CITY OF JOPLIN MISSOURI

REQUEST FOR PROPOSAL NO. 2021-RFP-11: Co-Managed Network Services & Upgrade

COPY

AUGUST 20, 2021

RAVENii LLC | 9664 MARION RIDGE, KANSAS CITY, MO 64137

RAVENii

RFP NO. 2021-RFP-11 | CONTENT REQUIREMENTS

Company Profile

A. Firm name and business address, including telephone and facsimile numbers, and e-mail address.

RAVENii, LLC
9664 Marion Ridge
Kansas City, MO 64137

844-317-0944

inquiries@ravenii.com

B. Year established (include former firm names and year established). Identify the country and state in which the firm was incorporated or adopted.

Established 2014 | United States | State of Missouri

C. Provide the Firm's type of ownership and, if applicable, parent company or subsidiaries. Include dates of any corporate mergers and/or acquisitions, including all present and former subsidiaries with dates of any and all restructuring since the founding date. Also, provide any licensure in Missouri.

State of Missouri | Certificate of Organization
State of Missouri | Corporate Division, Certificate of Good Standing

D. Clarify the business address and telephone number of the office(s) at which the work is to be accomplished (if different than item #A). Also include the 4 name, address, and telephone number of the project manager, if different than item A.

RAVENii Project Manager
Heidi Stokes
913-953-7700

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

Organizational Structure

RAVENii was launched in 2014 bringing decades of front-line experience across many domains of cybersecurity, while harnessing the power of its global network of seasoned security experts to keep abreast of the ever-changing threat landscape. Today, RAVENii supports data centers, school districts, public municipalities, non-profit organizations, transportation, utilities, manufacturing, financial, and healthcare organizations with its "Gray Matter" approach to cybersecurity in an unceasing effort to improve our customer's security posture.

The RAVENii team has over 100+ years of combined experience in designing, implementing, and operating secure network monitoring and infrastructure. We provide a complete suite of security services tailored to our specific customer needs.

Security Audit & Compliance Experience

- FFIEC since 2004
- PCI since 2003
- CJIS since 2003
- GLBA since 2005
- NIST is the foundation of all the above.
- RAVENii's deep understanding of regulation and cross alignment allows us to be extremely efficient in audit process, remediation, and advisory services.

RAVENii serves as the subject matter expert and advisor for security and compliance for all our active clients. Our U.S. based and geographically diverse SOC team is monitoring network environments, actively alerting on critical anomalies, and advising on remediation efforts with our clients daily.

RAVENii's team of skilled professionals works diligently and efficiently to meet deadlines for onboarding and implementation, provide timely and meaningful reporting, and stay within the budget. RAVENii has a seasoned team of network engineers, to ensure that the security configurations for the City's environment are designed to be scalable.

We have worked with multiple municipalities across the nation to improve their security posture, responsiveness, and cost efficiencies and we pride ourselves on being vendor agnostic. Being vendor agnostic allows RAVENii to be agile. We can leverage the experience we've accumulated over the years of monitoring and managing our clients' security programs to better serve and solve pain points faster for our entire client pool.

Our number 1 goal is to make sure our customers are maximizing their existing investments in information and security technology. Considering the recent increase in adversarial maneuvers against municipalities, RAVENii plans to take a risk-based approach to securing the City's environment. Our advisory team will walk you through the right steps to take and best practices to follow when rightsizing and protecting your infrastructure.

RAVENii is focused on fortifying the City of Joplin's security landscape and protecting your constituent's data from potential cyber-attacks. We've got you covered on all things cybersecurity so you can focus on your strategic goals and initiatives.

RAVENii has a team dedicated to providing security & SOC monitoring services to city municipalities. This team is comprised of several members of the RAVENii staff with diverse areas of expertise to ensure The City of Joplin's needs are met. RAVENii's City Team is ready to serve the City with 24x7x365 monitoring and alerting along with strategic planning concerning infrastructure and growth and potential redesign to ensure security monitoring integration and best practices are included.

The team listed below will all be available to assist The City of Joplin at any time during our contracted agreement.

RAVENii's City Team:

Jeff Shipley | CEO & Executive Sponsor
Michael Yelland | Chief Security Officer & Executive Sponsor
Eric Helm | VP of Network Engineering & Architecture & Executive Sponsor
Ashley Bell | Senior SOC Analyst
David Griffin | Senior SOC Analyst
Ray Panfil | Senior Information Security Advisor
Travis Salsbury | SOC Manager
Heidi Stokes | Cybersecurity-Business Development Executive & Project Manager

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

Key Staff Resumes

RAVENii will also assign a team to work directly with the City of Joplin so they can become intimately familiar with the City's resources and infrastructure.

Key Company Representatives:
SOC Manager | Travis Salsbury
Senior SOC Analyst | Ashley Bell
Senior SOC Analyst | David Griffin

RAVENii's City Team Resumes:

JEFFREY S. SHIPLEY, CHIEF EXECUTIVE OFFICER

Summary:

25 years of proven change agent with extensive experience in all aspects of information technology and executive leadership in healthcare insurance. Vast experience with technology platforms, vendor relations, information security, customer service and an in-depth understanding of emerging technologies.

Experience:

Leadership

Served as CEO for an Innovation/Cloud Strategy consulting company that he co-founded. Corporate spin-offs and emerging startups looking to rapidly accelerate the growth of new business models. They are a strategy collective focusing purely on getting the biggest idea to market fast.

Also served as Vice President and Chief Information Officer of Blue Cross and Blue Shield of Kansas City. In this role, Jeff is responsible for leading a responsive IT organization that consistently and efficiently delivers results by aligning technology with business goals while providing business/system high availability and performance.

Additionally, serves as Chairman of the Operations Committee, sits on the Board of Directors for Big Brothers and Big Sister of Kansas City, and the President of the Odessa Optimist Youth Wrestling Board.

Education, Certifications & Qualifications:

Bachelor of Science Degree in Actuarial Science
Master of Business Administration

MICHAEL YELLAND, CHIEF SECURITY OFFICER

Summary:

30 years of extensive experience in compliance and regulations, creating and deploying secure network solutions, systems, and information assets.

Experience:

Compliance

Provide network security support and compliance support to two (2) cooperative companies and their 47 power generation and distribution companies located in the Midwest.

Network Security Solutions

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

Certified Tenable Consultant 1999, Providing advisory on implementation of security center and proper methodology of vulnerability analysis SCADA, industrial IOT and Integrated control systems as it Relates to Utility's, Medical, and Transportation industries. Contributor to Digital Bond Tenable Nessus Policy Audits and its plugin ongoing development and application to Utilities and Industrial controls, Tenable Passive Vulnerability Management for Scada and Threat Identification as it relates to Utilities, and Transportation, NIST of FS-Test of FTK and Dc3dd imaging standards. Continued contributor and spokesperson for the UK and US Cyber Senate ICS, Railways, Nuclear Cyber Security Summit, PLC Cyber Security Research, Smart Meters, Smart Grids, and Utility Radio Mesh Networks. The key incident response team leader for proactive and post-incident response, Real-time incident response, system classification, containment, remediation, and forensic analysis based on enterprise and SCADA attacks.

Deployment

Architect and consulting for SIEM deployment and security operations center for SCADA, ICS, IIoT and Industrial Operation Technology (OT). Technical consultant and architect of core MSP products and hosting solutions (Tenable Security Center, Rapid 7 Meta Pro, Alien Vault SIEM deployment, cloud deployment).

Information Security Consultant

Provide consultation on the establishment of OT baseline assessment, strategic vision and gap analysis for complex enterprise and legacy OT security plans. Produced executive roadmaps for continuous improvement teams, technology, and processes, which resulted in increased capacity to withstand cyber-attacks, as measured by annual sophisticated attack simulations and Penetration Testing. Also, developed training materials and instruction courses for customers in ICS identification and risk management, offensive security team practices, vulnerability management plans, and data forensics laboratories; manages the preservation, acquisition, inspection, analysis, and reporting of digital evidence.

Education, Certifications & Qualifications:

Tenable Certified Security Professional
Rapid 7 Metasploit Certified Specialist
Rapid 7 Nexpose Certified Administrator
Defcon Security
HIPPA
COBIT
NIST
GLBA
PCI
FFIE
NERC/FERC
Centriq, Certified Ethical Hacker
VMware V-Deploy Secure and Analyze
American Bankers Association, Gramm-Leach-Bliley Act
America Bankers Association, FFIEC Safety, Sound Audit, and Compliance
Centriq, CISSP

ERIC HELM, VP of NETWORK ENGINEERING & ARCHITECTURE

Summary:

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

16 years of experience in the development, design, implementation, security and support of IP data, voice, and video networks.

