STRATEGIC RESILIENCE: ENHANCING INCIDENT RESPONSE CAPABILITIES FOR GOVERNMENT AND MILITARY OPERATIONS

A GUIDE TO ACCELERATING ASSURANCE: LEVERAGING AUTOMATION FOR SWIFT INCIDENT RESPONSE.

JUNE 2023

kineticdata.com
fedsales@kineticdata.com

KINETICDATA

INTRODUCTION

Effective incident response is vital to ensure the information security and operational continuity of every enterprise.

Cyber threats hold particularly significant consequences in military and national security applications. Rather than financial losses or business disruptions, the stakes involve safeguarding sensitive information that, if compromised, could directly impact lives and national security.

Government agencies in general and our armed services in particular also face unique constraints compared to the private sector, in terms of operational requirements, regulatory compliance, and international cooperation and coordination, among others.

Federal civilian agencies and the military need new approaches that address both the unique challenges and constraints in their incident response environments. Currently installed systems have a number of limitations, from complexity to compliance, speed, and information sharing issues.

> The ideal incident response solution for government and military applications would address the specific challenges and constraints of these environments in a **secure, compliant, flexible, and fiscally responsible manner.**

This solution would combine sophistication in capabilities with simplicity in use and implementation, resulting in a practical solution that maximizes security and uptime. Two clear benefits emerge: free up time for warfighters and resources to support the mission, and enable information sharing widely across the DoD environments.

WHAT IS INCIDENT RESPONSE?

Incident response is a set of processes and procedures that organizations use to identify, investigate, and respond to security incidents or other types of unexpected events that could have a negative impact on their IT infrastructure, data, or operations.

These incidents can include anything from cyberattacks and data breaches to hardware failures and natural disasters. The goal of incident response is to minimize the damage caused by these incidents and restore normal operations as quickly as possible.

Typically, incident response involves the following steps:

1. **Preparation**: Developing a plan and procedures for how to respond to potential incidents, including assigning roles and responsibilities, establishing communication channels, and creating backup and recovery strategies.
2. **Detection and Analysis**: Monitoring systems for signs of potential incidents, investigating any suspicious activity, and determining the scope and severity of the incident.
3. **Containment**: Isolating the affected systems or data to prevent further damage and implementing temporary measures to maintain operations while the incident is being investigated.
4. **Eradication**: Identifying and removing the root cause of the incident, such as malware, hardware component failure, or a misconfigured system.
5. **Recovery**: Restoring systems and data to their normal state and verifying that they are functioning properly.
6. **Lessons Learned**: Reviewing the incident response process to identify areas for improvement and update the incident response plan accordingly. A key component of this is measuring the satisfaction of everyone involved in the detection, correction, and recovery processes, as well as those impacted by the incident. Any concerns or issues raised should feed into the process improvement and response plan update cycle.

INCIDENT RESPONSE CHALLENGES FOR THE U.S. MILITARY AND DoD

Incident response within the federal government in general, and within the military and DoD specifically, involves a unique set of challenges and problems. Among the most significant are:

- **Sophisticated Cyber Threats**: The increasing sophistication and frequency of cyber attacks pose a significant challenge for incident response in the military. Adversaries constantly evolve their tactics, techniques, and procedures, making it difficult to detect and respond to their attacks effectively. These threats come from both state actors (e.g., foreign intelligence services) and non-state attackers (cyber criminals).[1] Attacks identified as "cyber warfare" increased 440% between 2009 and 2018.[2] There were 38 "significant cyber incidents" targeting government agencies, defense contractors, and tech companies in the U.S. and allied countries in just the first three months of 2023.[3]

- **Large, Complex Networks**: Military organizations operate vast and complex networks, comprised of numerous interconnected systems, devices, and platforms. Managing and securing these networks is a challenge, as incidents can occur at different levels and require coordinated response efforts. It's nearly impossible to find accurate data on the scope of the military's computer networks, but it was reported that the DoD was operating "more than 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe"—back in 2011[4]. The total defense information technology/cyberspace activities (IT/CA) budget for 2023 is estimated at $57.9 billion.[5] The DoD has acknowledged this massive scope and complexity and addressed it through strategic modernization plans in 2011[6], 2014, and 2019[7].

- **Limited Visibility and Attribution**: Military networks often present challenges in achieving comprehensive visibility into their systems and networks. Attribution, or identifying the source of an attack, is also complex due to the presence of sophisticated threat actors and the use of deceptive techniques to conceal their identity.

