```
root@apex-sec-lab:~/strategy-2026# ./init_deck.sh
```

ZERO-TRUST ARCHITECTURE & THREAT HUNTING

Next-Generation Cloud Infrastructure Defense & Continuous Attestation

STATUS: ACTIVE | CLEARANCE: CONFIDENTIAL | VER: 4.2.0

Presented By:

Dr. Alex Mercer (Principal Architect, Apex Lab)

Elena Rostova (Lead Threat Analyst, Vertex Security)

Target Environment:

Project Meridian Infrastructure

July 2026 // Global Cyber Operations

$ Executive Summary: The Threat Environment

Primary Objectives

- Eliminate implicit trust boundaries across multi-cloud setups.
- Enforce micro-segmentation at compute boundaries.
- Implement automated pipelines with sub-minute containment.
- Continuous identity attestation using Ephemeral PKI tokens.

2026 Key Risk Vectors

- API Credential Leakage in CI/CD pipelines (+42% YoY).
- Non-Human Identity (NHI) key escalation in microservices.
- Supply chain compromise via unverified container registries.
- Lateral movement through over-privileged service accounts.

```
syslog@vertex-node-04:~$ tail -n 2 /var/log/audit.log
[ALERT] Unauthenticated API call from 192.0.2.145 to /v2/keys (Blocked by PDP)
[INFO] Session token revoked for service-account:synapse-worker-09
```

$ Presentation Roadmap

cat /etc/cyber-deck/agenda.conf

[01] **Modern Threat Landscape & Vector Analysis**
Cloud API risks, identity sprawl, and non-human credential abuse.

[02] **Zero-Trust Architecture Foundations**
Policy Decision Points (PDP), micro-segmentation, and ephemeral authentication.

[03] **Real-Time Telemetry & Threat Hunting**
eBPF kernel tracing, log enrichment, and automated anomaly detection.

[04] **Automated Remediation & Playbooks**
SOAR integration, microservice isolation, and automated token revocation.

[05] **Case Study: Project Meridian Deployment**
Production metrics, incident MTTR reduction, and enterprise security posture.

SECTION 01

Modern Threat Landscape

Cloud-native attack surfaces, identity exploitation, and telemetry gaps.

cat /var/data/vectors_identity.json

1. Non-Human Identities (NHI)

> Service accounts outnumber human users 15 to 1.

> Long-lived API keys unrotated for > 180 days.

> Over-scoped IAM roles grant blanket admin rights.

cat /var/data/vectors_infra.json

2. Container & Kubernetes Risks

> Misconfigured Pod Security Standards (PSS).

> Exposed Kubelet APIs and open endpoints.

> Vulnerabilities in third-party base images.

🔑 **Key Takeaway:** Traditional perimeter firewalls cannot inspect microservice east-west traffic effectively.

Analysis of observed tactics, techniques, and procedures across enterprise environments:

Tactic ID	Attack Vector	Primary Target	Risk Level	Mitigation Status
T1078	Credential Access	CI/CD Pipeline Tokens	CRITICAL	Enforced Ephemeral
T1190	Exploit Public App	Ingress Gateway Endpoints	HIGH	WAF + PDP Filter
T1068	Privilege Escalation	Container Host Kernel	MEDIUM	eBPF Seccomp Profil
T1020	Data Exfiltration	Database Replica Endpoints	HIGH	mTLS + DLP Senso
T1496	Resource Hijacking	Unused Compute Nodes	LOW	Auto-Scaling Limit

Defense Posture Summary

100% of high-risk vectors are mapped directly to continuous policy decision enforcement points.

SECTION 02

Zero-Trust Architecture Foundations

Never trust, always verify: Identity attestation, PDP/PEP enforcement, and micro-segmentation.

$ The Core Pillars of Zero-Trust

1. Identity Attestation

- Dynamic mTLS certificate gen.
- Short-lived SPIFFE IDs.
- Hardware TPM key storage.

2. Micro-segmentation

- L4 and L7 network policies.
- Default-deny rule engine.
- Service-mesh proxies.