Experienced with multiple technologies in both service provider and enterprise campus environments including IP Routing, Ethernet Switching, Data Center Ethernet, Wireless LANs, Network Security/Firewalls, VPNs, IP Video, and VoIP.

Experience:

VP Engineering/Security Analyst

Manage & develop technology and processes for managed security services. Penetration testing, threat intelligence, incident response, security event/log analysis.

Senior Systems Engineer

Systems Engineer providing network design, configuration, security, documentation, and troubleshooting. Responsible for large scale IP and IP/MPLS network implementations. Design and implementation of complex firewall, VPN and IPS systems.

Network Engineer

Lead engineer overseeing the install and configuration of LAN/WAN networking equipment. Managed the deployment of several carrier class networks including broadcast IP Video and Voice over IP for over 10,000 subscribers in a service provider environment. Primary engineer for firewall and DHCP/DNS security in the ISP network.

Internet Technology Specialist

Participated and managed the design and implementation of several large, fixed wireless (Licensed and Unlicensed) data networks for voice and data access to subscribers in an ISP network. Designed and installed access network architecture for broadband DSL, Cable, and Wireless access.

Education, Certifications & Qualifications:

Brocade Networks Certified Network Professional (BNCNP) Brocade Networks Certified Network Engineer (BNCNE)
Brocade Networks Certified Ethernet Fabric Professional (BCEFP) Cisco Certified Network Associate (CCNA)
Cisco Certified Design Associate (CCDA)
Extreme Networks Specialist (ENS)
Juniper Networks Certified Internet Specialist - Enterprise Routing and Switching (JNCIS-ENT)
Juniper Networks Certified
Junos Associate (JNCIA-Junos)
Palo Alto Networks Certified Network Security Engineer (PCNSE)

ASHLEY BELL, SENIOR SECURITY OPERATIONS CENTER ANALYST

Summary:

3 years of experience in Help Desk, Network Monitoring and Reporting, Firewall Management, Patching, Endpoint Security, System Backups, and Server Builds.

Experienced with many technologies including Windows XP, Windows 7, 8.1 and 10; Windows Server 2003 - 2016; Linux/Unix and IOS, Tenable/Nessus/Security Center, PDQ Deploy and Inventory, PF Sense, Palo Alto, MixMode, Carbon Black, FortiGate, FortiManager, SonicWall, Cylance, MS Office Suite, O365, MSP 360 (Backup), Adobe Suite.

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

Experience:

Security Operations Center Analyst

Record, manage and monitor technology and processes for managed security services. Network monitoring, security research, firewall, endpoint security, incident response, and security event/log analysis.

Education, Certifications & Qualifications:

Master of Science – Cyber Security++
FortiManager
SonicWall

DAVID GRIFFIN, SENIOR SECURITY OPERATIONS CENTER ANALYST

Summary:

4 years of experience in Help Desk, Network Operations Center, Patching, Endpoint Security, System Backups, and Server Builds.

Experienced with many technologies including Windows XP, Windows 7, 8.1 and 10; Windows Server 2003 - 2016; Linux/Unix and IOS, Tenable/Nessus/Security Center, PDQ Deploy and Inventory, MixMode, Carbon Black, FortiManager, Cylance, Nmap, MS Office Suite, N-Able (n-central), O365, MSP 360 (Backup), VMware, and PRTG network monitoring.

Experience:

Security Operations Center Analyst

Manage, deploy, and monitor technology and processes for managed security services. Patching, endpoint security, incident response, manage backups, server builds and security event/log analysis.

Education, Certifications & Qualifications:

Microsoft Technology Associates Networking Fundamentals (MTA)
CompTIA A+

RAY PANFIL, SENIOR INFORMATION SECURITY ADVISOR

Summary:

30 years of experience in all aspects of information technology, specializing in Information Security and GRC within public and private sectors such as telecommunications, publishing, energy, automotive, government, healthcare, and manufacturing.

Experienced with many technologies including Windows XP, Windows 7, 8.1 and 10; Windows Server 2003 - 2016; Linux/Unix and IOS, Tenable/Nessus/Security Center, PDQ Deploy and Inventory, MixMode, Carbon Black, FortiManager, Cylance, Nmap, MS Office Suite, N-Able (n-central), MSP 360 (Backup), VMware, DUO, Splunk, Azure, AWS, Python, Gsuite, O365 and PRTG network monitoring.

Experience:

CIO/CSO/CTO

Analyzed acquisition targets to determine technology and process strengths and weaknesses. Evaluated the security status of all subsidiaries and formulate a migration plan based on the

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

security strategy. Forwarded security findings to the insurance companies Board and security audit remediation efforts. Conceptualized IT strategic plan for all subsidiary companies. Developed subsidiary safety policies and process manuals and business continuity plans. Manage multiple SOC2 audits, including response, remediation, and board reports. Migrated all subsidiaries from on-premises data centers to Azure and AWS cloud solutions.

Independent Cyber Security Consultant

Perform Security Risk Assessment (SRA) on company operations including its vendor partners, develop remediation plans to address SRA findings, develop a remediation plans for SOC2 audit readiness findings, recommend Technology solutions to address operational issues, develop Security, policy, and Procedures, using CSC Controls based on NIST, project Manage Remediation teams, develop Security Standards and Technology Roadmaps.

Director Information Technology

Manage the delivery web-based solutions, such as the redesign of consumer, member, broker, and provider portals. Establish Mobile Applications Development Program, which included process design, standards, and tool implementation for corporate mobile devices, Blackberry, and Apple operating system (OS) such as iPad and iPhone. Oversaw the design and execution of multiple application development projects. Restructured multiple data centers, involving data warehouse design and implementation, Exchange Server and cable plan replacement, network monitoring tools utilization, centralized firewall management and controls, and disaster recovery planning.

IT Management Consultant, Technical Project Manager, Systems Engineer

Education, Certifications & Qualifications:

NIST
CIS
SOC2
PIC
COSO
HIPAA
CJIS
CMMC

TRAVIS SALSURY, SECURITY OPERATIONS CENTER MANAGER

Summary:

21 years of experience in Security Operations Center; network penetration testing; Windows Server administration; data recovery and digital forensic work; software and hardware installation, configuration, support, and diagnostics.

Experienced with multiple technologies in Windows XP, Windows 7 and 8; Windows Server 2003, 2008, 2010, and 2012; Linux/Unix and IOS, Tenable/Nessus/Security Center, MixMode, Carbon Black, Metasploit/Nexpose, AD Audit+, AD Manager+, Exchange Audit+, AlienVault, EMC Discovery Manager, ASR SMART for Linux, Access Data Forensic Toolkit, FTK, Helix (Linux), Knoppix (Linux), Custom Hash Databases, Windows Forensic Toolchest, and MS Office Suite.

Experience:

Security Operation Center Manager

Lead Security Operations Center team. Manage, deploy, and monitor technology and processes for managed security services. Vulnerability Management, Penetration Testing, Endpoint Security, Network Monitoring, Incident Response, and security event/log analysis.

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

IT Security Engineer

Monitored, managed, and deployed multiple emailing systems, web filtering, BitLocker, AD infrastructure, AlienVault/OSSIM and vulnerability and patch management.

Network Engineer

Use network monitoring tools and daily server checks to check network health. Managed Symantec Endpoint Protection.

Network and Forensic Analyst, Data Recovery Technician, and Microcomputer Specialist 2 and 4

Acquire, examine, analyze, and report on digital evidence including network forensics. Data recovery, asset coordination, security policy consultation, threat analysis and patch management from damaged or destroyed electronic media. Perform LAN, build-out services and supported workstations, LANs, and software integration.

Education, Certifications & Qualifications:

CompTIA A+

HEIDI STOKES, CYBERSECURITY-BUSINESS DEVELOPMENT EXECUTIVE & PROJECT MANAGER

Summary:

25 years of experience in managing business relationships and serving as a client advocate. Three years of experience in developing & delivering customized and complex outsourced Cybersecurity solutions to clients. Key responsibilities lie in the management of client communications, education, and project tracking as well as providing personalized attention and support to the client throughout the deployment and installation process.

