6 Fundamentals of OT Network Security

Topics

- OT Security Best Practices
- Security Operations Center (SOC)
- Security Information and Event Management (SIEM)
- The Purdue Model
- Vendor and Supply Chain Security
- Patch Management
- Least Privilege and Access Control

OT Security Best Practices

Firewalls, IDS, and IPS

- **Stateful Firewalls**
  - Examine each packet and filter it based on rules
  - **Stateful**--remembers previous packets to determine if a packet is part of an established connection
- **Intrusion Detection Systems (IDS)**
  - Monitor network for known malicious patterns
  - Raise alerts if found
- **Intrusion Prevention System (IPS)**
  - Like IDS but blocks suspicious traffic

Security Monitoring

- Ongoing surveillance of OT network
- To identify anomalies, intrusions, or suspicious behavior
- Methods
  - Log analyzers
  - Network traffic analyzers
  - Behavior-based analytics

Security Operations Center (SOC)

SOC

- Centralized unit staffed with cybersecurity staff
- Monitoring OT networks and systems
- Technology
  - **Security Information and Event Management (SIEM)**
    - Consolidates security events for analysis
  - **IDS** and **IPS**
- **Threat Intelligence**
  - Trends, emerging threats

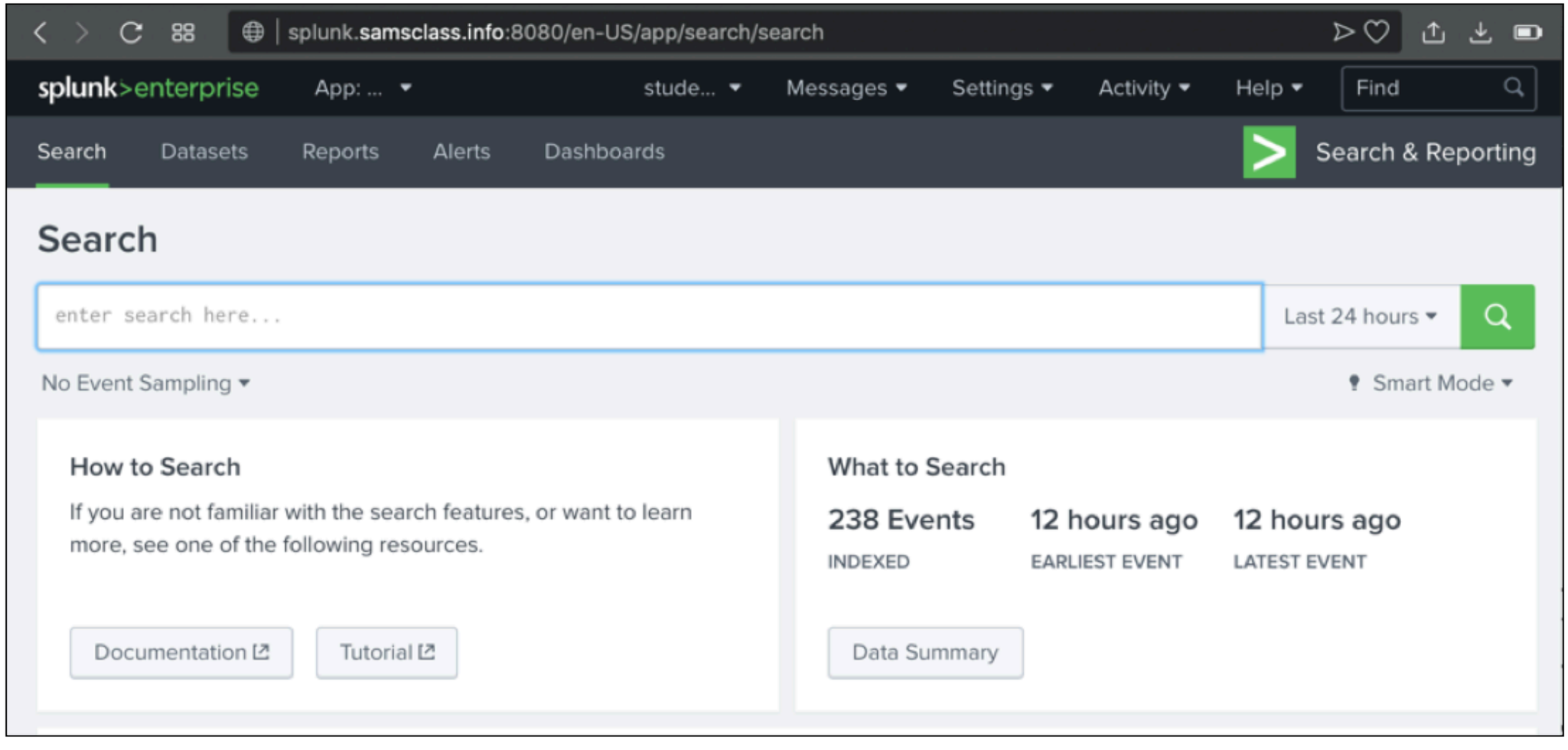
Security Information and Event Management (SIEM)