- **Strict Operational Requirements**: The military operates under strict operational requirements[8], such as mission readiness, operational security, and maintaining a high state of operational tempo. Balancing the need to respond to incidents promptly with these requirements can be challenging, requiring careful coordination and prioritization.

- **International Jurisdiction and Cooperation**: Incidents targeting military organizations frequently originate from foreign entities, raising challenges related to international jurisdiction and cooperation. Addressing these incidents effectively often requires coordination with other nations, sharing of information, and adherence to legal and diplomatic considerations. In one recent year, 69% of breaches and cyber attacks on the USA originated from outside the country.[9] Over the past two decades, cyber attacks have been launched against the U.S. government and military from more than 20 different countries—including some allied nations[10]. The U.S. Cyber Command has conducted multinational cyber exercises[11] to bolster international coordination, and the recently released National Cybersecurity Strategy emphasizes working with international allies and partners to enhance digital resilience[12].

- **Limited Resources**: Like any organization, the military faces constraints in terms of personnel, budget, and technology. These limitations can impact the availability of skilled incident response professionals, advanced tools, and sufficient training, making it harder to respond effectively to incidents.

- **Regulatory Compliance**: The US Department of Defense must adhere to various regulatory frameworks, such as the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)[13] and other compliance requirements. Ensuring compliance during incident response can be challenging, particularly when responding to complex and rapidly evolving threats.

- **Insider Threats**: The military faces risks from insider threats, where authorized personnel with access to sensitive information and systems can misuse or exploit their privileges. Detecting and responding to incidents caused by insider threats requires a delicate balance between trust and security. Allowing an insider breach to go undetected, such as during the Teixeira affair, damages our national security, puts our intelligence assets at risk, and undermines the trust of our allies.[14]

- **Strict Operational Requirements**: The military operates under strict operational requirements[8], such as mission readiness, operational security, and maintaining a high state of operational tempo. Balancing the need to respond to incidents promptly with these requirements can be challenging, requiring careful coordination and prioritization.

- **International Jurisdiction and Cooperation**: Incidents targeting military organizations frequently originate from foreign entities, raising challenges related to international jurisdiction and cooperation. Addressing these incidents effectively often requires coordination with other nations, sharing of information, and adherence to legal and diplomatic considerations. In one recent year, 69% of breaches and cyber attacks on the USA originated from outside the country.[9] Over the past two decades, cyber attacks have been launched against the U.S. government and military from more than 20 different countries—including some allied nations[10]. The U.S. Cyber Command has conducted multinational cyber exercises[11] to bolster international coordination, and the recently released National Cybersecurity Strategy emphasizes working with international allies and partners to enhance digital resilience[12].

- **Limited Resources**: Like any organization, the military faces constraints in terms of personnel, budget, and technology. These limitations can impact the availability of skilled incident response professionals, advanced tools, and sufficient training, making it harder to respond effectively to incidents.

- **Regulatory Compliance**: The US Department of Defense must adhere to various regulatory frameworks, such as the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)[13] and other compliance requirements. Ensuring compliance during incident response can be challenging, particularly when responding to complex and rapidly evolving threats.

- **Insider Threats**: The military faces risks from insider threats, where authorized personnel with access to sensitive information and systems can misuse or exploit their privileges. Detecting and responding to incidents caused by insider threats requires a delicate balance between trust and security. Allowing an insider breach to go undetected, such as during the Teixeira affair, damages our national security, puts our intelligence assets at risk, and undermines the trust of our allies.[14]

Beyond malicious insider attacks, unintentional errors by well-meaning employees and contractors can lead to breaches and intrusions. According to **Lieutenant Colonel Stephen A. Roberts, Ph.D.:**

> Non-malicious insiders can also have devastating, long term impacts, given their ongoing, sometimes multi-year interaction and decision-making related to DoD IT systems. Non-malicious insiders typically make a myriad of poor decisions (e.g., by clicking on spam email links, misplacing Common Access Cards [CAC], leaving devices unlocked, visiting insecure websites, introducing malware onto networks, leaving government assets unsecured, or ferrying DoD data across home and public resources).
>
> "The DoD employs about 3.5 million military and civilian direct employees, contractors, and reserve personnel[1]. In addition, over 50,000 contracted entities (e.g., groups and organizations) can connect to the DoD Information Network (DoDIN) to collaborate and protect DoD systems and sensitive data. These imperfect human users often interact with the DoD across multiple classification domains and IT systems. To illustrate the problem, if only 0.1% of the insiders produce one activity per year resulting in an incident, this equates to more than 3,500 annual incidents.[15]

Addressing these challenges requires a comprehensive incident response framework, collaboration among different military branches and agencies, advanced technologies for threat detection and response, continuous training and education for personnel, and a proactive approach to threat intelligence and information sharing.

