Canon | SUPRAITS MANAGED IT SERVICES PARTNER

Statement of Services

Supra ITS Extended Detection and Response (XDR)

Purpose of this Document

This document represents the scope of included services of Supra ITS (Provider) Extended Detection and Response and the respective deliverables and unique features of the included services.

Extended Detection and Response [SEIM, SOAR, Identity Protection] (XDR)

Scope: Provider delivers a comprehensive Security Information and Event Management/Extended Detection and Response (SIEM/XDR) service, offering centralized Log Management, Identity Monitoring, Real-time Monitoring, Cloud Threat Hunting & Containment, Event Correlation, Threat Detection, Compliance Reporting, and Dark Net Exposure Monitoring. Supported by a 24x7 Security Operations Center (SOC), the service leverages Security Orchestration, Automation, and Response (SOAR) capabilities to enhance Client's security posture across endpoints, networks, cloud environments, and web services. Automations include rapid response actions such as email and account protection, cloud visibility and response, web services monitoring, and network response (e.g., auto-blocking of threats). This turn-key solution provides full visibility into Client's environment, proactive threat hunting, and streamlined compliance reporting, with all activities tailored to the specified assets and systems.

Deliverables:

- Centralized log ingestion and analysis from Client's specified systems (e.g., network, endpoints, cloud), with real-time event correlation and threat detection enriched by threat intelligence.
- Real-time monitoring and identity monitoring, with automated alerts and escalation to Client for critical incidents.
- Cloud threat hunting and containment, including visibility into cloud environments and automated response actions to help mitigate risks.
- Network response capabilities, such as auto-blocking of malicious IPs or domains, and web services monitoring to protect online assets.
- Email and account security automations, including containment of compromised credentials and rapid response to phishing or account-based threats.
- Dark Net Exposure Monitoring to identify and alert Client of compromised data or credentials surfacing on the dark web.
- Compliance reporting tailored to Client's regulatory needs (e.g., PCI DSS, etc.), delivered as part of monthly performance reports.
- Monthly reports delivered via email or Account Manager, including key metrics such as detected threats, response actions, automation outcomes, compliance status, and SOC insights, with dashboard access provided for real-time visibility.

Unique Features:

- Client will ensure system compatibility (e.g., API access, log forwarding capabilities) and provide necessary permissions for SIEM/XDR deployment within 5 business days of, as applicable, order or SOW execution.

- Usage and Counts: based on total number of log Sources (e.g. Endpoint, server, network device, cloud service each constitute a "source")

On-Boarding Services

On-Boarding Services are required services that fast-track value by installing agents, tuning detections and handing your team clear policies and training materials.

General Provisions for All Services:

- **SLO Response Times:** Provider will respond to incidents or inquiries based on the following priority levels, measured from detection or notification:

Priority Level	**Example**	**Response Time**
Priority 1 (Critical)	active malware outbreak, data breach in progress, etc.	15 minutes
Priority 2 (High)	Suspicious activity, critical system alerts, etc.	30 minutes
Priority 3 (Standard)	Routine inquiries, low-risk alerts, etc.	4 hours

- **Service Availability:** Services are provided 24x7x365 with a target uptime of 99.9%, excluding scheduled maintenance per MSA terms.
- **Reporting:** Delivered monthly, via email, performance reports will be provided for all active services, detailing key metrics as outlined per service.
- **Escalation:** For incidents requiring Client input or approval, Provider will escalate to Client within 1 hour of identification by the SOC,
- **Client Communication:** All monthly reports will be delivered via email or via an Account Manager.

Client and SupraITS Responsibilities

- **SupraITS Responsibilities:**
    - Deploy, configure, maintain, and manage selected services as outlined in the Service Description.
    - Monitor and respond to incidents per the SLO Response Times in the General Provisions.
    - Deliver reports and notifications as specified per service.

- **Client Responsibilities:**
    - Provide all required system access, permissions, and initial asset/user lists within 5 business days of SOW execution, unless otherwise specified.
    - Respond to escalations from Provider for incidents requiring Client input or approval, unless otherwise agreed within a timeframe in accordance with our onboarding checklist, to facilitate timely decision-making and resolution.
    - Per the MSA, Client agrees to maintain any installed agent, hardware, or software as part of any service in an active, unaltered state throughout the Term and to promptly notify Provider of any issues affecting its functionality. Failure to comply may result in suspension of affected services up to and including termination of the contracted service.
    - Provider shall not be liable for any service failure, delay, or resulting damages to the extent caused by Client's negligence, including but not limited to failure to fulfill the responsibilities outlined herein (e.g., delayed access, unauthorized modifications to systems, or untimely responses to escalations), as further detailed in Exhibit A where applicable.
    - Provide a designated point of contact for all services.

Covered Items

This statement of Services applies to the following items:

7489C011 - SupraITS - Extended Detection and Response, Includes SIEM, SOAR, XDR, Dark Web Monitoring - Min 50 Sources - #010300601001

Any product, service, or deliverable not expressly set forth in the foregoing is out of scope of this Service.

About Supra ITS

Supra ITS, a Canon IT Managed Services partner, is based in Canada, established in 1999 and blends deep enterprise know-how with a “customer-first” mindset to deliver everything-as-a-service for growing organizations. Supra ITS has offices in the US, UK, India and Canada. More than 200 certified professionals operate four tier-3 data centers and run tightly integrated 24 × 7 SOC and NOC teams, so clients get prompt, around-the-clock support. The company’s portfolio spans managed IT and cloud, cyber-security, business-process outsourcing, and custom application development, all backed by top-tier credentials and strategic alliances. This combination of scale, pedigree, and nimble execution lets Supra ITS safeguard critical workloads, speed digital transformation, and simplify compliance.

Canon U.S.A., Inc.

Canon is a registered trademark of Canon Inc. in the United States and may also be a registered trademark or trademark in other countries. All other trademarks and product and service names are the property of their respective owners. Neither Canon Inc. nor Canon U.S.A., Inc. makes any warranty or representation as to any third-party product, service, or feature referenced herein. Due to the constant development of new network attack techniques, neither Canon Inc. nor Canon U.S.A., Inc. nor Supra Canada Technologies Ltd. can guarantee your systems will be free from vulnerability to intrusion or attack. All partner and partnership references or implications herein are outside the scope of the Uniform Partnership Act and similar laws. Canon U.S.A. does not provide advice concerning customers' legal or regulatory compliance. Customers should consult with qualified counsel to determine if they are in compliance with applicable law.