paloalto NETWORKS | ZERO TRUST

ZERO TRUST

The Strategic Approach to Stop Data Breaches

John Kindervag

Field CTO, Palo Alto Networks

@Kindervag

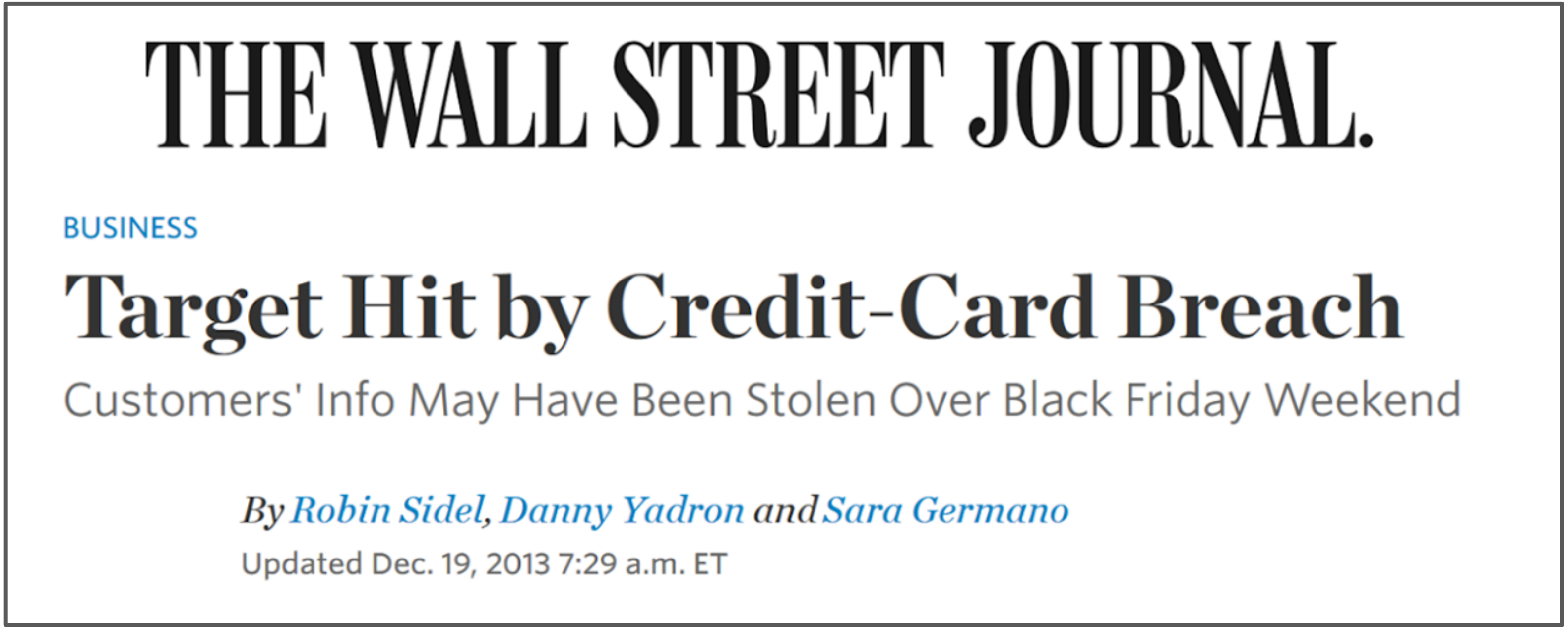
The Four Levels of Strategic Engagement

Grand Strategy	The Ultimate Goal
Strategy	The Big Idea
Tactics	The Things You Use
Operations	The Way You Use Them

The Four Levels of Cyber War

Grand Strategy	Stop Data Breaches
Strategy	Zero Trust
Tactics	Tools & Techniques
Operations	Platform & Policies

Cyber Security Grand Strategy: Prevent Data Breaches



THE WALL STREET JOURNAL.

