First I&C Cyber Security System Integrated at Kozloduy NPP

Asya Mihaylova, Senior Project Manager

Westinghouse

Westinghouse **VISION & VALUES**

- Customer Focus & Innovation
- Speed & Passion to Win
- Teamwork & Accountability

Safety • Quality • Integrity • Trust

Westinghouse

Full Suite Portfolio of Nuclear Technology & Services

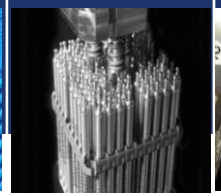
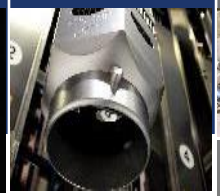
Develop & Deploy Leading Carbon-Free Technology

Design and Build

AP1000® Reactor	AP300™ SMR	Energy Storage	eVinci™ Microreactor
			

Lead All Phases of the Nuclear Operating Plant Lifecycle

Operations and Maintenance

Americas PWR	EMEA/Asia PWR	BWR	VVER	Outage & Maint. Svc.	Engineering Services	I&C	Parts
							

Long-term Operations

Global Operations Services

supports predictable delivery across all business while optimizing global resources and our supply footprint

Provide carbon-free advanced reactor technologies that enable the flex-load, carbon-free grid of the future to commercial and government clients

Maintain leadership in PWR and grow BWR, VVER and other advanced fuel capabilities

Achieve market leadership in digital products and services through innovation and increase penetration of OEM and non-OEM parts market

Westinghouse

The Challenge

- Meet IEC requirements:
  - IEC 63096 Nuclear power plants – Instrumentation, control and electrical power systems – Security controls
  - IEC 62645 Nuclear power plants – Instrumentation and control systems – Cybersecurity Requirements

- NPP requirements to security controls on the Ovation DCS:

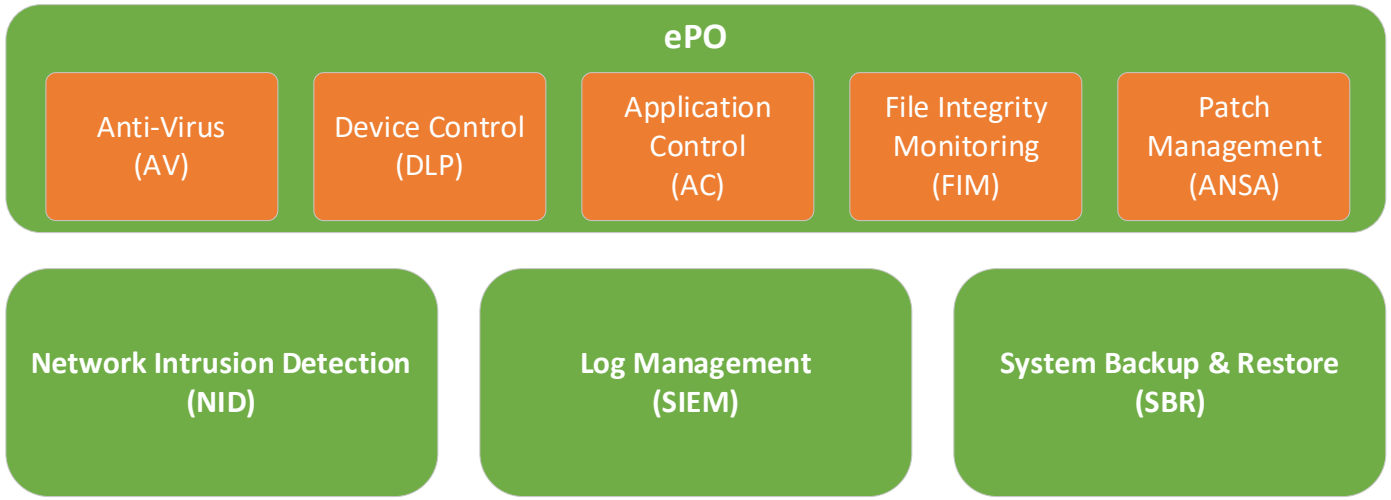
  - Antivirus
  - Application Control (Whitelisting)
  - Device Control
  - Integrity Control
  - Patch Management
  - System Backup and Recovery
  - System Hardening
  - Network Intrusion Detection Appliance.
  - Security Information and Event Management
- Connection to a planned for near future Security Operation Center
- Common Cybersecurity solution shared by three independent Ovation systems

