CCDC EDR Report

1. Introduction

1.1 Importance of EDR Solutions in Cybersecurity

Endpoint Detection and Response (EDR) solutions play a critical role in modern cybersecurity strategies.

- *They provide **real-time visibility** into endpoint activities, **detect suspicious behaviors or malicious file**s, and **automate responses to contain and remediate threats**.*
- *By monitoring endpoints continuously, EDR solutions help organizations **detect threats earlier**, **limit lateral movement of attackers**, and **maintain a robust security posture**.*

1.2 Scope of the Report

This report focuses on identifying EDR solutions that:

- ***Have a free or trial-based usage model** (covering at least several weeks to allow proof-of-concept testing).*
- ***Are compatible with both Linux and Windows operating systems**, ensuring broad coverage of common endpoint environments.*
- ***Offer central management capabilities**, either through seamless integration with an existing ELK (Elasticsearch, Logstash, Kibana) SIEM server or via a native, vendor-supplied dashboard.*

Additionally, this report provides a high-level overview of deployment processes, from installing and configuring agents on 8–10 client machines, to setting up a centralized management console, and ensuring that logs and threat detections flow properly for analysis.

2. EDR Software Options

2.1 CrowdStrike Falcon

- **Provider:** CrowdStrike
- **Key Features:**
  - **Threat Detection:** Machine learning-based detection, behavioral analysis, and cloud-based intelligence.
  - **Response Automation:** Automated quarantine, device isolation, and response workflows.
  - **Logging Capabilities:** Real-time event streaming; detailed endpoint activity logs.
  - **SIEM Integration:** Offers a REST API and log forwarding that can integrate with ELK, Splunk, or other SIEMs.
- **Trial Length:** Typically a **15-day free trial** (extendable upon request).
- **Estimated Implementation Time for 8–10 Clients:**
  - **Deployment & Setup:** ~1–2 days (depending on network policies).
  - **Configuration & Testing:** ~1 day to fine-tune policies and ensure

logs are flowing to the SIEM or CrowdStrike console.

- **Centralized Management Capabilities:**
  - **Integration with ELK:** Falcon provides APIs and sample scripts to export detection data to an ELK stack.
  - **Native Dashboard:** CrowdStrike Falcon Console is cloud-based and accessible through a web interface.
  - **Limitations on Number of Clients in Trial:** Typically no strict limit for proof-of-concept, but always confirm with CrowdStrike during registration.

2.2 Microsoft Defender for Endpoint (MDE)

- **Provider:** Microsoft
- **Key Features:**
  - **Threat Detection:** Uses behavioral sensors, cloud security analytics, and Microsoft threat intelligence.
  - **Response Automation:** Automated investigation and remediation of alerts, endpoint isolation, and threat hunting capabilities.
  - **Logging Capabilities:** Deep logs available in the Microsoft 365 Defender portal; can be forwarded to SIEM solutions via APIs or Azure Sentinel connectors.
  - **SIEM Integration:** Built-in integration with Azure Sentinel; can also forward logs to third-party SIEM (including ELK) using log forwarding or APIs.
- **Trial Length: 30-day free trial** (can sometimes be extended upon discussion with Microsoft reps).
- **Estimated Implementation Time for 8–10 Clients:**
  - **Deployment & Setup:** ~2–3 days (considering Microsoft 365 tenant setup and agent deployment steps).
  - **Configuration & Testing:** ~1 day for fine-tuning policies and ensuring data flows to the SIEM or Defender portal.
- **Centralized Management Capabilities:**
  - **Integration with ELK:** Possible via custom log forwarding from the Defender for Endpoint portal or by leveraging Azure APIs.
  - **Native Dashboard:** Microsoft 365 Defender portal, offering unified alerts and incident management.
  - **Limitations:** The main limitation is usually the trial duration rather than a client count restriction, but ensure your environment can connect to Microsoft services.