Clients assisted range from healthcare, insurance, manufacturing, financial, non-profit, municipalities, education, logistics and more. Leveraging the experiences of all clients from their respective industries and verticals allows for a better understanding of how to provide value to existing clients.

Experience:

Business Development & Relationship Management

Client advocate. Responsible for maintaining and growing trusted business relationships with clients and partners. Helping to identify issues and gaps in client environments that need resolved and providing the right solution to solve the problem.

Project Management

Excellent communication and organizational skills. Responsible for facilitating multiple projects. Serving as the hub for communications, task and time management, goal keeping, project tracking and reporting. Liaison between SOC Operations, Engineering, and Management teams for client deployments.

Leadership

Effective problem solver. Extensive experience leading diverse teams through projects, managing expectations and performance, delivering projects on time, and negotiating better rates or outcomes when needed.

Education, Certifications & Qualifications:

Bachelor's in Mass Communications and Journalism
Currently working towards project management professional and CISM certifications

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

Application Experience: Jira – Confluence – Salesforce – NetSuite – Prezi – Zoom – MS Office Suite – Teams – ActOn – SharePoint

Experience & Qualifications

RAVENii is transforming cybersecurity by "Humanizing the Hunt". We apply experienced human intuition to existing security solutions because we believe "Gray Matter" matters. Most organizations have made significant investments in security tools; however, have lacked the time, resources, or expertise to implement and realize the full value of these investments. RAVENii is tool agnostic which allows us to utilize and optimize our client's previous technology investments to achieve their cybersecurity requirements.

By monitoring the entirety of the IT environment, RAVENii moves beyond the sphere of security breaches; providing the most comprehensive discovery, analysis and mitigation of threats associated with an organization's presence. Our platform combines advanced analytics to assist in understanding attacks, assessing risks, and acting against digital threats.

The RAVENii Team is pleased to participate in the City of Joplin's Request for Proposal for Co-Managed Network Services and Upgrades. RAVENii plans to provide 24x7x365 professional security monitoring and response, follow best security practices, recommend best security practices when necessary, and support other security services for the City's network and security related technical infrastructure.

RAVENii is prepared and qualified to serve as an extension of your team by providing not only the centralized monitoring and alerting platform to integrate with the City's current toolset, but also the security specialists to monitor the platform, inform the City of high and critical alerts and assist with remediation plans.

It is RAVENii's intent to partner and grow with the City as you mature your security program. Our service offering includes the following per the request of the City of Joplin:

- General Tier 1 Support for emergent situations and unavailability of the City's IT staff to provide end-user support
- Endpoint Security Monitoring & Anti-Virus/Anti-Malware Protection
- Server Security with advanced threat protection, virus/malware protection, and visibility into encrypted traffic
- Network Protection for the City's cloud-based DNS connections, network, and users from cyber attacks at the domain level
- Daily Health & Safety Checks to monitor unauthorized login attempts and run system vulnerability checks
- Run comprehensive scans of the City's systems and logs to identify potential problems in advance
- Weekly Reporting with a detailed report on the health and security of the City's critical IT assets
- 24/7 Monitoring – deliver information to the City quickly about errors and highlight problems that need attention
- Quarterly Assessment with onsite visit to physically inspect the City's infrastructure, perform a network and security assessment and ensure the City's technology is properly aligned to best practices and business goals
- Annual Cybersecurity Training of all City employees and City Council members that use a computer
- Annual Penetration Testing | Periodic Phishing & Security Tests – campaign reports to be delivered to the City IT Director. Follow-up training plans and recommended best practices for repeat offenders.
- Firewall IPS/IDS with 24/7 Monitoring and threat detection
- Advisory for Network & Infrastructure Enhancement to bring long-term structure, stability, and enhancements
- Incident Response Plan Creation & Preparation – coordinate and train the City's IT staff on Incident Response roles and participation responsibilities. Annual 'exercise' on incident response and mitigation plan
- Air Gap Backup & Recovery – assist the City's Network Administrator with existing backup appliance and advise on enhancements
- SOC as a Service for Cybersecurity – establish systems and controls to satisfy SOC reporting requirements as it relates to the Cybersecurity framework and monitoring

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

RAVENii's SOC as a Service

RAVENii's SOC as a Service (SOCaaS) delivers powerful threat detection, incident response, and compliance management in one fully managed service. We combine all the security capabilities needed for effective security monitoring across your cloud and on-premise environments like:

- Asset discovery
- Vulnerability management
- Intrusion detection
- Endpoint detection and response
- Behavioral monitoring
- SIEM log management
- Compliance reports

RAVENii's Managed SOC provides:

- 24x7 monitoring
- System alerts
- Security alerts
- Prioritization of risks
- Remediation recommendations
- Troubleshooting
- 24x7 dashboard access for reporting
- Monthly executive briefings with RAVENii SOC subject matter experts
- RAVENii C-Level access and support
- Dedicated account & project manager for onboarding and account maintenance
- Co-managed, shared dashboards

RAVENii's SOCaaS eliminates the need to deploy, integrate, and maintain expensive solutions like a SIEM and maximizes your existing security investments like your firewall and anti-virus by including their logs in our analysis. SOCaaS offers low total cost of ownership (TCO) and flexible, scalable deployment options for municipalities like the City of Joplin.

RAVENii's SOC team will serve as the eyes for the City of Joplin when monitoring the City's network environment. The RAVENii SOC team will also serve as the voice for the City of Joplin by informing you of business-critical alerts and providing you consistent and meaningful reporting to share with your executives and board members that shows the status of your security posture and your roadmap for improvement. Lastly, RAVENii has partnered with MixMode to serve as the heart of our SOC platform and the nose for sniffing out the anomalies in the City's network.

RAVENii's Soc as a Service solution and technology we are proposing is powered by MixMode and its patented 3rd Wave Artificial Intelligence. It is the only platform with Real Time 3rd Wave AI and is in a classification all on its own.

DARPA (Defense Advanced Research Projects Agency) and the US Department of Defense define 3rd Wave Artificial Intelligence as:

1. Unsupervised
2. Context-aware
3. Predictive
4. Generative AI

MixMode is the only security platform that meets DARPA's 3rd wave AI criteria and delivers Negative Time to Detection. Meaning…RAVENii's SOCaaS Monitoring solution can identify Zero-Day Attacks in Real Time.

Zero-Day attacks have drastically increased by over 600% in the last few years with no signs of slowing down. Zero-Day Attacks are extremely difficult to catch because they do not have a threat signature. Traditional security tools operating with 1st & 2nd Wave AI functionality rely on threat signatures and historical data to identify anomalies. DARPA says 1st & 2nd Wave AI technology is unreliable, after the fact, dependent on human intervention, and does not have predictive threat detection capability.

Another cost saving feature of the MixMode platform is the fact that it serves as a multi-point tool. It replaces the need for SIEM, NDR & NTA solutions.

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

A third-wave self-supervised AI solution like MixMode mitigates many of the issues inherent to SIEM platforms. MixMode accomplishes the following:

- Creates a generative, responsive, real-time network baseline within a week without the need for humans to configure or tune the system.
- MixMode is a software-based system that does not rely on appliances.
- Is context-aware and triggers fewer false positives and catches more actual threats.
- Is not dependent on logging and reports that attract hackers and take up security analysts' time.
- Requires less human input and interaction, reducing the risk of human error and increasing overall team efficiency.

RAVENii's Log Storage Service is included with SOCaaS and will be fully managed for the City. RAVENii will collect the City's logs along with:

- AI Analytics
- Up to 5TB raw logs per month
- 30 days hot storage
- 1-year cold storage
- 1 hardware sensor
- 24/7 SOC monitoring
- Monthly reporting
- Ticket System
- 1 export of raw logs per quarter ($300 per additional export)

Another best security practice that RAVENii will include with SOCaaS is Vulnerability Management. RAVENii's Vulnerability Management Solution provides visibility into your network so you can manage and measure your cyber risk. This vulnerability analytics solution is built on leading technology to give you a comprehensive view of your attack surface so you can discover unknown assets and prioritize vulnerabilities within your network.