BUSINESS

Target Hit by Credit-Card Breach

Customers' Info May Have Been Stolen Over Black Friday Weekend

By Robin Sidel, Danny Yadron and Sara Germano

Updated Dec. 19, 2013 7:29 a.m. ET

The Four Levels of Cyber War

Grand Strategy	Stop Data Breaches
Strategy	Zero Trust
Tactics	Tools & Techniques
Operations	Platform & Policies

TRUST

is a dangerous

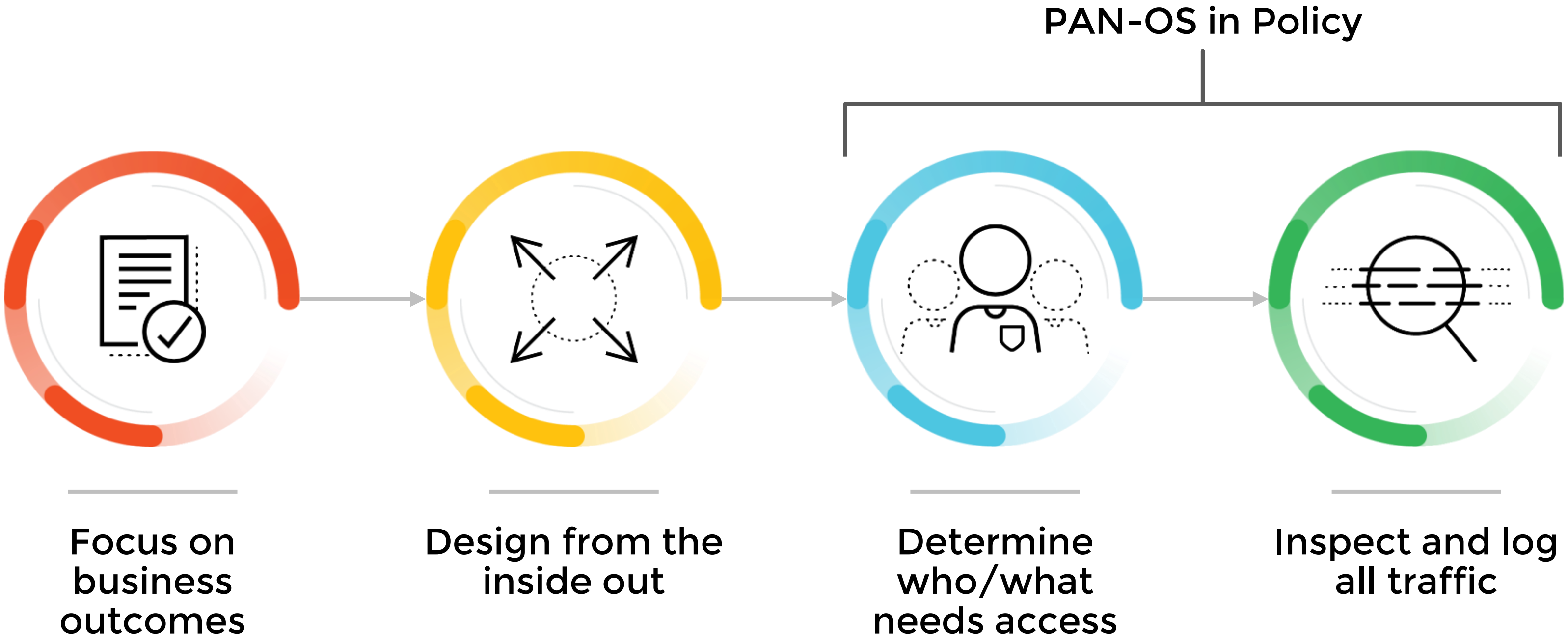
VULNERABILITY

that is

EXPLOITED

by **MALICIOUS** actors

Zero Trust Design Concepts



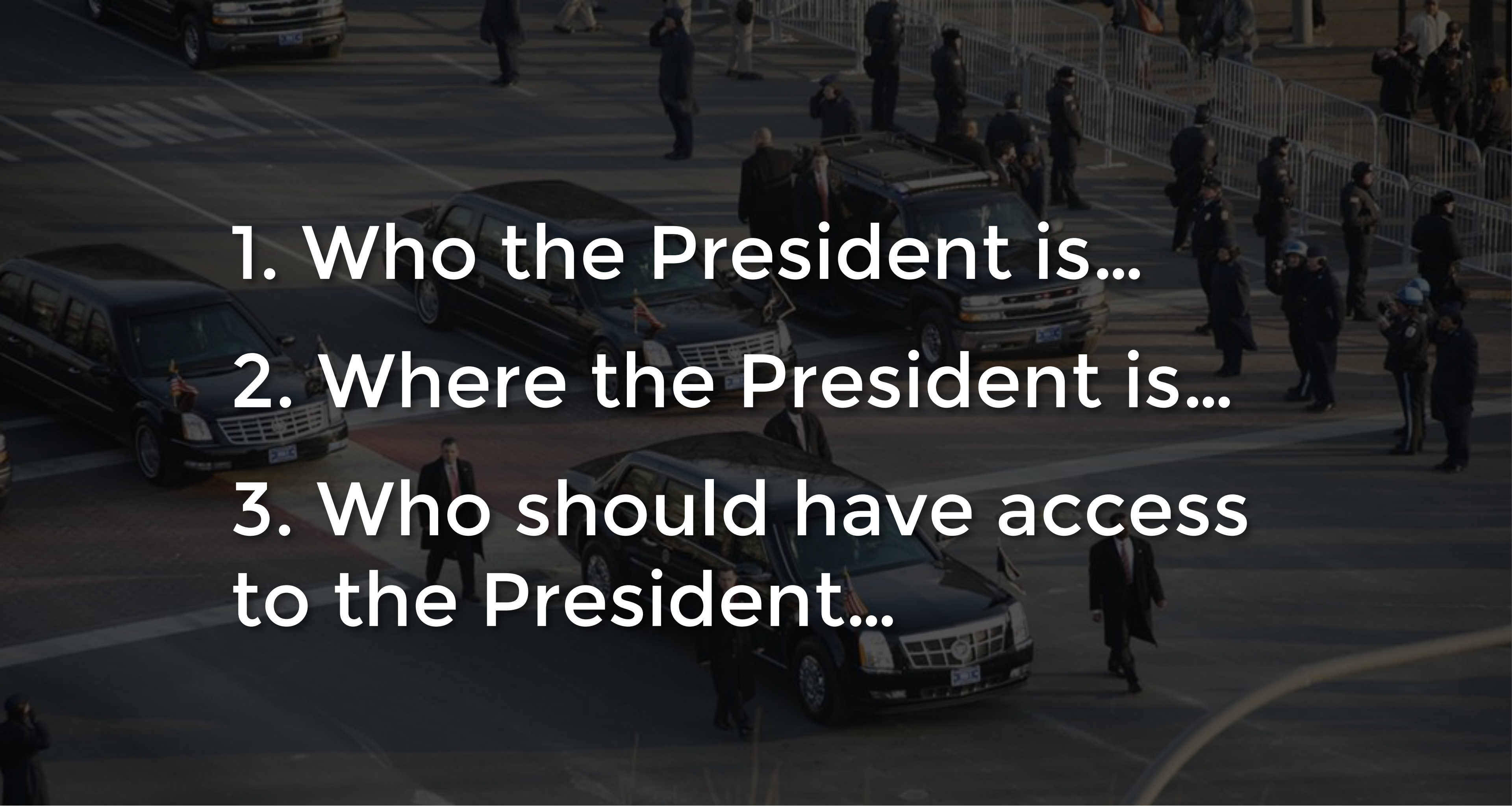
