



## **ArmorPoint OpenXDR**

## **Statement of Work**

## Contents

Armorpoint Platform and Technology .....	3
On-premise Intrusion Detection System.....	3
Open Extended endpoint Detection and Response Integration .....	3
Data Collection and Retention.....	3
Network Device Monitoring and Collection.....	3
Third Party / External System Integration.....	4
Managed SIEM Dashboard and Log Analytics.....	4
Armorpoint Security Operations Center (SOC).....	4
Management.....	4
Monitoring.....	4
Alert Definition.....	4
Incident Definition .....	4
Incident Response .....	5
Preparation .....	5
Identification.....	5
Containment.....	6
Eradication .....	6
Recovery.....	6
Lessons Learned .....	6
Standard Implementation Timeline .....	9
Project preparation phase .....	9
Phase I – Project initiation.....	10
Phase II – Deployment and validation.....	10
Phase III – Project Closure.....	10
Non-Standard Implementation Tasks and Timelines.....	10
Hours of Operation - 24x7x365 Support .....	13
Service Guidelines.....	13
Priority Definitions.....	13
Response Target Metrics .....	13
Resolution Target Metrics.....	13



# ArmorPoint OpenXDR Service Scope

## ARMORPOINT PLATFORM AND TECHNOLOGY

### ON-PREMISE INTRUSION DETECTION SYSTEM

For managed on-premise locations, a licensed Intrusion Detection System (IDS) will be provided to Client by ArmorPoint for real-time monitoring of network threats. The fully managed device will include:

- Web / URL Monitoring
- Geolocation Monitoring
- Network-based Antivirus Detection
- Application Control Monitoring
- Intrusion & Threat Detection

### OPEN EXTENDED ENDPOINT DETECTION AND RESPONSE INTEGRATION

ArmorPoint will provide EDR software integration into ArmorPoint. It is the responsibility of the customer to continue to manage and maintain their EDR and licensing needs. It is recommended for the EDR to have the following capabilities for ArmorPoint team to provide remediation services.

- Anti-Malware
- Exploit Protection
- PowerShell and .Net Protection
- Anti-Ransomware
- Remote Control

### DATA COLLECTION AND RETENTION

Data retention policy is as follows unless otherwise specified in Order Form:

- Security Alerts / Incidents / Vulnerabilities / Tickets
  - 365 Days Online and Searchable
- Benign Data (Anything not related to Alerts, Incidents, Vulnerabilities, Tickets)
  - Examples include unrelated Windows Event, Network Device and/or Agent Performance logs, etc.
  - 30 Days Online and Searchable
  - 365 Days Archived and Retrievable

### NETWORK DEVICE MONITORING AND COLLECTION

ArmorPoint will collect syslog from in-scope network devices. This information will be integrated into the SIEM Dashboard for insight into the environment.



## THIRD PARTY / EXTERNAL SYSTEM INTEGRATION

ArmorPoint will collect and event data from in-scope external systems via API or syslog. This information will be integrated into the SIEM Dashboard for insight into the environment.

## MANAGED SIEM DASHBOARD AND LOG ANALYTICS

ArmorPoint will provide a custom SIEM Dashboard for correlation and reporting of collected data and events.

## ARMORPOINT SECURITY OPERATIONS CENTER (SOC)

### MANAGEMENT

ArmorPoint will provide a fully-managed SIEM which includes:

- Platform Health, Security, and Maintenance
- Platform Support
  - User Training
  - Dashboard and Report Customization
  - Alert Rule Generation
  - Event-Handling
  - Log Parsing
- Continuous Device Monitoring
  - Agent Log Collection
  - Syslog Log Collection
  - File Tailing
  - EDR Data Collection
  - Performance Monitoring
  - 3<sup>rd</sup> Party / External Integration

### MONITORING

#### Alert Definition

An Alert is an observable, measurable anomalous occurrence in a system or network. An example of an alert is an instance of unsuccessful logon, system crash, unplanned reboot, degradation in service performance, or network traffic spike. Alerts are monitored, reviewed, and analyzed by the ArmorPoint SOC Team and either confirmed to be benign or escalated to the level of an Incident.

#### Incident Definition

An Incident is an observable, measurable event taking place in a system or network that deviates from the normal behavior and implies harm or threat to do harm. Additionally, an event involving accidental loss of sensitive information is also classified as an Incident. An example of an Incident would be any



unauthorized access and/or disclosure of confidential information, successful or repeated network intrusion attempt, or detection of any unwanted / malicious application or process. Upon confirmation of an Incident, ArmorPoint Incident Response services are invoked.

## INCIDENT RESPONSE

ArmorPoint maintains a Security Incident Response Plan (IRP) that will be reviewed and tested annually. Appropriate training will be provided to any staff with responsibilities as part of the Security Incident Response Team (IRT).