RAVENii's Vulnerability Management Solution will provide:

- Access to advanced analytics, user customizable dashboards, reports, and workflows.
- Access to real-time insight to help prioritize patching.
- Access to vulnerability prioritization to determine the likelihood a vulnerability will be exploited in your unique environment.
- Continuous asset discovery capabilities for all mobile devices, physical, virtual and cloud instances on the network, including unauthorized assets. This is done on a weekly basis as discovery scans are run.
- Capabilities to perform non-credentialed and credentialed scanning for deep analysis and configuration auditing.
- Capabilities to perform agent-based scanning for mobile and hard to reach assets.
- Access to compliance validation of business defined standards, industry standards and regulatory mandates, such as CERT, DISA, STIG, DHS CDM, FISMA, PCI DSS, HIPAA/HITECH, etc.
- Vulnerability advisory and monthly review.

All active RAVENii SOCaaS clients have RAVENii's Incident Response Team on retainer. Once the City declares an incident, RAVENii will have a team assembled and available to stop the bleeding for the City in less than 30 minutes.

All active RAVENii SOCaaS clients also benefit from having a team of security subject matter experts focused on their environments and making sure they are following security best practices. We will serve as an extension of your team to help you support your security goals. We will educate you about security and compliance, talk to you about risks, help you prioritize remediation efforts, and ultimately teach you how to sustain a healthy security program moving forward.

RAVENii's Managed Endpoint Protection

The RAVENii Managed Endpoint Protection Service helps businesses block threats and other attempts to gain access into their networks. RAVENii will defend all access points with 24/7 monitoring for any malicious activity.

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

The service follows security best practices and ensures that the endpoints of security; the client devices, are protected against advanced threats, keeping networks running and corporate assets safe. With RAVENii's Managed Endpoint Protection Service you can protect your intellectual property, customer data, and reputation. You can also devote more IT resources to your core business.

RAVENii's Managed Endpoint Protection Service includes:

- Malware Protection
- Internet Filtering
- Device lockdown, alarming and wiping
- Device Tracking and Reclamation
- Daily Asset Inventory of hardware and software
- Microsoft OS patching
- 3rd Party Application patching
- 24x7 Hacker monitoring
- 24x7 Event Log Collection
- Daily backup of folders or entire systems
- Remote Assistance
- Regular executive indicator and reporting debriefs
- Access to RAVENii's Security Incident Response and Management Team
- Anytime/Anywhere management of endpoints

RAVENii will provide 24x7 Management and Monitoring of the City's endpoint protection software for all endpoints within the City's scope.

RAVENii will:

- Notify customer of security issues identified for all endpoints/devices in scope;*
- Provide remediation of security issues identified for all endpoints/devices in scope;*
- Provide a Root Cause Analysis of security issues identified for all endpoints/devices. The RCA will outline the details of discovery and remediation for issues related to endpoints/devices;
- Review and recommend updates to agents, and support for agent and console issues related;
- Open and manage Support issues related to the functionality of subscribed endpoint protection products on behalf of the customer until resolution.
- Other (Out of Scope) Services will be mutually agreed upon. Incident Response is considered Out of Scope on any Customer endpoint/device that the Customer creates exceptions or deviations to the configuration guidelines for the endpoint protection product.

* Everything related to a virus being detected by the endpoint protection product managed by RAVENii is in scope. The definition of an In Scope incident is something that is detected by RAVENii on an endpoint/device with their endpoint protection product deployed on it in the Customer's environment that requires remediation action. RAVENii will quarantine, contain, or clear any endpoint/device as long as RAVENii has access to the endpoint/device.

RAVENii's Network Security Monitoring

RAVENii offers 24X7 Network Security Monitoring of your network and strongly recommends deploying this solution in your environment. Our platform utilizes context-aware AI, a dynamic network baselining technology which allows us to identify pre-attack behavior and stop attacks before they happen.

A full baseline of your typical network behavior can be created in just 7 days. This allows us to see your entire attack surface. Having this greater transparency allows for faster detections, better correlation, and less noise so you can focus on what matters. The AI functionality eliminates 95% of the false positive alerts that typically send IT teams down the wrong track. The value to you is real and actionable threats to focus on, not distractions and wild goose chases.

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

RAVENii will monitor all of your network traffic, incoming, outgoing, and local in the cloud, on premise, or in hybrid environments. With full layer 2-7 visibility, full packet capture, and deep packet inspection, we can give you the visibility you need to see and take action before damage is done.

RAVENii will enhance your security by doing the following:

- Establishing an evolving baseline of acceptable network behavior for anomaly detection in 7 days or less, without requiring months of historical data, human intelligence or forensics;
- Providing predictive and "zero day" threat, attack, and anomaly intelligence layer without human intervention; and
- Delivering an average of 95% reduction in false positive alerts.

RAVENii's Network Security Monitoring Service Includes …

- Malware detection with built-in threat intelligence;
- Real-time attack surface measuring;
- Real-time on-the-wire passive vulnerability assessment and threat monitoring;
- Real-time indicator of compromise alerting;
- Real-time detection of botnet and command & control traffic;
- Forensics;
- Trending Data;
- Access to RAVENii's Security Incident Response and Management Team; and
- Access to RAVENii's web based SOC for managed devices, workflows, alerting and incidents.

RAVENii's External Penetration Test & Quarterly Scans

RAVENii's Certified Ethical Hackers will perform External Network Penetration Tests to discover, actively exploit, and report vulnerabilities to the City about the health of its network environment.

RAVENii has adopted a methodology based on guidance provided by the Penetration Testing Execution Standard (PTES, www.pentest-standard.org). Penetration tests are conducted following this methodology and documentation, where applicable, and will be conducted to support the findings contained in the report.

Tools that may be utilized:

- Scanning and Enumeration:
- Nmap *I* Nmap Scripting Engine (NSE)
- Netcat
- Ike-scan
- Eyewitness

Vulnerability Scanning:

- Tenable Nessus
- Ikeprobe

Password Attacks:

- Medusa
- THC Hydra

Penetration Testing:

- Metasploit I Armitage
- Misc. Kali Tools
- Ikeforce
- Standalone Exploits
- Veil Framework
- Powershell Empire

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

RAVENii's Managed Security Awareness & Phishing Training

RAVENii will provide the SANS Security Awareness Training licensing and manage the training platform for the City of Joplin. This service follows best practices for educating your human firewall on how to treat your sensitive data and be security aware. Management of your Security Awareness Training platform will include:

- Ongoing security awareness training & testing to ensure the Customer's employees understand and exhibit the necessary behaviors and skills to help protect the security of the organization.
- Coordination with Customer's Security & Compliance Teams to ensure training meets the Customer's business requirements.
- Training to all City employees and Council members on how to utilize secure authentication, how to identify social engineering attacks, how to identify and properly manage sensitive data, how to identify causes for unintentional data loss, how to identify the most common indicators of an incident, etc.
- Remediation plans for repeat offenders.
- Campaign and status reports.

The managed SANS Security Awareness Training platform also includes:

- Initial Onboarding
- New Hire Onboarding
- Offboarding
- User Management & Support
- Phishing Campaigns (up to 12 per year)
- Full access to content library, including Compliance training modules

RAVENii's Firewall Monitoring Service

RAVENii will monitor the City of Joplin's firewalls and provide daily alerting and weekly/monthly reporting.

- RAVENii will monitor the firewalls daily for uptime, usage, and overall health of the system interface.
- RAVENii will perform ongoing firewall traffic analysis.
- RAVENii will monitor the firewall manufacturer's site for system updates/upgrades, provide a summary of the possible effects, and will seek approval from the City before proceeding with the work.
- RAVENii will provide technical analysis of the firewall systems to ensure the City is leveraging the best practice functionalities of the tool for security purposes.
- RAVENii will provide a Best Practice Assessment for newly acquired firewall assets as they are integrated into the City's network.
- RAVENii will provide a Best Practice Assessment for all firewall assets on an annual basis.

RAVENii's Backup Management Solution

The following details define RAVENii's Backup Service that we recommend for the City of Joplin:

- Centralized management console
- Agent based
- Full back up with differentials to follow
- Cloud & Local backups
- File based backups & restores
- Image based backups & restores
- Office 365 mailbox backups
- Individual email restores
- Customized scheduling
- Customized retention policy & restore times
- Local Backups per device as required

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

*NAS/SAN for local backups must be provided by customer

RAVENii will initiate restore requests within 4 business hours from the receipt of the request. Restore requests will be done during regular business hours: Monday through Friday from 8 am – 5 pm. Restore time is dependent upon the amount of data to be restored.

All data restore requests should be submitted to RAVENii via a support ticket through our web-based service desk.