SIEM

- Ingests data from firewalls, IDS, servers, endpoints, etc.
  - Through syslog messages, APIs, or agents
- Can send alerts when suspicious patterns are found
- Can be used by incident response teams to research attacks
  - Determine root causes
- Produce reports for management

Splunk

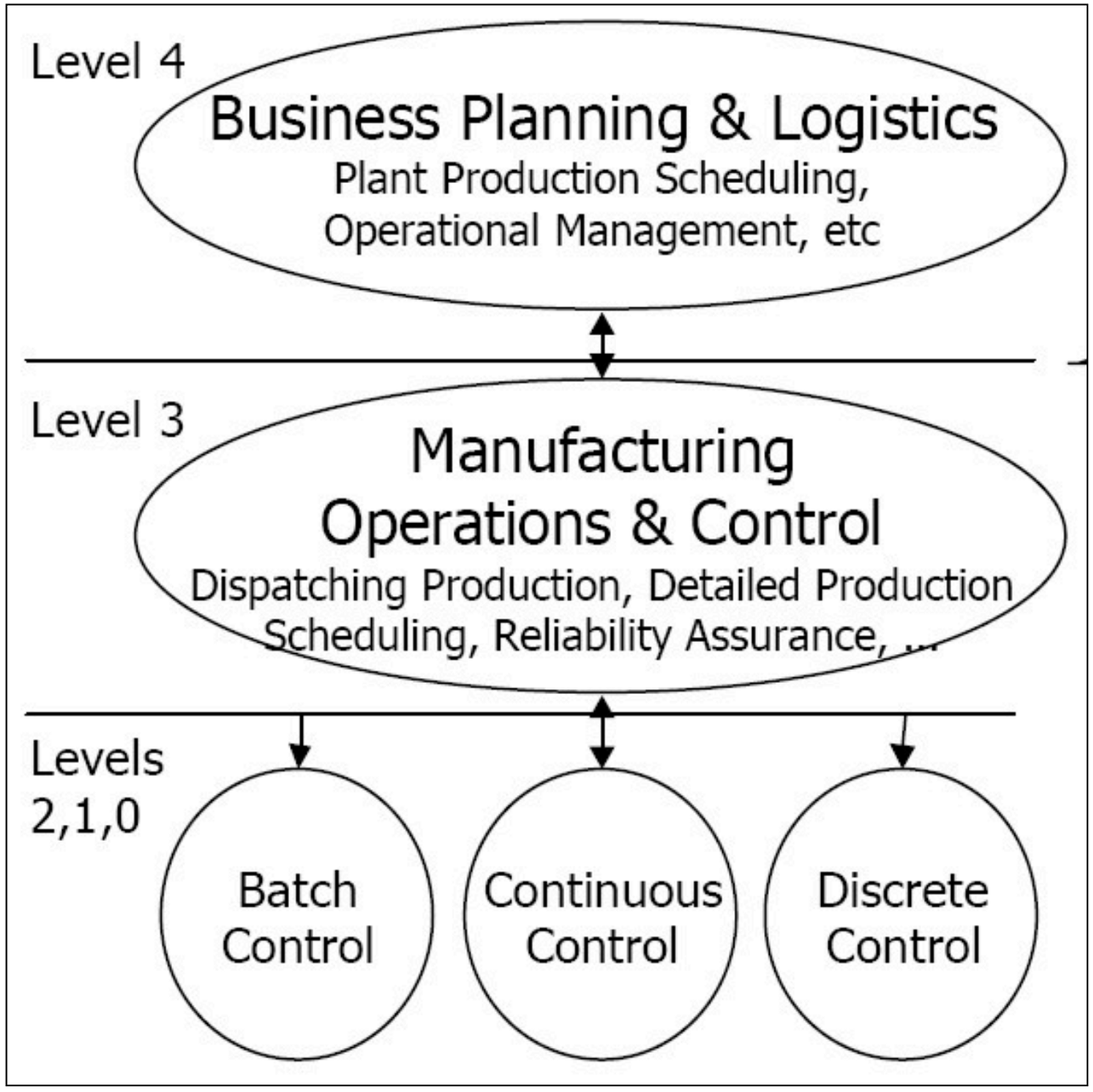
- The industry leading SIEM
- Google for log data