2.3 Sophos Intercept X with EDR

- **Provider:** Sophos
- **Key Features:**
  - **Threat Detection:** Deep learning and signature-less threat detection,

anti-ransomware capabilities, exploit prevention.
    - **Response Automation:** Automated threat containment, remote isolation, and removal of malicious files.
    - **Logging Capabilities:** Detailed endpoint event logs; can export logs via syslog or direct API integration.
    - **SIEM Integration:** Supports SIEM integration through syslog, making it compatible with ELK.
- **Trial Length: 30-day free trial**.
- **Estimated Implementation Time for 8–10 Clients:**
    - **Deployment & Setup:** ~1 day for cloud console provisioning and agent deployment.
    - **Configuration & Testing:** ~1–2 days for policy configuration, testing detection, and ensuring SIEM ingestion.
- **Centralized Management Capabilities:**
    - **Integration with ELK:** Syslog-based integration or data export to the ELK stack.
    - **Native Dashboard:** Sophos Central, a cloud-based management console, manages all endpoints and alerts.
    - **Limitations:** During the trial, all features are typically available; confirm exact feature restrictions upon sign-up.

2.4 SentinelOne Singularity

- **Provider:** SentinelOne
- **Key Features:**
    - **Threat Detection:** AI-driven detection, static and behavioral AI models, storyline-based attack visualizations.
    - **Response Automation:** Automated rollback for ransomware, one-click remediation, and device isolation.
    - **Logging Capabilities:** Comprehensive real-time log streaming; can export detection logs.
    - **SIEM Integration:** Offers APIs and integrated connectors for common SIEM platforms, including ELK.
- **Trial Length: Free trial** offered for a limited time (usually **14–30 days**).
- **Estimated Implementation Time for 8–10 Clients:**
    - **Deployment & Setup:** ~1–2 days (easy cloud-based or on-prem management console).
    - **Configuration & Testing:** 1 day to refine policies and ensure integration with SIEM.
- **Centralized Management Capabilities:**
    - **Integration with ELK:** API-based or syslog forwarding into Elasticsearch.
    - **Native Dashboard:** SentinelOne Singularity Console (cloud or on-

prem).
    - **Limitations:** Typically no strict endpoint limit for a short trial, but contact SentinelOne for specifics.

3. EDR Implementation & Deployment Plans

Below are generalized steps for implementing and deploying each EDR solution. While details vary slightly across products, these steps outline the typical process you would follow.

Note: Refer to the official vendor documentation for specific instructions and screenshots. Links or references to documentation are provided where applicable.

3.1 CrowdStrike Falcon

1. **Set up Central Management (Falcon Console)**
    - Sign up for the CrowdStrike Falcon free trial on the CrowdStrike website.
    - We'll receive login credentials for the Falcon Console.
    - Configure necessary settings such as data collection regions, security policies, and user roles.
2. **Integrate with ELK (Optional)**
    - In the Falcon Console, generate API keys with appropriate permissions.
    - Use CrowdStrike's Event Streams API to forward detection and incident data to Logstash.
    - Configure Logstash to parse Falcon data and index it into Elasticsearch.
    - Create Kibana dashboards to visualize alerts and detections.
3. **Connect Linux and Windows Clients**
    - **Windows:** Download the Falcon sensor installer (EXE) from the console, run it on Windows endpoints, and provide the **customer ID** during installation.
    - **Linux:** Download the Falcon sensor RPM or DEB package (depending on distro), install using the command line, and register with the Falcon Console.
    - The endpoints will automatically appear in the Falcon Console under "Hosts."
4. **Deploy and Configure Agents**
    - From the Falcon Console, confirm the policy settings (e.g., detection, prevention, firewall, USB device control).
    - Assign policies to each endpoint or group.
    - Monitor the real-time alerts to ensure logs and threat data are received properly.

3.2 Sophos Intercept X with EDR

1. **Set up Central Management (Sophos Central)**
   - Sign up for a Sophos Intercept X trial via the Sophos website.
   - Create your Sophos Central admin account and log in to the web-based console.
   - Define global settings, administrative roles, and initial policies (e.g., threat protection, web control).
2. **Integrate with ELK (Optional)**
   - In Sophos Central, enable **Syslog** or **Log Exporter** to forward logs to your SIEM.
   - Configure Logstash to parse Sophos log data and ingest it into Elasticsearch.
   - Set up Kibana dashboards for real-time monitoring of detections.
3. **Connect Linux and Windows Clients**
   - **Windows:** Download the Intercept X installer from Sophos Central and run it on each endpoint.
   - **Linux:** Sophos provides a Linux agent package (DEB or RPM). Install via command line and register the device with Sophos Central using your account credentials.
   - Confirm the devices appear in Sophos Central under "Devices."
4. **Deploy and Configure Agents**
   - Assign policies (threat protection, device control, web control) to the endpoints.
   - Test detection capabilities by running EICAR test files or safe simulation tools.
   - Verify that alerts appear in Sophos Central and that logs are forwarded to ELK if configured.

