

SecGuru National Security Defense Plan

Aldo
Marion
Afrika
Max
Alex
Derelys

Cybersecurity Practical Applications

July 12, 2025

Contact/ Team Lead: Aldo Leveroni



Executive Summary

Purpose

Address urgent cyber threats due to rising risks to national infrastructure

Deploy full defense strategy:

- 1.) Cyber simulations
- 2.) Incident response plans
- 3.) Recommendations / Roadmap

Actions

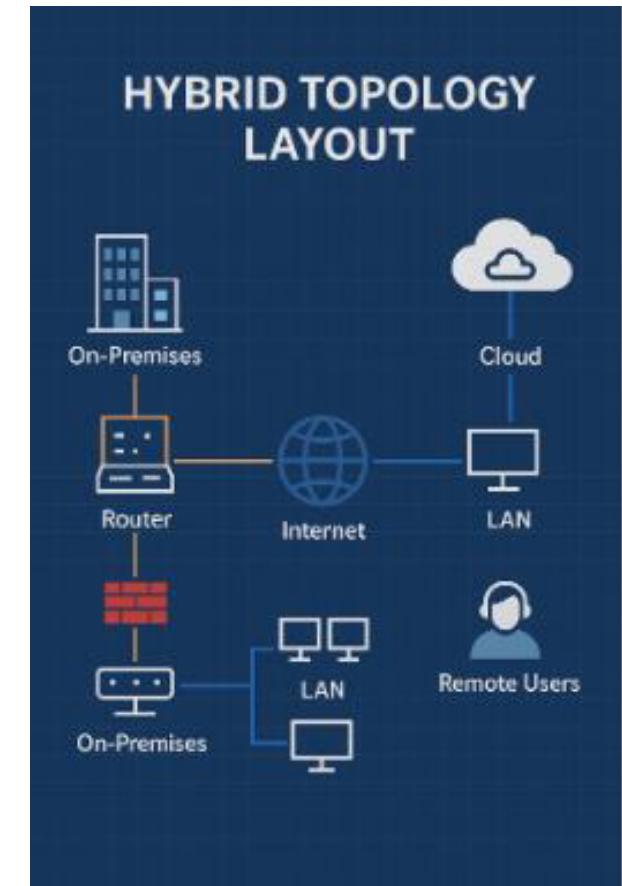
The SECGURUS team executed a comprehensive, cross-functional assessment to fortify CyberDome's infrastructure.

This included:

- Designing a hybrid network topology and layered defense strategy
- Implementing role-based access control and MFA
- Developing SIEM monitoring and incident response playbooks
- Establishing business continuity and disaster recovery plans
- Deploying physical access controls and insider threat detection
- Running Red vs. Blue Team simulations using MITRE techniques
- Integrating real-time threat intelligence and behavioral analytics

Topology & Layered Defense Strategy

- SecGuru is a hybrid network architecture combining on-premises systems, cloud infrastructure, and secure remote access. Routers, firewalls, and LAN components support connectivity and enforce perimeter security. Cloud platforms provide scalability, while VPNs ensure secure remote user access.
- The layered defense model segments the network into:
 - **DMZ** for public-facing services
 - **Internal Zone** for business operations
 - **Admin Zone** with restricted access
- Next-gen firewalls, SIEM, and IDS/IPS tools are strategically placed to monitor, detect, and respond to threats. Physical HQ security includes surveillance, entry controls, and biometric authentication. Together, these layers provide strong cyber-physical protection and limit breach impact.





SecGuru's Cybersecurity Plan

Asset inventory

- List of critical systems
- Email server (Microsoft Exchange)
- Web servers, databases
- IoT devices
- VPN gateway (GlobalProtect, Fortinet)
- SIEM system (Splunk/Security Onion/elk slack)
- Database server (SQL)
- Secure network zones (DMZ)
- Entry/exit points for physical layout (HQ blueprint style)
- Labeled departments (Ops Center, Server Room, Restricted Zones, LAN, WAN)
- Switches and routers
- Mobile devices
- Generator, UPS



Network Defense strategy

SecGurus' defense model applies a layered, proactive approach to protect critical infrastructure. Key components include:

- **Firewalls** – Deployed at all network boundaries (DMZ, internal, admin), enforcing strict rules that block unauthorized traffic and log denied attempts.
- **IDS/IPS** – Intrusion systems detect and block suspicious behavior and threats in real time, helping stop attacks before they spread.
- **VPN Access** – Secure, encrypted tunnels for remote users with 2FA, centralized monitoring, and no split tunneling.
- **Segmentation** – The network is divided into zones (DMZ, Internal, Admin) with firewalls and RBAC to contain breaches and minimize lateral movement.

