

drut.

# DRUT Cyber Security Operations Intelligence Platform

By  
Drut

Edition  
March 2026



# Operationalizing Continuous Cyber Threat Monitoring & Security Operations Visibility for Financial Institutions

## Market Place

Modern financial institutions operate in an increasingly complex cyber threat environment where real-time visibility into security operations is critical.

Security Operations Centers (SOCs) are responsible for monitoring threats, detecting anomalies, and responding to incidents across an organization's digital infrastructure.

**However, many organizations struggle to gain comprehensive operational visibility due to:**

1. Fragmented monitoring tools across security environments
2. Siloed security telemetry across multiple platforms
3. Lack of centralized operational dashboards for SOC leadership
4. Difficulty correlating alerts across security layers
5. Limited executive-level visibility into cyber threat posture

# Market Place

As cyber threats continue to evolve, organizations require integrated operational intelligence that consolidates security monitoring across systems into a unified SOC view.

**Several solutions in the market attempt to address parts of this challenge. These include:**

S\* /S\*\*\*\*\*platforms\*\*

Providing SIEM-based threat monitoring

L\* analytics tools\*\*

Focused on log aggregation and alert correlation

G\*I security analytics platforms

Providing threat detection analytics

X\*\*\* security platforms\*\*

Delivering endpoint detection and response dashboards

While these tools provide valuable telemetry, they often operate as isolated security monitoring systems rather than unified operational intelligence platforms.



# A Different Approach: Cyber Security Operations Intelligence

**DRUT introduces a new category:**

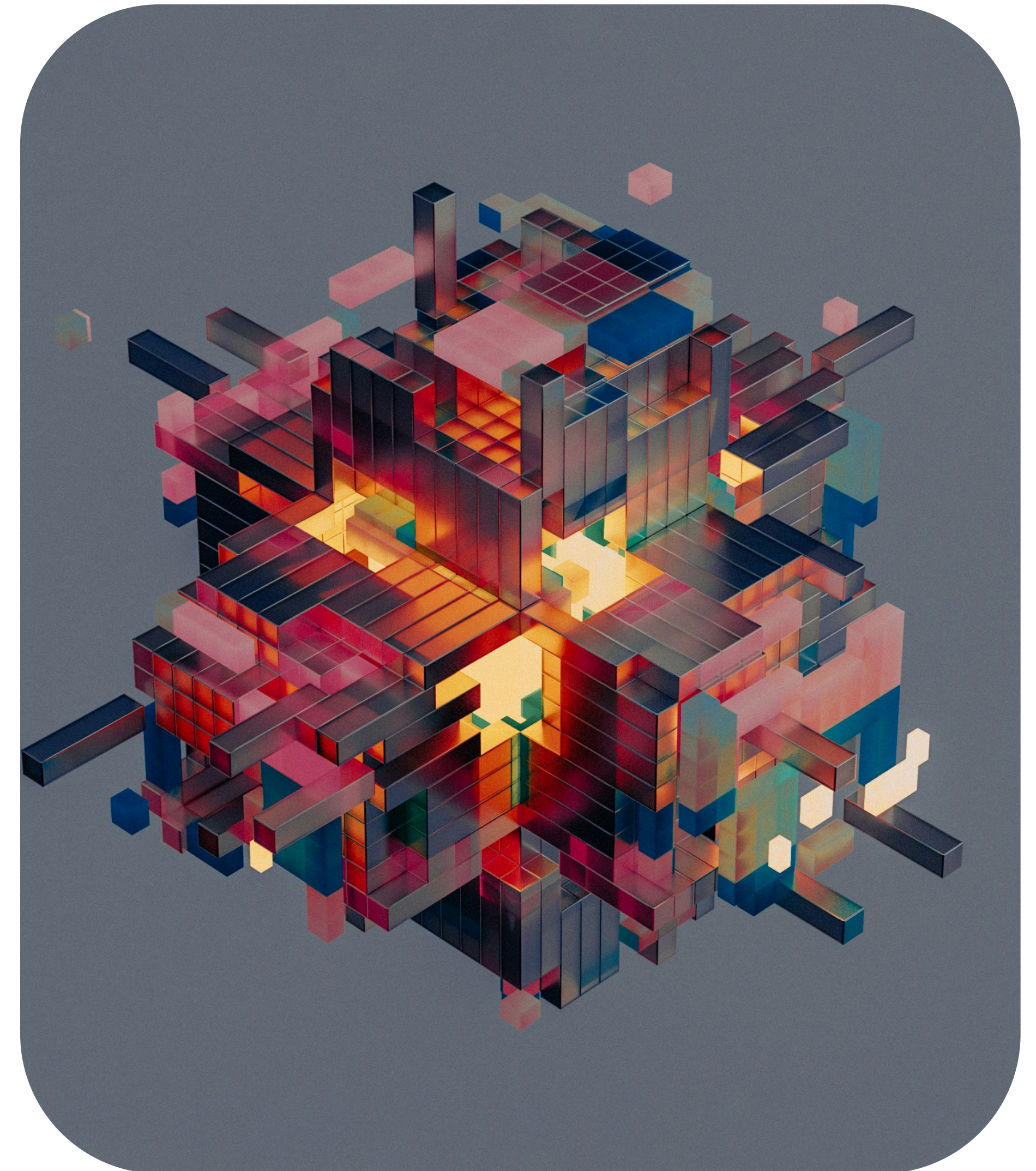
## **Cyber Security Operations Intelligence Platform**

