Managed Security Services - Addendum

Submitted By

Alan Jones

Layer 3 Communications, LLC

1450 Oakbrook Drive, Suite 900

Norcross, GA 30093

(770) 225-5300

3/29/2023

This report contains proprietary and confidential information. It is not to be released or disclosed, in whole or in part, other than to those individuals who are directly involved in evaluating this report, without the prior express written consent of Layer 3 Communications and Dekalb County Government. The logos in this document are the property of the respective entities.

Table of Contents

Revision History

Version	Date	Author	Sections Changed and Synopsis of Changes
1	March 29, 2023	Alan Jones	Original Draft
2	March 29, 2023	Ryan Greene	Edits

1 INTRODUCTION

Layer 3 Communications is a professional services firm specializing in wired and wireless data networking, data center design and implementation, and information security. Founded in 1998, Layer 3 Communications is based on the principal that the highest levels of expertise and professionalism are the keys to ensuring happy clients. The organization, headquartered in Norcross, GA, has locations across the southeastern United States. Our offices are located in Texas, Alabama, Tennessee, Georgia and the Carolinas.

Layer 3 Communications' value to our clients is in our technical expertise and professionalism. Our technical services staff outnumbers our sales and operations personnel by a ratio of 3:1. We maintain the highest level of certifications with our manufacturer partners, and in many cases provide technical support to our clients on their behalf. Our three areas of expertise include:

Wired and Wireless Data Networking

Layer 3 Communications data networking practice is one of the three core service offerings of our firm. A cornerstone of the business since its founding, Layer 3 Communications provides the highest quality turnkey network implementations for our clients. From simple hardware refreshes to complete network redesign, management and support, our network engineers work with some of the largest and most complex networks in the region.

Information Security Services and Consulting

A natural complement to Layer 3 Communications data networking offering is our expertise in information security services and consulting. Our security engineers continually train with our manufacturer partners to ensure the highest levels of expertise with their products. In addition, our managed services and consulting teams research modern attacker tools and techniques on an ongoing basis. This ensures that we are able to address the ever-evolving threat landscape effectively for our clients.

Data Center Design and Implementation

The technology industry's shift to horizontally scaled, software-based data center solutions has allowed for tremendous efficiencies to be gained. However, this increased efficiency has come at the cost of ever more complex environments. Our data center expertise allows Layer 3 Communications to assist our clients in ensuring that they are not only getting the best value for their data center investments, but also ensures that the systems built are high performance, scalable, and stable.

Building Next Generation Networks, One Layer at a Time

2 Executive Summary

DeKalb County is located in the north central portion of the U.S. state of Georgia. As of the 2020 census, the population was 764,382, making it Georgia's fourth-most populous county. Its county seat is Decatur. In recent years, some communities in North DeKalb have incorporated, following a trend in other suburban areas around Metro Atlanta. Dunwoody and Brookhaven are now the largest cities that are entirely contained within the county.

Dekalb County Government (DCG) has asked Layer 3 Communications to produce a proposal for providing security monitoring and element management services for their information technology assets. Security monitoring services will be run out of Layer 3 Communications' Norcross headquarters Security Operations Center (SOC). Layer 3 Communications SOC engineers will perform 24 x 7 x 365 alerting. Layer 3 Communications will alert DCG's IT staff based on the SLA required, time of day, location of the IT asset, and responsible party. Layer 3 Communications will also meet on a periodic basis with DCG's information technology staff to report on the health and security posture of the monitored network assets.

This document is an addendum to the previously executed Managed Security Services document, and should be read in the context of the entire service offering.

A detailed explanation of these services and their associated costs is included in the "Scope of Work" and "Pricing Table" sections of this document. We are prepared to begin within two weeks of written authorization to proceed. Thank you for your continued interest in Layer 3 Communications and the products and services that we provide. We are pleased to have the opportunity to present this proposal to Dekalb County Government for your review.

3 Scope of Work

The following section defines the details of the scope of work to be performed by Layer 3 Communications on behalf of Dekalb County Government.

3.1 Security Monitoring Services

Layer 3 Communications will provide Security Information and Event Management (SIEM) services to Dekalb County Government using our in-house security monitoring platform. This solution is offered as a replacement for Dekalb County Government's existing Rapid7 InsightIDR solution. Layer 3 Communications will configure Dekalb County Government technology assets to forward logging telemetry to the existing on-premise collection appliance. This telemetry data is normalized, compressed, and correlated against a broad and growing rule set to search for security anomalies. Should a security or performance issue arise it is investigated and triaged by our SOC team, based on service level.

