Cybersecurity Action Team

Modernizing the U.S. Federal Government's Approach to Cyber Threat Management with Autonomic Security Operations

How Google can drive agencies' ability to meet the White House cybersecurity analytics requirements of EO 14028 and OMB M-21-31

Iman Ghanizada, Daniel B. Prieto, Asjad Nasir, Haywaad Ahmadzai

Table of Contents

Executive Summary

Our nation is facing acute and escalating cyber threats.

- Sophisticated cyber campaigns increasingly target the U.S. public and private sector, threatening both our individual security as Americans and national security.
- Cyber attackers are constantly innovating. In the last year alone, cyber attackers have increasingly automated ransomware attacks, targeted COVID-related remote work infrastructure, executed software supply chain attacks, and disrupted US critical infrastructure.
- The expansion of visibility beyond on-premise environments to cloud, hybrid environments and Information Technology (IT) and Operational Technology (OT) systems has led to an exponential growth in data volume that agencies are not equipped to manage.

New federal cybersecurity policies are essential to address the threat, but their effectiveness will ultimately depend on agencies' ability to implement them.

- The White House signaled its commitment to addressing these challenges through EO 14028 which proposed cybersecurity requirements on federal departments and agencies that span zero trust, software supply chain security, cyber threat management and more.
- OMB issued M-21-31 in support of the cybersecurity event log management requirements of the EO.
- Adherence to the recommendations set forth in EO 14028 and M-21-31 can strengthen cyber detection and response. However, implementation can be a challenge for many agencies due to cost, scalability, engineering, and a lack of resourcing.
- Meeting the requirements of the EO and OMB guidance will require not just technology modernization, but also transformational changes around workforce and business processes.

Autonomic Security Operations can help departments and agencies overcome these hurdles to enhancing their cybersecurity.

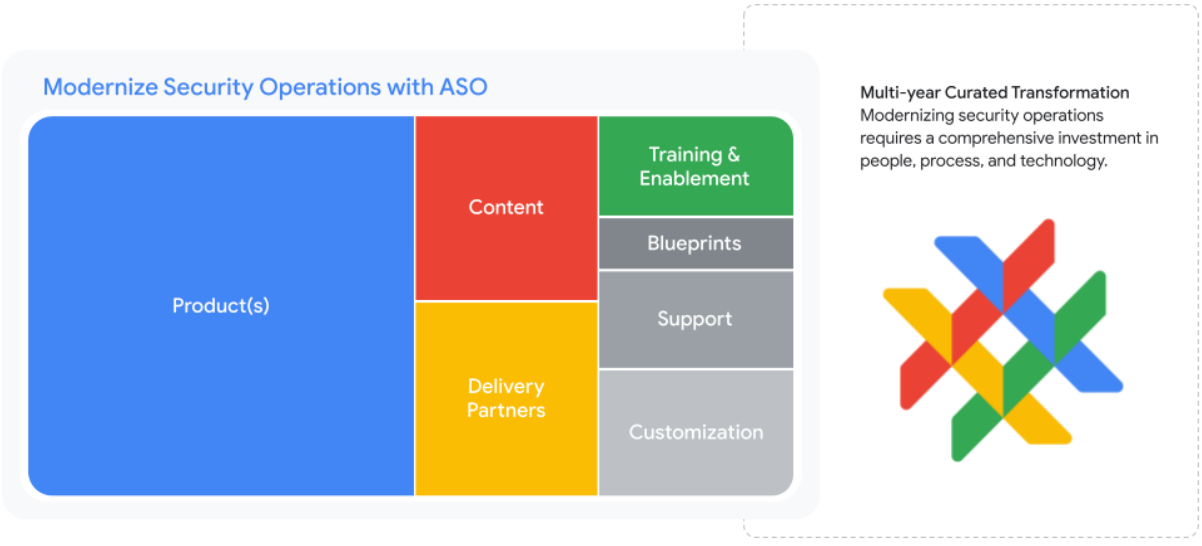
- Google Cloud developed Autonomic Security Operations (ASO), a solution to modernize threat management, in line with the objectives of EO 14028.
- ASO is a transformational approach to security operations, powered by cloud-native tools, to comprehensively detect and respond to cyber telemetry across an agency.
- ASO can help federal agencies to achieve continuous detection and response so that cyber defenders can increase their productivity, reduce detection and response time, and stay ahead of attackers.
- We recognize that implementation of the requirements in EO 14028 is a multi-year journey, and look forward to helping agencies meet the requirements to improve their cybersecurity.

