**1. Deploy Purview and Varonis SaaS Platform for a DLP Strategy, and Rubrik’s DSPM Solution**

**Goal:** Implement a comprehensive Data Loss Prevention (DLP) strategy using a combination of Microsoft Purview, Varonis, and potentially Rubrik’s DSPM solution.

**1.1 How would each tool complement each other?**

* **Microsoft Purview:** Primarily helps with data governance, classification, and DLP. It allows you to categorize data and define protection policies around it. It will be particularly useful in ensuring compliance and monitoring data lifecycle.
* **Varonis:** Specializes in security analytics, monitoring user behavior, detecting anomalies, and ensuring that sensitive data is protected. It would complement Purview by adding additional monitoring and auditing capabilities, especially focusing on insider threats.
* **Rubrik DSPM:** Rubrik’s Data Security Posture Management (DSPM) would be used for automating the discovery of vulnerabilities in your data environment, enforcing data security policies, and providing cloud-native protection for data. If your organization is heavily reliant on cloud infrastructure, Rubrik could help secure that environment.

**1.2 Major Milestones in Deployment:**

* **Assessment Phase:**
  + Identify key stakeholders and define data classification levels (Public, General, Confidential, Highly Confidential).
  + Map out your current data landscape (databases, storage, endpoints).
  + Evaluate your existing security posture (data security, access control).
* **Solution Design:**
  + Architect the integration of Microsoft Purview for classification and DLP policies.
  + Plan deployment of Varonis for monitoring user behavior and access to sensitive data.
  + Plan for Rubrik integration (if decided to buy) for automating data protection, vulnerability management, and policy enforcement.
* **Deployment Phase:**
  + Implement Purview for data classification and protection.
  + Deploy Varonis agents for monitoring and auditing.
  + If integrating Rubrik, deploy DSPM tools in the cloud and configure data security posture policies.
* **Testing & Validation:**
  + Test the DLP and data classification policies.
  + Validate Varonis alerts and incident responses.
  + Verify Rubrik's effectiveness in automating security posture management.

**1.3 Do you need Rubrik’s DSPM solution?**

* **Necessity:** Rubrik’s DSPM is beneficial if you’re operating heavily in the cloud and need a cloud-native tool to secure and monitor data across your environment. If your data protection needs are more focused on on-prem, Purview and Varonis may be sufficient. However, for a comprehensive cloud-native security strategy, Rubrik could be valuable.
* **Cost-Benefit:** If cloud security is a significant concern, Rubrik could be worth it. If your needs are more on-prem, you may save costs by relying on Varonis and Purview.

**1.4 Strengths of Each Setup:**

* **Microsoft Purview:** Ideal for data governance, classification, and compliance, especially for public sector needs (e.g., ensuring compliance with FOIA).
* **Varonis:** Great for data security and behavior monitoring, especially for detecting insider threats and auditing data access.
* **Rubrik DSPM:** Best for securing data in cloud environments and automating the discovery of vulnerabilities across hybrid and cloud-native infrastructures.

**2. Configure 8000 Laptops Using Intune AutoPilot**

**Goal:** Deploy 8000 laptops securely using Intune AutoPilot.

**2.1 How Does Intune AutoPilot Work?**

* **Intune AutoPilot** automates the deployment of Windows 10/11 devices directly from the manufacturer to end-users. It configures the devices with predefined settings (e.g., security policies, apps, configurations) before the user even turns on the device.
* Devices are registered with Azure AD and pre-configured to the user’s profile via AutoPilot.
* Security configurations, applications, and policies (including DLP and encryption) are applied during setup.

**2.2 Secure and Easy Deployment as an Outsourcing Partner:**

* **Preparation:**
  + Register the laptops in Intune AutoPilot by uploading hardware IDs.
  + Create configuration profiles in Intune for device enrollment, security, and app deployment.
  + Set policies such as BitLocker encryption, VPN configuration, and DLP rules.
* **Deployment:**
  + When the end-user powers on the device, it connects to AutoPilot, downloads the configuration profiles, and applies security policies and apps.
  + Devices are automatically joined to Azure AD and enrolled into Intune for ongoing management.
* **Security Measures:**
  + Enforce multi-factor authentication (MFA) for user login.
  + Apply endpoint protection policies, including Windows Defender, application whitelisting, and DLP settings.