Kozloduy DCS Ovation

	БЛОК 5	БЛОК 6
Cabinets	180	180
I/O Modules	> 2700	> 2700
I/O Signals	> 36000	> 36000
Network Switches	34	34
Controllers	70*2	70*2
Servers	30	30
Control Sheets	> 9700	> 9700
Graphics	> 2500	> 2500
Macros	> 990	> 990
Total Points in Database	> 340000	> 340000
Points from DataLinks (Externel Systems)	2800	2800
Archive points 200000	90000	90000

Components of the System

- Firewall Switch – First line of defense
- VM Host Server
  - ePolicy Orchestrator (ePO)
  - System Backup and Recovery
  - Security Information and Event Management
  - Network Intrusion Detection System
- System Backup and Recovery
- User Interface Server



Westinghouse

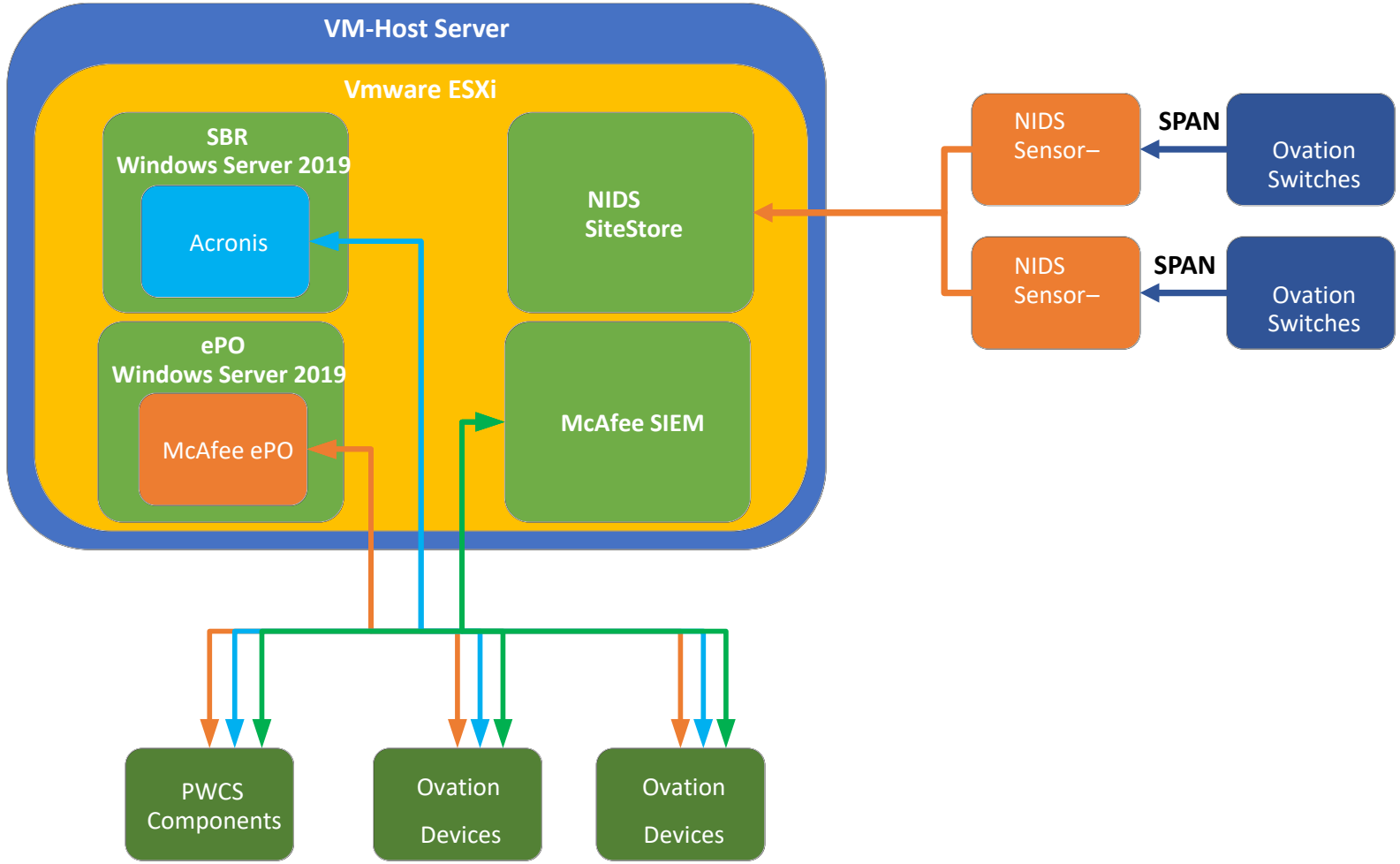
Firewall Switch – First line of defense

The PWCS firewall isolates the internal components (of the cybersecurity system) from the monitored Ovation endpoints.
The Firewall provides a pathway for the communication lines from the cybersecurity system to the Unit 5,6 & Aux building Ovation Systems.

