GENERAL DYNAMICS
Information Technology

RESEARCH STUDY

Bedrock Defenses

Agency Guide to Defensive Cyber Operations

In partnership with

splunk>

Foreword

In an era where the threats and technologies are ever increasing and data is expansive, federal agencies find themselves constantly balancing on a tightrope of reducing risks and balancing costs. On one side lies the vast expanse of opportunities that technology offers and on the other is an ever-evolving mosaic of cyber threats. It is within this dynamic environment that the principle of "bedrock defenses" emerges, solidifying our commitment to creating foundational, unyielding strategies in defensive cyber operations.

The federal government's 2024 budget for civilian agencies includes a 13 percent increase over this year's spending levels. Many of the budget priorities focus on reducing the risk and impact of cyber incidents based on data-driven and risk-based assessments of agency cyber postures. This increased focus is on securing and modernizing digital infrastructure, ranging from improving incident sharing and reporting to protecting critical infrastructure, maturing cyber reporting and analytics, enabling zero trust, and even transitioning to quantum-safe cryptography. Cyber threats are a continued top risk to delivering critical government services as adversaries perennially pursue new and advanced measures to compromise agency systems.

The very essence of "bedrock" is stability, strength, and resilience, and it is these principles that must be mirrored in our cyber defense foundations. This report explores the robust layers of cyber defense, analyzing the most pressing challenges, evaluating the effectiveness of current strategies, and highlighting the impactful technologies driving our cyber fortifications.

The landscape of cyber threats is vast and ever evolving, but our research paints a picture of federal agencies innovating, adopting proactive measures, and adapting their strategies as needed. Our research provides insights into the role of real-time data, the potential of AI, and the impact of automation; and this report provides a clear-eyed view of where we stand and where we need to go.

DR. MATTHEW MCFADDEN
Vice President, Cyber
GDIT

Executive Summary

Agencies must wrestle with where to focus and mature while also navigating competing budget priorities, unfunded mandates with tight timelines, and new cybersecurity strategy directives. This research study identifies the "bedrock defenses" that will help prioritize and mature the most important technologies necessary to confront the ever-increasing cybersecurity threat.

Bedrock Defenses delineates a holistic approach, fusing foundational strategies with innovative solutions to safeguard digital assets, data, and the nation's cybersecurity infrastructure.

Defensive cyber operations (DCO) emerge as a paradigm shift from mere reactive strategies to a proactive, resilience-focused approach. Rooted in stability and adaptability, DCO is not just about countering present threats but foreseeing potential challenges and arming agencies with the tools and tactics to navigate and mitigate the vast and intricate cyber threat landscape.

Harnessing quality data effectively, leveraging the predictive capabilities of AI, championing automation, and emphasizing proactive security designs are among the pivotal strategies explored in this guide. Additionally, while compliance remains a cornerstone, the guide underscores the importance of transcending standard benchmarks to fortify defenses, ensuring not just adherence but excellence in securing digital assets.

This guide shines a light on the current cyber terrain while also charting a path toward a comprehensive, resilient, and forward-leaning cyber defense strategy for agencies.

1

FOUNDATION OF CYBERSECURITY

Agencies unanimously affirm that the cornerstones of defensive cyber operations rest upon cyber threat intelligence, network detection, intrusion prevention, security incident event management, and scrupulous vulnerability management.

2

NAVIGATING DATA ABUNDANCE

A significant 41% of respondents find themselves submerged in data, requiring analytical prowess. Additionally, 36% of respondents highlighted a stark need for more skilled personnel and 31% advocated for enhanced real-time analytic tools.

3

HUMAN FACTOR IN CYBER THREATS

The human element remains a considerable vulnerability, with 41% of agencies pinpointing misconfigurations and human error as pivotal challenges that amplify cyber threats.

4

AI: THE PREDICTIVE POWERHOUSE

Agencies recognize the potential of artificial intelligence in cybersecurity, with 26% valuing its capacity for real-time threat detection and 25% underlining the consequential role of automation in real-time mitigation and countermeasures.