PAN-OS in Policy

Focus on business outcomes

Design from the inside out

Determine who/what needs access

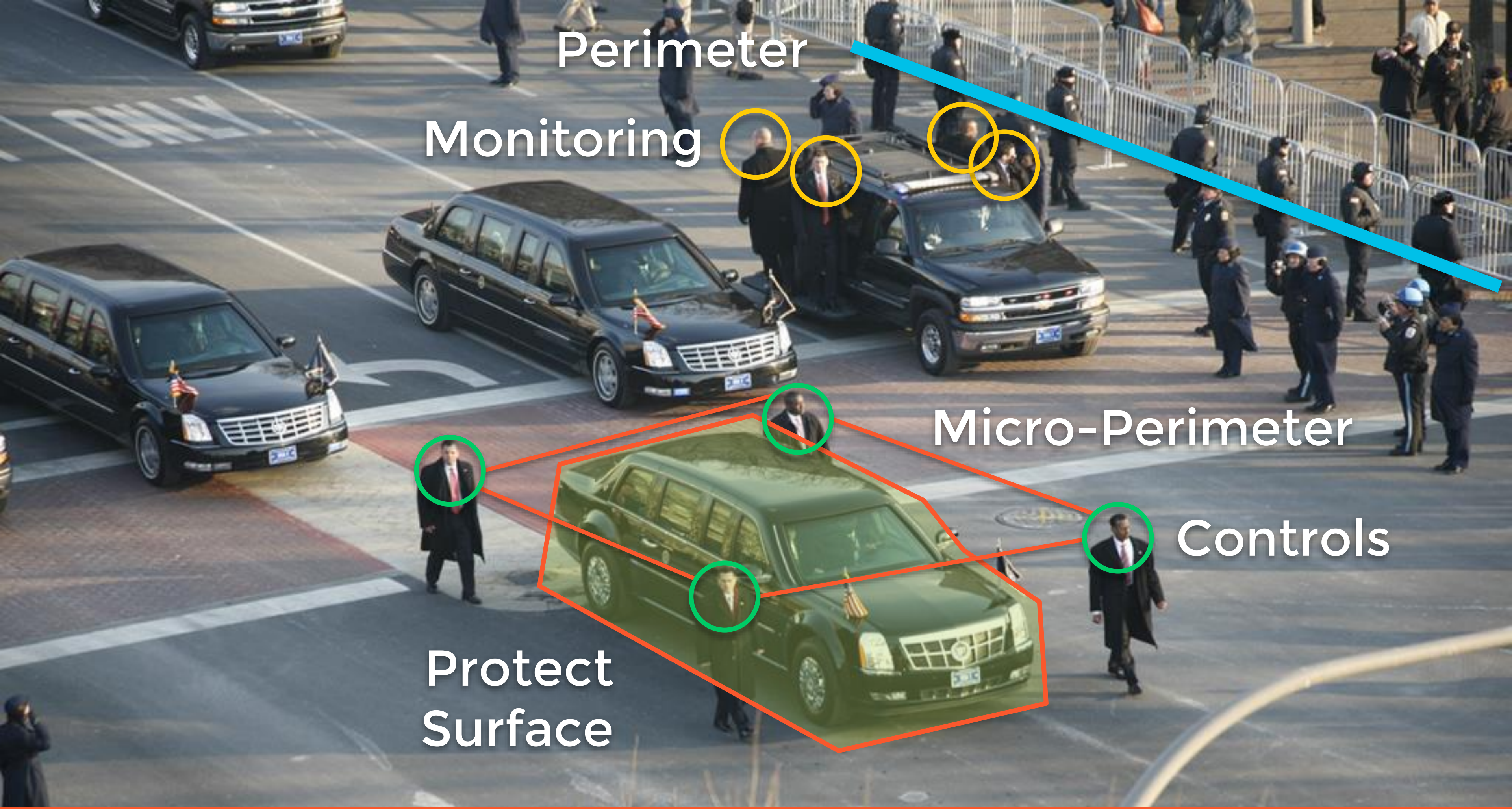
Inspect and log all traffic



1. Who the President is…

2. Where the President is…

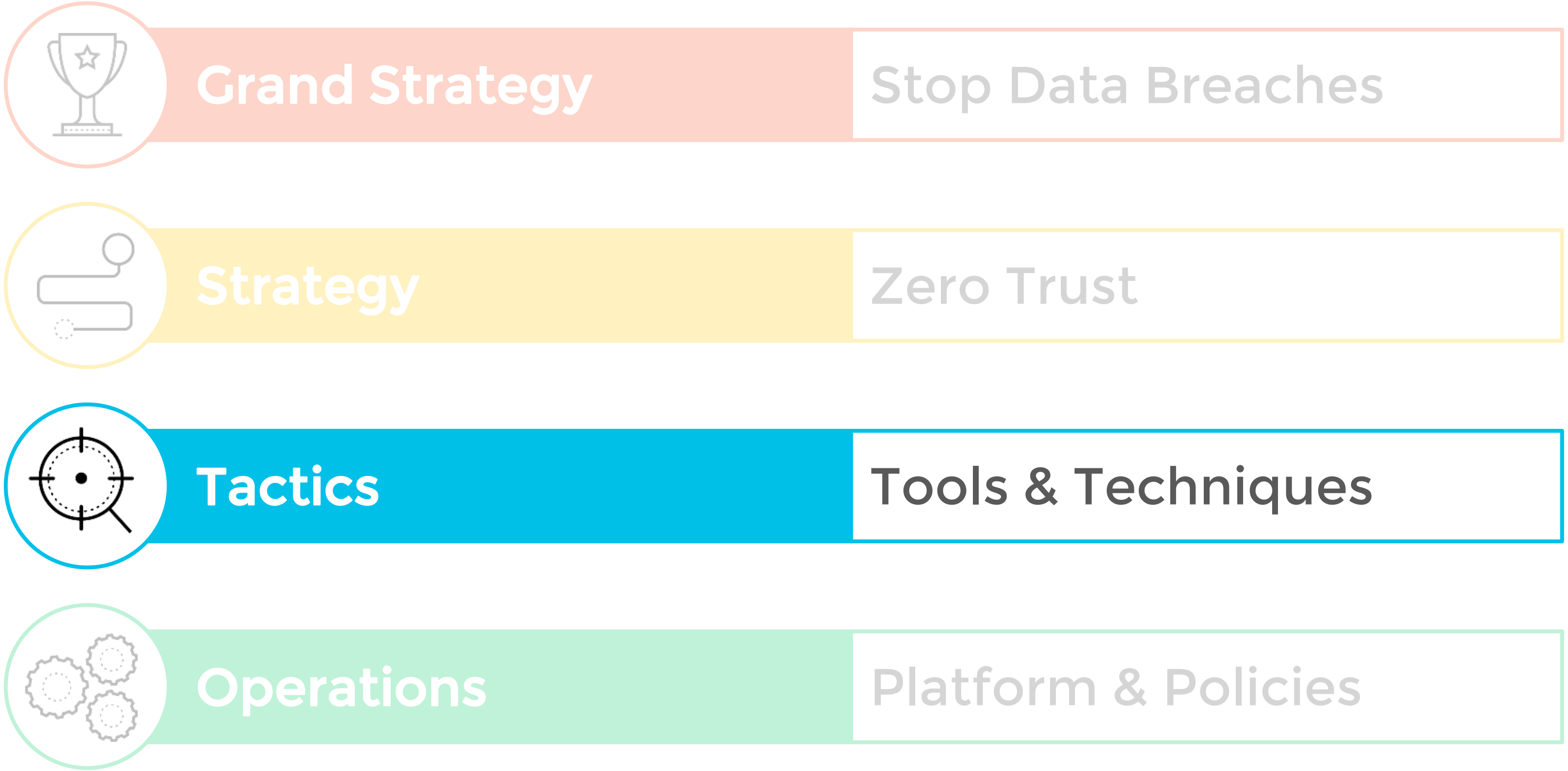
3. Who should have access to the President…



Perimeter
Monitoring
Micro-Perimeter
Controls
Protect Surface
ONLY

ZERO TRUST

The Four Levels of Cyber War



Grand Strategy	Stop Data Breaches
Strategy	Zero Trust
Tactics	Tools & Techniques
Operations	Platform & Policies