Introduction

In May 2021, the White House issued Executive Order 14028 (EO) on Improving the Nation's Cybersecurity to address "increasingly sophisticated malicious cyber campaigns" affecting Federal Government systems. The EO recognized that incremental improvements to cybersecurity are no longer sufficient to thwart attacks and that "to keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity." In response, it outlined a set of measures designed to improve the security of federal networks, assets, and supply chains, and to better protect against, detect, and respond to cybersecurity threats – while investing in both the technology and personnel to support these modernization goals.

The recommendations in Section 8 of the EO focus on strengthening investigative and remediation capabilities. The White House Office of Management and Budget (OMB) Memorandum M-21-31 set forth implementation guidance, laying out a four-tiered maturity model for agencies' threat-logging capabilities, ranging from the lowest level of capability ("EL0: not effective") to the highest ("EL3: Advanced"). Given the complexity of modern computing environments, it's important for U.S. Public Sector agencies to identify a holistic strategy to modernize security operations that takes into account personnel and processes, in addition to the technology enhancements called for in EO Section 8 and M-21-31.

Google Cloud has developed a comprehensive solution–Autonomic Security Operations (ASO)–that can help transform Federal threat management and support agencies progress against the event logging maturity model set forth in OMB 21-31. ASO is powered by Google Cloud's detection & response platforms, Chronicle and Siemplify, and augmented by additional tools that provide enhanced threat and business intelligence, curated playbooks, over 300 third-party integrations, and implementation partners who can support our customers through their security transformation journey.



Modernizing threat management in the U.S. Public Sector is not simply a matter of adding new technology tools. It will require strategic transformation of people and processes as well. Through ASO,

we hope to support the U.S. Federal Government in its journey to transform threat management and improve the security of our nation.

Achieving Autonomic Security Operations

We define ASO as a combination of principles, practices, and tools that improve an organization's ability to withstand security attacks through an adaptive, agile, and highly automated approach to threat management.[1] In this vision for security operations, data comes to inform nearly all aspects of security operations in near-real time.

ASO recognizes that human capital in the security field is increasingly strapped. There is a global shortage of cybersecurity and data analytics professionals spanning both the public and private sectors. With security teams stretched thin, attackers are gaining the advantage over defenders. Between 2020 and 2021, the "breakout time" for attackers to move laterally within compromised systems after initial penetration dropped by nearly 70% from four-and-a-half hours to just an hour-and-a-half.[2] On the other hand, defenders often take weeks to months, sometimes even years, to discover intrusions. The only way for defenders to keep pace is to increase their productivity by an order of magnitude–10x–or more.

The ASO approach to security operations focuses on a concept of Continuous Detection and Continuous Response (CD/CR). It is grounded in best practices and lessons learned from modern engineering practices – DevOps, Agile, and Site Reliability Engineering – around software development and IT operations. A more modern approach to threat detection can allow organizations to unlock four pillars of transformational improvement in security operations:

- **10x People**, by empowering overworked security teams to do their jobs more effectively, without increasing the human toll;
- **10x Processes**, by using automation to increase the speed, consistency, traceability, and auditability of a range of security tasks;
- **10x Technology**, by deepening interoperability of products and vendors; and
- **10x Influence** across the enterprise through better reporting and information sharing to improve collective defense.