RAVENii's vCISO Advisory Program

The City of Joplin has requested recommendations for tools and/or security best practices to follow in this RFP. RAVENii always recommends our vCISO Advisory Program to anyone interested in building or fortifying a security program. We recommend it to anyone wanting a thorough audit of your current state of security as well as for strategizing and building a roadmap for your end state goal.

RAVENii believes a complete and sound security program consists of policies and procedures that govern the use of security tools. RAVENii's vCISO program is a 12-month advisory service designed to evaluate your current security footprint, expose your security vulnerabilities, create a full set of security policies, and facilitate a plan of action to continually be improving your security posture.

RAVENii's vCISO program follows the Top 18 CIS Controls, a set of prioritized security actions that aid in finding ways to stopping today's most dangerous attacks. The 18 Controls cover most cyber-attack vectors and takes leading threat data from forensic experts across all industries and transforms it into actionable controls to achieve a better overall cybersecurity defense.

RAVENii's vCISO program will:

- Evaluate, create, and direct an Information Security Program Plan for the City of Joplin;
- Itemize, catalogue, evaluate and, as necessary, further develop your Information Security Policies and Procedures;
- Identify and confirm your vulnerabilities to information systems from internal and external threats by auditing the current architectures and system configurations;
- Itemize, quantify, and rank your information security risks, based upon the potential impacts to the organization;
- Minimize or eliminate business risks and exposures by identifying short- and long-term options and solutions for remediation of identified vulnerabilities;
- Determine the appropriate approach to develop or improve upon your existing Information Security program;
- Establish and/or evaluate Security Policies & Procedures to govern the security of your network, data, and applications;
- Ensure that security programs are in compliance with applicable laws, regulations, and policies to minimize or eliminate risk and audit findings;
- Develop an incident response plan with key staff, including incident response plan documentation developed specifically for your existing infrastructure; and
- Assist the City in determining and mitigating third party vulnerabilities.

Four (4) hours per month of vCISO level consulting activities. Example activities include, but are not limited to the following:

- Identification of priority action items to close gaps quickly
- Strategic Roadmaps with Level of Effort (LOE)
- Maturity modeling gaps to help show business context
- Network infrastructure segmentation & architecture planning
- Creation of Incident Response Plan & Communications Plan
- Table Top testing for Incident Response
- Security Policy & Process Creation
- Security Tools Assessment

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

- Security Program Evaluation
- Security Program Development
- SOC2 Audit Preparation Assistance
- Vendor Management Program
- Regulatory and Compliance Issues
- Critical Security Controls
- Map to CJIS Controls

RAVENii's Deliverables

RAVENii will provide the following deliverables to the City:

- ✓ SOCaaS as listed above.
  - Daily Health Checks
  - Weekly Operational Reporting
  - Monthly Executive Reporting
- ✓ Managed Endpoint Protection (Carbon Black) as listed above.
  - Daily Health Checks
  - Weekly Operational Reporting
  - Monthly Executive Reporting
- ✓ Network Security Monitoring as listed above.
  - Daily Health Checks
  - Weekly Operational Reporting
  - Monthly Executive Reporting
- ✓ Firewall Management as listed above.
  - Daily Health Checks
  - Weekly Operational Reporting
  - Monthly Executive Reporting
- ✓ External Penetration Test with Quarterly External Scans as above.
  - This report outlines any exceptions identified during the external penetration testing periods as well as recommendations to mitigate those risks.
- ✓ Managed Security Awareness & Phishing Training
  - Managed SANS Security Awareness Training as listed above.
  - Level 1 & 2 Support* (RAVENii will serve as the escalation path for Level 3 Support with SANS)
  - Monthly Executive Report
  - Mapped to Critical Security Controls (vCISO clients)
- ✓ vCISO Advisory Service as listed above.
  - Compliance Framework Assessments, Analysis, and Mapped to CJIS.
- ✓ Managed Backup services as listed above.
  - Daily Health Checks
  - Weekly Operational Reporting
  - Monthly Executive Reporting
- ✓ Web-based Service Desk to open tickets, track workflows, manage devices, alerting and incidents.
- ✓ Reporting as needed for business or compliance requirements.

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

Project - Overview

Objective

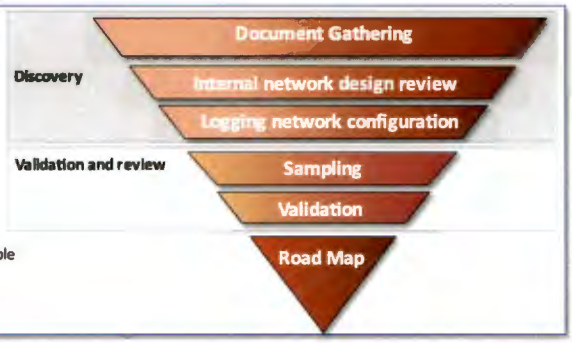
- Replace current log aggregation tool and archive historical logs to gold storage
- Design and deploy MixMode sensors to obtain maximum visibility

Goals

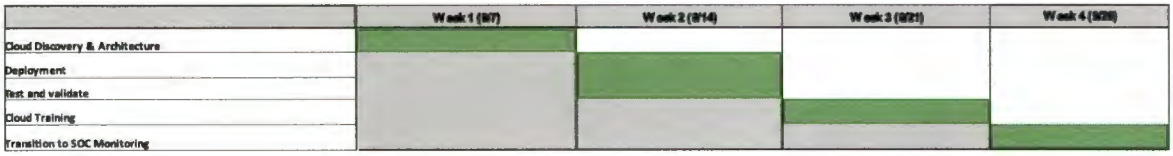
1. **To identify and document the client's current logical and physical security posture**
2. To determine the IP address for the new log aggregator and ship the log collection sensor for install
3. **To develop a set of actionable recommendations to address**

Process

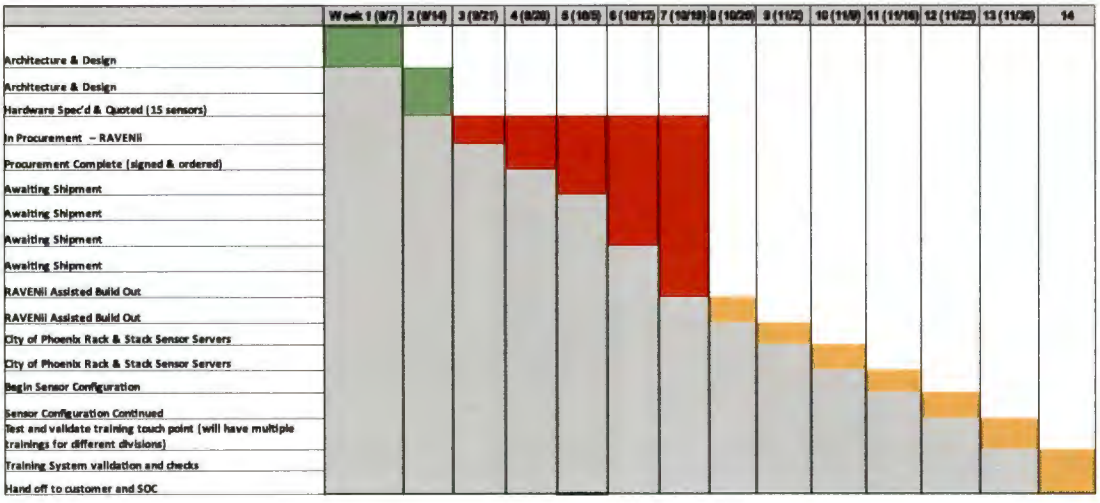
- ☐ Project Scope
- ☐ Kickoff
- ☐ Request current network diagrams
- ☐ Request current logging configurations
- ☐ Request current IP for log destination
- ☐ Prepare internal design for sensor placement
- ☐ Determine # virtual vs # physical
- ☐ Ship new log collection sensor
- ☐ Start with virtual sensors and cloud
- ☐ Procure any physical sensors
- ☐ Validate data flow and taps with each sensor
- ☐ Establish roadmap based on team and timetable