Together, these measures provide visibility, control, and rapid response to evolving threats.



Monitoring & Logging (SIEM)

Logs that are collected:

- **System logs (OS information)**
- **Network logs (Routers, Switches, and other network devices)**
- **Application logs (Apache/Nginx)**
- **Security logs (Firewall, IDS, IPS, EDR/Anti-virus alerts)**
- **Firewall logs**
- **Email gateway logs**

Anomalies that are monitored:

- **Multiple failed login attempts:** Possible brute-force attack
- **Unusual outbound connections:** Data-exfiltration or command and control (c2) activity
- **Unauthorized file changes:** Potential malware or Insider threat
- **Phishing or malware attachment detected:** Email gateway alert
- **Access to sensitive files outside business hours:** Insider threat or compromised credentials

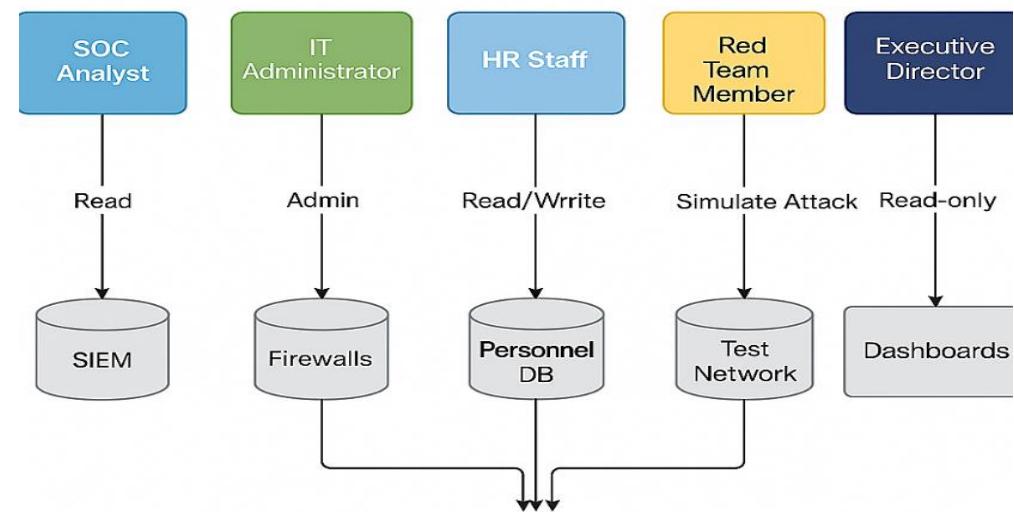
Authentication & Access Control

SecGuru enforces Zero Trust with:

- MFA for all access (tokens, biometrics, CAC)
- Strict password policies and RBAC by role
- Offline recovery protocols for account backup

Threat intelligence is integrated into SIEM/EDR using:

- Feeds from OTX, MISP, VirusTotal, and CISA
- Real-time IoC ingestion, threat hunting, and automated response
- Intel-sharing with partners under TLP for national defense coordination



Incident Response Playbook

- Structure of the Incident Response Playbook

- **Detection**

- **Objective:** Clearly states the goal of identifying and confirming security incidents.
 - **Actions:** Lists specific, actionable steps that can be taken to monitor and analyze potential threats. This includes leveraging technology (like IDS and threat intelligence) and encouraging employee reporting.

- **Containment**

- **Objective:** Focuses on limiting the impact of the incident.
 - **Actions:** Provides practical measures to isolate affected systems and communicate with stakeholders, ensuring that business operations are minimally disrupted.

- **Eradication**

- **Objective:** Aims to remove the root cause of the incident.
 - **Actions:** Details steps for identifying the source of the incident, removing threats, and applying necessary updates to prevent future occurrences.

