simpleplan it

Overwatch Managed Security Services

Service Level Target Summary

This Service Level Target (SLT) applies to the Incident response commitments for all Overwatch Managed Cybersecurity services. Incident response times vary according to the priority level assigned to the incident. The priority level is a computed value based upon both impact and urgency.

1 Incident Response Times

The following table describes the various priority levels and Service Level Target commitments (SLT). The start of the process originates when an incident is opened via the Overwatch Ticketing System.

Commitment	Definition	Priority	Objective	Quarterly Measurement
Incident Response				
Incident Response is measured from receipt of notification via Overwatch Ticket System.	Notification to Incident	MAJOR	<=30 Minutes	90% Aggregate
		CRITICAL	<=15 Minutes	
Incident Assignment				
Incident Assignment period is measured from the time the incident has been opened.	Notification to Incident	MAJOR	<=30 Minutes	90% Aggregate
		CRITICAL	<=30 Minutes	

- SLT timer begins immediately when a system alert is created.
- SLT timer is paused when ticket status is changed to Pending.
- Overwatch Patch Managed Service is governed by the availability of the vendor release of updates, testing, and criticality.

2 Exclusions

- Scheduled or planned downtime
- Conduct of Customer
- Downtime resulting from the actions or inactions of Customer or third parties with whom Simple Plan IT has no direct contractual arrangement
- Service interruptions, deficiencies, degradations or delays due to access to site restrictions (physical or electronic), CPE, planned or unplanned maintenance, or removal of service
- Waiting on Customer
- Changes due to government regulations
- Force Majeure conditions
- Customer employee work causing issue
- Outage of service due to reliance of non-supported item(s)
- Waiting on 3rd Party
- Failure of performance of power, equipment, services, or systems

simpleplan it

Are You Ready to Simplify Cybersecurity?

info@simpleplanit.com | www.simpleplanit.com | 614-484-0918

3 SLT Compliance and Reporting

SLT compliance and associated remedies are based on fully functional network environments, Internet and circuit connectivity, and properly configured servers. If SLT compliance failure is caused by reasons other than those directly within SPIT control, such as failure of CUSTOMER owned hardware or software, all SLT remedies are not applicable. SPIT will provide SLT compliance reporting through requested reports.

4 Internet Emergencies

In the event Overwatch Managed Cybersecurity experiences an Internet emergency, it is SPIT's objective to notify each CUSTOMER'S specified point of contact, per your specific playbook, via phone or SMS Text within sixty (60) minutes of emergency declaration. This notification will include an Incident tracking number, telephone bridge number, and the time that SPIT will conduct a situation briefing. The Overwatch Security Delivery Appliance (SDA) has the capacity to store logs for up to 24 hours. SPIT will not be able to process network flow or syslog data until all required systems are back online.