To understand the transformational potential of ASO, it is instructive – as an analogy – to take a closer look at how the adoption of DevOps, Agile, and Site Reliability Engineering allowed software delivery teams to move away from the longstanding "waterfall" approach to software development. In the legacy software development life cycle (SDLC), this "waterfall" approach was highly linear and phased (development, testing, IT operations), which made it cumbersome, and slow. This assembly-line

[1] For more information about Google's ASO solution, please see the original whitepaper, "Autonomic Security Operations: 10X Transformation of the Security Operations Center."
[2] "Nowhere to Hide,2021 Threat Hunting Report," Crowdstrike, as reported in Culafi, Alexander, "Breakout time decreased 67% in 2021", TechTarget, accessed at https://www.techtarget.com/searchsecurity/news/252506395/CrowdStrike-threat-report-Breakout-time-decreased-67-in-2021

approach to software development faced many of the same challenges currently faced by traditional Security Operations teams when it comes to visibility, speed, quality, reliability, and productivity.

- When Agile software development started being practiced as a way to iteratively improve collaboration and release times over the Waterfall framework, many organizations said they did not have the talent and resources to modernize until it became a very clear competitive disadvantage.

- DevOps ushered in a focus on continuous integration and continuous delivery (CI/CD) in application development. It focused on microservices and increased automation as an antidote to monolithic architectures that inhibited rapid iteration. When DevOps created the construct of continuous delivery and feedback, many organizations were slow to adopt it at first due to talent and resource shortages. As DevOps became an industry best practice, late adopters suffered competitive disadvantages.

- When Site Reliability Engineering became a best practice for implementing automation and engineering improvements that improved the reliability of IT operations, many organizations were slow to adopt it due to talent and other resource gaps. For late adopters, a lack of reliability risked becoming a competitive disadvantage.

What these practices have in common, is that their widespread adoption has transformed the way organizations are able to provide services to their customers, enter new markets, and scale on-demand. The technologies that are used today are built around updated expectations of how we work, not vice-versa. CxOs in organizations that employ these best practices are confident in their ability to build software and deploy infrastructure. Banks can focus on banking, hospitals can focus on healthcare, and technology companies can focus on launching products. The on-demand elasticity of software and infrastructure becomes an “autonomic” element of an organization's technology function. The rapid adoption of the cloud reinforces the gains in automation, agility, scale, and flexibility.

ASO is an embodiment of these principles in the context of security operations. It brings tools, practices, and principles together to provide a framework for modernizing threat management for all manner of organizations–private sector and public sector, large and small, and with or without a Security Operation Center (SOC). It presents an opportunity to transform the discipline of security operations akin to the impact of DevOps on software development.

Why ASO in the U.S. Public Sector?

To address the acute cyber threat facing the nation, the White House issued EO 14028. OMB 21-31, provides further implementing guidance and requirements for U.S. Federal departments and agencies to strengthen detection, investigation and remediation through the enhanced collection, use, and analysis of cybersecurity log data. Specifically, OMB M-21-31 establishes four tiers against which U.S. Federal agencies should measure the effectiveness of their threat event logging systems. It’s also worth noting that in 2020, NIST added proactive hunt as a best practice in its Special Publication 800-53

Security and Privacy Controls for Information Systems and Organizations (NIST SP-800-53).

Event Logging Tiers	Rating	Description	Timeline
EL0	Not Effective	Logging requirements of highest criticality are either not met or are only partially met	N/A
EL1	Basic	Only logging requirements of highest criticality are met	6 months
EL2	Intermediate	Logging requirements of highest and intermediate criticality are met	18 months
EL3	Advanced	Logging requirements at all criticality levels are met	24 months