5 Steps to a Zero Trust Environment

Data

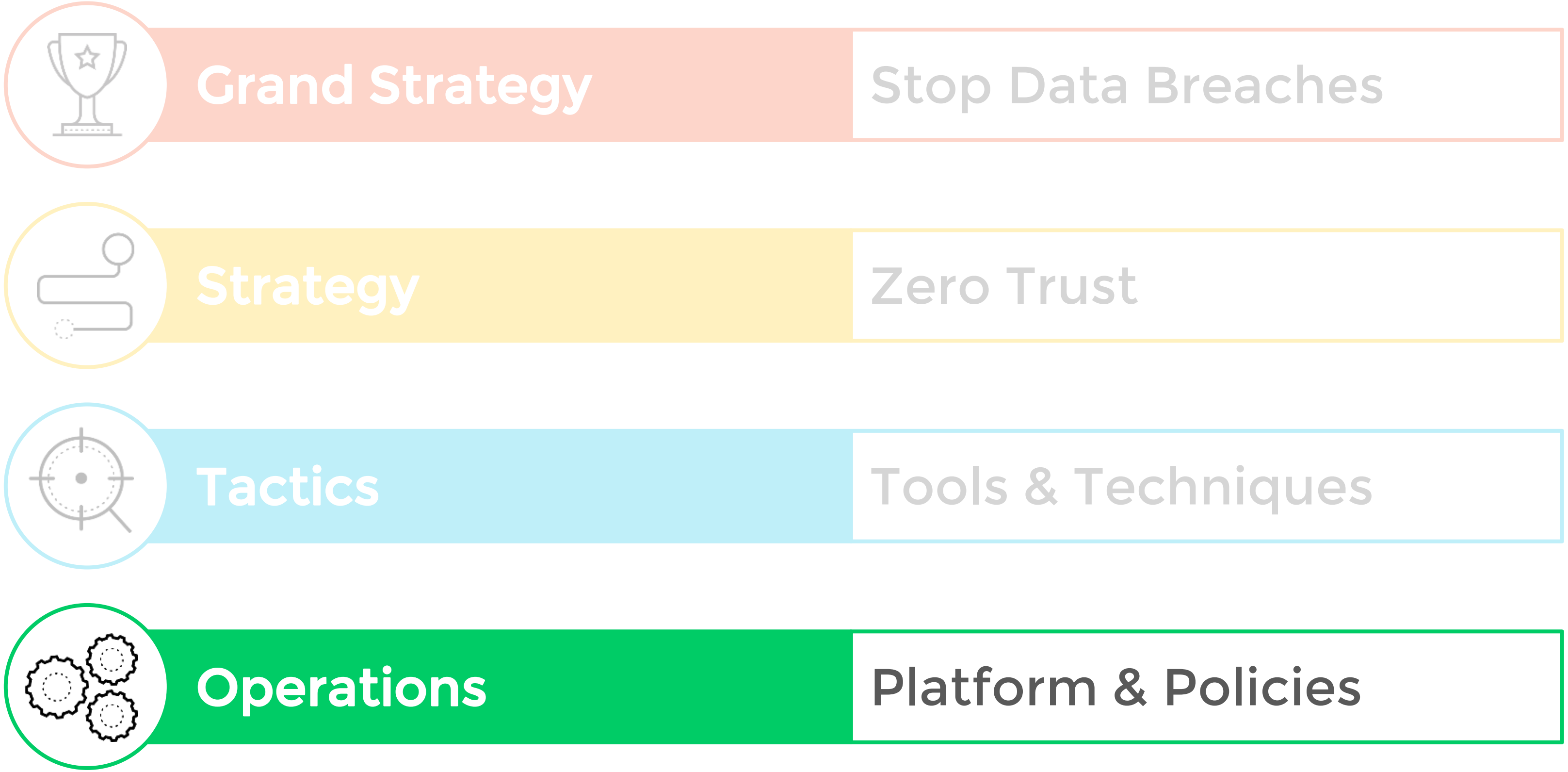
Applications

Assets

Services

1. Define your Protect Surface	Next-Generation Firewall VM Series Cortex™ XDR Cortex™ Data Lake Transformation Services
2. Map the Transaction Flows	Next-Generation Firewall VM Series Cortex™ XDR Cortex™ Data Lake Cortex™ XDR Prevent Transformation Services
3. Architect a Zero Trust Environment	Next-Generation Firewall VM Series Cortex™ XDR Cortex™ Data Lake Cortex™ XDR Prevent GlobalProtect Prisma Access Transformation Services
4. Create Zero Trust Policy	Panorama WildFire Threat Prevention URL Filtering Prisma SaaS DNS Service Transformation Services
5. Monitor and Maintain the Network	AutoFocus Cortex™ XDR Cortex™ Data Lake MineMeld Prisma Public Cloud Cortex XSOAR Transformation Services

The Four Levels of Cyber War



Grand Strategy	Stop Data Breaches
Strategy	Zero Trust
Tactics	Tools & Techniques
Operations	Platform & Policies