- **Recovery**

- **Objective:** Restores systems to normal operations.
 - **Actions:** Emphasizes the importance of restoring data safely, monitoring for residual threats, and validating system functionality before full operational resumption.

- **Lessons Learned**

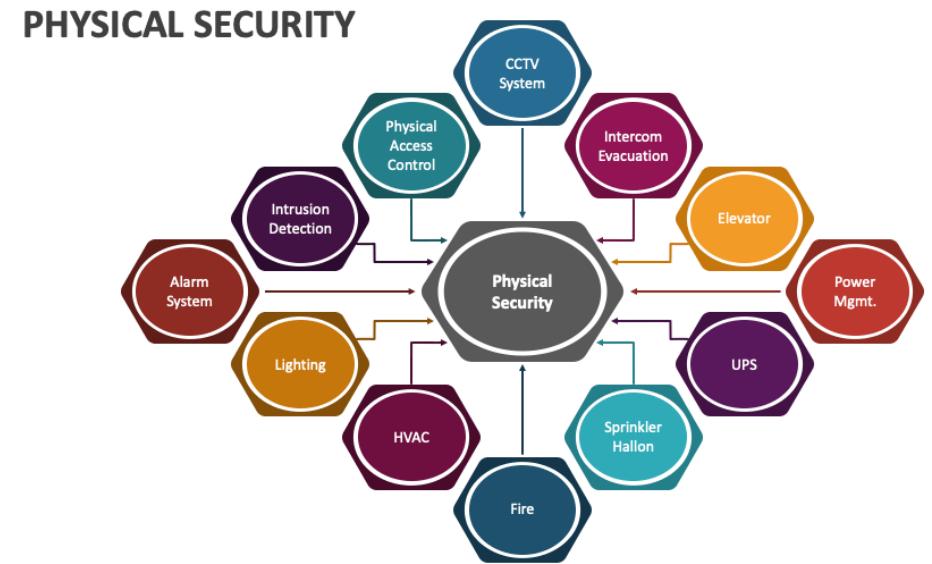
- **Objective:** Focuses on continuous improvement.
 - **Actions:** Encourages post-incident reviews and documentation to enhance future responses and strengthen the organization's security posture.

Physical Security Blueprint

SecGuru's physical security strategy protects people, assets, and infrastructure from threats like intrusion, theft, natural disasters, and sabotage. Security controls are integrated with cybersecurity to ensure operational continuity.

- Core measures to access to SecGuru's HQ include:
 - **Access Control** – Biometric scans, keycards, and restricted zones
 - **Perimeter Defense** – Fencing, barriers, and surveillance coverage
 - **Intrusion Detection** – Alarms and systems that trigger alerts in real time
 - **Emergency Preparedness** – Fire, disaster, and security breach response planning
 - **CPS Protection** – Securing systems that link digital controls to physical processes
 - **Insider Threat Monitoring** – Behavioral analysis, role-based access, and activity logging

This convergence of cyber and physical controls ensures defense-in-depth across all facilities.



Source: es gulf

Insider Threat Mitigation Plan

SecGuru's Insider Threat Analyst plays a crucial role in safeguarding organization, including those involved in National Cyber Defense and Facility Security.

- Threat Detection and Analysis: analyze data, identify threats, and suspicious behavior.
- Investigation and Response: determine root cause and implement appropriate response actions.
- Program Development and Enhancement: develop and recommend improvements based on metrics and reporting.
- Collaboration: here, teams played crucial role among themself to ensure the insider threat program aligns with organizational goals and compliance requirements.
- Reporting: prepare and present analysis and findings to stakeholders, including government leads and managers.

SecGuru's Insider Threat in these fields combines technical expertise with investigative skills to protect sensitive information, systems, and facilities from threats originating from within the organization. SecGuru's used the following tools: Coralogix, Wazuh, OSSEC, Anodot for real time detection which analyze data in real-time and flag anomalies, which could indicate errors, fraud, or other critical situations. SecGuru's performed regular training to all users.



