Justin Lew

Business Case for Security Investment: Implementing an Endpoint Detection & Response (EDR) Solution

1. Executive Summary

Cybersecurity threats are evolving rapidly, requiring advanced solutions to protect critical systems. This document outlines the need for an Endpoint Detection & Response (EDR) solution within the Security Operations Center (SOC). EDR will improve threat detection, automate incident response, and reduce the impact of cyberattacks on business operations.

2. Business Impact Analysis

Current Security Challenges

- Limited visibility into threats targeting endpoints.
- Manual detection and response prolongs reaction time.
- Increased financial and reputational risks from security incidents.

Proposed EDR Solution Benefits

- **Improved Threat Detection:** Uses AI and behavioral analytics to detect and mitigate threats in real-time.
- **Automated Incident Response:** Reduces response time through automated containment and remediation.
- **Regulatory Compliance:** Supports adherence to industry standards such as NIST, MITRE ATT&CK, and CIS Controls.
- **Operational Efficiency:** Reduces SOC analysts' workload, allowing them to focus on higher-priority security tasks.

3. Cost-Benefit Analysis

Estimated Costs

Item	Annual Cost Estimate
EDR Licensing (500 endpoints)	$150,000
Implementation & Integration	$50,000
Training & Maintenance	$30,000
Total Cost	**$230,000**

Projected Benefits

Benefit	Annual Estimated Savings
Faster incident response (SOC efficiency gain)	$100,000
Avoiding data breaches (legal, reputational costs)	$300,000
Reduced downtime from security incidents	$80,000
Total Savings	**$480,000**

Net ROI: $250,000 (Savings - Cost)

4. Risk Assessment

Key Risks and Framework Alignment

Risk Categories:

- **Operational Risk:** Unsecured endpoints increase exposure to malware and ransomware.
- **Financial Risk:** Potential fines and costs due to regulatory non-compliance.
- **Reputational Risk:** Customer trust and business reputation could suffer in the event of a data breach.

Industry Standards Alignment:

- **NIST Cybersecurity Framework (CSF):** Supports Detect (DE) and Respond (RS) functions.
- **MITRE ATT&CK:** Maps attack techniques and countermeasures.
- **CIS Controls:** Enhances endpoint monitoring and malware defense (CIS Controls 7 & 8).

Mitigation Strategies

- **Prevention:** AI-driven detection prevents advanced persistent threats (APTs).
- **Detection:** Continuous monitoring for anomalies.
- **Response:** Automated playbooks accelerate threat containment.
- **Recovery:** Forensic tools aid in post-incident analysis.

5. Justification & Strategic Alignment

Key Stakeholders

- **CISO & Security Teams:** Gain improved visibility and threat response.
- **CFO & Finance Teams:** Ensures cost-effective security investment.
- **IT & Compliance Teams:** Helps meet security and regulatory requirements.

Justin Lew

Integration with Existing Security Systems

- **SIEM Integration:** Connects with Security Information & Event Management (SIEM) platforms.
- **Firewall & Network Security:** Strengthens endpoint security through enhanced protection.
- **Threat Intelligence Integration:** Incorporates real-time threat intelligence for proactive defense.

Implementation Plan

1. **Phase 1 - Pilot Deployment (Months 1-3):** Test EDR on key systems.
2. **Phase 2 - Full Deployment (Months 4-6):** Expand implementation across the organization.
3. **Phase 3 - Optimization & Monitoring (Months 7-12):** Fine-tune policies and integrate with SIEM.

Performance Metrics

- **Incident Detection Time (MTTD):** Targeting a 50% reduction.
- **Incident Response Time (MTTR):** Aiming to cut response time by 40%.
- **Number of Security Incidents:** Expected reduction in security events post-implementation.

Vendor Comparison & Recommendation

Vendor	Key Features	Cost	Support	Market Reputation
CrowdStrike	AI-driven detection, automation	High	Excellent	Industry Leader
SentinelOne	Behavioral analytics, rollback	Medium	Good	Strong
Microsoft Defender	Deep integration with Windows	Low	Moderate	Growing

Recommended Solution: CrowdStrike provides the most robust feature set despite a higher cost.

Ongoing Monitoring & Optimization

- **Quarterly Reviews:** Assess EDR performance and fine-tune configurations.
- **SOC Analyst Input:** Gather feedback on system efficiency and usability.
- **Regular Updates:** Maintain up-to-date threat intelligence and security patches.

6. Conclusion

Deploying an EDR solution is a necessary investment to enhance the organization's security defenses. It improves threat detection, automates response actions, and ensures compliance with regulatory standards. The cost-benefit analysis indicates strong financial justification, with significant risk reduction and operational efficiencies.

By integrating EDR with existing SOC tools, the organization can proactively mitigate cyber threats. Moving forward with this investment will strengthen overall cybersecurity resilience.