Instead of treating security monitoring as isolated alert streams, DRUT enables organizations to consolidate operational security telemetry into an integrated command-level SOC dashboard.

This allows organizations to move from:

Alert Monitoring → Operational Cyber Intelligence

DRUT provides real-time operational visibility into cybersecurity events, control performance, and threat exposure across enterprise environments.





# Core Capabilities

## Unified Security Operations Dashboard

DRUT provides a centralized Cyber Security Operations Center (CSOC) dashboard that consolidates monitoring data across security systems.

### This enables SOC teams to view:

1. Real-time security alerts
2. Threat detection events
3. System health indicators
4. Incident response activities
5. Operational security metrics

Through a single operational interface.

DRUT acts as an operational intelligence layer across the existing SOC technology stack, enabling security teams to visualize alerts, threat indicators, and operational metrics from multiple security platforms within a unified command dashboard.

# Multi-Source Security Telemetry Integration

**DRUT introduces a new category:**

**Typical integrations include:**

- |                                                   |                                            |
|---------------------------------------------------|--------------------------------------------|
| 1. Security Information & Event Management (SIEM) | 6. Vulnerability management platforms      |
| 2. Endpoint Detection & Response (EDR)            | 7. Threat intelligence feeds               |
| 3. Network Detection & Response (NDR)             | 8. Ticketing and incident response systems |
| 4. Identity & Access Management (IAM)             |                                            |
| 5. Privileged Access Management (PAM)             |                                            |

By correlating telemetry across these systems, DRUT enables SOC teams to identify patterns and respond to threats faster.



# Designed for Existing SOC Tooling Environments

Modern SOC environments operate with multiple specialized security tools across endpoint protection, identity security, network monitoring, and threat analytics.

DRUT is designed to integrate seamlessly with these existing security ecosystems and consolidate telemetry into a unified operational dashboard.



