Outsmarting Cyber Adversaries Webinar

AGILEBLUE | elastic | carahsoft

Outsmarting Cyber Adversaries:

Advanced Threat Detection for State & Local with Elastic SIEM & AgileBlue AI

WEBINAR

PETER BURG
VP of Sales, AgileBlue

STEVE GEHRIS
Channel Sales Director, AgileBlue

AGILEBLUE | elastic | carahsoft

About Carahsoft

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider, supporting Federal, State and Local Government and Education and Healthcare organizations with IT products, services and training through our partners and contracts.

AGILEBLUE | elastic | carahsoft

Continuing Professional Education (CPE)

Carahsoft is pleased to offer **1.2** CPE credit to those that attend today's event.

To qualify for the credits, you must be:

- Actively listening and participating in the webinar
- Answer all 3 polling questions that will be presented through the presentation

If you meet the requirements, you will receive your certificate in 2 weeks.

WEBINAR

AGILEBLUE elastic carahsoft

Polling Question:

Did you have coffee today?

WEBINAR

AGILEBLUE elastic carahsoft

Featured Speakers:

PETER BURG
VP of Sales, AgileBlue

STEVE GEHRIS
Channel Sales Director, AgileBlue

WEBINAR

AGILEBLUE elastic carahsoft

Polling Question 1:

What is one of the biggest challenges currently facing SLED organizations?

A. AI-powered malware
B. Too many cybersecurity vendors
C. Alert fatigue and lack of 24/7 monitoring
D. Access to fast internet

WEBINAR

AGILEBLUE elastic carahsoft

Answer:

C. Alert fatigue and lack of 24/7 monitoring

Top Cybersecurity Challenges Facing State & Local Teams

Outdated, disconnected security tools

SLED is Highly Targeted

Regulatory compliance pressure (CJIS, NIST, HIPAA)

Lack of Product Integrations

Alert overload with limited staff to triage

24/7 threats without 24/7 response capability

Difficulty securing modern cloud infrastructure

Tight budgets and limited technical resources

A Unified Platform to Detect, Respond, and Secure Faster

8 critical defenses, in 1 powerful platform.

SAPPHIRE AI INSIGHTS

Sapphire, the platform's AI brain, delivers 98%+ accurate autonomous investigations, decisions, and responses.

ELASTIC SIEM

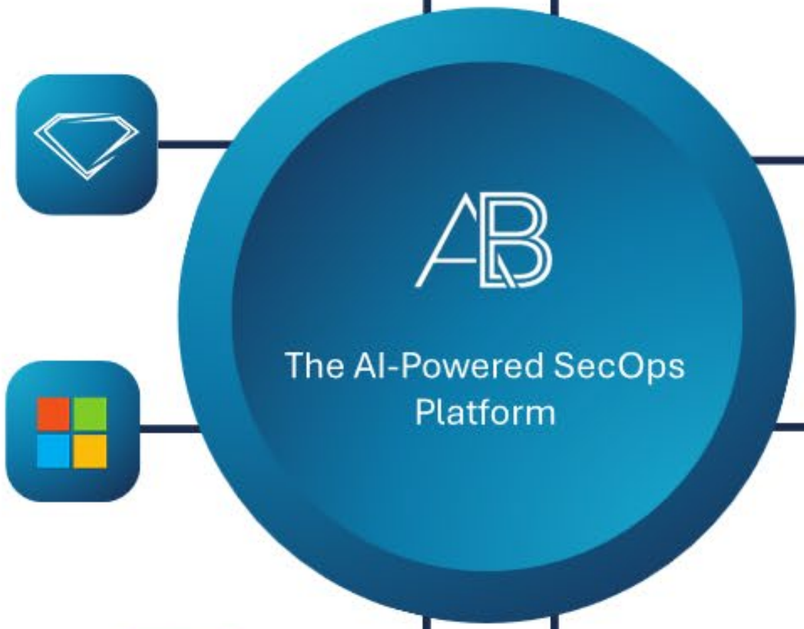
AI-powered SIEM optimizes threat detection, investigation, and response.

SAPPHIRE AI SOC ANALYST

Sapphire automates 90% of Level 1 and 2 tasks, boosting SOC efficiency and collaboration.