LIMITATIONS OF TODAY'S INCIDENT RESPONSE SYSTEMS IN GOVERNMENT AND THE MILITARY

U.S. federal government agencies and military service branches face a number of limitations and issues with the incident response systems currently in place. These include:

1. **Fragmentation and Lack of Coordination:** Various federal government agencies and military branches often operate their own incident response systems, leading to fragmentation and a lack of coordination[16]. This can result in challenges in sharing information, coordinating response efforts, and achieving a unified and effective incident response across the entire government. According to the DoD, "Complex and fragmented information systems environments plague Warfighters on the ground." Consequently, among its recommended strategic guiding principles for zero trust execution is, "Simplify and automate: Establish appropriate governance controls that continuously modernize the existing fragmented approaches to data management, IT modernization, and cybersecurity policies and solutions."[17]
2. **Slow Response and Remediation:** The complexity of government systems and bureaucratic processes can lead to slow response and remediation times. Delays in detecting and responding to incidents can allow attackers to persist within networks, potentially causing significant damage before they are identified and mitigated. The SolarWinds hack remains a disturbing example[18]. While government-specific data isn't available, IBM has reported that across industries, the average time to detect and contain a cyber attack is 287 days[19] (more than nine months), while Verizon has found that 56% of breaches take months or even years to detect.[20]
3. **Limited Information Sharing**: While there has been noteworthy progress in improving information sharing between government agencies, barriers and challenges still exist. Sharing classified or sensitive information across agencies, and between government entities and private sector contractors working with the government[21], can still be complex, hindering timely and effective incident response.
4. **Inadequate Training and Workforce Shortages**: The shortage of skilled cybersecurity professionals and the need for ongoing training create challenges for incident response in government agencies and the military[22]. There were 40,000 unfilled cyber security jobs open in the public sector as of April 2022[23]. Limited resources and budget constraints may make it difficult to attract and retain qualified personnel, resulting in a workforce gap and potentially slower response times.

5. **Legacy Systems and Infrastructure**: Many government agencies and military branches still rely on legacy systems and outdated infrastructure[24]. These systems may lack modern security controls and capabilities, making them more vulnerable to component failure as well as attacks, and hampering incident response efforts.
6. **Compliance Burdens**: Government agencies must comply with numerous regulatory frameworks and compliance requirements, as noted above. Ensuring compliance during incident response activities can be burdensome and time-consuming, diverting resources from timely incident handling.
7. **Resource Constraints**: Government agencies and the military often face budget constraints and limited resources[25]. Insufficient funding can restrict investments in advanced technologies, tools, personnel, and training necessary for effective incident response.

Problems related to speed, outdated technology, and resource constraints are not purely budgetary issues. As pointed out in Foreign Policy magazine:

> "There are many hindrances to efficiently divorcing the U.S. military from old technologies. First, for technology to be widely adopted across an enterprise like the Pentagon, it needs to be woven into bureaucratic structures, which are inherently sticky. Recruitment and training of personnel for specialized skill sets, the development and implementation of standard operating procedures, costly facilities, maintenance, and other supporting investments are necessary to enable the use of technology.
>
> "Furthermore, bureaucracies often build their identities around technology, turning threats to the technology into threats to the organization's very essence. The resulting entities are often large, complex, and full of self-interested actors who seek to maintain and expand their bureaucratic realms. Once these organizations exist, they are extremely difficult to dismantle."[26]

Addressing these limitations and issues requires improved interagency and private sector collaboration, enhanced information sharing mechanisms, investment in modernizing infrastructure and systems, increased recruitment and training of cybersecurity professionals, and adequate funding to support incident response capabilities across government agencies and the military.

THE KINETIC DATA APPROACH TO INCIDENT RESPONSE

There is certainly no shortage of private-sector technology companies promising to solve the unique problems and address the specific issues of federal government agencies and the military.

Unfortunately, their answer is frequently to undertake yet another large-scale, multi-year IT project or platform implementation. The logic seems to be that since the federal government is a large entity with complex needs, the solution must be a large, complex software suite.

That is flawed logic.