5

METRICS-DRIVEN FUTURE OUTCOMES

Adopting a forward-thinking stance in defensive cyber operations, 25% of agencies emphasize the criticality of metrics such as the frequency and severity of security incidents, underscoring the need to strategize for the impending future, not just the present moment.

Threat Landscape Overview

At the heart of the defensive cyber operations mission lies the imperative to defend against an ever-evolving array of cyber threats and attacks. It's crucial for agencies to stay ahead, equipping themselves with cutting-edge cyber defense strategies, techniques, capabilities, and timely alerts to proactively reduce threat exposure and mitigate potential attack vectors. This, in turn, optimizes an agency's security posture

As agencies continue their journeys in defensive cyber operations, it's essential to prioritize capabilities that offer the best value, make a tangible impact in reducing organizational risk, and can scale in response to the threat landscape of today and tomorrow.

Challenges in Defensive Cyber Operations

THREAT LANDSCAPE

Monitoring data across hybrid environments, critical infrastructure, and operational technology is becoming increasingly challenging. With data and environments continually expanding, resources for response remain limited. Compounding this issue is the ever-complex nature of the attack surface.

COMPLIANCE AND MANDATES

The push for cybersecurity modernization means agencies are contending with a growing list of mandates. These encompass areas like zero trust adoption, secure supply chain, enterprise endpoint detection and response, effective log management, and cloud adoption.

CYBER AUTOMATION

The expanding threat landscape and hybrid environments amplify complexity. Agencies must increasingly rely on automation to reduce the burden on their workforce and expand capabilities, thus ensuring near real-time threat response.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING (AI AND ML)

AI and ML stand as a beacon for advanced threat detection and response. A plethora of cyber solutions integrate AI capabilities for detection and response. The challenge lies in identifying the use cases to apply these capabilities most effectively.

OPERATIONAL TECHNOLOGY

The spotlight on operational technology, which encompasses internet of things (IoT) devices, mission technology, weapons systems, and industrial control systems, has grown brighter, especially given its integration with enterprise IT. This convergence has highlighted significant risk areas, particularly around critical infrastructure.

PRIORITIZATION AND VISIBILITY

Understanding cyber capability rationalization and its effectiveness remains a significant hurdle. Agencies, rightfully, aim for meaningful cyber risk reduction rather than mere compliance. It's essential to execute a strategy that ensures the best return on investment and bridges visibility gaps in large agency enterprises.

PREVENTION

Many agencies prioritize response over prevention. This approach might overlook the essential capabilities, sensors, and processes required for effective cybersecurity analytics, especially when aligned with cyber threat intelligence. The goal is to gravitate toward autonomous and proactive threat detection and response.

TALENT SHORTFALL

The cybersecurity domain continues to face a significant talent gap. This shortfall not only hinders proactive defense measures but also leaves agencies reactive in the face of novel cyber threats. Investing in training and talent acquisition remains paramount to bridge this gap and bolster defense mechanisms. AI and automation also offer promising solutions. While automation streamlines routine tasks and threat detection, AI plays a crucial role in predictive analytics and threat pattern recognition. These technologies can free up skilled professionals for higher-level priorities and strategy planning.

WHO WE SURVEYED

GDIT's Digital Consulting Practice partnered with an independent research firm to design an online survey of 200 federal government leaders across defense, civilian, intelligence and homeland security agencies. Respondents were GS-12 and above and involved in either the selection or management of firms that provide cybersecurity capabilities and services. These respondents represent a cross section of the individuals and roles that are responsible for driving their agency's cybersecurity technology and mission decisions focused on defensive cyber operations

Foundations of Defensive Cyber Operations

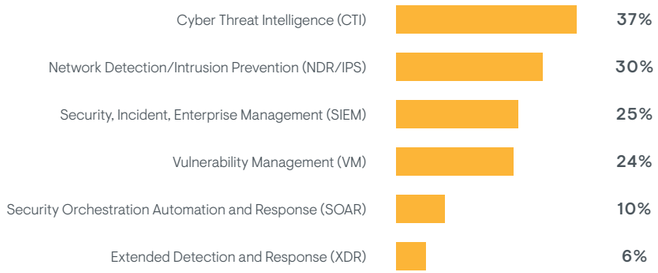
At the heart of defensive cyber operations lies the security operations center (SOC). Serving as the linchpin for an organization's security and cyber defense, the SOC continuously monitors and defends against potential threats. Its core responsibility revolves around timely detection, analysis, and response to cybersecurity challenges.