## Typical SOC technology environments may include platforms such as:

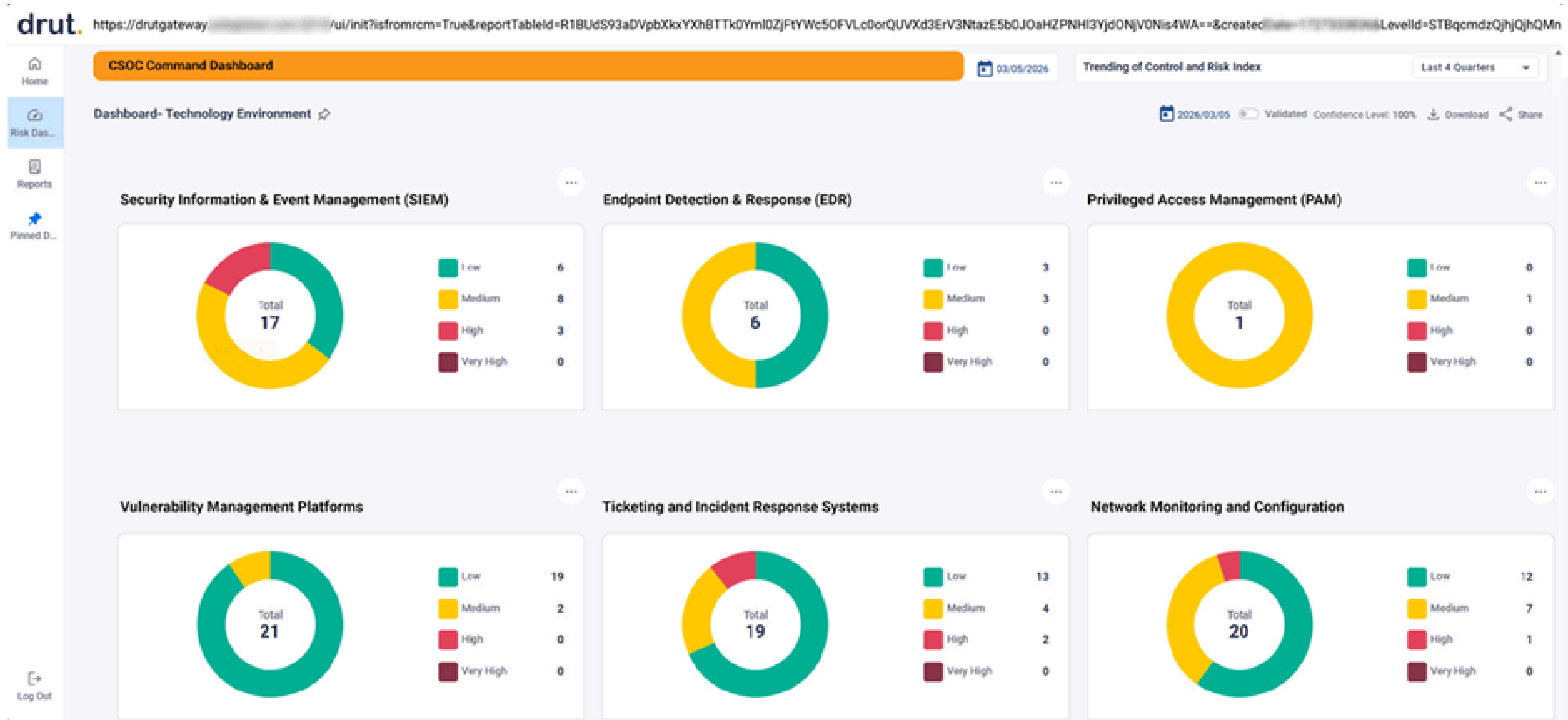
1. Endpoint protection and anti-malware systems (e.g., Trend Micro)
2. Advanced threat detection platforms (e.g., Trellix, Deep Discovery)
3. Breach and attack simulation platforms (e.g., Picos)
4. Data protection and DLP platforms (e.g., Seclore, Trend Micro DLP)
5. Identity and privileged access management solutions (e.g., Arcon)
6. Network monitoring and configuration platforms (e.g., AlgoSec, ManageEngine)
7. SIEM platforms (e.g., LogRhythm, Splunk)
8. SOAR platforms for incident orchestration (e.g., Palo Alto Cortex XSOAR)
9. vulnerability management platforms (e.g., Tenable Nessus)
10. Network access control platforms (e.g., Aruba, FortiAuthenticator)

By ingesting telemetry across these security layers, DRUT enables organizations to correlate alerts, visualize operational security posture, and monitor threat activity from a centralized SOC command dashboard.



# DRUT CSOC Operational Dashboard

DRUT CSOC dashboard showing alerts, threat indicators, and operational metrics.



# SOC Operational Visibility & Incident Traceability

Effective security operations require visibility into how threats evolve across systems.

**DRUT provides traceability across the incident lifecycle:**

Security Event → Alert Correlation → Incident Investigation → Response Monitoring

**This enables SOC teams to:**

1. Understand the origin of security incidents
2. Monitor response workflows
3. Track containment and remediation actions
4. Maintain incident investigation history



# How drut C-SOC helps take the leap ahead

## Continuous Threat Monitoring

Traditional security monitoring often involves reviewing alerts across multiple independent systems.

