3-Year Security Brutalism Implementation Plan

This plan outlines a 3-year strategy for implementing Security Brutalism principles within an organization. It provides a roadmap for gradually transitioning from a potentially complex and costly security approach to a more streamlined, resilient, and efficient one.

Vision: To establish a security posture that is robust, resilient, and cost-effective, aligned with the principles of Security Brutalism, and that effectively protects the organization's assets while enabling business objectives.

Disclaimer

The information and suggestions in this booklet are provided as is, and without a warranty of any kind. You assume all risks that might come from following or using anything on this website. I am not responsible if things don't work, things get broken, or security gets bypassed or compromised. You are the only responsible party here. If you don't agree, do not read this booklet, and do not apply anything depicted here.

The opinions expressed in this booklet are mine, and are not official statements of my current or past employer, current or past team, current or past customers, or anyone else but mine.

Guiding Principles

- **Simplicity:** Prioritize straightforward, easy-to-understand security measures.
- **Resilience:** Build systems and processes that can withstand attacks and recover quickly.
- **Transparency:** Ensure security mechanisms are visible, auditable, and well-documented.
- **Functionality:** Focus on security measures that directly address identified threats and risks.
- **Efficiency:** Optimize security operations to minimize overhead and maximize resource utilization.
- **Defense in Depth (Simplicity Focused):** Implement layered security, ensuring each layer adheres to the above principles.

Year 1: Assessment and Foundation

- **Phase 1: Security Assessment and Gap Analysis (3 Months)**
    - **Objective:** Evaluate the current security posture, identify areas of excessive complexity, and determine where Security Brutalism principles can be applied.
    - **Activities:**
        - Conduct a comprehensive security audit.
        - Analyze existing security tools, technologies, and processes.
        - Identify critical assets and data flows.
        - Perform risk assessments to prioritize areas of focus.
        - Document the current security architecture.
        - Identify quick wins – areas where simple changes can have a big impact.
    - **Deliverables:**
        - Detailed security assessment report.
        - Gap analysis document outlining areas for improvement.
        - Prioritized list of Security Brutalism implementation projects.
- **Phase 2: Establish Brutalism Principles and Governance (3 Months)**
    - **Objective:** Define the organization's specific interpretation of Security Brutalism and establish governance structures to guide its implementation.
    - **Activities:**
        - Develop a Security Brutalism policy document.
        - Define clear standards for security solutions and practices.
        - Establish a Security Brutalism Working Group with representatives from relevant departments.
        - Create a process for evaluating and approving new security projects.
        - Develop communication and training materials to educate employees about Security Brutalism.
    - **Deliverables:**
        - Security Brutalism policy document.
        - Security standards and guidelines.
        - Security Brutalism Working Group charter.
        - Communication and training plan.
- **Phase 3: Pilot Project Implementation (6 Months)**
    - **Objective:** Implement Security Brutalism principles in a limited scope to test their effectiveness and gather lessons learned.
    - **Activities:**
        - Select a pilot project (e.g., a specific system, application, or department).
        - Design and implement security measures based on Brutalism principles.
        - Monitor the pilot project's performance and security effectiveness.
        - Gather feedback from stakeholders.
        - Document the implementation process and lessons learned.
    - **Deliverables:**
        - Successful implementation of the pilot project.
        - Pilot project evaluation report.
        - Refined implementation plan based on lessons learned.

Year 2: Broadening Implementation

- **Phase 4: Expand Brutalism Implementation (12 Months)**
    - **Objective:** Extend the implementation of Security Brutalism principles to a broader range of systems and processes.
    - **Activities:**
        - Prioritize systems and processes for Brutalism implementation based on risk and business impact.
        - Implement Security Brutalism principles in phases, focusing on areas with the highest potential return on investment.
        - Continuously monitor and evaluate the effectiveness of implemented measures.
        - Refine security standards and guidelines based on ongoing experience.
        - Provide ongoing training and awareness programs for employees.
    - **Deliverables:**
        - Increased adoption of Security Brutalism across the organization.
        - Improved security metrics (e.g., reduced incident response time, fewer vulnerabilities).
        - Updated security standards and guidelines.