3.1.1 Activities

In the course of providing security and performance monitoring services to Dekalb County Government, Layer 3 Communications will:

- Meet with Dekalb County Government information technology staff to discover relevant network information to provide an optimized security monitoring environment
- Take the results of the IT staff discussion, and incorporate the information into our security monitoring ruleset
- Determine the additional requirements of Dekalb County Government regarding notifications and escalations, as related to host-based alerts
- Incorporate the additional requirements into the standardized playbook that is used for Dekalb County Government security incidents
- Conduct an activation activity in conjunction with Dekalb County Government IT staff to ensure that appropriate connectivity and alerting have been established.
- Depending on services level, perform the following:
  - Configure covered elements to forward telemetry
  - Provide Dekalb County Government IT staff with relevant configuration for covered elements, including syntax, files, or software agents as appropriate
  - Assist with logging agent installs (if required)
  - Assist with log forwarding configuration for applicable devices
- Validate that covered devices are sending telemetry appropriately

- Over a 3-month period, conduct weekly discussions with Dekalb County Government IT staff to optimize alerting for their environment
- After 3 months, perform routine monitoring and alerting according to the process defined in the Dekalb County Government playbook
- Establish quarterly meetings with Dekalb County Government staff to provide updates on their environment, suggest improvements, and report performance

3.1.2 Onboarding and Tuning

After initial installation, Layer 3 Communications will provide tuning and onboarding services. These efforts generally occur over a 30-day span. Tuning will be an iterative process of defining and winnowing down security events to eliminate false positives. Onboarding will consist of the creation of playbooks, dashboards and reports specific to Dekalb County Government's environment. Layer 3 Communications Security Operations Center (SOC) Engineers will provide onboarding and tuning services in conjunction with DevOps engineers. During tuning and onboarding, Layer 3 Communications will work with Dekalb County Government to:

- Developing allow lists of permitted activities
- Apply appropriate security rules, based on design conversations above
- Define and winnow down security events
- Reduce false positives
- Refine parsers (if required)
- Develop SOC playbooks for incident handling (severity/time of day)
- Review Security Incident Reports (SIR)
- Review P1 (priority 1) security procedures
- Provision SIEM dashboard – including remote training (if required)
    - Incident Overview
    - Network Incidents
    - Host Incidents
- Create Executive reports

3.2 Security Operations (SOC) Services

To complement our Cloud SIEM Service, Layer 3 Communications will provide Security Operations (SOC) services for Dekalb County Government for elements covered in section 3.3. This service is provided from Layer 3 Communications operations center in Atlanta, Georgia, USA. These services will commence once the above SIEM service is fully deployed and onboarded.

For equipment listed in Section 3.3, Layer 3 Communications Operations Center staff will:

- Provide security monitoring and notifications for SIEM related incidents
- Provide Incident Reports based on the result of SIEM alerts
- Provide online ticketing for SOC events
    - Auto-generation of ticketing
    - Online tracking of ticket status
    - Stale ticket escalation
- Provide SOC dashboards based off onboarding requirements
    - Custom dashboards are available but may require additional SOW and fee
- Document change control and approval processes
    - For incident response execution only
- Provide Quarterly Business Reviews (onsite or remote at customer request)
    - Review ticketing
    - Review upcoming changes
    - Make recommendations for improvements to security hygiene

3.2.1 SOC Service Level Agreements

Layer 3 Communications will provide managed services for the devices listed in 3.3 in accordance with the following service levels.

- Security Incident Report – in accordance with priority levels listed below
- Moves/Adds/Changes – based on separate Element Management Contract, with the exception of the Trellix Endpoint Security Manager.
- Documented Change management process

Layer 3 Communications will keep Dekalb County Government appraised of all security incidents and provide regular reports detailing operational status of the network. Layer 3 Communications uses the following service level definitions for ticket workflow:

- High Priority (P1) – Critical security incident or service impacting outage – immediate notification upon identification of issue and root cause analysis report within 8 hours of remediation
- Medium Priority (P2) – Major security incident or severely degraded services – notification within 2 hours and root cause analysis report within 24 hours of remediation
- Low Priority (P3) – Minor security incident (e.g., false positive review) – notification within 24 hours

- No Priority (P4) – Non-service impacting request (e.g., allow list or SIEM rule creation) – acknowledgement within 24 hours and completion within 72 hours (assumes manufacturer engagement is not required)

3.2.2 Covered Elements and Service Levels

The following devices will be covered by Layer 3 Communications' security and performance monitoring services with the associated service level. Please note these are in ADDITION to the data sources in the existing security monitoring agreement.

- Approximately 9000 end users
- Estimated 1000 events per second (EPS) throughput, in addition to existing telemetry
- Data retention requirements as follows:
    - 90 days "hot" (indexed, and ready for immediate search)
- High Availability; currently not required.

