ME/PSO

HANDBOOK

Technical Handbook for Administrators

An artificial intelligence-based system for detecting and preventing cyber attacks

Companion material for the training course:
"Technical Training for Administrators"

Document No. MEPSO-PRI-ADM-005 · Classification: Internal Use
Information and Cyber Security Department · MEPSO AD Skopje

Contents

1. Introduction

System administrators are on the front line of the organization's technical defense. Your decisions and practices directly determine the security posture of the entire infrastructure.

This handbook is intended for technical personnel responsible for administering and protecting systems. We will cover advanced concepts of network and system security, with a special emphasis on modern approaches, including artificial intelligence in threat detection.

As an operator of critical infrastructure, MEPSO has heightened security requirements. Protecting the systems is not merely a technical task — it is a responsibility with consequences for the security of the national power grid.

> **The importance of the role.** Administrators have privileged access and great responsibility. A single security lapse at the administrator level can expose the entire infrastructure. That is why the highest security standards are mandatory.

2. The system administrator's role in security

The administrator is not merely an operator of systems — they are a guardian of security.

2.1 Key responsibilities

- ✓ Configuring and maintaining the security controls
- ✓ Monitoring the systems for suspicious activity
- ✓ Managing access and privileges
- ✓ Applying security updates
- ✓ Responding to security incidents
- ✓ Maintaining backups and recovery plans

2.2 The principle of least privilege

Every user and process should have only the rights they strictly need. This limits the potential risk if an account is compromised.

> **Critical.** Administrator privileges should be used only when necessary. Everyday work should be performed under an ordinary user profile, with administrative rights activated only for specific tasks.

3. Fundamentals of network security

The network is the connective tissue of the infrastructure and a frequent target of attacks.

3.1 Network segmentation

Dividing the network into segments limits an attacker's ability to move freely. Critical systems should be isolated from less secure zones.

3.2 Firewalls

Firewalls control network communication according to defined rules. A proper configuration allows only the necessary traffic.

Concept	Purpose
Segmentation	Isolating critical zones
Firewall	Controlling network traffic
VPN	Secure remote access
Monitoring	Tracking network activity

4. Intrusion detection systems (IDS/IPS)

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) monitor traffic for signs of an attack.

4.1 The difference between IDS and IPS

System	Function
IDS (Detection)	Detects and alerts on suspicious activity
IPS (Prevention)	Detects and actively blocks threats

4.2 Detection methods

- **Signature-based** — recognizing known attack patterns;
- **Anomaly-based** — detecting deviations from normal behavior;
- **Hybrid** — a combination of both approaches.

> **The challenge.** Traditional signature-based systems cannot detect new, unknown attacks. This is where the advantage of artificial intelligence comes in.

5. Artificial intelligence in cyber defense

Artificial intelligence (AI) is revolutionizing the way we detect and respond to threats, making it possible to detect previously unknown attacks.

5.1 Advantages of the AI approach

✓ Detecting new, unknown threats through behavioral analysis

- ✓ Processing enormous volumes of data in real time
- ✓ Reducing false alarms through learning
- ✓ Automatic adaptation to new types of attacks
- ✓ Fast response without human intervention for known patterns

5.2 How it works

AI-based systems learn the normal behavior of the network and the systems. When they notice a deviation — unusual traffic, atypical access patterns, suspicious activities — they alert or react automatically.

> **The advantage.** Unlike traditional systems, which require prior knowledge of every threat, AI can recognize suspicious behavior it has never seen before — which is key against new attacks.

5.3 The administrator's role

AI systems are powerful tools, but they require expert management. The administrator configures them, monitors the results, investigates the alerts and takes appropriate measures. The technology helps, but human expertise remains indispensable.

6. Log analysis and monitoring

Logs are records of the activities in the systems — an invaluable source for detecting and investigating incidents.

6.1 What to monitor

- ✓ Login attempts (successful and failed)
- ✓ Configuration changes
- ✓ Access to sensitive resources
- ✓ Unusual network traffic
- ✓ Activities under administrative privileges

6.2 Centralized monitoring

Collecting logs in one place enables better analysis and correlation of events. A security information and event management (SIEM) system is a key tool for this.

> **Important.** Logs are useful only if they are reviewed. Regular monitoring and analysis are key to detecting incidents in time.

7. Access and privilege management

- ✓ Apply the principle of least privilege
- ✓ Regularly review the access rights

- ✓ Remove access immediately once the need ends
- ✓ Use strong authentication for administrative accounts
- ✓ Separate administrative accounts from ordinary ones
- ✓ Log all activities involving privileged access

8. System hardening

Hardening is the process of reducing the attack surface by removing unnecessary functions and applying secure configurations.

- ✓ Disable unnecessary services and functions
- ✓ Remove default accounts and passwords
- ✓ Apply secure configuration settings
- ✓ Restrict network access to the minimum
- ✓ Install only the software that is necessary

> **Principle.** Every unnecessary function is a potential vulnerability. Fewer functions means a smaller attack surface.

9. Security update management

Applying security updates promptly is one of the most important tasks, but it requires care so as not to disrupt operations.