ArmorPoint's SOC bases its IRP on the SANS Institute's Incident Handling methodology. The SANS Incident Handling methodology divides the response process into six phases: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. The basic premise of this methodology is that organizations are constantly in a state of Incident response and are responsible for performing actions based on the phase they are in; the default phase is Preparation.

The Incident response process is determined by the severity level of the Incident. As the impact of an Incident becomes more significant or wide spread, the escalation level increases, bringing more resources to assist in addressing the Incident. At each escalation level, individuals who will be needed at the next higher level of escalation are alerted to the Incident so they will be ready to respond when they are needed. The ArmorPoint SOC maintains 24x7 availability of IT individuals with additional on-call support as required for Incident response and monitoring coverage for any evidence of unauthorized activity, unauthorized system use, and alerts.

### Preparation

The Preparation phase for an Incident takes place before the Incident is identified and establishes the capability to identify Security Incidents in a timely manner and provide guidance to minimize damage from identified Incidents.

The ArmorPoint SOC IRT is authorized to leverage all necessary equipment, communication methods, offices, conference rooms, and other ArmorPoint resources for handling an Incident. This includes contacting all available on-call support personnel.

### Identification

The objective of the Identification phase is to determine if a Security Incident has occurred and determine its severity based on the impact and scope of the Incident.

The ArmorPoint SOC Team is responsible for the monitoring of events and identification of suspicious activity on information systems and networks. The SOC monitors events and alerts from provided security tools and notifies the Client in the event that suspicious activity is identified as per established Service Level Agreements (SLA's) corresponding to determined event criticality.

All Security Incidents / notifications are documented and tracked within the ArmorPoint platform.

Where communication is required, the SOC will reference an Incident Response Plan (IRP) contact list provided by the Client to ensure the appropriate individual or group is getting the appropriate level of communication.



If it is suspected that the email system has been compromised, this communication will not take place via email unless email encryption not controlled by the email server is used. Alternatively, other secure communication methods may be utilized.

### **Containment**

The objective of the Containment phase is to mitigate risk of additional exposure or damage from a Security Incident. Containment efforts may include actions such as quarantining systems, terminating processes, and/or blocking network traffic. All Incident response activities must be carried out in a manner which does not further jeopardize the confidentiality, availability, or integrity of systems and information.

The ArmorPoint SOC Team will provide all available information, to include containment recommendations, to the Client's designated support team prior to implementing changes. In the event containment services are initiated, specific containment steps are at the discretion / approval of the Client.

### **Eradication**

The objective of the Eradication phase is to directly address the Security Incident and eliminate the root cause. Eradication efforts may include actions such as quarantining processes or files, uninstalling software, or creating/modifying firewall rules.

The ArmorPoint SOC Team will provide all available information, to include eradication recommendations, to the Client's designated support team prior to implementing changes. In the event containment services are initiated, specific eradication steps are at the discretion / approval of the Client.

### **Post-Eradication Incident Response Scope**

ArmorPoint OpenXDR includes **five (5)** "use it or lose it" hours per month of the following Incident Response services. Any hours above the use of originating five (5) hours, will be billed at \$300.00/Hour:

### **Recovery**

The objective of the Recovery phase is to resume normal operations and return any compromised systems, applications, and devices into production. After the system has been returned to production, its operation must be monitored to ensure the compromise does not recur and the system(s) are operating properly. Required steps during recovery could include unblocking an IP address, allowing or exempting processes / applications from being blocked.

### **Lessons Learned**

The objective of the Lessons Learned phase is to identify root causes of the Incident and develop a plan for preventing similar Incidents from occurring in the future.

The ArmorPoint team will provide documentation of all Incident Response activity within the ArmorPoint portal. Reporting will include information on how the incident was identified, the impact of the incident, any persons notified of the incident, and steps taken to remediate the incident. Client follow-up will be initiated before incident closure.



Closing meetings should occur no later than two weeks after completion of the Recovery phase. This meeting should review the incident report and is an opportunity to reflect on the incident response process to identify opportunities for improvement.

### Disclaimer

ArmorPoint strongly recommends the Client adhere to the following best practices:

- Install ArmorPoint at all event sources across their network
- Set EDR agent in prevention mode, not detection mode
- ArmorPoint is not responsible for security incidents originating from unmonitored devices. System Requirements are as follows, if system requirements are unable to be met, alternative agentless approach will be discussed with client. (Additional fees may apply)
  - Machine RAM: 4GB
  - CPU: Dual Core 2GHZ Core I3 and above or equivalent
  - Available Disk Space: 1.5 GB Minimum
  - Network Connectivity: Ethernet or Wi-Fi

### End of Life Device and Operating System Risk Acceptance Agreement

The Parties agree to the following relating to End of Life Devices and Operating Systems.