The broader defensive cyber operations framework deploys a combination of technical, managerial, and operational controls. These controls encompass a wide range of tools for scanning, monitoring, and responding. The aim is to collate, correlate, and analyze threat and security-related data from diverse sources, including perimeter defenses, network devices, cloud platforms, and endpoint agent feeds. By harnessing these myriad data streams, DCO capabilities provide a panoramic situational awareness, enabling organizations to gauge and refine their security postures and respond in real-time.

To execute DCO tasks effectively, teams need to employ a harmonious mix of cybersecurity tools and integrations. Coupled with pertinent cybersecurity data analytics and threat intelligence, this combination facilitates a comprehensive approach to identify, protect, detect, respond, and recover. The pivotal decision lies in selecting the appropriate defensive cyber capabilities to preempt and thwart potential attacks.

CRITICAL TECHNOLOGIES

Technologies most critical for proactive defensive cyber operations (DCO)



Our research highlights certain "bedrock" technologies deemed indispensable by most agencies:

- Cyber threat intelligence
- Network detection and intrusion prevention
- Security incident event management
- Vulnerability management

By emphasizing these foundational capabilities, agencies can bolster their protection mechanisms and heighten situational awareness. Interestingly, extended detection and response (XDR/EDR) capabilities ranked lower in priority, at just 6%. Given the growing emphasis on cloud-native security, DevSecOps, containers, and no code and low code solutions, this might signal a shift in focus.

AI-Driven Cyber Defense Strategies

In light of the White House's recent executive order on artificial intelligence, agencies are poised to further integrate AI to bolster their cyber defenses. This directive catalyzes a strategic shift, encouraging a proactive stance in adopting AI-driven solutions to anticipate, identify, and neutralize cyber threats more efficiently.

To maintain robust cyber defenses, agencies must strike a balance between foundational cybersecurity capabilities and the integration of innovative defensive technologies. By rooting their strategies in core best practices while also harnessing cutting-edge measures, such as AI, agencies can amplify their defense capabilities.

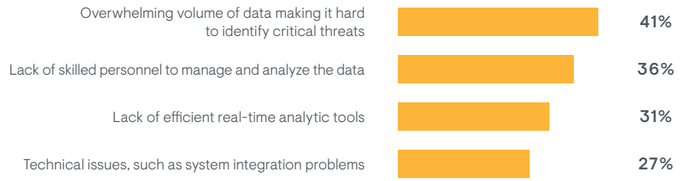
Harnessing AI to Navigate the Data Surge

The digital landscape creates vast volumes of data, often masking genuine threats. A significant 41% of agencies share this concern. This data surge is accentuated by a notable skills gap, with 36% of respondents saying they lack the skilled personnel to manage and analyze data. Moreover, 31% spotlight a lack of efficient real-time analytic tools.

The way forward hinges on adeptly navigating this burgeoning data landscape, bolstering real-time analytics with AI-driven tools, and harnessing skilled personnel for deeper data insights. Adopting security data management strategies, especially for hybrid environments, and leveraging cloud-native security paired with advanced AI and ML tools, can provide agencies with a decisive edge in tackling these challenges.

DATA CHALLENGES

Most significant challenges to obtaining and utilizing real-time security data



Automating to Offset Human Error

Human oversights, often unintentional, can create significant vulnerabilities, a sentiment echoed by 42% of respondents. These missteps can inadvertently open doors for cyber adversaries. Alongside this reality, 24% of respondents point to malware and ransomware threats as significant risks, and another 24% say social engineering and phishing attacks pose significant risks as well. The roadmap to fortification involves focusing on resilience, repeatability, and automation, adopting a "secure by design" ethos, and integrating AI to enhance decision-making processes.