3.3 SentinelOne Singularity

1. **Set up Central Management (Singularity Console)**
   - Request a free trial on the SentinelOne website.
   - Access the Singularity Console (cloud-based) or deploy an on-prem version if provided.
   - Create your account, configure global policies, and define user roles.
2. **Integrate with ELK (Optional)**
   - In the Singularity Console, generate an API token with read access to detections and incidents.
   - Configure a Logstash pipeline to pull detection data from SentinelOne's API endpoints.
   - Adjust Elasticsearch and Kibana to properly map and visualize the

data.

3. **Connect Linux and Windows Clients**
    - **Windows:** Download the SentinelOne agent from the console and install on Windows endpoints using your site token or key.
    - **Linux:** Obtain the .rpm or .deb package from the console and install via command line. Provide the site token for registration.
    - After installation, endpoints appear in the Singularity Console.
4. **Deploy and Configure Agents**
    - Assign agents to groups with the desired policies (e.g., detection-only, detection and prevention).
    - Test threat detections, remote isolation, and automated remediation to verify functionality.
    - Monitor the console or your ELK stack for real-time alerts and security events.

Additional Notes & Recommendations

- **Documentation & Screenshots:**
  For each solution, consult the official deployment guides. These usually include detailed screenshots for agent installation, console navigation, and SIEM integration steps:
    - CrowdStrike: CrowdStrike Documentation
    - Sophos: Sophos Support
    - SentinelOne: SentinelOne Tech Docs
- **Limitations & Considerations:**
    - Trial lengths vary and may require an extension from the vendor if you need more time.
    - While most vendors do not strictly limit the number of endpoints in a short proof-of-concept, confirm your environment size with the vendor.
    - Verify that your Linux distribution is supported before rolling out at scale (common distros like Ubuntu, CentOS/RHEL, and Debian are typically supported).
    - Consider network bandwidth and overhead when sending large volumes of logs to ELK.
    - Ensure you have sufficient disk space on Elasticsearch and robust pipelines in Logstash to handle real-time security data.
- **Selecting the Right EDR:**
    - **Feature Parity:** Confirm that Linux endpoints get the same (or comparable) protection and feature set as Windows endpoints, as some solutions have more mature Windows coverage.
    - **Management Overhead:** Some solutions offer simpler cloud-based

consoles, while others require on-prem deployments.
    - **Budget & Long-Term Costs:** Trials are free, but eventually, you will need to compare licensing models for ongoing usage.
    - **Integration Depth:** If an ELK SIEM is central to your environment, evaluate how seamlessly each EDR solution can push alerts, logs, and telemetry into Elasticsearch and Kibana.

Conclusion

Each of the EDR solutions covered—**CrowdStrike Falcon, Microsoft Defender for Endpoint, Sophos Intercept X, SentinelOne Singularity,** and **ESET PROTECT**—offers free or trial periods, supports Windows and Linux endpoints, and provides either direct or indirect integration pathways to an ELK SIEM environment. They also include a native management console, which is vital for organizations that may not want to rely solely on ELK for operational endpoint oversight.
When deciding which EDR solution best our needs, consider factors such as:

- **Depth and accuracy of threat detection**
- **Automation and remediation capabilities**
- **Ease of deployment and management**
- **Trial limitations and vendor support**
- **Compatibility with existing infrastructure and processes**

By following the step-by-step instructions for central management setup, agent deployment, and SIEM integration (where applicable), your organization can effectively evaluate each solution and choose the EDR platform that strikes the right balance between robust security features, manageability, and cost-effectiveness.