Further, we expect to collect data from the following additional sources:

Name	Device Type	Quantity
Microsoft Windows	Operating System	5024 sources
InfoBlox DDI	DDI Appliance	1 log source
Trellix Endpoint Protection	Endpoint Security	Alerts Only Ingestion and Element Management

Table - Log Sources

4 CLIENT REQUIREMENTS

With the understanding that any managed service agreement is a partnership, certain requirements will be placed at Dekalb County Government to ensure that Layer 3 Communications provides the best possible service to the organization. DCG will be responsible for providing:

- Appropriate staff/resources during the initial data gathering phase including but not limited to, network administrators, engineers, and technicians if a survey is required.
- Any passwords required
- Any community or naming conventions
- Remote access, where required, to finalize configuration and deploy of the managed service solution
- Contact list information based on SLA, time of day and severity for element and interface issues
- Allowed re-configuration of monitored network elements to send alert information to Layer 3 Communications Security Operations Center (SOC)

4.1 Assumptions

The following assumptions have been made by Layer 3 Communications:

- Quarterly reviews are required and will facilitated by the Layer 3 Communications account teams
- Any monthly reporting will begin after the first quarterly review to allow for a baseline to be established. All subsequent monthly reporting will include any deviation datasets, general network trend data and recommendations
- Proactive alerting will begin after the first quarterly review to allow for a baseline to be established. Once established, the Layer 3 Communications NOC will investigate elements that exceed pre-defined thresholds and respond accordingly
- While a managed security service significantly improves the security posture of an organization, it is not a guarantee against data breaches. Layer 3 Communications provides the services detailed in this document on a best effort basis.
- The contract will be initiated based on the total number of elements on the current support contracts excluding all software licenses
- Any additional elements discovered will be added to the contract at a predetermined per element costs
- Any ‘net new’ purchase will include co-termed SOC services; on the net new quotes / orders to Dekalb County Government

- Any replacement purchase will inherit the outgoing elements SOC service; Dekalb County Government to notify Layer 3 Communications of decommissioned electronics
- Layer 3 Communications and Dekalb County Government will adhere to change control process to ensure that all elements are monitored correctly.
  - Dekalb County Government will notify Layer 3 Communications SOC of element moves, adds, or changes that are not part of a joint Dekalb County Government /Layer 3 Communications project
  - Layer 3 Communications engineers will notify the Layer 3 Communications SOC of any project related moves adds or changes
  - Layer 3 Communications SOC will recognize all moves, adds, or, changes and report to both Dekalb County Government administrators and the Layer 3 Communications account team
  - Layer 3 Communications SOC will review all changes as part of the quarterly review process

5 ASSUMPTIONS

The following assumptions have been made by Layer 3 Communications:

- Quarterly reviews are required and will be facilitated by the Layer 3 Communications account teams.
- Any monthly reporting will begin after the first quarterly review to allow for a baseline to be established. All subsequent monthly reporting will include any deviation datasets, general network trend data and recommendations.
- Proactive alerting will begin after the first quarterly review to allow for a baseline to be established. Once established, the Layer 3 Communications SOC will investigate elements that exceed pre-defined thresholds and respond accordingly.
- While a managed security service significantly improves the security posture of an organization, it is not a guarantee against data breaches. Layer 3 Communications provides the services detailed in this document on a best effort basis.
- Layer 3 Communications and Dekalb County Government will adhere to change control process to ensure that all elements are monitored correctly.
    - Dekalb County Government will notify Layer 3 Communications SOC of element moves, adds, or changes that are not part of a joint Dekalb County Government /Layer 3 Communications project.
    - Layer 3 Communications engineers will notify the Layer 3 Communications SOC of any project related moves, adds, or changes.
    - Layer 3 Communications SOC will recognize all moves, adds, or changes and report to both Dekalb County Government administrators and the Layer 3 Communications account team
    - Layer 3 Communications SOC will review all changes as part of the quarterly review process.

6 PRICING TABLE

Customer: DeKalb County Government Proposal No.: RG-230329-01

Address: 3630 Camp Circle Proposal Date: March 29, 2023

____

Decatur, GA 30032

Attn: Vernon Greene

Telephone: (404) 780-4105

Email: vgreene@dekalbcountyga.gov

Managed Security Services - Addendum	Notes	Pricing
• L3-SEC-MGD-SVCs	*Please refer to the statement of work contained within this proposal*	$149,782.56
• Onboarding-SIEM/SOC	*One Time fee*	$6,500.00
	Total:	**$156,282.56**

DeKalb County Government's Approval: __________________ Date: ____________________

Please Print Name ________________________________ P.O. Number ____________