CYBER THREATS

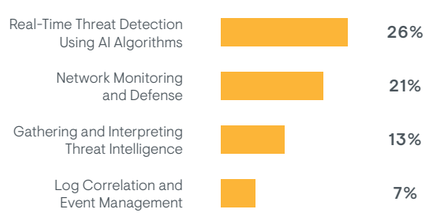
Most significant threats to agency cyber defense strategies

Enhancing Cyber Incident Responses through Automation and AI

Emerging cyber threats, with their unpredictable nature, pose a constant challenge. This is where AI and automation shine. The predictive prowess of AI can preemptively identify threats, a belief held by 26% of agencies focusing on real-time threat detection. Another 21% see AI's potential in network monitoring and defense. AI-driven insights, amplified by automation, can rapidly counter human errors, a perspective shared by 25% of respondents, emphasizing automation's role in real-time mitigation. The transformative impact of AI and ML, especially in handling vast data and bolstering real-time analytics, can be game-changing. Their ability to scale the cyber workforce, provide in-depth analysis, and target high-priority objectives can redefine cybersecurity paradigms.

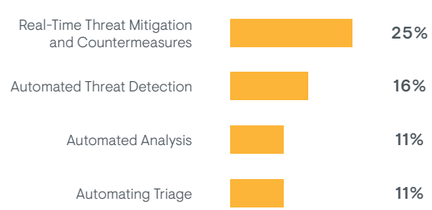
AI'S IMPACT

The greatest impact of AI in defensive cyber operations



AUTOMATION'S IMPACT

The greatest impact of automation in defensive cyber operations



Measuring Success

Anchoring DCO in compliance with cybersecurity standards and regulations – the benchmark for 36% of agencies, according to our survey – ensures fundamental adherence to vital requirements. This data shows that respondents view DCO as a critical element of compliance, ensuring that agencies meet statutory guidance and requirements.

Compliance is an enabler to driving effective security operations and countering cyber adversaries. Agencies view this as an important area of focus in order to validate, improve, and measure the quality of their cyber operations.

Cyber adversaries are innovators, perpetually devising new strategies to bypass defenses. So, merely adhering to existing standards can leave agencies perennially a step behind.

- DCO offers agencies the tools, capabilities, and strategies to not only meet but surpass compliance requirements, enhancing their cybersecurity scorecards and audit results.
- DCO serves as a tangible measure of compliance, validating agencies' adherence to mandated criteria.
- It's essential for agencies to leverage DCO's potential in driving meaningful outcomes and achieving broader objectives.
- Central to DCO is its role in equipping agencies to anticipate, defend, and counter both present and emergent threats.

Proactive Defense and Anticipation

A forward-leaning DCO posture requires agencies to not just respond to the present but also anticipate the future. The frequency and severity of security incidents are vital metrics, indicated by 25% of surveyed agencies, providing insights into the resilience and adaptability of cyber defenses against current threats.

- Embracing proactive defense tools, like AI and ML, can optimize threat detection across diverse organizational landscapes.
- Defenses are only as good as the data they draw upon. This necessitates accounting for dynamic environments, including hybrid clouds and unconventional security data, which also present adversary targets.
- Crafting an impactful data security strategy is paramount for harnessing data effectively, accommodating an expanding threat horizon, and ensuring comprehensive situational awareness.

Swift and Decisive Response

In our survey, 18% of respondents underscored the time to detect and respond to incidents as a key operational effectiveness metric, melding swift reactive capabilities with proactive defense innovation. It is therefore critical to integrate automated systems that not only detect and respond to threats in real-time but also learn from them to enhance future responses.

- Accelerating toward autonomous cyber defense is vital for enabling agencies to counter threats in real-time, ensuring broad-spectrum responsiveness.
- Such an approach requires a nuanced balance of trust and fostering collaboration across the organization while also keeping all stakeholders informed and engaged.
- Enhanced automation allows the cyber workforce to focus on critical threats and high-priority tasks, fostering a more mature and agile defensive cyber strategy.
- Prioritizing metrics like mean time to detect and respond can also ensure better ROI on deployed capabilities.