**DRUT enables continuous cyber threat monitoring within a unified operational interface, allowing SOC teams to:**

1. Detect anomalies earlier

---

2. Monitor system-wide threat exposure

---

3. Prioritize security alerts effectively

---

4. Improve incident response coordination

This significantly improves SOC operational efficiency.

# Cyber Threat Posture Insights

**DRUT provides analytical insights into an organization's cyber threat posture through:**

1. Threat activity monitoring

---

2. Security alert trend analysis

---

3. Incident response performance metrics

---

4. Attack surface exposure monitoring

---

5. SOC operational effectiveness dashboards

These insights allow security leadership to understand operational cyber risk and optimize SOC performance.



# Advanced Security Operations Analytics

**DRUT transforms operational monitoring into actionable cyber intelligence through advanced analytics including:**

1. Security alert heatmaps

---

2. Attack pattern analytics

---

3. Anomaly detection insights

---

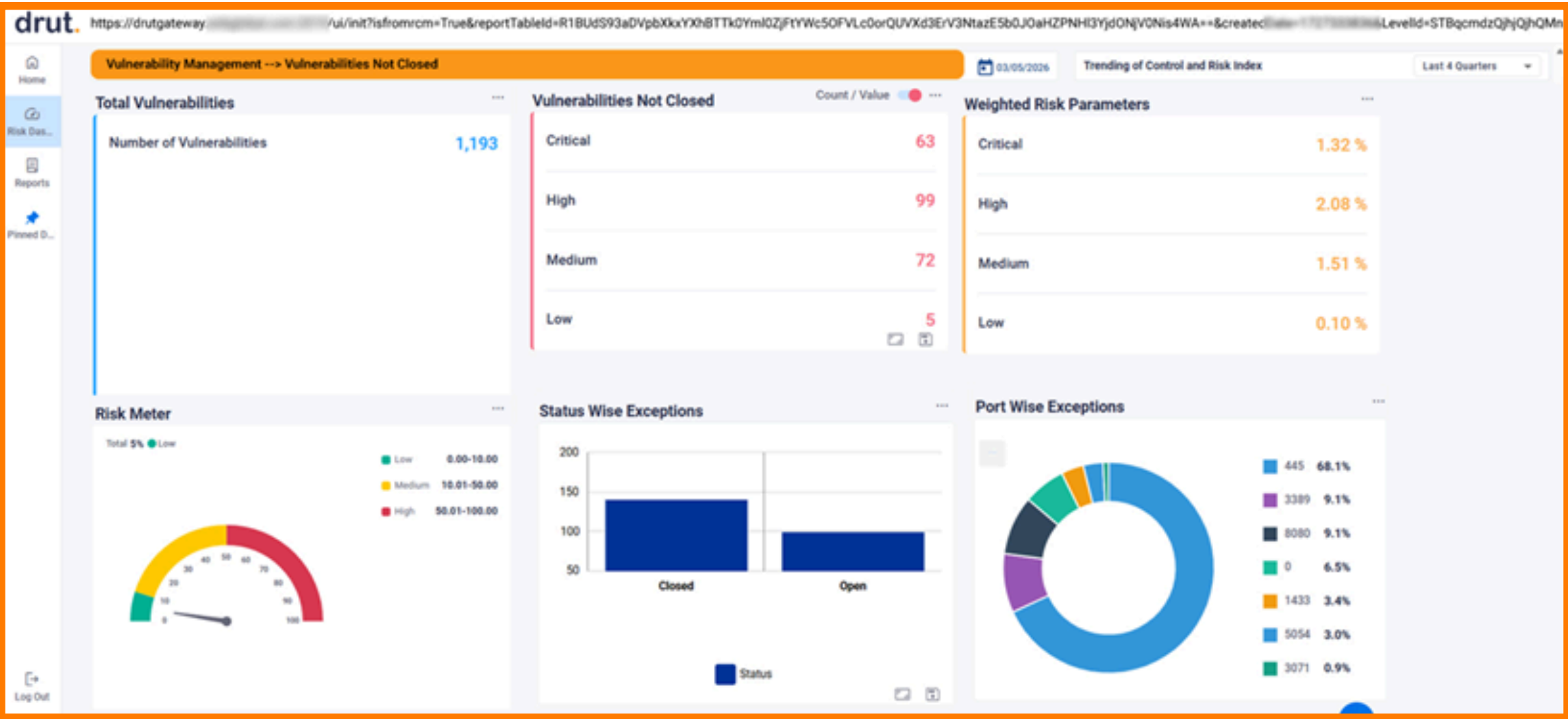
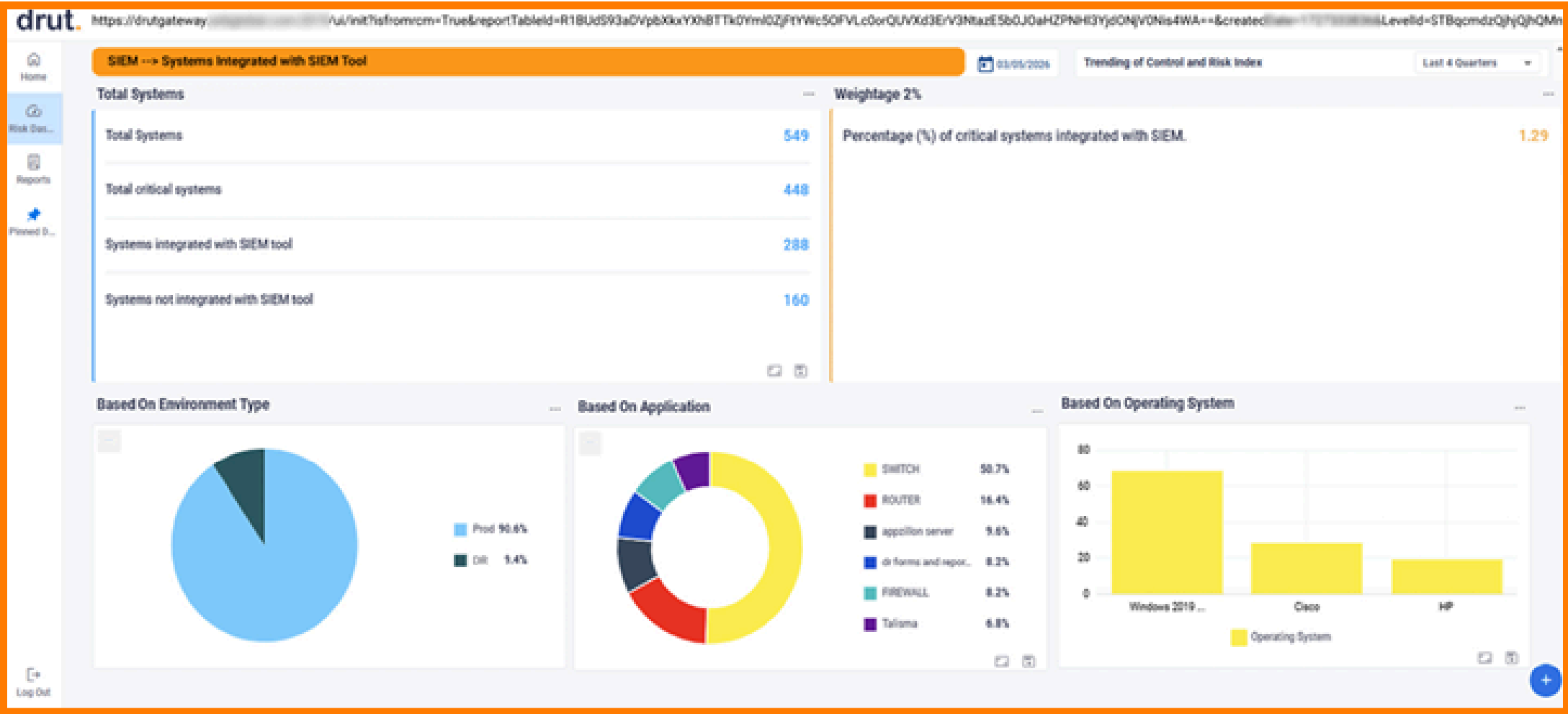
4. Incident response metrics

---

5. Threat exposure trends

This enables SOC teams to transition from reactive alert handling to proactive threat intelligence.