The Purdue Model

Purdue Enterprise Reference Architecture (PERA)

- Level 4: **Business Planning and Logistics**
- Level 3: **Operations Management**
- Level 2: **Supervisory Control**
- Level 1: **Basic Control**
- Level 0: **Process**



- Image from Wikipedia

Risk Profiles

- Different levels of the Perdue model have different risk profiles
- The lower levels require real-time communication and high availability
- Upper levels may prioritize data integrity and confidentiality

Vendor and Supply Chain Security

Third-Party Vendors

- **Secure Remote Access**
  - For approved personnel or third-party vendors
  - Remote connections to OT systems
  - For maintenance, troubleshooting, and support
- **Advantages of Employing Third-Party Vendors**
  - Specialized skills, alternate viewpoints
- **Pitfalls of Third-Party Vendors**
  - Unapproved access, data breaches, insider threats
  - Must assess reputation, reliability, and security of vendors first

Vendors and Supply Chain Security

- Assess security practices, policies, and procedures of vendors
  - To uphold integrity of the supply chain
- **Authentication and Access Controls**
  - Multi-factor authentication
  - Role-based access controls to limit vendor access
- **Secure Communication**
  - Encrypt connections with TLS or a VPN
- **Auditing and Monitoring**
  - Track remote access for suspicious behavior

Vendor Security Assessments

- Assess security practices, protocols, incident response capabilities, and compliance with industry standards

Patch Management

Patch Management

- **Basics**
  - Updates to software and OS to rectify security vulnerabilities
  - Management
    - Identify available patches
    - Determine relevance
    - **Test them for bad effects (not in textbook)**
    - Apply them in a controlled manner
    - Monitor to ensure no adverse effects arise

Patch Management

- **In OT Environments**
  - Often run on legacy hardware and software
  - Patches, if available, may be very important
- **Implementing Patch Management in OT**
  - Test patches thoroughly before deployment

Patch Management Key Considerations

1. Inventory Management

- Inventory all hardware and software components in OT environment
- With versions, configurations, and dependencies

2. Patch Prioritization

- Consider severity of vulnerabilities, criticality of the affected systems, and risk of exploitation

3. Testing

- Test on a limited scale in a controlled environment
- Test functionality and stability

Patch Management Key Considerations

4. Scheduling and Downtime Management

- Scheduled maintenance windows

5. Documentation and Auditing

- Maintain records and audit the process

6. Automated Patch Management

- Can streamline the patching process

Patch Management Key Considerations

7. Contingency Planning

- Rollback plan and backups
- If patch causes issues

8. Training and Awareness

- Staff should be aware of the importance of patches

Least Privilege and Access Control

Least Privilege

- Users should only have the access they need to do their job
- Aligned with user's role and responsibilities
- This control shrinks attack surface and limits the harm of security incidents

Access Control Measures

- **Authentication**
  - Passwords, biometrics, smart cards, etc.
  - Multi-factor authentication is MUCH stronger
- **Authorization**
  - Permissions and privileges attached to each user or role
- **Role-Based Access Control (RBAC)**
  - Permissions depend on job role
- **Attribute-Based Access Control (ABAC)**
  - Access based on other factors, like time of day, location, or attributes of the device being used

User and Privileged Account Management

- **User Provisioning**
  - Creation, modification, and deactivation of user accounts
- **Privileged Account Management**
  - Robust authentication, session recording, and privileged session monitoring
  - Of privileged accounts (administrators)
- **Regular Access Reviews**
  - Audit access rights
  - Identify and revoke unnecessary or outdated privileges

Ch 6