9.1 The update process

- ✓ Follow the announcements about security vulnerabilities
- ✓ Test the updates in a controlled environment first
- ✓ Plan the deployment to minimize downtime
- ✓ Keep a backup before critical updates
- ✓ Document the changes that were applied

> **Balance.** Critical security updates should be applied quickly, but on critical infrastructure every update must be carefully tested so as not to disrupt operations. The balance between security and stability is key.

10. Incident response

When an incident occurs, a structured response limits the damage.

10.1 Response phases

1. **Identification** — recognizing that an incident is occurring;

2. **Containment** — preventing the damage from spreading;
3. **Eradication** — removing the cause;
4. **Recovery** — restoring normal operation;
5. **Lessons learned** — analysis to prevent future incidents.

11. Backups and continuity

- ✓ Maintain regular and tested backups
- ✓ Keep copies in a separate, secure location
- ✓ Test the restore process regularly
- ✓ Have a business continuity plan
- ✓ Document the recovery procedures

12. Best practices

- ✓ The principle of least privilege everywhere
- ✓ Defense in depth — multiple layers of protection
- ✓ Regular monitoring and log analysis
- ✓ Prompt but tested application of updates
- ✓ Strong authentication for all privileged accounts
- ✓ Regular and tested backups
- ✓ Documented procedures and response plans

13. Frequently asked questions

Does the AI system completely replace human analysis?

No. AI is a powerful tool that detects and prioritizes the threats, but human expertise is indispensable for investigation, decision-making and responding to complex situations.

How often should I review the logs?

Critical alerts should be reviewed immediately. A regular log review should be a daily practice, supported by automated tools for correlation and alerting.

How do I balance security and availability on critical infrastructure?

Every security update or change must be carefully tested before deployment. Plan the changes for periods with minimal impact and always keep a backup for a quick rollback.

What is defense in depth?

A strategy of multiple layers of protection, so that if one layer fails, the others keep protecting. You do not rely on a single measure.

Why do administrative accounts require special attention?

Because they carry the highest privileges. A compromised administrative account gives an attacker broad access. That is why they require the strongest protection and careful management.

14. Glossary

Term	Meaning
IDS	Intrusion detection system — alerts on threats
IPS	Intrusion prevention system — actively blocks threats
SIEM	Security information and event management
Hardening	Reducing the attack surface
Segmentation	Dividing the network into isolated zones
Least privilege	Granting only the rights that are necessary
Defense in depth	A multi-layered security strategy
Anomaly	A deviation from normal behavior

Security of industrial control systems (SCADA)

As an operator of an electricity transmission system, MEPSO manages industrial control systems (SCADA) that supervise and control the transmission of electricity. These systems require a specialized security approach.

Particularities of SCADA security

- ✓ Availability is critical — outages have serious consequences
- ✓ Many systems were designed before modern cyber threats
- ✓ Updates require exceptionally careful planning
- ✓ Isolation from the corporate networks is key
- ✓ Specialized monitoring for the operational technologies

Protective measures

- ✓ Strict segmentation between the IT and OT (operational technology) networks
- ✓ Controlled and logged access to the control systems
- ✓ Monitoring specialized for industrial protocols
- ✓ Response plans adapted to their critical nature

A critical responsibility. The security of the industrial control systems has implications beyond the organization itself — it affects the stability of the national power grid. That is why it demands the highest level of attention and expertise.

Continuous education

Cyber threats constantly evolve, and attacks on critical infrastructure grow more complex. Administrators must continuously upgrade their knowledge, follow new threats and apply best practices. This training is part of that continuous professional development.

Practical scenarios for administrators

Scenario 1: Unusual network traffic

The AI detection system alerts on an unusual traffic pattern from an internal system to an unknown external address, at an atypical time.

Correct approach: You do not ignore the alert. You investigate the source, isolate the affected machine if necessary, analyze what caused the traffic, and document. This may be a sign of a compromised system.

Scenario 2: A request for an urgent update

A critical security vulnerability has been published, requiring an urgent update, but the system is part of the critical infrastructure in operating mode.

Correct approach: You assess the risk, test the update in a controlled environment, plan the deployment for minimal impact, ensure a backup, and deploy with the ability to roll back quickly if a problem arises.

Scenario 3: Suspicious administrative activity

The logs show administrative activity from an account at a time when the corresponding employee was not at work.

Correct approach: You investigate immediately. This may be a compromised account. You check with the account's owner, review what was done, and take measures to secure it if unauthorized access is confirmed.

The common denominator. In all scenarios, the key is not to ignore the alerts, to investigate thoroughly, and to document. Vigilance and a structured approach are the foundation of an effective defense.

15. Conclusion

As an administrator, you are a key guardian of the security of the critical infrastructure. The combination of solid fundamental practices, modern tools including artificial intelligence, and constant vigilance forms an effective defense.

> **Key message.** Technology, including AI, is a powerful tool, but your expertise, vigilance and responsibility are irreplaceable. The best defense combines advanced technology with expert human management.

MEPSO AD Skopje — Electricity Transmission System Operator of North Macedonia
Document No. MEPSO-PRI-ADM-005 · Classification: Internal Use