ArmorPoint does not provide SIEM agent installers for end of life devices and/or operating systems.

Trapp recommends all clients upgrade to supported versions as soon as possible.

End of life devices and/or operating systems are unable to continue to be patched from a security perspective and are high risk security profiles for both client and ArmorPoint to support.

With this understanding, Client accepts this risk and acknowledges the following:

- ArmorPoint does not provide installers or collectors for device logs to be collected by the SIEM;
- ArmorPoint will provide EDR agent to devices where an EDR package has an approved installer on specific end of life devices;
- If the EDR agent does not install properly on an end of life device, troubleshooting becomes responsibility of the Client;
- ArmorPoint will provide an EDR agent and installer, but there is no guarantee on performance or protection of those devices;
- Any such non-supported devices are not included in the bucket of support hours provided by ArmorPoint; and,
- Any remediation work specifically tied to end of life devices and/or operating systems will be billed at \$300.00 / hour by Trapp



\*End of Life Devices and/or Operating Systems are defined as any device or operating system that has ended or limited support on the product and/or version from originating manufacturer or software company for maintenance purposes (software updates and security patches) and/or troubleshooting. Find ArmorPoint's current list of [in-scope Operating Systems here](#).

## Client Environment Failures

Client agrees that ArmorPoint will not be liable for any failure to provide the SOC Services if such failure is caused by Client's failure to meet the applicable requirements for each Service. At a minimum, Client is responsible for ensuring the following environmental failures do not negatively impact the Services:

Service interruptions or degradations due to any Client supplied internet or private access whether provided by Client or third parties engaged by Client or equipment when provided by Client or third parties engaged by Client.

Failure or deficient performance of Client-supplied power, equipment, services, or systems.

Client's failure to adhere to SOC recommended configurations on managed or unmanaged equipment that affects the Service.

Failure to provide a secure environment for on-premise devices, including, but not limited to secure mounting/racking, appropriate cooling and air handling, secure from theft, etc.

Service interruptions or degradations in Service caused by a piece of equipment, configuration, routing event or technology required to be operative in order to perform that is under the management and control of Client.







## Implementation

ArmorPoint's Implementation process is delivered in three phases and requires intense collaboration between the ArmorPoint Implementation Team and Client to achieve project success within the proposed 30 to 60 day Implementation Timeline.

Any delays in delivery of Client-owned Deliverables will extend the Implementation duration.

Agreement is effective upon contract start date as designated per ArmorPoint Order Form, by which ArmorPoint will have dedicated environment provisioned.

### Definition of Standard Implementation vs. Non-Standard Implementation

- Standard Implementations hold a 30 day goal timeline to completion.
- Non-Standard Implementations hold a 60 day goal timeline to completion.

A Non-Standard Implementation is defined when any of one of the following are true:

- Client has more than 6 Physical Sites
- Client has more than 750mb of bandwidth utilization at any site
- Client has an international location(s)
- Client requires a to-be-developed custom ArmorPoint integration
- Client has any MAC or Linux Devices
- Client is adding vulnerability scanning to solution
- Client has a Proxy or Private Environment (VDI, Virtual Appliance, Azure, AWS, etc.)
- Client does not have ability to mass deploy to windows devices (using RMM tool, GPO or ability to deploy agent via script)

## STANDARD IMPLEMENTATION TIMELINE

***\* Indicates Client-owned Deliverables. Adherence to Implementation Timeline is dependent upon completion and delivery of Client-owned Deliverables.***

### PROJECT PREPARATION PHASE

- Day (-14): Contract Signature – ArmorPoint Order Form
- ***\*Day (-13): Client Submits Billing and Payment Information, ArmorPoint Confirms all necessary paperwork is completed\****
- Day (-12): Implementation team receives new Implementation request and delivers ArmorPoint Pre-Implementation Checklist
- ***Day (-12 to -7) Client Completes Pre-Implementation Checklist Successfully\****
- Day (-7) ArmorPoint acknowledges successful Pre-Implementation Checklist and Schedules Implementation Kickoff Call directly with client in upcoming week.
- Day (0) Planned for Contract Start Date per agreement – ArmorPoint provides system access for dedicated Client ArmorPoint Environment



- Day (0) ArmorPoint Service Activation

## PHASE I – PROJECT INITIATION

- Day 1: Implementation Kickoff Meeting with Client Completed
- Day 1: ArmorPoint Agent and MDR Agent Delivered to Client
- Day 1: Instructions for Self-Service Integrations Provided to Client
- Day 2-14: ArmorPoint Configures Network Sensor Device for Client
- Day 15: ArmorPoint Network Sensor Shipped to Client