The firewall has been configured to forward log to the SIEM

System Functions

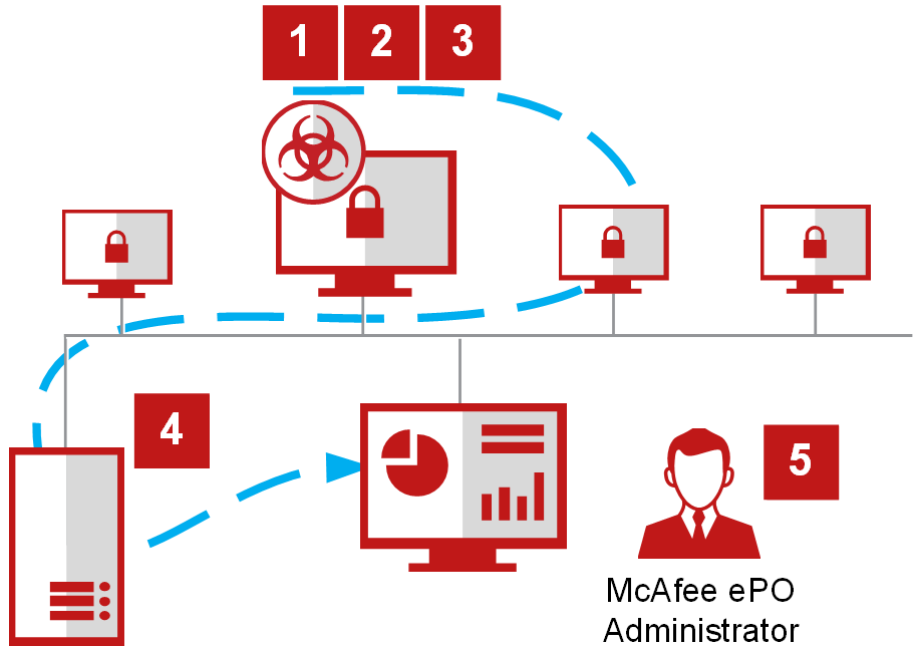
- The VM-Host server contains the Servers that provide the different cyber security functions to the Ovation Equipment



What happens during an attack

Sequence of events:

1. Malware attacks a computer in the Trellix (McAfee) ePO managed network.
2. Trellix (McAfee) product software, for example Trellix (McAfee) Endpoint Security, cleans or deletes the malware file.
3. McAfee Agent notifies McAfee ePO of the attack.
4. McAfee ePO stores the attack information.
5. McAfee ePO displays the notification of the attack on the dashboard and saves the history of the attack in the Threat Event Log.



ePolicy Orchestrator

- The Trellix (McAfee) Suite is a client/server program that utilizes various applications to protect a network from security risks. Trellix (McAfee) ePolicy Orchestrator (ePO) is a Web-based console for the McAfee product family.
- ePO provides a centralized console to enforce policies and automate client tasks.
- McAfee security software and McAfee ePO work together to stop malware attacks on your systems and notify you when an attack occurs.

- The McAfee ePO Server deploys and manages Agents that contain the different security software