Year 3: Optimization and Refinement

- **Phase 5: Optimize and Mature (12 Months)**
    - **Objective:** Optimize the implemented Security Brutalism measures, mature the program, and ensure its long-term sustainability.
    - **Activities:**
        - Conduct regular security assessments to identify areas for further optimization.
        - Automate security processes where possible to improve efficiency.
        - Develop and implement a continuous improvement program.
        - Establish key performance indicators (KPIs) to measure the effectiveness of the Security Brutalism program.
        - Regularly review and update the Security Brutalism policy and standards.
        - Foster a security-conscious culture throughout the organization.
    - **Deliverables:**
        - Optimized security operations and processes.
        - Established KPIs for measuring security effectiveness.
        - Mature and sustainable Security Brutalism program.
        - Organization-wide security awareness and a strong security culture.

Security Brutalism Runbook

This runbook provides detailed, step-by-step instructions for implementing specific Security Brutalism principles within the organization. It is a living document that will be updated and expanded as the implementation progresses.

I. Core Principle: Simplicity

- **Objective:** To reduce complexity in security systems and processes.
- **Process:**
    - **Identify Complex Systems:** List all security systems and processes, and rate them on a scale of 1 to 5 (1 = very simple, 5 = very complex).
    - **Analyze Complexity Drivers:** For systems rated 4 or 5, identify the root causes of complexity (e.g., excessive features, redundant tools, lack of standardization).
    - **Simplify or Eliminate:**
        - **Eliminate:** Remove unnecessary systems or processes.
        - **Consolidate:** Combine redundant tools or functions.
        - **Simplify:** Streamline configurations, reduce the number of options, and automate tasks.
        - **Standardize:** Adopt common standards and best practices.
    - **Document:** Clearly document the simplified systems and processes.
    - **Train:** Provide training to ensure staff can effectively use the simplified systems.
    - **Review:** Regularly review systems for potential complexity creep.
- **Example:**
    - **System:** Vulnerability Management
    - **Complexity Driver:** Using three different scanning tools with overlapping functionality.
    - **Solution:** Consolidate to a single, comprehensive vulnerability management platform, and automate scanning and reporting.

II. Core Principle: Resilience

- **Objective:** To ensure security systems and processes can withstand attacks and recover quickly.
- **Process:**
    - **Identify Critical Systems:** Determine the systems and data that are most critical to business operations.
    - **Assess Resilience:** Evaluate the resilience of these systems against potential threats (e.g., hardware failure, network outages, cyberattacks).
    - **Implement Resilience Measures:**
        - **Redundancy:** Implement redundant systems and components to ensure failover capability.
        - **Fault Tolerance:** Design systems to tolerate faults and continue operating.
        - **Backup and Recovery:** Establish robust backup and recovery procedures.
        - **Disaster Recovery:** Develop a comprehensive disaster recovery plan.
        - **Incident Response:** Create and regularly test an incident response plan.

    - **Test and Exercise:** Regularly test resilience measures through simulations and exercises.
    - **Monitor:** Continuously monitor the health and performance of critical systems.
- **Example:**
    - **System:** Authentication System
    - **Resilience Measures:** Implement a redundant authentication server setup with automatic failover, and use multi-factor authentication (MFA) to reduce the impact of compromised credentials.

III. Core Principle: Transparency

- **Objective:** To ensure security mechanisms are visible, auditable, and well-documented.
- **Process:**
    - **Identify Opaque Systems:** Identify security systems or processes that are poorly documented or difficult to understand.
    - **Improve Documentation:**
        - Create clear and concise documentation for all security systems and processes.
        - Use diagrams and visual aids to illustrate complex concepts.
        - Establish a central repository for security documentation.
    - **Enhance Auditability:**
        - Implement logging and monitoring for all security-related activities.
        - Ensure logs are stored securely and are easily accessible for auditing.
        - Conduct regular security audits to verify compliance and identify potential issues.
    - **Promote Openness:**
        - Where appropriate, use open-source security tools and technologies.
        - Share security information and best practices with relevant stakeholders.
    - **Communicate:** Communicate security policies and procedures clearly to all employees.
- **Example:**
    - **System:** Firewall Rules
    - **Transparency Improvements:** Document each firewall rule with a clear description of its purpose, the systems it applies to, and the justification for its existence. Use a centralized firewall management system with audit trails.