**3. DLP for Mobile Phones**

**Goal:** Research tools for DLP for mobile phones (IBM Maas360, Intune, Varonis, Palo Alto).

**3.1 Can Varonis do DLP for Mobile Phones?**

* **Varonis** is primarily focused on data security, user behavior monitoring, and insider threat detection, rather than mobile-specific DLP. It doesn't have native mobile device management (MDM) capabilities.

**3.2 Can Intune or IBM Maas360 Do It?**

* **Intune:** Yes, Intune provides mobile device management (MDM) and DLP capabilities for mobile phones, including iOS and Android. It allows you to enforce security policies such as encryption, remote wipe, app control, and access controls. DLP policies can prevent the unauthorized sharing of sensitive data from mobile apps.
* **IBM Maas360:** IBM Maas360 also provides mobile security and DLP capabilities, including secure app management and containerized environments to protect sensitive data.

**3.3 Can Palo Alto Do It?**

* **Palo Alto Networks** offers a mobile DLP solution through their Prisma Access and Global Protect platforms. They can enforce security policies across mobile devices and integrate with other security solutions for comprehensive protection.

**3.4 What Tool is the Best for Mobile DLP?**

* **Best Option:** Microsoft Intune is likely the best choice for a Microsoft-centric environment, as it integrates seamlessly with your existing tools and provides robust mobile DLP features.
* **Cost-Benefit:** If you already have Intune, there may be no need for an additional investment in tools like Maas360 or Palo Alto.

**4. Repairing the Relationship with Your External SOC**

**4.1 Understanding the Concern:**

* The concern is the delay in alerts due to the cron job schedule from the SOC, which doesn't align with real-time needs.

**4.2 Steps to Repair the Relationship:**

* **Communication:** Schedule a meeting with the SOC to discuss the impact of delayed alerts on security operations. Understand their processes and propose ways to align with your organization's needs.
* **Addressing the Cron Job Timing:**
  + **Shorten Interval:** Work with the SOC to reduce the cron job interval to near-real-time alerts or implement an event-driven model instead of relying on a cron job.
* **Automation and Integration:** Consider integrating the SOC with your existing security tools for real-time notifications rather than batch-based schedules.

**5. Handling FOIA Requests and iMessage Capture**

**5.1 What is SELECTCapture?**

* **SELECTCapture** is a tool that can capture iMessages for compliance purposes, including FOIA requests. It allows you to capture iMessages without disabling encryption, enabling compliance without blocking iMessage.

**5.2 Can It Help You Keep Using iMessage?**

* Yes, **SELECTCapture** can help you continue using iMessage while ensuring that you can respond to FOIA requests. It works by capturing iMessages for archival without compromising encryption, which addresses the issue with Smarsh.

**6. Google Workspace for Disaster Recovery (DR)**

**6.1 How Does Google Workspace Help in DR?**

* **Google Workspace** offers cloud-based collaboration tools (Gmail, Drive, Docs, etc.) that provide built-in redundancy and availability. If Microsoft services are down, users can continue using Google Workspace for email, file sharing, and collaboration.
* You can set up cross-platform email forwarding and ensure that all critical communication can be handled through Google Workspace during Microsoft outages.

**7. Designing a Recovery Solution with Rubrik Cyber Recovery**

**7.1 Recovery Plan Design:**

* **Step 1:** Implement Rubrik for data backup and cyber recovery. Rubrik ensures rapid recovery in case of a cyberattack, including ransomware.
* **Step 2:** Add secondary recovery solutions for identity and network restoration, like Azure Active Directory (AD) backups, and multi-region backup systems.
* **Step 3:** Test and validate the recovery process through simulation exercises (tabletop testing).