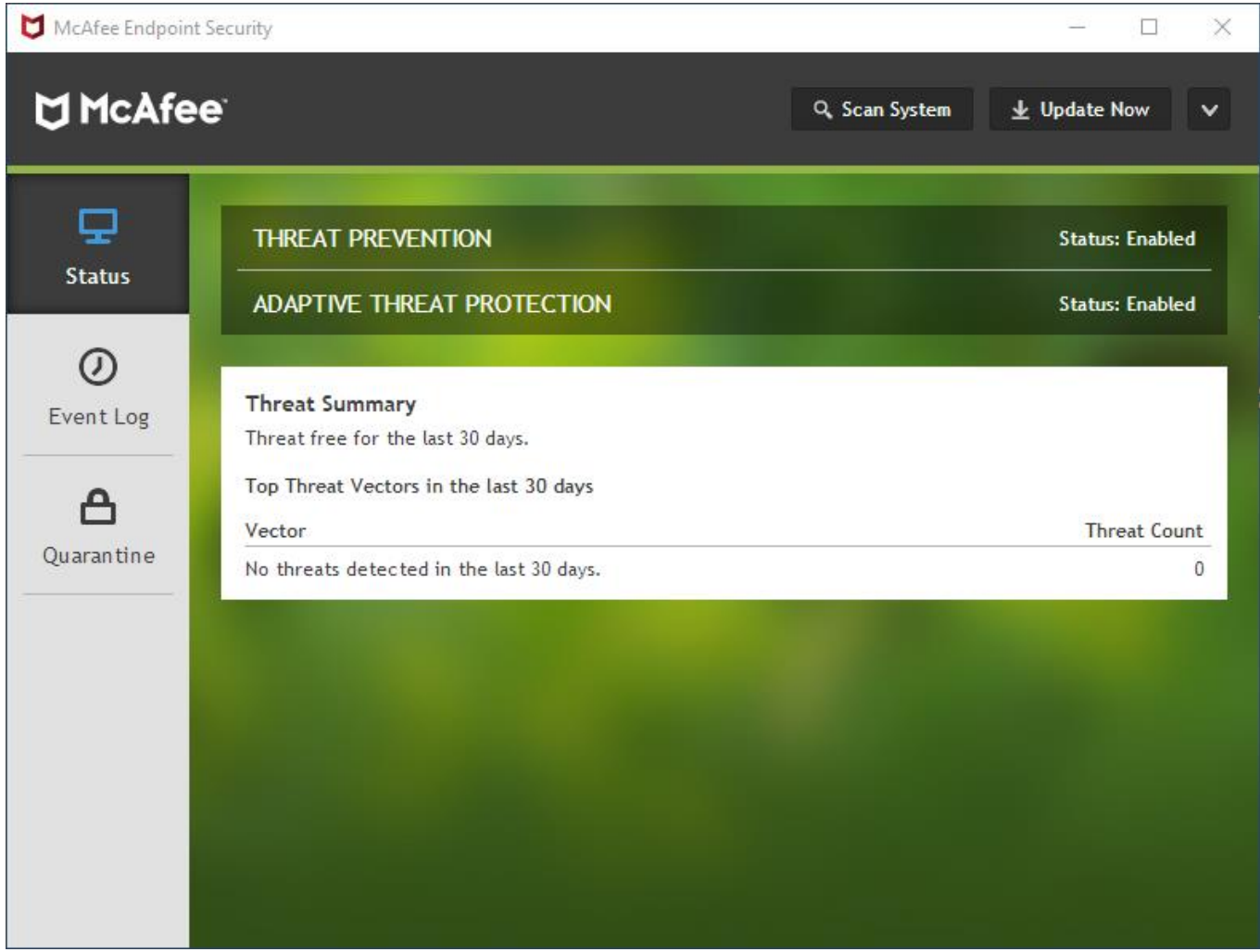
- McAfee ePO Agents and its components processes stop an attack, notify you when the attack occurs, and record the incident on the Agent and the ePO Server.

ePolicy Orchestrator (ePO)

- The PWCS McAfee Suite product includes the following applications:
  - Anti-Virus (AV) (MAV)
  - Device Control (DLP or DC) (MDC)
  - Application Control (AC) (MAC)
  - File Integrity Monitoring (FIM)
  - Patch Management (Windows, Java, Adobe updates only) (PM) (APM)