IV. Core Principle: Functionality

- **Objective:** To ensure that security measures directly address identified threats and risks.
- **Process:**
    - **Identify Threats and Risks:** Conduct regular threat and risk assessments to identify the specific threats facing the organization.
    - **Prioritize Security Measures:** Focus on implementing security measures that directly mitigate the identified threats and risks, and prioritize those that address the highest risks.
    - **Avoid Unnecessary Measures:** Avoid implementing security measures that do not provide a clear benefit or address a specific threat.

  - **Regularly Review:** Regularly review existing security measures to ensure they remain relevant and effective.
  - **Test Effectiveness:** Conduct penetration testing and vulnerability assessments to verify that security measures are functioning as intended.
- **Example:**
  - **Threat:** Phishing Attacks
  - **Functional Security Measure:** Implement a multi-layered approach that includes:
    - Employee training and awareness programs focused on recognizing phishing emails.
    - Email filtering to block known phishing attempts.
    - Technical controls to prevent users from clicking on malicious links or downloading malicious attachments.

V. Core Principle: Efficiency

- **Objective:** To optimize security operations to minimize overhead and maximize resource utilization.
- **Process:**
  - **Identify Inefficient Processes:** Analyze current security processes to identify areas where resources are being used inefficiently.
  - **Automate Tasks:** Automate repetitive or manual tasks, such as security monitoring, vulnerability scanning, and patch management.
  - **Streamline Workflows:** Simplify and streamline security workflows to reduce the number of steps and handoffs.
  - **Centralize Management:** Consolidate security management tools and platforms to reduce complexity and improve visibility.
  - **Optimize Staffing:** Ensure that security staff are allocated effectively and have the skills and resources they need to perform their jobs.
  - **Use Managed Services:** Consider using managed security services for tasks that can be outsourced, such as security monitoring or incident response.
- **Example:**
  - **Inefficient Process:** Manually reviewing firewall logs.
  - **Efficiency Improvement:** Implement a Security Information and Event Management (SIEM) system to automate log analysis and alert on suspicious activity.

VI. Core Principle: Defense in Depth (Simplicity Focused)

- **Objective:** To implement layered security, ensuring each layer is simple, robust, and effective.
- **Process:**
  - **Identify Critical Assets:** Determine the organization's most valuable assets that require protection.
  - **Map Security Layers:** Define the different layers of security that protect these assets (e.g., perimeter security, network security, host security, application security, data security).

    - **Simplify Each Layer:** Ensure that each security layer is implemented as simply and effectively as possible, adhering to the principles of Simplicity, Resilience, Transparency, and Functionality.
    - **Ensure Layer Independence:** To the extent possible, make each layer independent of the others, so that a failure in one layer does not compromise the security of other layers.
    - **Regularly Test:** Test the effectiveness of each security layer and the overall defense-in-depth strategy through regular penetration testing and red teaming exercises.
- **Example:**
    - **Asset:** Customer Database
    - **Security Layers:**
        - **Perimeter Security:** A simple, well-configured firewall with only essential ports open.
        - **Network Security:** Network segmentation to isolate the database server, and intrusion detection/prevention.
        - **Host Security:** A hardened operating system with only necessary services running, and host-based intrusion detection.
        - **Application Security:** Secure coding practices, input validation, and output sanitization in the database application.
        - **Data Security:** Encryption of the database at rest and in transit, and strict access controls.

This 3-year plan and runbook provide a comprehensive framework for implementing Security Brutalism. Remember that this is an iterative process, and the plan and runbook should be regularly reviewed and updated as needed.