Illustrative operational views from the DRUT CSOC platform are shown below



# Partner GTM Opportunity

DRUT enables cybersecurity partners and MSSP providers to deliver modern SOC transformation programs for financial institutions and regulated organizations.

## Partner-led offerings may include:

1. SOC modernization initiatives

---

2. Security monitoring optimization

---

3. Threat intelligence integration

---

4. Incident response workflow automation

---

5. Cyber operations governance dashboards



# Strategic Value for Organizations

DRUT enables organizations to maximize the value of their existing security investments by transforming distributed telemetry into centralized cyber operations intelligence.

## Organizations implementing DRUT can:

1. Centralize SOC operational visibility

---
2. Improve threat detection and incident response

---
3. Consolidate security monitoring across platforms

---
4. Reduce alert fatigue through correlated threat intelligence

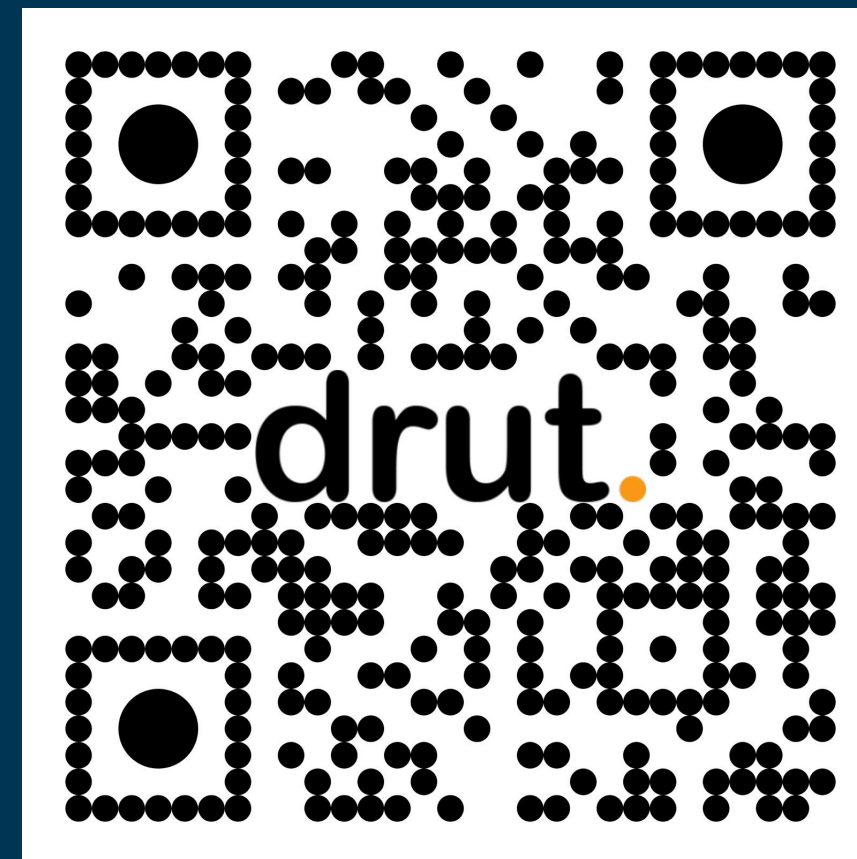
---
5. Enhance executive visibility into cyber threat posture

---
6. Strengthen cybersecurity operations governance

## Closing Statement

DRUT transforms fragmented security monitoring into a unified Cyber Security Operations Intelligence capability, enabling organizations to gain real-time visibility into threats, incidents, and operational cyber risk.

drut.



For any queries or feedback reach out to us on

**[PREETI.KOTHARI@DRUT.COM](mailto:PREETI.KOTHARI@DRUT.COM)**

**[KUNAL.MEHTA@DRUT.COM](mailto:KUNAL.MEHTA@DRUT.COM)**

**[SANJIV.VANKER@DRUT.COM](mailto:SANJIV.VANKER@DRUT.COM)**