Antivirus

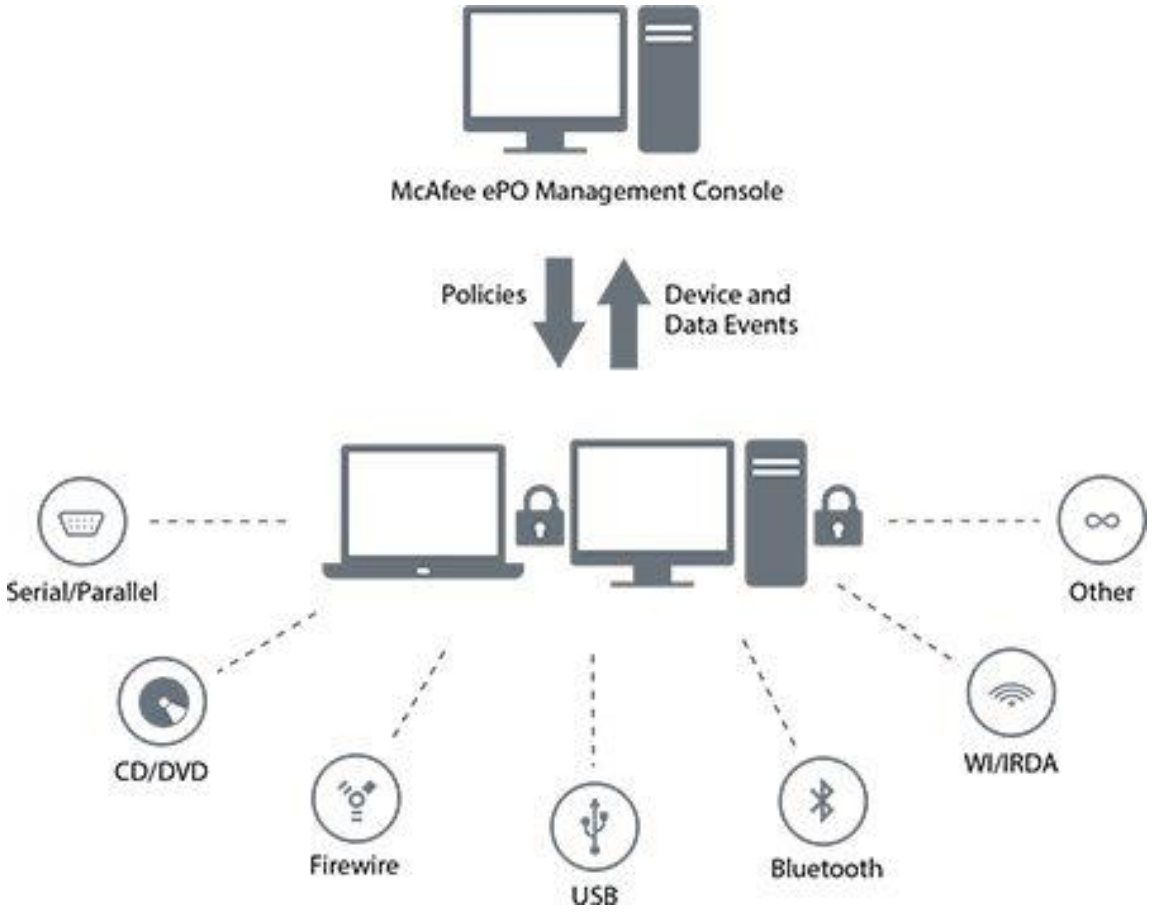
- Antivirus software is a program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.
- McAfee Antivirus software is installed on all Windows servers.
- A central McAfee antivirus management server is provided and operated in a virtualized environment, utilizing an agent that is installed on each managed workstation. Antivirus signature updates are validated for compatibility with the Ovation System.



Device Control

- Device Control (DC) is an anti-malware technology that protects the system from the unauthorized use of removable media such as USB flash drives and CDs. DC intercepts requests from removable media to usage policy.

- The McAfee Data Loss Prevention (DLP) agent is installed on each host to communicate back to the ePO server and perform local device control functionality



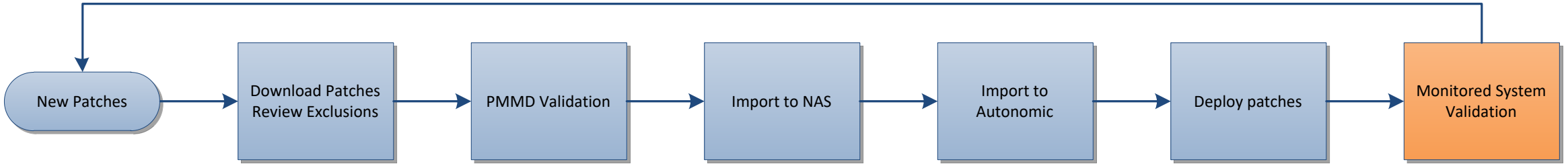
Application Control

- Application Control (AC) is an antimalware technology that can protect the system from custom or previously unknown malware. A software agent on the client intercepts requests to execute a program. The agent will only allow a program to execute if it is in the white list of allowed programs. White listing software usually stores hashes or checksums of the white listed files in order to detect unauthorized alterations to application files.

- The Solidcore application control solution uses the ePO server to provide configuration and control of the agent installed on each workstation. Default white lists are provided to prevent conflicts with critical software such as the operating system, Ovation, Oracle, or antivirus protection.