CERULEAN XDR AGENT

Secures endpoints, networks, apps, and cloud with AI and top-tier threat intelligence.



M365 SECURITY MODULE

Identifies Microsoft 365 misconfigurations with prioritized remediation plans.

CLOUD SECURITY

CDR tackles cloud attacks; CSPM secures configurations with full visibility.

VULNERABILITY SCANNING

Continuous vulnerability management, real-time protection, and rapid remediation.

CYBER RISK & POSTURE SCORING

Identify gaps, monitor risks, and reduce cyber threats by 75%.

WEBINAR

AGILEBLUE elastic carahsoft

How AI Is Changing the Cybersecurity Landscape

AI for Threat Actors

- Create more evasive, automated attacks
- Generate sophisticated phishing attempts

AI for Defenders

- Triage alerts and prioritize real threats
- Automate responses for faster mitigation

WEBINAR

AGILEBLUE elastic carahsoft

Polling Question 2:

2. Which of the following is a key benefit of integrating AI into threat detection and response?

A. It guarantees 100% threat prevention
B. It replaces all human analysts
C. It automates triage and reduces false positives
D. It eliminates the need for compliance frameworks

WEBINAR

AGILEBLUE elastic carahsoft

Answer:

C. It automates triage and reduces false positives

WEBINAR

AGILEBLUE elastic carahsoft

Sapphire AI:

AgileBlue's AI-Driven Threat Engine

Insights & Triage

Decisioning

Autonomous Response

WEBINAR

AGILEBLUE elastic carahsoft

Full Visibility, Meets Smart Automation

elastic

See threats across your entire environment in real time

Cut through alert noise with meaningful, high-fidelity insights

Detect unusual behavior before it becomes a breach

+

AGILEBLUE

Understand what's happening through simple, clear dashboards

Respond faster, with less manual effort. Get support when you need it, 24/7

Spend less time chasing alerts and more time securing what matters

Case Study: Nassau County

WEBINAR

Scaling Security Without Scaling Headcount

Challenge: Too many low-priority alerts, not enough staff

Result:

- 70% less time wasted on benign alerts
- 48% faster response to real threats
- 90% of triage automated

Lesson: Automation freed the team to focus on what mattered most

Case Study: Lee College

Going From Gaps to 24/7 Security in 3 Weeks

LEE COLLEGE

WEBINAR

Challenge: Needed 24/7 coverage, had limited staff

Result:

- Implemented AgileBlue in under 3 weeks
- Analysts investigated 2,500+ cases, filtered from 25,000 alerts
- Prevented 100+ O365 breach attempts

Lesson: Speed to protection + analyst backup made the difference

WEBINAR

AGILEBLUE elastic carahsoft

Polling Question 3:

3. Why is real-time visibility critical for modern SecOps in state and local government?

A. It helps catch low-priority alerts faster
B. It supports proactive response to emerging threats
C. It reduces the number of firewalls needed
D. It increases password complexity

WEBINAR

AGILEBLUE elastic carahsoft

Answer:

B. It helps catch low-priority alerts faster

WEBINAR

AGILEBLUE elastic carahsoft

Q&A

You bring the questions. We'll bring the clarity.

WEBINAR

AGILEBLUE elastic carahsoft

Let’s Keep the Conversation Going.

Peter Berg

VP of Sales

pberg@agileblue.com

/in/peteraburg/

Steve Gehris

Channel Sales Director

sgehris@agileblue.com

/in/steve-gehris-2468361/

Thank you for viewing AgileBlue & Elastic's Presentation! Carahsoft is pleased to serve AgileBlue & Elastic, working with an extensive ecosystem of resellers, system integrators, and solution partners who are committed to helping government agencies select and implement the best solution at the best possible value.

To learn how to take the next step toward acquiring AgileBlue's solutions, please check out the following resources and information:

For additional AgileBlue resources:
carah.io/AgileBlue Resources

For additional AgileBlue solutions:
carah.io/AgileBlueSolutions

To purchase, check out the contract vehicles available for procurement:
carah.io/AgileBlueContracts

To set up a meeting:
AgileBlue@carahsoft.com or 703-581-6680