Cloud Sensor Logging Architecture & IT Security Timeline



Network Sensor Logging Architecture & IT Security Timeline



© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

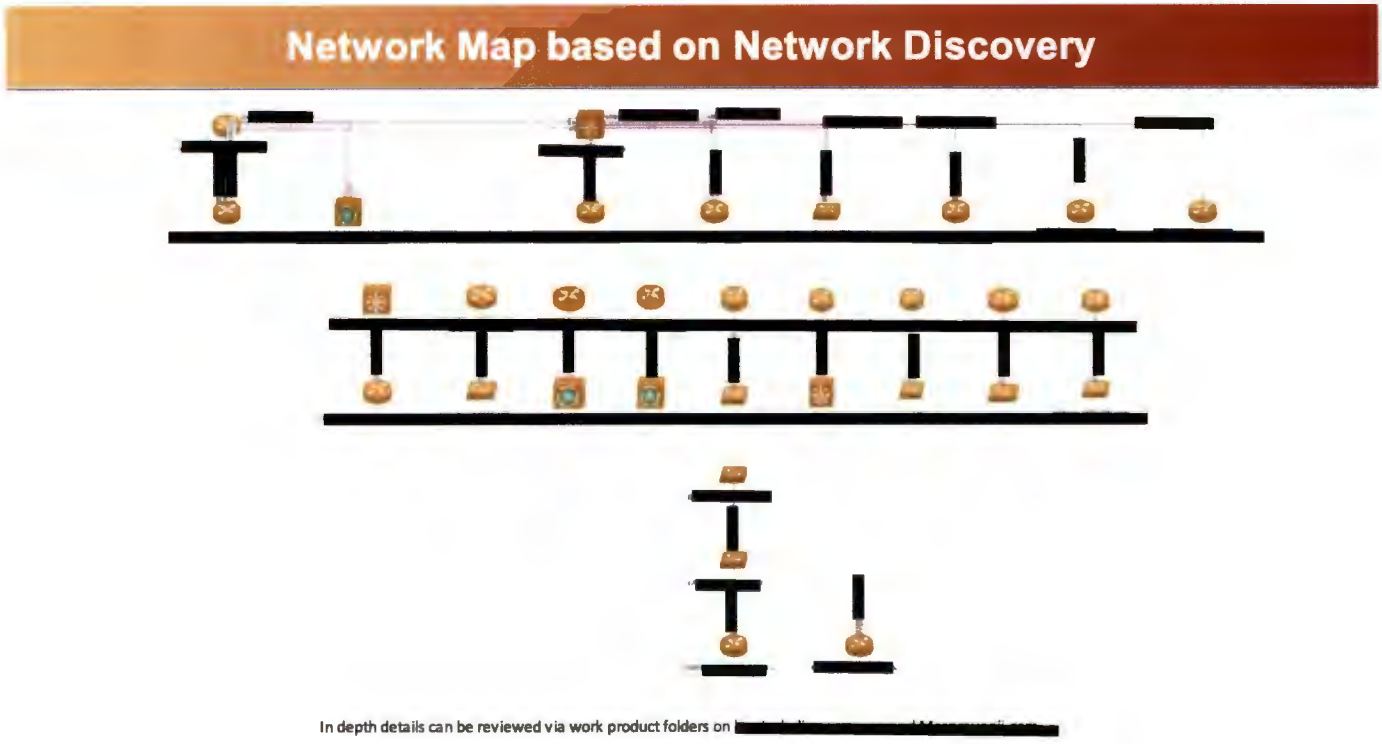
SAMPLE PROJECT TRACKING

PROJECT TASKS	TASK OWNER	STATUS
Whitelist 10.XXX.100.XXX-XXX	Client	In progress
Grant Domain & Local Admin Access	RAVENii	RAVENii is testing
Service Account Inventory Based on Application (Carbon Black, PDQ, etc.)	RAVENii	RAVENii is testing
Nessus Scanner in San Diego is down	Client/RAVENii	This scanner is down due to the coronavirus. However, access may be restored once connectivity, ACLs, etc. get fixed.
PDQ Deployment Inventory	RAVENii	RAVENii is testing
MixMode Deployment	Client	In progress. The goal is to be online by 12/12/21.
MixMode Cabling & Mitigation	Client/RAVENii	Client is ordering the Cat6 cables. The goal is to be online with MixMode by 12/12/21.
Logging/SIEM Solution	Client	Client reported they are still evaluating solutions. Once a solution is in place, RAVENii will need READ ONLY access.
Managed Firewall Procurement Requirements	Client	FortiManager is installed, Client needs to provide access and visibility to RAVENii. The goal is to be online by 12/12/21.
Firewall Access	RAVENii	RAVENii is testing
PDQ Access	RAVENii	RAVENii is giving Client access to PDQ for inventory management.

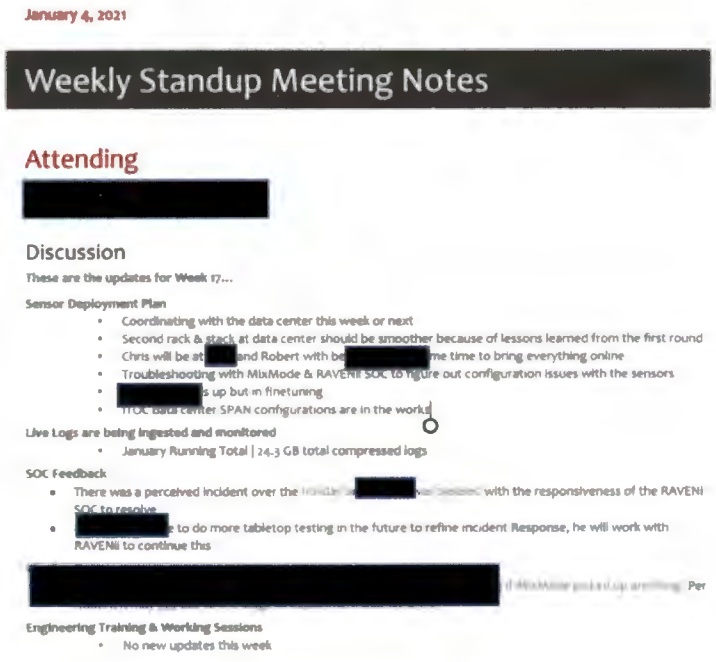
| THIS SPACE LEFT INTENTIONALLY BLANK |

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

SAMPLE ARCHITECTURE DESIGN



SAMPLE TRACKING NOTES



January 4, 2021

Weekly Standup Meeting Notes

Attending

[redacted]

Discussion

These are the updates for Week 17...

Sensor Deployment Plan

- Coordinating with the data center this week or next
- Second rack & stack at data center should be smoother because of lessons learned from the first round
- Chris will be at [redacted] and Robert with be [redacted] me time to bring everything online
- Troubleshooting with MixMode & RAVENii SOC to figure out configuration issues with the sensors
- [redacted] s up but in finetuning
- TTOC data center SPAN configurations are in the works

Live Logs are being ingested and monitored

- January Running Total | 24.3 GB total compressed logs

SOC Feedback

- There was a perceived incident over the [redacted] with the responsiveness of the RAVENii SOC to resolve
- [redacted] to do more tabletop testing in the future to refine incident Response, he will work with RAVENii to continue this

[redacted] Per

Engineering Training & Working Sessions

- No new updates this week

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

Reporting

- Storyboard executive summaries are in the process of being created for C-Levels

Action Items

[redacted]