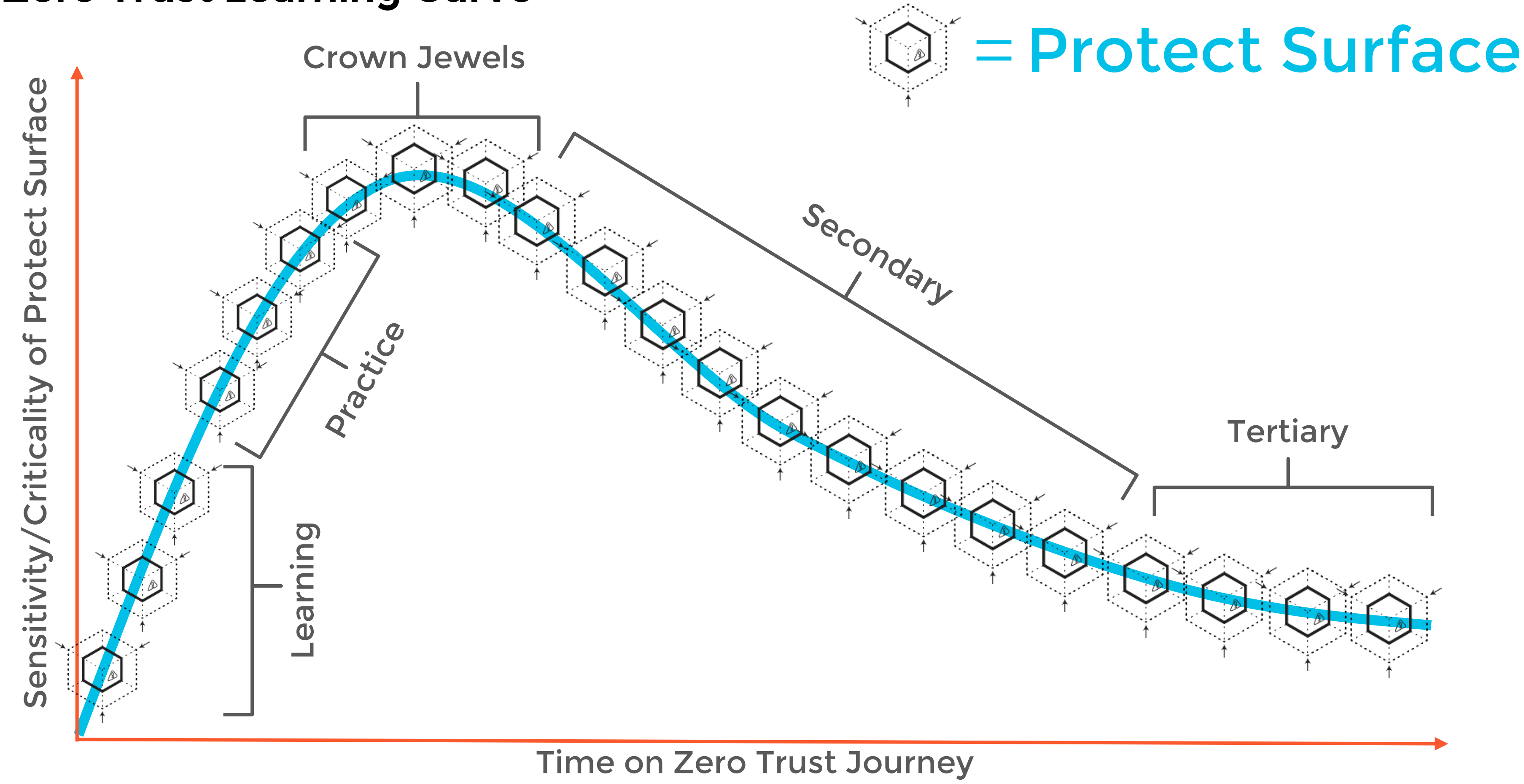
The Kipling Method of Zero Trust Rule Writing

Who	What	When	Where	Why	How
User ID	**Application ID**	Time Limitations	**Device ID**	Classification	**Content ID**
Auth type			System Object	Data ID	Threat Protection
			Workload		SSL Decryption
			Geolocation		URL Filtering
					Wildfire

Cloud:
IF Who (UID) = Sales, What (AID) = Salesforce, When (TOD) = Working Hours, Where (LOC) = US, Why (CLASS) = Toxic, How (CID) = SFDC_CID, THEN Allow.

On Prem:
IF Who (UID) = Epic_Users, What (AID) = Epic, When (TOD) = Any, Where (LOC) = Epic_Srvr, Why (CLASS) = Toxic, How (CID) = Epic_CID, THEN Allow.

Zero Trust Learning Curve


= Protect Surface
Crown Jewels
Practice
Secondary
Tertiary
Learning
Sensitivity/Criticality of Protect Surface
Time on Zero Trust Journey

ZERO TRUST

John Kindervag

Field CTO

✉ jkindervag@paloaltonetworks.com

@Kindervag

paloalto NETWORKS