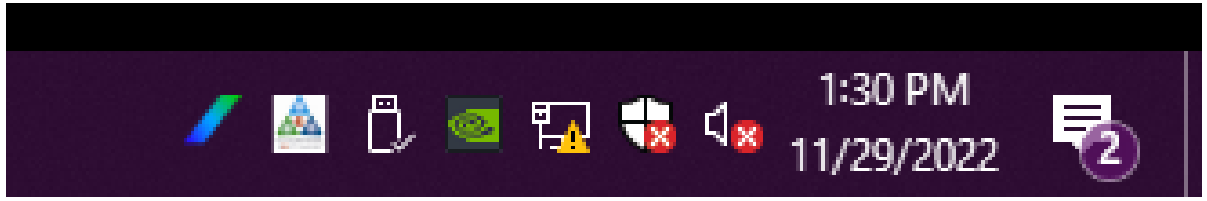
Patch Management

- Patch management is a system maintenance technology that provides a centralized, automated installation for software updates. Additionally, patch management tracks configuration information about each endpoint on the network and assists in maintaining patch levels.



Patch Management

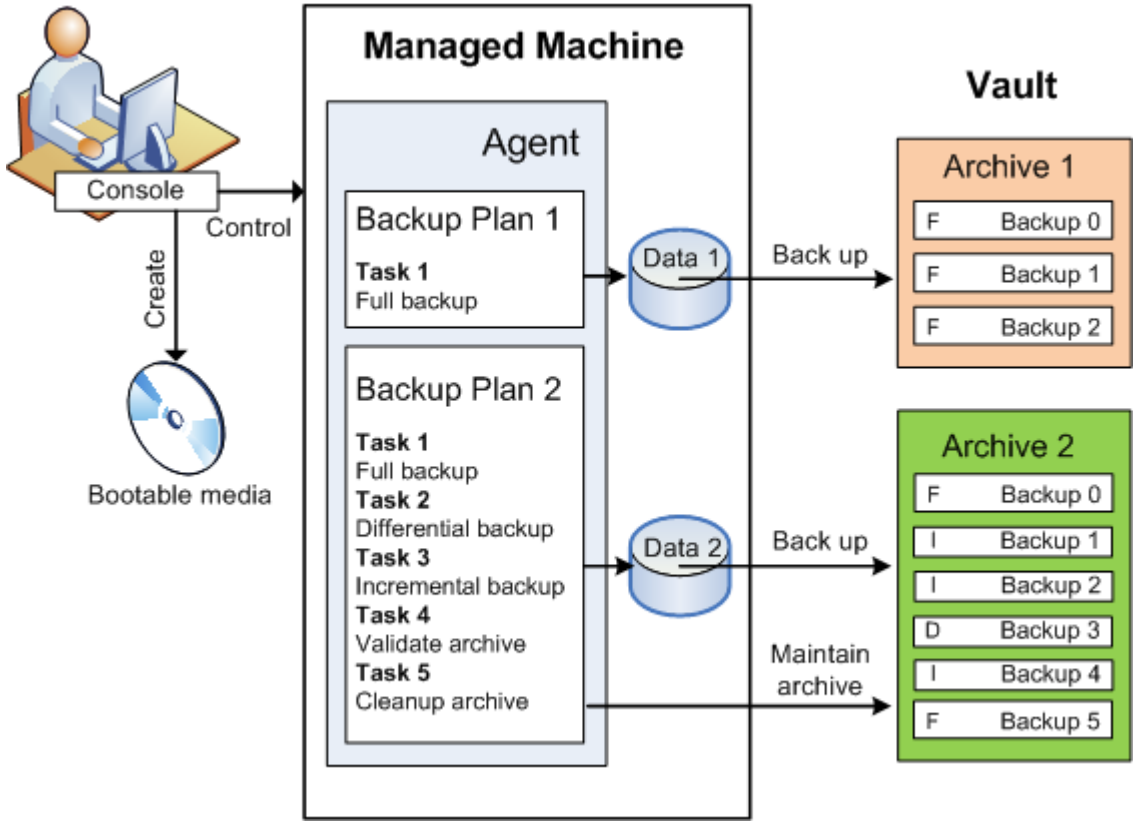
- The cybersecurity contains a centralized patch management server in a virtualized environment which is used to monitor patch levels and deploy patches in batches on each endpoint. The Autonomic Network & System Administrator (ANSA) patch management agent is installed on each endpoint to communicate back to the central server and perform local patching functionality.
- ANSA Patch Manager can scan patches that are on the endpoints, report what patches are available to be installed to the endpoints, and push patches to them. The patches that are be managed by ANSA are Microsoft Updates and Security Patches, Adobe Reader, Adobe, and Java updates.