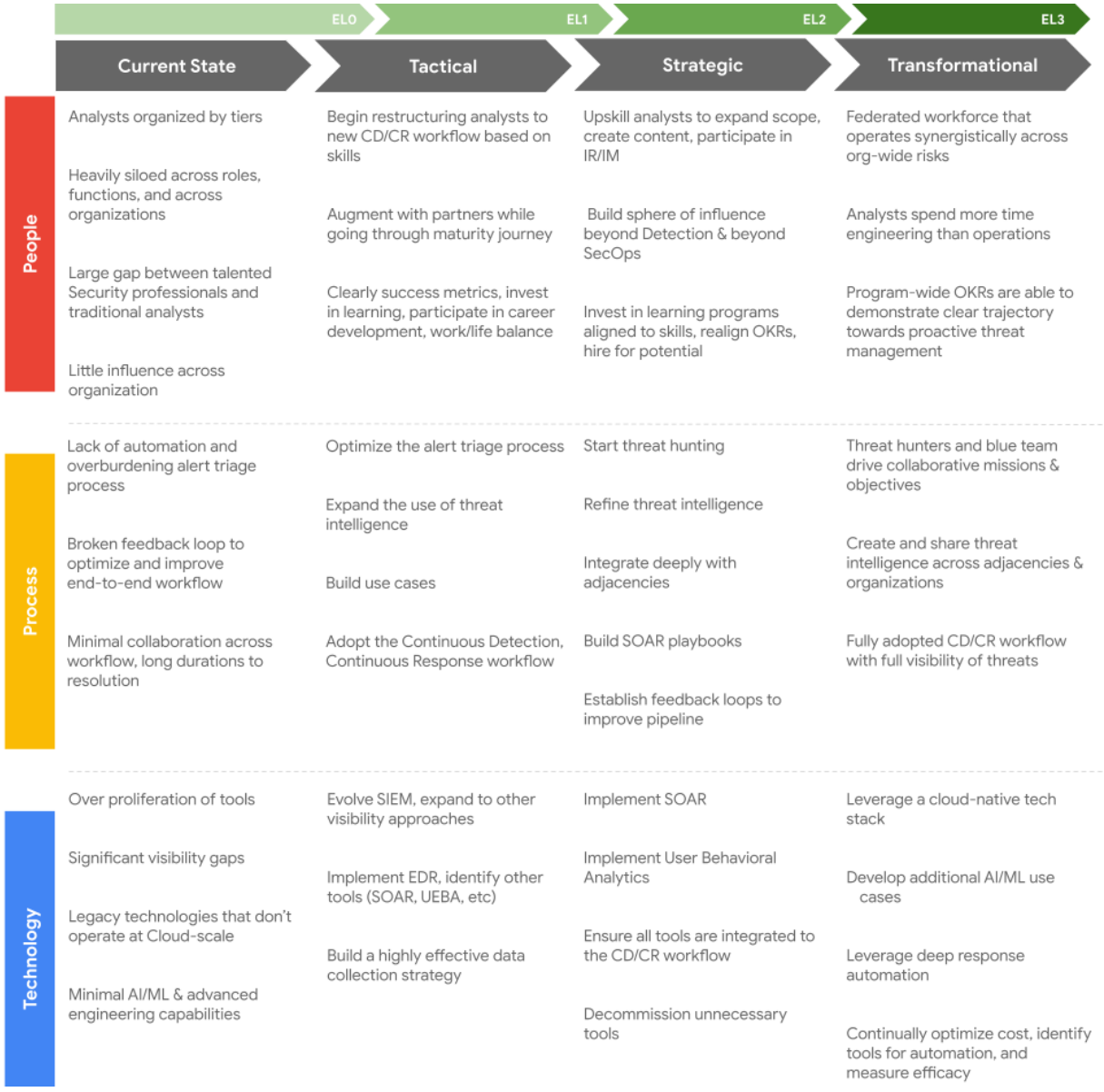
While 96% of U.S. Federal IT leaders believe that the EO will improve cybersecurity, less than half feel well prepared to respond to its directives.[3] U.S. Federal security leaders already feel stretched thin, concerned about lack of personnel, lack of technical capability, lack of funding, expected timelines, too many competing priorities, and concerns about shifting resources from existing priorities.

Complicating matters even further, the requirements of the EO for maintaining logs and implementing endpoint detection and response (EDR) can increase the data volumes that agencies have to manage by 10x or more. Without the ability to simultaneously 10x their workforce or their budgets, defenders will need to transform their productivity to make effective use of the logs.

To help government leaders meet the demands of the EO around cyber analytics and threat management, Google's ASO solution can help agencies rise to the challenge. ASO brings together Google Cloud's detection and response platforms–Chronicle and Siemplify–along with additional Google and partner capabilities. It can help agencies comply with the logging requirements set forth in OMB M-21-31, taking them from where they are today toward full achievement of EL3.