Threat Intelligence Integration

Sources of Threat Intelligence

- SecGuru leverages open-source threat intelligence sources, tailored for critical infrastructure protection:

Open-Source Threat Intelligence (OSINT) & Community Platforms:

- AlienVault Open Threat Exchange (OTX): A community-powered threat intelligence platform where security professionals share threat data, enabling collaborative research and rapid dissemination of IoCs (IPs, domains, file hashes, URLs). We integrate OTX pulses directly into our SIEM and other security tools.
- MISP (Malware Information Sharing Platform): Used for sharing, storing, and correlating threat information, including IoCs, malware samples, and attack patterns. MISP facilitates structured information exchange within our organization and with trusted partners.
- VirusTotal: For analyzing suspicious files and URLs, providing insights into known malware signatures and detection rates across various antivirus engines.
- SANS Internet Storm Center (ISC): Provides daily insights into internet threats and vulnerabilities.
- Threat Intelligence Blogs & Research Papers: Monitoring reputable cybersecurity blogs (e.g., from major security vendors, independent researchers) and academic research for emerging threats and vulnerabilities.

Examples of Threat Alerts

ICS/SCADA Vulnerability (e.g., Log4Shell)

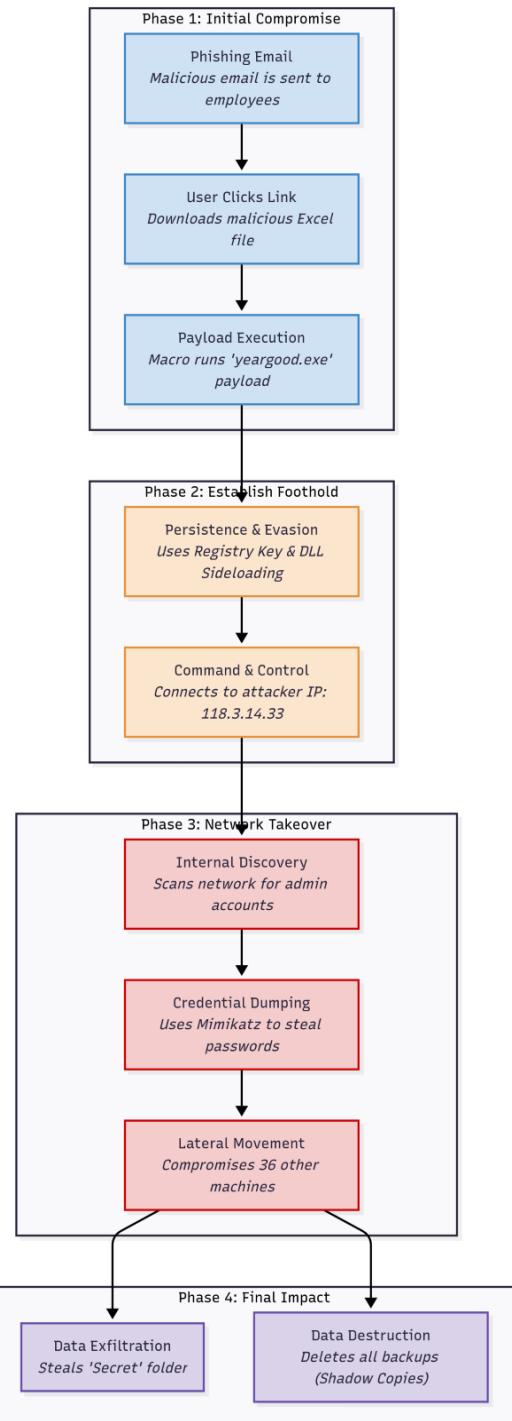
Source: CISA + Commercial Feeds (Recorded Future)

Action Taken:

- Asset Identification → Segmentation → Patching
- IoC Hunting via SIEM/EDR
- Firewall/IPS Updates
- Internal & Partner Dissemination (AIS, TLP protocols)