DATA CHALLENGES

Most significant challenges to obtaining and utilizing real-time security data

36%
Compliance with cybersecurity standard and regulations

25%
Frequency and severity of security incidents

21%
Regular passing of cybersecurity audits

18%
Time to detect and respond to incidents

Advancing Defensive Cyber Operations

Cyberspace is not only a conduit for innovation and progress but also a dynamic arena of constant and evolving threats. Navigating that complex landscape demands an integration of fundamental and advanced strategies.

DCO safeguards the integrity, confidentiality, and availability of digital assets and data. Recognizing and fortifying the foundational elements of DCO is more than a strategic advantage—it's an imperative for national security, public trust, and the seamless operation of critical infrastructures.

As we chart the future course, these insights underscore the need for agencies to continually evolve, anticipate challenges, and implement both foundational and cutting-edge measures to maintain robust defenses in the face of cybersecurity threats. The following are recommendations to further mature the defensive cyber operations journey.

1

FOCUS ON DEFENSIVE CYBER OPERATIONS "BEDROCK" CAPABILITIES

Prioritizing core elements of defensive cyber operations, such as cyber threat intelligence, network detection and intrusion prevention, security incident event management, and vulnerability management, form the bedrock of a resilient cyber defense. Doing these well and maturing them proactively reduces threats to the organization.

2

EMPHASIZE CYBERDATA STRATEGY

As we move into an era of data abundance, architecting a coherent cybersecurity data strategy becomes crucial. Harnessing quality data and pairing it with real-time analytics augments situational awareness and aids in incisive decision making.

3

SECURE BY DESIGN

A preemptive approach to security involves embedding resilience and repeatability into infrastructure and application design, thus hardening the architecture. This proactive stance ensures security operations have the telemetry needed for the early detection of vulnerabilities and misconfigurations before they can be exploited.

4

ELEVATE COMPLIANCE

Harnessing defensive cyber operations tools and operations can drive more mature and demonstrable compliance. Such integration validates control mechanisms and offers tangible outcomes, spanning governance, risk management, and compliance.

5

FORCE MULTIPLY WITH AI AND ML

The exponential growth of data and increasingly complex threat vectors make AI indispensable. By deploying AI, agencies can preemptively defend, sift through vast data troves, measure key outcomes, and bolster the efficiency of the cybersecurity workforce, offering real-time threat detection and mitigation.

6

CHAMPION AUTOMATION

Embracing an "automation-first" approach provides agility in cybersecurity initiatives. Automation, from hardening to real-time threat response, offers speed, precision, and scalability.

GDIT

About GDIT Digital Consulting

General Dynamics Information Technology (GDIT) stands at the nexus of digital consulting and mission-centric innovation in the public sector. As the pace of technology changes and as mission demands accelerate, GDIT's Digital Consulting Practice supports agencies navigating intricate landscapes and harnessing the transformative potential of AI, cybersecurity, and cloud solutions. Partnering with visionary leaders across the public domain, we craft strategies that catalyze digital evolution, drive sustainable modernization, and position our clients at the forefront of excellence.

About GDIT

GDIT is a global technology and professional services company that delivers consulting, technology and mission services to every major agency across the U.S. government, defense and intelligence community. Our 30,000 experts and consultants extract the power of technology to create immediate value and deliver solutions at the edge of innovation. We operate across 30 countries worldwide, offering leading capabilities in digital modernization, AI/ML, Cloud, Cyber and application development. Together with our clients, we strive to create a safer, smarter world by harnessing the power of deep expertise and advanced technology. More information about GDIT is available at **www.gdit.com**.

splunk>

About Splunk

For public sector leaders entrusted with mission success, Splunk offers an enterprise-wide solution with a unified security posture and data analytics capabilities to help them make confident decisions — and take action. Splunk's ability to provide real-time, data-driven insights helps agencies unlock innovation, improve security and prepare for the mission ahead. More information about Splunk is available at **www.splunk.com**.

Contact

GENERAL INQUIRIES

Christopher Aiello
Senior Marketing Manager
GDIT
Email: christopher.aiello@gdit.com

Jay Srinivasan
Senior Public Relations Manager
GDIT
Email: jayendran.srinivasan@gdit.com