CLOUD SECURITY TOOLING STARTER PACK

v1.0 2023.11.08.

AV to EDR/CNEP

Traditional AV used signatures; EDR uses behavior detection; CNEP adapts EDR for cloud environments

WAF to CNAPP

WAFs protect web apps at the HTTP level; CNAPP evolved to provide a holistic security posture in the entire cloudnative application lifecycle, including development, deployment, and runtime

Firewalls to SASE Firewalls manage network traffic rules; Network Security in SASE provides comprehensive network control and security in the cloud

SIEM to XDR

SIEM aggregates logs for analysis; XDR extends this by integrating more data sources for threat detection and response across systems

Rise of SOAR

SOAR automates and orchestrates responses to security alerts, integrating with other tools

Secure Access Service Edge SASE provides a broad, SaaS integrated framework to secure cloud access. SASE SSE · SSE focuses on the Security Service Edge security services within that framework. • CASB offers cloud Cloud Access Security Broker **PaaS** visibility and compliance ZTNA delivers secure **CASB** access based on the zero-Zero Trust Network Access trust model **ZTNA** Cloud Native Application Protection CNAPP can be seen as the all-encompassing solution that CSNS IaaS aims to provide a unified Cloud Security Network Services approach to cloud security, incorporating aspects of · CSPM for configuration and **CSPM** compliance. Cloud Security Posture Management CNAPP • CWPP for workload protection at runtime. · CSNS for network security Cloud Workload Protection Platform services **CWPP** Sec. Orchestration, Automation and Response SOAR can be implemented as an overarching system using data **XDR** and alerts of other platforms to automate and coordinate Extended Detection and Response security response and Network **EDR** playbooks across the security **SOAR** infrastructure · XDR for collecting events Endpoint Detection and Response and respond across the network, · EDR: to automate endpoint **CNEP** threat response, Cloud Native Endpoint Protection . CNEP as the next 'AV' for Endpoint cloud-native endpoints

Created by FORTIX Consulting.
This work is licensed under CC BY-NC-SA 4.0. To view a copy of this license,
visit http://creativecommons.org/licenses/by-nc-so/4.0/