roles in defining classification levels and retention policies.
Threat Intelligence, Monitoring & Response	**SIEM:** SIEM: Security Information & Event Management **SOAR:** SOAR: Security Orchestration, Automation & Response **UEBA:** UEBA: User and Entity Behavior Analytics	SOC analysts typically monitor SIEM dashboards, investigate alerts, and orchestrate responses. Threat intelligence teams maintain updated feeds and share insights with other groups.

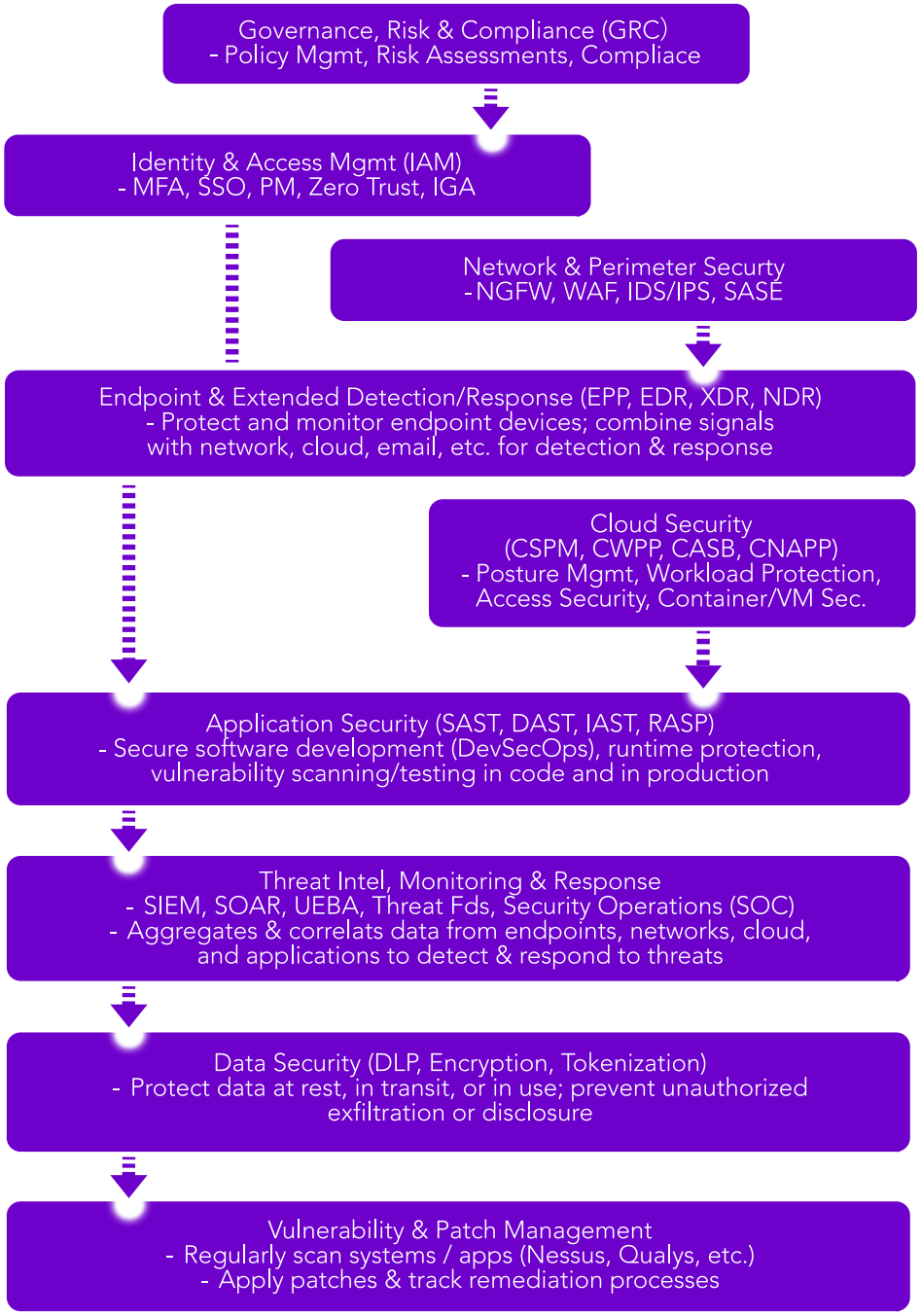

Figure 1: Cybersecurity Taxonomy

This structure shows **one way** to visualize relationships. In a modern environment, these tools often feed data into each other (e.g., **XDR** might pull logs from **SIEM**, or **CSPM** might feed alerts into a **SOAR**). The goal is a **layered defense** with **shared context** across categories.

How to Read This Diagram

1. **Governance, Risk & Compliance (GRC)**
   Sits at the top because it defines policies, standards, and compliance needs that influence all other security domains.