Across a massive, decade-long study of large-scale IT project, McKinsey[27] found that:

- More than 40% of projects exceed their initial budget.
- Less than half are completed on time, or deliver the intended benefits.
- Just one in 200 projects meet all three measures: schedule, budget, and benefits.
- Public-sector projects are more likely to exceed budgets and timelines than private-sector initiatives.
- Eight out of 10 public-sector projects take longer than expected, and half run over budget.

A better approach is to adopt an agile framework. Start with a small project of limited scope with limited resource requirements (i.e. people) to prove value. Iterate, modify, and scale up to solve larger problems for more users. Apply lessons learned at each stage to enable continual improvement. This process is formally outlined in our Kinetic Automation Maturity Model.

With an agile approach, cost, time, and risk are all reduced. Users see real benefits, faster, increasing adoption and avoiding resistance to change. Training time is slashed. The Kinetic Platform from Kinetic Data enables organizations to adopt this agile, iterative approach. It provides solutions for incident response that are comprehensive but can be rolled out incrementally, at the speed of each agency or department. What might key processes look like?

This simple table outlines four foundational processes for Incident Response:

Automation Incident Process:	**Workflow automation can be used to…**
Notification	Automatically notify the appropriate personnel of an incident, including the incident response team, the affected employees, and the public. This can help to ensure that everyone who needs to know about the incident is notified quickly and efficiently.
Triage	Automatically triage incidents, which means to assess the severity of the incident and determine the appropriate response. This can help to ensure that incidents are responded to in a timely and effective manner.
Response	Automate the response to incidents, which means to take the necessary steps to resolve the incident and mitigate the damage. This can help to reduce the time and resources required to respond to incidents.
Reporting	Automatically generate incident reports, which can be used to track the progress of incidents and identify areas for improvement. This can help to improve the overall incident response process.

Rather than requiring a large-scale, time-consuming, risk-laden “rip and replace” type implementation, the Kinetic Platform lets you create a purpose-built, user-friendly system of engagement atop the systems of record[28] already in place. Workflows can be automated through integrations to existing back-end systems.

THE KINETIC PLATFORM PROVIDES:

- **Security**: ABAC (Attribute Based Access Control) approach meets military standards and supports the ongoing Zero Trust initiative. Software is delivered on premise or in the cloud. In the near future, Kinetic Data will be FedRamp certified for utilization across DoD entities.
- **Multitenancy**: Providing one platform for multiple accounts brings faster route to value, reduces cost and allows for unique handling of processes per tenant.
- **Scalability**: Horizontal scale allows the Kinetic Platform to both scale for 100,000s of users, as well as the ability to scale down to a single server for a small number of users in an air-gapped environment for example.
- **Integration-friendly**: The capability to connect and communicate with any number and variety of cloud-based and legacy systems.
- **Flexibility**: The Kinetic Platform and its starter templates are "built for mission". Users design and control the entire end to end experience, from field selection, integrations, and underlying workflow processes - to get exactly what is needed for greater speed and faster time to resolution.
- **Continuous Improvement**: Clone and modify existing workflow processes to create new options; use conditional branching to simplify the front-end interface and improve user experience by requesting only the information required for the task.
- **Compliance**: Common Access Card (CAC) integration, Zero Trust model, and STIG compliance.
- **Visibility**: See what's happening at any time within workflows and check the current status (e.g., has a request been approved, or if not, how long has it been waiting), and view workflow processes after-the-fact to monitor performance, audit incidents, and continually improve process design.

In short, the Kinetic Platform provides federal agencies and military service branches with a secure, flexible, compliant incident response system that meets the unique needs in these environments. Its usage-based pricing model avoids unnecessary costs. And its agile, iterative implementation approach delivers tangible benefits faster while reducing project risk.

Contact us to learn more about our Incident Response solution for our military, Department of Defense, and federal government agencies.

ABOUT KINETIC DATA

Kinetic Data provides workflow automation software to government agencies. We focus on high-volume, complex, mission-critical workflows that automate processes and speed decision-making for the war fighter. Our solutions turn paperwork into digital experiences, always ensuring the routine work is handled correctly, the first time. We do this by focusing on processes that aren't flashy or fashionable, by creating the standards departments can confidently build upon and by choosing a win-win economic model with the government.

Ultimately, we help our government customers optimize their routine processes so they can focus on what's important - defending our nation. Founded in 1998, Kinetic Data is based in Minneapolis, Minnesota, and online at kineticdata.com.