System backup and recovery

- System backup and recovery (SBR) is a disaster recovery technology that creates a backup of Windows based workstations so that the workstation can be restored after a failure or disaster. The SBR solution periodically saves images of system assets to a separate file system.

- The system contains the Acronis centralized backup and recovery server in a virtualized environment which is used to manage backup and recovery on each workstation. The Acronis backup and recovery agent is installed on each host to communicate back to the central server and perform local backup and recovery functionality. The SBR solution periodically saves images or backups of the systems to the cybersecurity network attached storage (NAS).



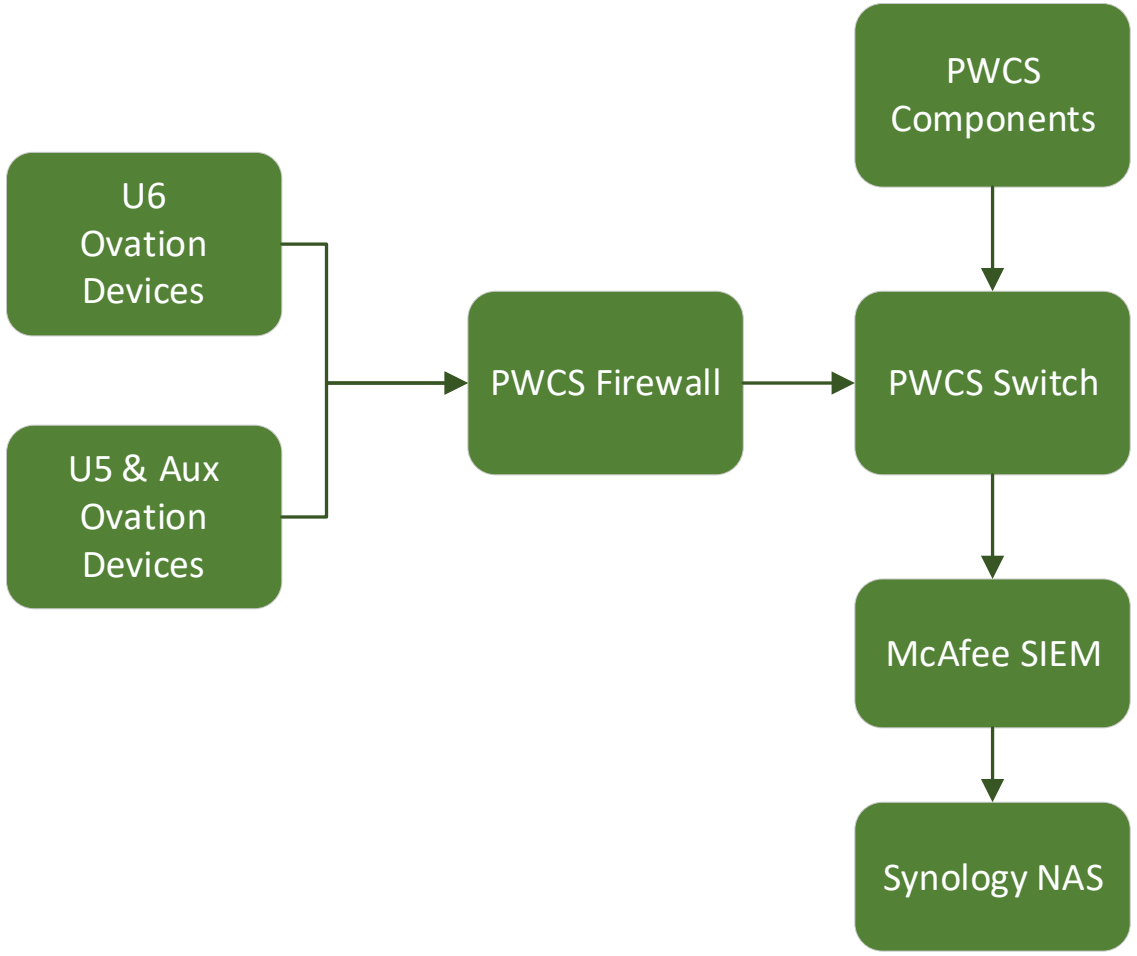
Security Information & Event Management

- Security Information & Event Management (SIEM) is an application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface. [https://csrc.nist.gov/glossary]