2. **Identity & Access Management (IAM)**
   Critical for controlling who/what has access to resources. It enforces the policies set by GRC.
   - **IAM** also feeds into/perimeter controls and is fundamental for Zero Trust.

3. **Network & Perimeter Security**
   Protects traffic entering, exiting, or moving laterally within the environment. Integrates with IAM to enforce access policies at the network boundary.

4. **Endpoint & Extended Detection/Response (EPP, EDR, XDR, NDR)**
   Monitors devices and correlates endpoint data with network/other sources for broader threat detection and response.

5. **Cloud Security (CSPM, CWPP, CASB, CNAPP)**
   Addresses the unique risks of cloud platforms and services—configuration, workload protection, SaaS application access, and container security.

6. **Application Security (SAST, DAST, IAST, RASP)**
   Secures the software development lifecycle and running applications, typically fed by GRC requirements and integrated with IAM.

7. **Threat Intelligence, Monitoring & Response (SIEM, SOAR, UEBA, Threat Feeds)**
   Gathers telemetry from endpoints, networks, cloud, and applications. Security teams (SOC) use these tools to detect and respond to threats.

8. **Data Security (DLP, Encryption, Tokenization)**
   Focuses on protecting the confidentiality and integrity of data in all stages. Works closely with IAM (for access control) and the monitoring layer (to detect suspicious data transfers).

9. **Vulnerability & Patch Management**
   Spans across all layers to ensure continuous scanning for weaknesses and timely application of patches. Ties back to GRC for reporting risk posture.

Glossary

Application Security (AppSec)
Secures software during development and runtime using tools like SAST, DAST, IAST, and RASP.

CASB (Cloud Access Security Broker)
Enforces policies between cloud users and providers for access, encryption, and threat control.

CSPM (Cloud Security Posture Management)
Monitors and corrects cloud misconfigurations to maintain compliance and visibility.

CNAPP (Cloud-Native Application Protection Platform)
Combines CSPM and CWPP to secure cloud-native apps across build and runtime.

CWPP (Cloud Workload Protection Platform)
Protects workloads like VMs, containers, and serverless apps across cloud environments.

Cybersecurity Taxonomy
Framework mapping how cybersecurity domains connect across IT systems and defenses.

DAST (Dynamic Application Security Testing)
Tests running applications for flaws by simulating real-world attacks.

DLP (Data Loss Prevention)
Prevents unauthorized sharing or leakage of sensitive data.

EDR (Endpoint Detection and Response)
Monitors endpoint activity to detect and respond to advanced threats.

EPP (Endpoint Protection Platform)
Combines antivirus, firewall, and controls to block malware and unauthorized access.

Encryption
Encodes data to protect confidentiality in storage or transit.

GRC (Governance, Risk, and Compliance)
Manages security policies, risk assessment, and regulatory adherence.

IAM (Identity and Access Management)
Controls user identities and permissions across systems; includes MFA, SSO, PAM, IGA.

IAST (Interactive Application Security Testing)
Analyzes applications during runtime to find vulnerabilities.

IDS/IPS (Intrusion Detection and Prevention Systems)
Detects and blocks malicious network traffic automatically.

IGA (Identity Governance and Administration)
Manages identity lifecycles, access rights, and compliance.

MFA (Multi-Factor Authentication)
Uses multiple verification steps for stronger access control.

NDR (Network Detection and Response)
Analyzes network traffic to identify and stop threats.

NGFW (Next-Generation Firewall)
Inspects and filters traffic to block advanced network attacks.

PAM (Privileged Access Management)
Restricts and monitors admin-level access to critical systems.

RASP (Runtime Application Self-Protection)
Protects applications internally by detecting and blocking live attacks.

SASE (Secure Access Service Edge)
Merges network and security services into a unified cloud-delivered model.

SAST (Static Application Security Testing)
Scans source code for security weaknesses before deployment.

SIEM (Security Information and Event Management)
Collects and correlates logs to detect and analyze incidents.

SOAR (Security Orchestration, Automation, and Response)
Automates workflows to speed up detection and response.

SOC (Security Operations Center)
Centralized team monitoring and responding to cyber incidents.

Tokenization
Replaces sensitive data with non-exploitable tokens.

UEBA (User and Entity Behavior Analytics)
Uses AI to spot unusual user or device activity.

UTM (Unified Threat Management)
Bundles firewall, antivirus, and intrusion prevention in one platform.

Vulnerability & Patch Management
Finds and fixes security flaws across systems and apps.

XDR (Extended Detection and Response)
Integrates data across endpoints, cloud, and network for unified defense.

Zero Trust
Eliminates implicit trust—requires constant verification and minimal access.