THE ANATOMY OF MODERN ENDPOINT DETECTION AND RESPONSE

FROM KERNEL HOOKS TO ZERO TRUST

A SECURITY PROFESSIONAL'S GUIDE

KERNEL-LEVEL INSTRUMENTATION

BEHAVIORAL TELEMETRY

DETECTION ENGINEERING

THREAT HUNTING AND INVESTIGATION

ZERO TRUST INTEGRATION

SERGEI LEBEDEV

The Anatomy of Modern Endpoint Detection and Response

From Kernel Hooks to Zero Trust — A Security Professional's Guide

Steve T. Publications

This book is available at
https://leanpub.com/theanatomyofmodernendpointdetectionandresponse

This version was published on 2026-07-03

This is a Leanpub book. Leanpub empowers authors and publishers with the Lean Publishing process. Lean Publishing is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

Contents

From Kernel Hooks to Zero Trust — A Security Professional's Guide

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Introduction: Why Endpoints Matter More Than Ever

The average organization now manages more than 10 endpoints per employee. Laptops, desktops, servers, mobile devices, IoT sensors, and cloud workloads all represent attack surfaces where adversaries can establish a foothold, move laterally, and exfiltrate data. The endpoint is no longer just a computer sitting on a desk. It is the primary interface between users, applications, and the broader network, making it simultaneously the most valuable target and the richest source of security telemetry.

This book exists because modern Endpoint Detection and Response has become too complex to understand from vendor documentation alone. EDR systems now operate at kernel level, collect billions of events per day, run machine learning models in real time, and integrate with identity platforms, cloud security posture management tools, and security orchestration engines. A security professional who only understands EDR as "better antivirus" is operating with a significant blind spot.

What You Will Learn

This book takes you on a journey from the historical foundations of endpoint security through the technical internals of how EDR systems work, to advanced detection methodologies and future trends. Specifically, you will learn:

- How EDR evolved from signature-based antivirus through heuristic engines to behavioral detection platforms
- The architecture of modern EDR agents, including kernel-level hooks on both Windows and Linux
- How telemetry is collected, normalized, and transformed into actionable detection signals
- Rule-based detection using YARA and Sigma, and how to engineer detections that reduce false positives

- Machine learning approaches to malware classification and anomaly detection at scale
- Threat hunting methodologies, from hypothesis-driven investigations to intelligence-led programs
- Incident response automation through SOAR integration and playbook design
- How EDR fits into zero-trust architectures, including device health attestation and continuous verification
- The evolution toward XDR platforms and the role of AI in next-generation security operations

Who This Book Is For

This book targets security professionals who need to understand EDR at a technical level. SOC analysts will find practical guidance on tuning, hunting, and investigation. Security engineers and architects will gain insight into agent design, data pipelines, and integration patterns. CISOs and security leaders will find frameworks for vendor evaluation, program maturity assessment, and ROI measurement. The technical chapters assume familiarity with operating system fundamentals, networking concepts, and basic security operations. Where specialized knowledge is required, the book provides enough context to follow the discussion without requiring a separate text on kernel programming or machine learning theory.

How to Read This Book

The chapters build on each other in a deliberate sequence. Chapters 1 through 3 establish the historical context, threat landscape, and architectural foundations. Chapters 4 and 5 dive into the technical internals of how EDR systems observe endpoint behavior. Chapters 6 through 8 cover detection methodologies, from rules to machine learning to human-driven hunting. Chapters 9 through 11 address response, integration, and evolution. Chapter 12 provides practical guidance on building and operating an EDR program at enterprise scale.

You can read the book sequentially for the complete narrative, or jump to specific chapters based on your immediate needs. The technical deep dives

in Chapters 4 and 7 are self-contained enough to serve as reference material, while the practical guidance in Chapter 12 assumes you have absorbed at least some of the earlier material.