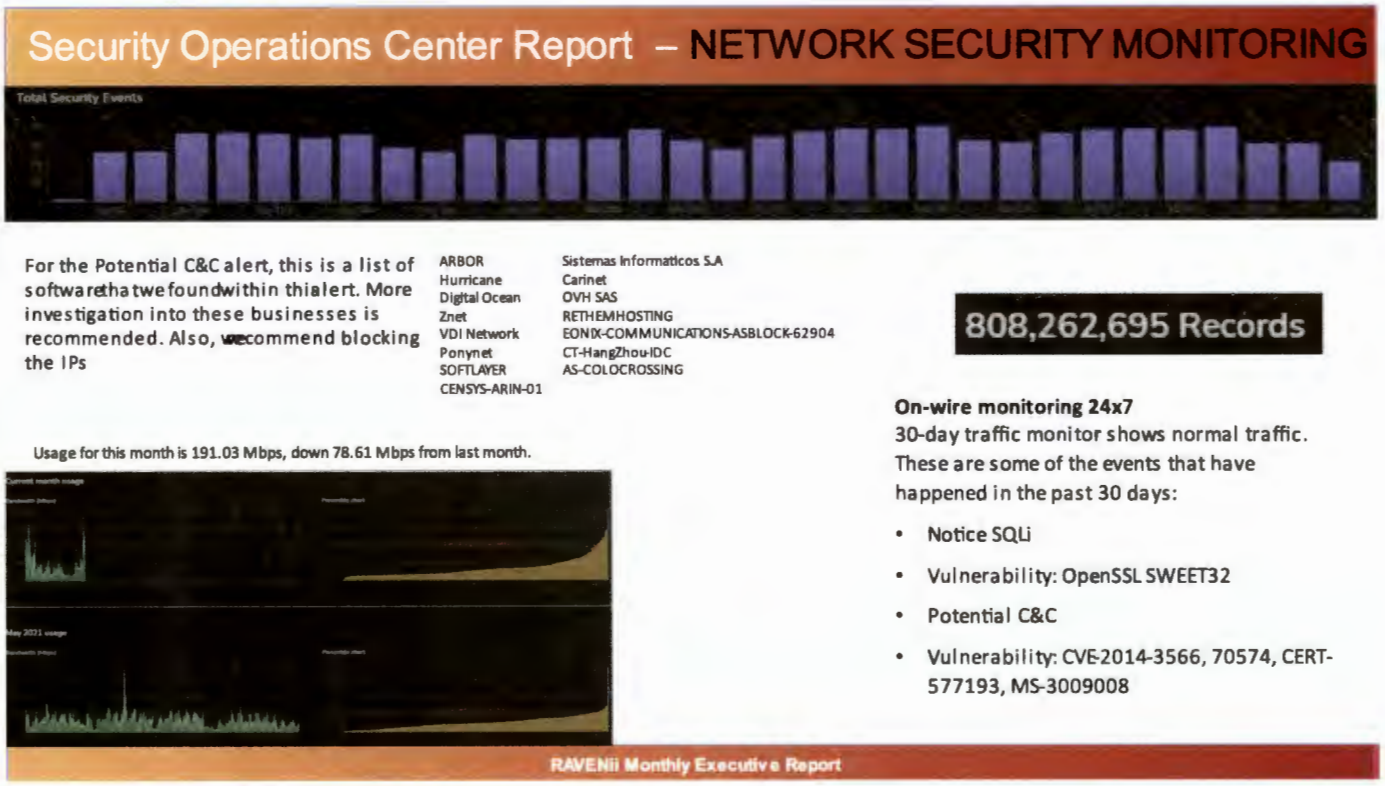
- Back end Stack in [redacted]
- Complete SpanTap configurations [redacted]

[redacted]

- Check to see if anything was picked up by MixMode between the dates of 12/7-12/20 due to the black box pen test

RAVENii

SAMPLE REPORTS & DASHBOARD ACCESS



| THIS SPACE LEFT INTENTIONALLY BLANK |

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

Security Operations Center Report – NETWORK SECURITY MONITORING

- Vulnerability: CVE-2014-3566, 70574, CERT-577193, MS-3009008

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, which makes it easier for man -in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

The POODLE attack can be used against any system or application that supports SSl3.0. This affects most current browsers and websites, but also includes any software that either references a vulnerable SSl/TLS library (e.g. OpenSSL) or implements the SSL/TLS protocol suite itself. By exploiting this vulnerability in a likely web-based scenario, an attacker can gain access to sensitive data passed within the encrypted web session, such as passwords, co okies and other authentication tokens that can then be used to gain more complete access to a websit(impersonating that user, accessing database content, etc.).

Some of the same researchers that discovered the vulnerability also developed a fix for one of the prerequisite conditions. LS_FALLBACK_SCSV is a protocol extension that prevents MITM attackers from being able to force a protocol downgradeOpenSSL has added support for TLS_FALLB ACK_SCSV to their latest versions and recommend the following upgrades

OpenSSL 1.0.1 users should upgrade to 1.0.1j.
OpenSSL 1.0.0 users should upgrade to 1.0.0o.
OpenSSL 0.9.8 users should upgrade to 0.9.8zc.
Both clients and servers need to support TLS_FALLBACK_SCSV to prevent downgrade attacks.
Other SSL 3.0 implementations are most likely also affected by POODLEContact your vendor for details. Additional vendor inf ormation may be available in the National Vulnerability Database(NVD).

orig [redacted]7HURRICANE
resp [redacted]
orig [redacted]7 DIGITALOCEAN -ASN
resp [redacted]
orig [redacted]3 DIGITALOCEAN -ASN
resp [redacted]
orig [redacted]5DEDICATED -FIBER-COMMUNICATIONS
resp [redacted]
orig [redacted]QUICKPACKET
resp [redacted]



Security Operations Center Report – ENDPOINT PROTECTION

Threats

Detected in Last 30 days: 3
Setup_1026.exe = malware (m[redacted]el)
Wavebrowser (pup)= p[redacted]o
Osclient (game launcher) j[redacted]n
All have been auto quarantined



© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

Security Operations Center Report – Vulnerability Management

Mitigation Summary - Vulnerabilities by Severity

	Total Mitigated	Mitigated <10d	Mitigated 10-30d	Mitigated >30d	Total Unmitigated	Exploitable	Patch Available >30d	Exploitable Hosts
Total Vulnerabilities	153	39%	18%	43%	989	12%	8%	100
Critical	5	60%	28%	28%	2	50%	0%	1
High	8	50			13			0
Medium	127	40%	17%	43%	891	13%	6%	100
Low	13			54%	83			0

- Total Vulnerabilities Mitigated this month: 13.40%, down 0.81% from last month.
- Critical Vulnerabilities Mitigated this month: 71.43%, no change from last month.
- High Vulnerabilities Mitigated this month: 38.10%, up 7.67% from last month.
- Medium Vulnerabilities Mitigated this month: 12.48%, down 0.96% from last month.
- Low Vulnerabilities Mitigated this month: 13.54%, down 1.17% from last month.

Security Operations Center Report – Vulnerability Management

Risk Reduction Recommendations

Solution	Risk Reduction	Hosts Affected	Vulnerabilities	VPR	CVSS v3 Base Score
Fix SSL Certificate Cannot Be Trusted	13.19%	108	129		6.5
Fix SSL Self-Signed Certificate	11.96%	103	117		
Fix TLS Version 1.0 Protocol Detection	8.49%	64	83		6.5
Fix SSL RC4 Cipher Suites Supported (Bar Mitzvah)	6.65%	53	65	4.4	5.9
- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is	4.91%	48	48	4.8	
Contact the Certificate Authority to have the certificate reissued	2.45%	28	28	4.4	7.5
Fix Unix Operating System Unsupported Version Detection	1.36%	1	1		10.0
Fix SSH Weak Algorithms Supported	0.82%	8	8		
Fix SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	0.72%	6	7	5.3	6.8

RAVENii Monthly Executive Report

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

SAMPLE COMMUNICATIONS PLAN

RAVENii Security Operation Center
Communications Plan

RAVENii Security Operation Center

Welcome to the RAVENii Security Operation Center for incident response and support requests. We offer a self service portal for opening and tracking requests and a manned 24/7 SOC to handle incoming requests. Please fill out the information below and email a copy to soc@ravenii.com, keep a copy for instructions for accessing the **Service Operation Center**. We look forward to our partnership and providing quality, timely service for your security and infrastructure business needs.

Customer Information

Company Name:

Primary Contact:

Name	Email	Phone

Additional Contacts:

Name	Email	Phone

RAVENii SOC will only communicate and share information with contacts listed on this form. It is the client's responsibility to notify RAVENii SOC of employees that need added or subtracted from the list. Please email employee change requests to support@ravenii.com.

Weekly Communications

RAVENii SOC will send a 'health & wellness' weekly summation via email to the contacts listed above. This email focuses on lower-level alerts that require your attention but are not considered business critical such as clear text passwords being seen on wire.