Westinghouse

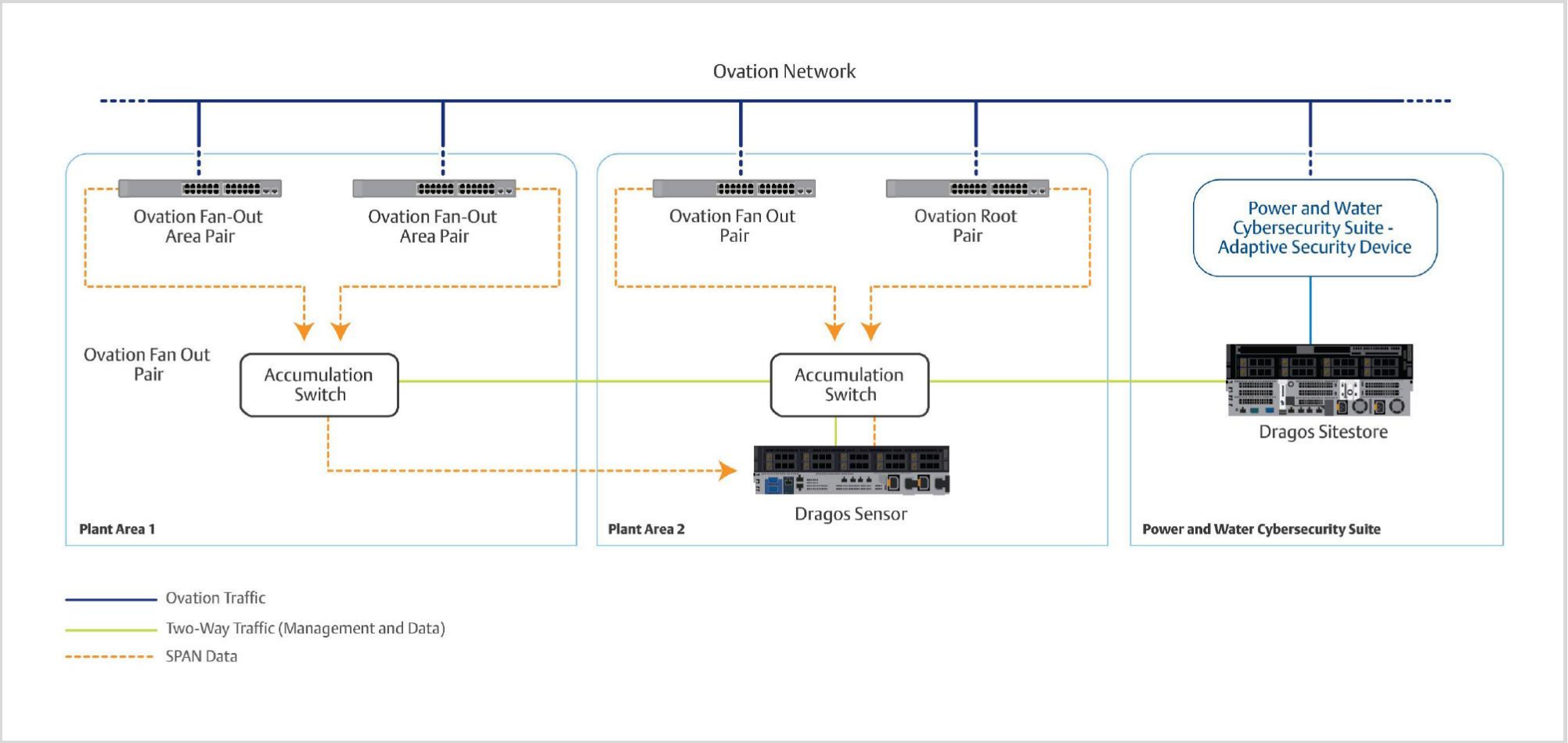
Security Information & Event Management

- SIEM is located inside VM-Host Server as a Virtual Machine
- Monitored system communication is filtered by network firewall.
- SIEM stores raw log data on NAS
- UI Server used to access ESM Console using the ESM App in the Desktop



Westinghouse

Network Intrusion Detection System



User Interface Server

- The PWCS-UI Server provides an interface to the different software solutions hosted on the VM-Host Server
- The PWCS-UI Server is accessed through the KVM located in the cabinet.

System Hardening

- System hardening is performed in multiple system components, these include Windows 10 machine(PWCS-UI), Windows 2019 Server (SBR, ePO), Synology NAS, the PWCS Firewall and Switch.

- The standard implementation includes the following:
  - Unused ports and services are disabled to enforce least functionality
  - Role-based access is applied to enforce least privilege
  - User activity is audited and logged
  - Access to Ovation equipment and software components
  - The principle of least privilege is applied to user access
  - System Use Notification is configured
  - Password Requirements are enforced.