SOURCES

[1] DOD: It's Not Just State Actors Who Pose Cyber Threat to U.S., U.S. Department of Defense: https://www.defense.gov/News/News-Stories/Article/Article/3039462/dod-its-not-just-state-actors-who-pose-cyber-threat-to-us/
[2] The Largest Battlefield in History – 30 Cyber Warfare Statistics, DataProt, May 2023: https://dataprot.net/statistics/cyber-warfare-statistics/
[3] Significant Cyber Incidents, Center for Strategic & International Studies (CSIS): https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[4] Defense Strategy for Operating in Cyberspace, July 2011: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf
[5] Department of Defense Information Technology and Cyberspace Activities Budget Overview, FY23 Budget Request: https://www.cape.osd.mil/content/SNAPIT/files/FY23/DoD_PB23_IT_Budget_Overview_Finalv2_revised.pdf
[6] Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap, September 2011, U.S. Department of Defense: https://dodcio.defense.gov/portals/0/documents/announcement/signed_itesr_6sep11.pdf
[7] DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan, FY19-23: https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF
[8] DoD IT Enterprise Strategy and Roadmap, September 2011
[9] Largest Battlefield, DataProt
[10] Cyber Operations Tracker, Council on Foreign Relations: https://www.cfr.org/cyber-operations/
[11] DOD's Largest Multinational Cyber Exercise Focuses on Collective Defense, U.S. Department of Defense: https://www.defense.gov/News/News-Stories/Article/Article/2863303/dods-largest-multinational-cyber-exercise-focuses-on-collective-defense/
[12] Announcing the Release of the Administration's National Cybersecurity Strategy, U.S. Department of State, March 2023: https://www.state.gov/announcing-the-release-of-the-administrations-national-cybersecurity-strategy/

[13] Security Technical Implementation Guides (STIGs), DoD Cyber Exchange, DISA: https://public.cyber.mil/stigs/
[14] Intel leaks suspect is a flight risk and could have access to more classified docs, prosecutors say, NBC News, April 2023: https://www.nbcnews.com/news/us-news/intel-leaks-suspect-jack-teixeira-classified-docs-judge-detention-rcna81714
[15] DoD Has Over 3.5 Million Insiders – Now What?, The Cyber Defense Review, Fall 2021: https://cyberdefensereview.army.mil/Portals/6/Documents/2021_fall/09_Roberts_CDR_V6N4-Fall_2021.pdf
[16] DoD Zero Trust Strategy, U.S. Department of Defense, November 2022, p. 7: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf
[17] Ibid.
[18] A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack, NPR, April 2021: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
[19] Why the biggest cyber-attacks go undetected, SecurityBrief Australia, November 2021: https://securitybrief.com.au/story/why-the-biggest-cyber-attacks-go-undetected
[20] Why 56% of Data Breaches Go Unnoticed for Months, Ensighten, December 2020: https://www.ensighten.com/blog/why-56-percent-of-data-breaches-go-unnoticed-for-months
[21] Improving the Nation's Cybersecurity, Executive Order, Federal Register, May 2021: https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf
[22] Challenges and way ahead for cybersecurity workforce in today's federal government, DISA, August 2022: https://www.disa.mil/en/NewsandEvents/2022/Cybersecurity-Workforce
[23] Pentagon to Release New Cyber Workforce Strategy 'Any Day Now', Nextgov, February 2023: https://www.nextgov.com/cybersecurity/2023/02/pentagon-release-new-cyber-workforce-strategy-any-day-now/382788/
[24] The Value of Consolidation 2.0 for Federal IT, Kinetic Data Blog, December 2022: https://kineticdata.com/value-of-consolidation-2-0-for-federal-it/
[25] Top Management and Performance Challenges Facing Multiple Federal Agencies, Council of the Inspectors General on Integrity and Efficiency: https://www.oversight.gov/sites/default/files/oig-reports/CIGIE_Top_Challenges_Report_April_2018.pdf
[26] America's Military Is Choking on Old Technology, Foreign Policy: https://foreignpolicy.com/2018/01/29/americas-military-is-choking-on-old-technology/
[27] Unlocking the potential of public-sector IT projects, McKinsey and Company, July 2022: https://www.mckinsey.com/industries/public-and-social-sector/our-insights/unlocking-the-potential-of-public-sector-it-projects
[28] Systems of Engagement: How to Get Revolutionary Business Results from an Evolutionary IT Approach, Kinetic Data Blog: https://kineticdata.com/system-of-engagement-request-management/