Red Team / Blue Team Exercise Report

- Red Team / Blue Team Exercise
- A simulated multi-stage attack tested SecGuru's defenses against realistic threats like credential theft, data exfiltration, and persistence. The scenario used phishing, macro payloads, DLL sideloading, and command-and-control (C2) communications to emulate an advanced intrusion.
- **Red Team Tactics (MITRE-aligned):**
 - Phishing via malicious Excel attachments
 - Macro execution and persistence via registry keys
 - DLL sideloading for evasion
 - Credential dumping with Mimikatz
 - Lateral movement through RDP
 - Data destruction and outbound C2 traffic
- **Blue Team Response:**
 - Detected key indicators via SIEM, endpoint monitoring, and network analysis
 - Flagged macro activity, DLL hashes, and unauthorized memory access
 - Isolated affected hosts and triggered containment playbooks
- **Key Gaps Identified:**
 - Phishing bypassed email filters
 - No MFA on privileged accounts
 - Excessive user privileges enabled compromise
 - C2 traffic remained active for hours
- **Lessons Learned:**
 - Enforce MFA and least privilege
 - Improve email filtering and segmentation
 - Enhance behavioral detection and outbound traffic controls
 - Conduct regular simulation training



Business Continuity Plan

To ensure SecGuru's mission-critical operations remain functional during cyberattacks, outages, or disasters, we developed a robust Business Continuity Plan. This plan minimizes downtime, protects data integrity, and ensures rapid recovery by combining technical safeguards, structured response protocols, and continuous testing.

- **Critical Systems Identified:** BIA outlines RTO/RPO for assets like SIEM, VPN, and SQL databases.
- **Redundant Infrastructure:** Encrypted backups (cloud + on-site), generator power, and internet failover.
- **Continuity of Operations (COOP):** VPN/VDI access and a fully equipped alternate HQ ensure resilience.
- **Secure Communication Protocols:** Contact tree, encrypted messaging, and pre-approved response templates.
- **Ongoing Testing & Updates:** Quarterly drills and post-incident reviews improve readiness.
- **Vendor Compliance:** Partners must meet ISO 27001 and SOC 2 standards with proven BCPs.

Recommendations

- **Enforce Multi-Factor Authentication (MFA):** Apply MFA across all privileged and sensitive user accounts to reduce the impact of credential theft.
- **Implement Least Privilege:** Remove unnecessary administrative rights and ensure role-based access control is enforced.
- **Strengthen Email Filtering & User Awareness:** Enhance filtering rules and run regular phishing simulation training to reduce human risk.
- **Improve Network Segmentation:** Isolate sensitive systems to reduce lateral movement opportunities.
- **Enhance Endpoint & Memory Monitoring:** Deploy advanced detection tools (e.g., Sysmon, EDR) to catch in-memory attacks.
- **Expand Threat Intelligence Integration:** Leverage platforms like CISA alerts and AlienVault OTX to stay ahead of emerging threats.
- **Audit and Test Incident Response Plans:** Simulate attacks routinely to refine detection and response playbooks.
- **Integrate Physical and Cybersecurity:** Strengthen building access control, surveillance, and emergency readiness in parallel with cyber defenses.

Conclusion and Final Thoughts

This SecGuru presentation has successfully demonstrated a comprehensive, layered security architecture that integrates both technical and physical safeguards to defend critical infrastructure and data assets. Through the collaborative efforts of the SecGuru team, we have identified strengths in detection, containment, and response across network, endpoint, and physical domains.

The Red Team/Blue Team exercise revealed valuable insights. While the Blue Team showed strong detection capabilities against lateral movement, credential theft, and data destruction, the Red Team's initial phishing campaign exposed vulnerabilities in email filtering, privilege access, and outbound traffic monitoring. These lessons reinforce the need for continuous hardening of your security posture.

This SecGuru presentation reflects a real-world approach to securing hybrid infrastructures. Continued testing, simulation, and policy enforcement will ensure that SecGuru remains resilient in the face of evolving threats.

Appendices

- Roles
- Aldo – Executive Team Lead
Marion – Security Architect
Afrika – SIEM Lead
Max – Physical Security Analyst
Alex – Red/Blue Simulation Lead
Derelys – Threat Intelligence Lead
- Citations
- <https://attack.mitre.org/>
- Montgomery College. TechMAP *Cybersecurity*. Instructed by Prof. Reza Mirabrihami, Cyber Department, Spring 2025. Montgomery College, Germantown Campus. Lecture.

THANK YOU!

ANY QUESTIONS?

