paloalto NETWORKS | CORTEX

JOURNEY TO ZERO TRUST:
The Role of the SOC

What, Why & How

What?

The concept of Zero Trust was introduced by Forrester Research analyst John Kindervag as a way of addressing threats that were circumventing traditional security models.

This new model assumed previously "trusted" infrastructure was, in fact, compromised and potentially hostile, and this assumption completely changed the way we think about IT security.

How Palo Alto Networks Defines Zero Trust
A strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of digital interaction.

Why?

The purview of the SOC has traditionally been focused on the perimeter, yet perimeter-centric strategies for security don't work anymore. The location of security infrastructure and systems extends beyond the traditional network perimeter to the public/private cloud and every connected device or endpoint. Each of these requires some level of visibility and control over respective activity and behavior to prevent compromises and breaches.

Factors Fueling the Expanding Attack Surface

- Shift to remote and hybrid work launched by the pandemic
- Applications and data moving off-premises, driven by cloud migration
- Continued growth of connected "smart" devices

Users are everywhere.
76%
of employees want to be hybrid, even after the pandemic.[1]

Apps are everywhere.
80%
of organizations have a hybrid cloud strategy,[2] and the average organization uses 110 SaaS apps.[3]

Traditional Approaches to Security Aren't Working

51%
of security professionals are not satisfied with their ability to detect attacks

78%
of security analysts say each security alert takes 10+ minutes to investigate

207 Days
Mean time to identify (MTTI) a breach

How?

Reassess Trust Decisions

With digital transformation initiatives, including applications and data moving off-premises, driven by cloud migration and the continued growth of connected "smart" devices, our collective attack surface knows no bounds. As such, our trust decisions need to be reevaluated to secure modern enterprise ecosystems.

Securing Users with Zero Trust

Identity
Validate developers, DevOps and admins with strong authentication

Device/ Workload
Verify user's device integrity

Access
Enforce least-privileged access for workloads accessing other workloads

Transaction
Scan all content for malicious activity and data theft

Securing Applications with Zero Trust

Identity
Validate developers, devops, and admins with strong authentication

Device/ Workload
Enforce least-privileged access for workloads accessing other workloads

Access
Least-privileged access segmentation for native and third-party infrastructure

Transaction
Scan all content for malicious activity and data theft

Securing Infrastructure with Zero Trust

Identity
Validate all users with access to the infrastructure

Device/ Workload
Identify all devices including IoT

Access
Least-privileged access segmentation for native and third-party infrastructure

Transaction
Scan all content within the infrastructure for malicious activity and data theft

SOCs Make Better Trust Decisions

The SOC double-checks trust decisions that have already been made using tools focused on user and entity behavioral analytics (UEBA), threat hunting, anomaly detection and correlation rules in the SIEM.

Validate continuously with an ongoing audit function for Zero Trust policies and actions.

Prevent and limit the impact of attacks.

Automate threat data collection and response workflows.

Provide a second layer of verification to find threats you can't easily prevent (like insider attacks or advanced persistent threats).

Focus People Effort on Right Side of Cyberattack Lifecycle

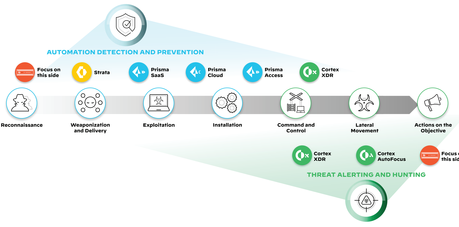

Figure 1: The SOC plays a critical role in continuous monitoring and the Cyber Kill Chain

Better Together

Our Cortex portfolio – Cortex XDR, Cortex XSOAR, Cortex Xpanse and now, Cortex XSIAM – is ready to make Zero Trust possible for any size SOC.

CHOOSE FROM BEST-IN-CLASS INTEGRATED PRODUCTS

Cortex XDR
Prevent, detect and investigate attacks across the enterprise

Cortex XSOAR
Automate response and improve with every incident

Cortex Xpanse
Discover and protect your entire internet attack surface

SELECT OR EASILY MIGRATE TO A UNIFIED SECOPS PLATFORM

Cortex XSIAM
Unify SOC operations with an integrated, AI-driven platform

ENLIST UNIT 42 EXPERT SECURITY SERVICES

Managed Security Services
Unit 42 trusted security and operations management choices

Figure 2: The Cortex suite offers flexibility and growth

Ready to Learn More?

" A Practical Guide to Adopting Zero Trust Best Practices in the SOC"

Download our whitepaper →

1 The State of Hybrid Workforce Security 2021, Palo Alto Networks, August 25, 2021.
2 Flexera 2021 State of the Cloud Report, Flexera, March 2021.
3 Cloud Apps Statistics - "Average number of SaaS apps used by organizations worldwide 2015-2020," Statista, February 16, 2022.