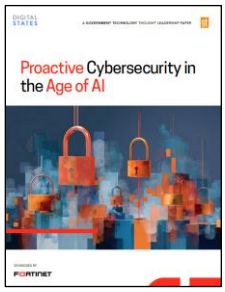

Proactive Cybersecurity in the Age of AI

Whitepaper

Thank you for downloading this Fortinet whitepaper. Carahsoft is the distributor for Fortinet cybersecurity solutions available via CMAS, NASPO, COTS, and other contract vehicles.

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

For additional resources:
carah.io/FortinetResources

For additional cybersecurity solutions:
carah.io/CybersecuritySolutions

To set up a meeting:
Fortinet@carahsoft.com
866-468-3868

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

For upcoming events:
carah.io/FortinetEvents

Fortinet@carahsoft.com 866-468-3868

DIGITAL STATES

A **GOVERNMENT TECHNOLOGY** THOUGHT LEADERSHIP PAPER

Proactive Cybersecurity in the Age of AI

SPONSORED BY:

FORTINET

The days of reactive cybersecurity should be over. Cybercriminals are faster, smarter and more persistent as they use AI to find new ways into systems. This calls for a new proactive model from security leaders in government.

By acting on real-time information, thinking ahead and adopting AI tools, agencies can disrupt and defend against insidious tactics from cybercriminals.

Turn Intelligence into Action

Many agencies collect threat intelligence but fail to act on it. "Too often, it just sits in reports instead of being mapped against adversary behaviors or integrated into detection playbooks," says Jason Palm, SecOps specialist engineer at Fortinet.

True security value happens when intelligence directly informs daily defense. Leaders should:

- Integrate threat intelligence into a continuous threat exposure management (CTEM) framework
- Use knowledge bases such as MITRE ATT&CK, which helps analysts improve detection and response
- Weave threat data into security information and event management (SIEM) and endpoint detection and response (EDR) systems
- Update detection playbooks
- Train analysts to map adversary behaviors

Use AI and Automation

AI and automation are best applied to routine, repetitive tasks. AI has the greatest impact in reducing alert noise, detecting anomalies and correlating data across multiple data sources.

Know Your Enemy:
The Biggest Threats to Government

"The problems agencies should be paying the most attention to are ransomware, supply chain attacks and identity-based threats," Palm says.

Ransomware remains the most significant threat, with bad actors using double and triple extortion techniques. They no longer just encrypt files — they also threaten to leak sensitive data.

Meanwhile, attacks on trusted vendors and software create new vulnerabilities. Agencies that rely on third-party providers may find attackers entering their systems through software updates or managed services.

Finally, identity-based threats such as credential theft and phishing are increasing as agencies move to cloud and hybrid environments.

Automation excels in handling routine and repetitive tasks such as triaging alerts, resetting accounts and enriching incident data.

"Using AI and automation extends the reach of small teams by removing a lot of the manual workload," says Palm. "Often, these repetitive tasks are what lead to job dissatisfaction and analyst burnout. AI and automation unburdens your staff from those tedious tasks, which allows them to focus once again on more meaningful and rewarding work, like threat hunting."

Stop Reacting and Start Anticipating

The key to successful cybersecurity is for agencies to be proactive and anticipate threats rather than waiting for alerts.

Palm notes that the 5th-century treatise, "The Art of War," is strikingly applicable to cybersecurity today.

"It says that if you know the enemy and you know yourself, you need not fear the result of 100 battles," says Palm. "If you know yourself, but not the enemy, for every victory gained, you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

That's why proactive practices, such as reconnaissance services, threat hunting, and tabletop or red team exercises, are critical. Agencies need to understand what adversaries may do and train staff to respond effectively. Many breaches can be reduced or even prevented if organizations focus on understanding adversary behaviors.

Map Attacks to Find Weaknesses

Breaking down an attack into tactics, techniques and procedures (TTPs) creates multiple points where agencies can detect and disrupt it, even after initial access. The approach provides more opportunities to catch the attackers during later phases, such as lateral movement, installing persistence mechanisms or starting to exfiltrate data.

Breaking down an attack into tactics, techniques and procedures (TTPs) helps you detect and disrupt it.

Recognizing and defending against known attack patterns helps expose blind spots and strengthens layered defenses, increasing the chance of avoiding damage.

Maintain Human Judgment

Human analysts remain essential. AI can detect patterns and suggest responses, but it's humans who understand mission context, exercise judgment and maintain ethical oversight. These are elements of institutional knowledge that let you align a threat response with an organization's specific priorities.

Collaboration makes for the strongest security operations model. AI adds speed, scale and efficiency, while humans validate, interpret and make final decisions that address organizational goals.

Conclusion

Adversaries will continue to innovate as AI becomes more sophisticated, so agencies must assume breaches will happen and focus on resilience.

Turning potential breaches into manageable incidents requires strong detection, rapid containment and practiced response.

Agencies that plan ahead, conduct exercises, and use AI and proactive frameworks will be best prepared for the threats they face today and those that emerge in the future.

This piece was written and produced by the Government Technology Content Studio, with information and input from Fortinet.

government technology

Produced by Government Technology
Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com

FORTINET

Sponsored by Fortinet
Visit us for more information on securing state and local governments with Fortinet's integrated security solutions, protecting critical infrastructure and meeting compliance standards.

www.fortinet.com/solutions/industries/government/state-and-local

ADOBESTOCK/AI GENERATED