A Note on Scope and Limitations

This book focuses on enterprise-grade EDR systems deployed on Windows, Linux, and macOS endpoints. It does not cover mobile endpoint security in depth, though many principles apply. The technical internals chapters emphasize Windows and Linux because these platforms represent the majority of enterprise endpoints and the most mature EDR instrumentation. Where vendor-specific details are included, they are presented as examples rather than endorsements, and the focus remains on architectural patterns that apply across platforms.

The threat landscape continues to evolve rapidly. Techniques, tools, and frameworks described in this book reflect the state of the art as of mid-2026. EDR vendors release new capabilities monthly, and adversaries adapt their tradecraft continuously. The principles and architectures discussed here are designed to remain relevant even as specific implementations change.

Chapter 1: The Endpoint Awakening

The Signature Era and Its Limits

When Antivirus Failed — Key Breaches That Changed Everything

The Birth of EDR as a Category

Why Endpoints Became the New Battleground

Chapter 2: The Modern Threat Landscape

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Living-off-the-Land Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Fileless Malware and Memory-Only Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Supply Chain and Initial Access Brokers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

The MITRE ATT&CK Framework as a Lens

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Ransomware Economics and Endpoint Targeting

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Chapter 3: EDR Architecture Fundamentals

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

The EDR Agent — Design and Deployment

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Data Collection Pipeline Architecture

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Cloud vs On-Premises Backend Models

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Performance Overhead and Resource Management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Multi-Tenant and Enterprise Scale Considerations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Chapter 4: Kernel-Level Hooks and System Instrumentation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Windows ETW and Sysmon — The Telemetry Backbone

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Linux Audit Subsystem and eBPF

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Kernel Callbacks and SSDT Hooking

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Process Injection Detection Mechanisms

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

File System Filter Drivers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Chapter 5: Behavioral Telemetry and Signal Engineering

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Process and Execution Telemetry

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Network Connection and DNS Signals

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

File System and Registry Activity

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

User and Authentication Events

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Signal-to-Noise Ratio — The Core Challenge

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Chapter 6: Rule-Based Detection and Signature Engineering

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

YARA Rules for Endpoint Detection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Sigma Rules and Normalized Detection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Heuristic Analysis Engines

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Detection as Code Practices

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Tuning and Reducing False Positives

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Chapter 7: Machine Learning in Endpoint Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Supervised Learning for Malware Classification

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Unsupervised Anomaly Detection at Scale

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Behavioral Scoring and Risk Models

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Model Training Data and Feature Engineering

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

A Walkthrough — Building a Behavioral Anomaly Detection Model

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Adversarial ML — Attacking the Detector

Chapter 8: Threat Hunting Methodologies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Hypothesis-Driven Threat Hunting

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Intelligence-Led Hunting from Indicators

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Data-Driven Anomaly Investigation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Building a Threat Hunting Program

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Real-World Hunt Case Studies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Chapter 9: Incident Response and Automated Playbooks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Containment Strategies — Isolate, Block, Kill

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Automated Response Playbooks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Forensic Data Collection at the Endpoint

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Memory Dumping and Artifact Preservation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Integration with SOAR Platforms

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Chapter 10: Integration with Zero Trust Architecture

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Zero Trust Principles and Endpoint Posture

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Device Health Attestation and Conditional Access

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Identity-Aware Endpoint Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Microsegmentation and Lateral Movement Prevention

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Continuous Verification in Practice

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

A Walkthrough — Implementing EDR-Based Conditional Access at Scale

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Continuous Verification in Practice (Revisited)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Chapter 11: The XDR Evolution and Beyond

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

From EDR to XDR — Data Convergence

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Cloud-Native Endpoint Protection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

AI-Assisted Analysis and Auto-Investigation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

The Role of Open Source and OSSEC Modern Successors

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Future Trends and Emerging Capabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Chapter 12: Building and Operating an EDR Program

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Vendor Selection and Evaluation Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Deployment Strategies — Phased Rollout

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

A Walkthrough — Deploying EDR at a 10,000-Endpoint Organization

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Tuning for Your Environment

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Building the SOC Team Around EDR

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Measuring ROI and Program Maturity

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

Conclusion: The Endpoint as Security Foundation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.

References

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/theanatomyofmodernendpointdetectionandresponse.