## PHASE II – DEPLOYMENT AND VALIDATION

- **Day 15: Client Deployment of ArmorPoint Agents and MDR Agents Completed\***
- **Day 15: Client completes configuration of self-service integrations\***
- **Day 16: Client Enables Detection Policy on MDR Agents\***
- Day 17: ArmorPoint Validates Successful Deployment of Agents + Integrations + Policies
- **Day 25: Client Installation Deployment of ArmorPoint Network Sensor Completed\***
- Day 26: ArmorPoint Validates Successful Deployment of Network Sensor

## PHASE III – PROJECT CLOSURE

- Day 30: ArmorPoint Closing Call Completed & Account Management Transition
- **Day 31: Client signs off on Project Closure Report and Provides Feedback\***

## NON-STANDARD IMPLEMENTATION TASKS AND TIMELINES

\*Non-Standard Timelines below will be added into the process above, but should keep overall delivery timeline at 60 Days start to completion

- +14 Day Delivery Timeline for Network Sensor Configuration and Shipping if above 6+ Network Sensor Quantity
- +7 Day Delivery Timeline for Network Sensor Configuration and Shipping with greater bandwidth throughput
- +30 Day Delivery Timeline for Network Sensor Configuration and Shipping for International Sites
- +14 Day Delivery Timeline for Manual Installation of Agents on MAC/Linux Devices
- +14 Day Delivery Timeline for Vulnerability Scanning Setup
- +30 Day Delivery Timeline for setting up syslog forwarding for proxy or private environments
- +30 Day Delivery Timeline for Clients needing to manually install agents on Windows Devices
- (Needs Resource Scoping) for Custom Integration Development



## Contractual Changes

This SOW may change and ArmorPoint may update this SOW from time to time. It is your responsibility to check this SOW periodically for changes.

The following Governance structure defines the Contract Change Process:

Change To	Vehicle	Process
Service scope	Change of scope presented with justification and supporting data. Changes that cause a change to the monthly cost to Client of more than \$1,000 will require further Executive Approval through a Contract Change process.	Order Form
New project or effort	Each proposed effort or initiative will be presented to executive leadership and/or board with supporting charter, solution outline and estimates.	Order Form
Change to the overall service requirements and performances	Each change will be presented to the Executive and be processed with further Executive Approval	Contract CCR or Addendum
Change to the scope, terms and conditions of the current	Each change will be presented to the Executive and be processed with further Executive Approval	Contract Addendum

## Exclusions

The following exclusions apply to the scope of the work stated above and have been incorporated into the pricing stated below:

- Any work or services not expressly provided for herein
- Any application development or integration efforts not expressly provided for herein
- Any actual hardware purchases for on-premise needs
- Any migration or upgrade of infrastructure (servers, network, etc.)
- Any actual implementation of the recommendations made by ArmorPoint unless specified in this document
- Any efforts tied to re-installing OS due to virus or malware or any system instability after the removal of a virus
- Any work related to being crypto-locked. ArmorPoint will work to mitigate the spread by blocking at the edge and/or taking machines offline
- Any data recovery and forensics work due to purposeful or malicious Client or application errors
- Any software license or physical hardware expenses
- Any software license that's not explicitly mentioned, and not covered by ArmorPoint
- All Travel and lodging costs
- Any fees related to shipping, handling, customs, duties and/or taxes
- Any additional work requested beyond the scope of this Agreement will be expressly set forth by subsequent agreement, including, but not limited to, a Contract Change Request ("CCR")





## Service Level Agreement

The following constitutes the reference for performance and expectations regarding this entire agreement. Updates to the Service Level Agreement will automatically become enforced upon their execution or approval by both Client and ArmorPoint unless specified otherwise.

### HOURS OF OPERATION - 24x7x365 SUPPORT

#### SERVICE GUIDELINES

The ArmorPoint Service Desk uses a Triaged Response Metrics system to prioritize Client Alerts or Incidents. The below Triaged Response Metrics outlines our standard service level commitments for communicating the Alert or Incident status to Client.

#### PRIORITY DEFINITIONS

Priority of a ticket is defined by its impact and urgency. Impact and urgency are determined according to the chart below and assigned by ArmorPoint:

	Urgency		
Impact	Tertiary System	Secondary System	Core Business Service
All users	High	High	Critical
Group of users	Medium	High	Critical
One User	Low	Medium	High

#### RESPONSE TARGET METRICS

ArmorPoint's definition of a "response" is the time it has taken a SOC analyst to start an investigation after an alert or incident has been created.

Priority	Response Target
High or Critical Priority	30 Minutes
Medium Priority	2 Hours
Low Priority	4 Hours

#### RESOLUTION TARGET METRICS

Resolution targets are best effort with priority given based on severity.



#### Revision History

<u>Document Version</u>	<u>Published Date</u>	<u>Description or Notes</u>
5.1	11/30/2022	Initial Version