Customer Communication Plan for Alerts

RAVENii SOC will notify the contacts listed above for alerts that are ranked 10. An alert that is ranked 10 is typically a breach attempt or a malfunction in the network that could bring the environment down. In the event of a 10 alert, RAVENii SOC will:

1. **Call the Primary Contact listed above at the phone number provided;**
2. **Email the entire customer contact list about the alert; and**
3. **Open a bridge and offer troubleshooting assistance when needed.**

9864 Marion Ridge
Kansas City, MO 64137
844.317.0944
RAVENii.com

Contacting RAVENii Security Operation Center

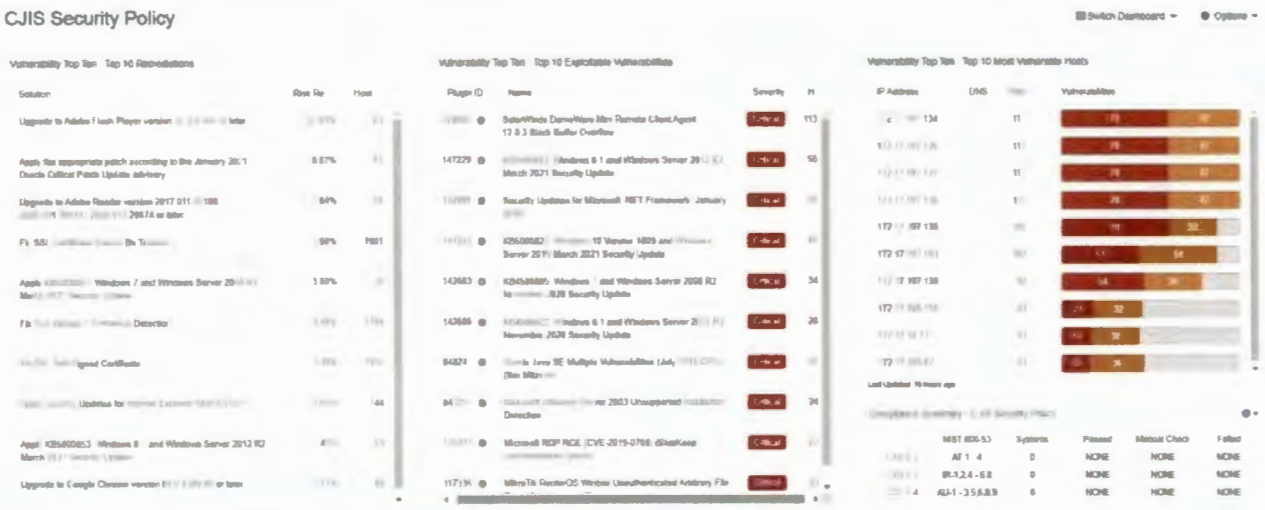
In the event that you need to contact the RAVENii SOC, below are three options based on the severity of your request.

1. **Go to https://ravenii.maxdesk.us/ and create an account from the registered email domain. This is the preferred method of managing all non-outage issues and requests. Once this is created customers can create tickets by clicking on the Submit Ticket button. Tickets can be created for any incident, support request or sales questions. Customers can track and update all open tickets from this self-service portal.**
2. **Email support@ravenii.com with the Email Subject as a brief description of the ticket and add any ticket details in the Body of the email. This will also open a ticket in the web-based service desk portal.**
3. **Customers can call RAVENii Service Operations Center 24/7 at 844-317-0944 #2 to open requests with a support representative. This is the preferred method for issues needing immediate attention; like service or business impacting issues. The support representative will immediately engage the correct engineering team for your service and SLA to resolve any issues.**

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

SAMPLE COMPLIANCE & ADVISORY REPORTS

SOC – Compliance view



Critical Security Control Domains

Workstream Tracking

A	B	C	D	E	F	G	H	I	J
[illegible]	CJIS Control Detail	[illegible]	Sensor or Baseline	Implemented	Policy	Process	Defined or Hypothesis	Risk Attestation	Workstream
1.1	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory	Identify	Active Device Discovery System	Yes	Yes	No	LANSweeper KACE		Document Process
1.2	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory	Identify	Passive Device Discovery System	Yes	Yes	No	WUG, Microtik		Document Process
1.3	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory	Identify	Log Management System / SIEM	No	No	No			Review Control
1.4	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not	Identify	Asset Inventory System	Yes	Yes	Yes	ITEQ		Complete
1.5	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	Identify	Asset Inventory System	Yes	Yes	No	ITEQ		Review Control
1.6	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	Respond	Asset Inventory System	No	No	No			FortiNAC
1.7	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	Protect	Network Level Authentication (NLA)	No	No	No			FortiNAC
1.8	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	Protect	Public Key Infrastruture (PKI)	No	No	No			Review Control
2.1	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	Identify	Software Application Inventory	No	No	No	Manual process		Review Control
	Ensure that only software applications or operating								

Critical Security Control Domains

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

Roadmap

- **2020 Gap Remediation**
  - **Review FortiGate Security Fabric Implementation and update controls summary**
  - **Review Workstream Tracking worksheet (next session)**
  - **Prioritize on closing out first 6 controls, the basics of CIS, NIST and CJIS**
  - **Focus on creating process documentation**
    - Ravenii will provide templates and work with team on refining
  - **Mixmode remediations**
    - Create workstreams to address AI Events in Mixmode
  - **CSC 20 – Penetration Testing Program**
    - Already do weekly Internal Pen testing with Tenable
    - External Penetration Testing, Cadence, rotation of vendors
    - Down the road Red/Blue Team exercises
  - **Goal: Achieve 3.75 maturity rating**

Critical Security Control Domains

References

RAVENii serves as the Security Operations Center and Managed Security Services Provider for the following clients:

City of Phoenix
Shannon Lawson, ACIO/CISO
(480) 536-3018
Shannon.Lawson@phoenix.gov

City of Overland Park
Tony Sage, CIO
(913) 954-7029
Tony.Sage@opkansas.org

IBT Industrial Solutions
Paul Stubitsch, CIO
913-261-2168
pstubitsch@ibtinc.com

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

Pricing

Option 1

RAVENii does not package and price our services in the same manner as outlined in the City's Request for Proposal. We have added our description next to yours so we can provide the most accurate bid possible.

Based on the information provided by the City of Joplin, we are confident we can support and co-manage the security infrastructure for the City. Pricing is an estimation only and is subject to change. RAVENii will require more information about the City's current state of security and detailed descriptions of your toolset before we can provide a firm quote.

City of Joplin | Item Description	RAVENii | Item Description	Monthly Bid Price
General IT Support, as needed	SOCaaS (includes logging & vulnerability scanning)	**$7500.00***
Endpoint Security	Managed Endpoint Protection | 550 Endpoints	**$3750.00***
Server Security	Network Security Monitoring | 100 Mbps	**$1220.00***
Network Protection	Network Security Monitoring | 100 Mbps	*Included in Network Security Monitoring Pricing*
Security Monitoring	Network Security Monitoring | 100 Mbps	*Included in Network Security Monitoring Pricing*
Daily Health & Safety Checks	SOCaaS	*Included in SOCaaS Pricing*
Weekly Reporting	SOCaaS	*Included in SOCaaS Pricing*
24/7 Monitoring	SOCaaS	*Included in SOCaaS Pricing*
Quarterly Assessment	External Penetration Test & Quarterly Scans | 4 Tests | sub 256 IPs	**$1000.00**
Annual Cyber-Security Training	Managed SANS Security Training | 550 Users	**$575.00***
Annual Penetration/Periodic Security Tests	External Penetration Test & Quarterly Scans / Managed SANS Security Training	*Included in External Penetration Test & Quarterly Scans & Included in Managed SANS Security Training*
Firewall IPS/IDS with 24/7 Monitoring	Firewall Monitoring	**$600.00**
Network Advisement & Infrastructure Enhancement	vCISO Advisory Program	**$1500.00**
Incident Response Plan & Preparation	vCISO Advisory Program	*Included in vCISO Advisory Pricing*
Air Gap Backup & Recovery	Managed Backup Solution | 100 Devices	**$2100.00***
Cyber-Security SOC	vCISO Advisory Program	*Included in vCISO Advisory Pricing*
TOTAL		**$18,245.00**

**Pricing is based on RAVENii providing the licensing and monitoring. Pricing is also based off utilization (user, IP, bandwidth, device, etc.). If the City exceeds utilization, RAVENii will work with you to right size the environment or add more resources before charging any overage fees. Special configurations for departmental needs may increase cost. See rate card below.*

RAVENii rate schedule for services beyond the scope of activities as listed in this proposal:

- Security Engineer: $225/hour
- Security Architect: $250/hour
- Security Consultant: $325/hour
- Incident Response: $400/hour

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution

Option 2: All-Inclusive	**Bid Price**
Annual All-Inclusive Service All Items included in Scope of Work	$16,420.50/Month

© 2014 - 2021 RAVENii | Private & Confidential - Not for Redistribution