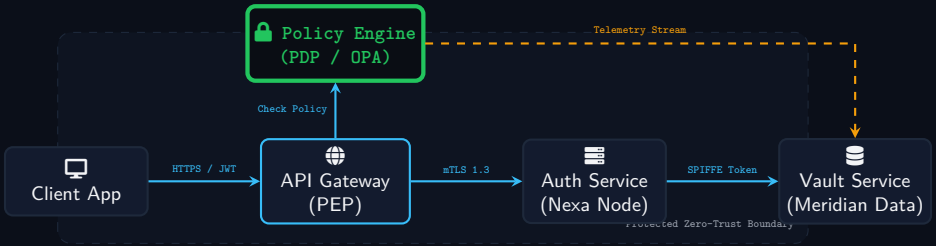
3. Continuous Telemetry

- Kernel-level eBPF tracing.
- Real-time behavior profile.
- Automated risk engine.

```
zt-policy-check -service nexus-api

[PASSED] Identity token verified (SPIFFE: spiffe://apex.internal/sa/nexus-api)
[PASSED] mTLS Handshake completed with Cipher:  TLS_AES_256_GCM_SHA384
```

$ Zero-Trust Control & Data Plane Architecture



PEP = Policy Enforcement Point | PDP = Policy Decision Point | OPA = Open Policy Agent | mTLS = Mutual TLS

SECTION 03

Real-Time Telemetry & Detection

eBPF event stream capture, rule evaluation, and log anomaly identification.

$ Telemetry Analysis & Detection Logic

auditd_event.json

```
{
"timestamp": "2026-07-24T09:12:04Z",
"event_type": "EXECVE",
"process": "/usr/bin/curl",
"parent": "synapse-worker-app",
"user": "www-data",
"cmdline": "curl -s http://169.254.169.254/",
"container_id": "c9a8f42d11",
"threat_score": 0.94
}
```

detection_rule.py

```
def evaluate_event(event):
# Check for IMDS SSRF Attempt
if "169.254.169.254" in event.cmdline:
if event.user != "root_admin":
emit_alert(
severity="CRITICAL",
action="KILL_CONTAINER",
target=event.container_id
)
return True
return False
```

Anomaly Detected: Metadata SSRF Probing

Automated rule matched execution pattern. Container c9a8f42d11 isolated in 120ms.

$ Security Operations Benchmarks (2026 Targets)

APEX-SEC // LABS

MEAN TIME TO DETECT

14s

✔ -82% vs 2025

MEAN TIME TO RESPOND

45s

✔ Fully Automated

FALSE POSITIVE RATE

0.4%

✔ Tuned ML Rules

TELEMETRY RATE

2.4M

events / second

```
telemetry-status -cluster meridian-prod
[OK] eBPF Sensors active on 1,420 nodes | Zero loss buffer | Latency:  4.2ms
```

SECTION 04

Automated Response Playbooks

Closed-loop mitigation: Isolation, key rotation, and patch deployment.

$ Automated Incident Response Workflow


```
soar-engine -playbook auto_contain_v4.yaml
```

1. **Revoke OAuth Token:** Invalidation across Redis cache nodes.
2. **Cilium Policy:** Apply drop-all egress rule to target.
3. **Memory Dump:** Capture volatile RAM state to S3 storage bucket.
4. **Ticket Gen:** Auto-create P1 incident in Vertex Ops Center.

$ Case Study: Project Meridian Production Rollout

Legacy Infrastructure (Pre-2026)

- Perimeter firewall with flat internal network.
- Static 90-day API keys for microservices.
- Manual SOC triage (avg MTTR: 4.2 hours).
- Audits performed once per quarter.

Zero-Trust Mesh (Post-2026)

- Granular L7 network micro-segmentation.
- Ephemeral SPIFFE tokens (15-min TTL).
- Automated SOAR playbook (avg MTTR: 45s).
- Continuous real-time compliance attestation.

✔ **Outcome:** Zero unauthorized lateral movement incidents recorded during Q2 2026 Red Team audit.

cat /opt/apex/roadmap_checklist.md

[X] **Phase 1: Identity & Ephemeral Credentials**
Complete migration from static keys to SPIFFE/SPIRE PKI tokens.

[X] **Phase 2: eBPF Telemetry Sensor Deployment**
Deploy kernel event filters across all Kubernetes worker nodes.

[>] **Phase 3: Automated East-West Policy Tuning**
Transition from audit mode to enforcing default-deny in production.

[ ] **Phase 4: AI Threat Simulation & Red Teaming**
Implement continuous adversarial validation pipelines.

root@apex-sec-lab:~# ./shutdown_presentation.sh -success

THANK YOU

Questions & Discussion

CONTACT & LAB RESOURCES

Apex Cyber Security Research Lab // Vertex Security Alliance

Email: contact@apex-sec.internal |

Docs: https://meridian.apex.internal

Session Terminated Successfully. Press [ESC] to Exit.