While the focus of OMB M-21-31 is on the implementation of technical capabilities, transforming security operations will require more than just technology. Transforming processes and people in the security organization is also critical for long-term success. ASO provides a more comprehensive lens through which to view the OMB event logging capability tiers, which can help drive a parallel transformation of security-operations processes and personnel.

[3] See a joint survey of government leaders by Google and Meritalk, "The Push and Pull of Federal Cybersecurity," January 2022, available at https://www.meritalk.com/study/push-and-pull-of-federal-cybersecurity/

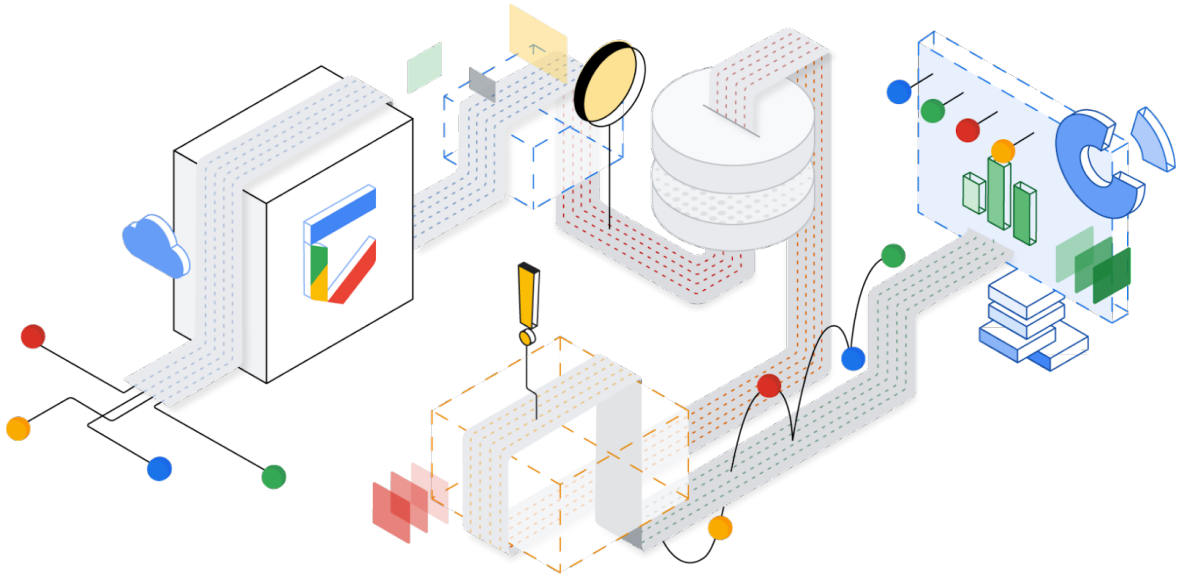


Departments and agencies at various levels of maturity can selectively implement components of ASO to meet the recommendations in the White House guidance. At the same time, ASO provides a comprehensive framework and capabilities to empower a full transformation of an organization's cybersecurity analytics, threat detection and threat management capabilities over the longer term.

Government agencies have an obligation and an opportunity to radically rethink security operations. ASO capabilities and principles give U.S. Public Sector security teams an opportunity to implement new technologies, modernize outmoded business processes, and transform the productivity of their people.

If defenders can transform their operations, they can become a model for attracting top talent to government and a model for the transformation of security operations in other sectors.

Transforming Security Operations



The technologies and delivery models that security teams rely on to conduct threat detection and management vary across organizations. Some prefer to build, others prefer to buy. Some prefer managed tooling, others prefer the flexibility and control of owning and operating the tools themselves. Regardless of the exact delivery model, though, most organizations implement a monolithic model of security operations. That model typically relies on a dominant security application–traditionally a SIEM–implemented alongside a fragmented assembly-line of processes and workflows that rely on dozens of disparate security tools for detection and response.

This traditional structure relies upon a rigid, tiered, and analyst-centric approach. Security alerts, threat events, and investigative efforts are managed by analysts on a case-by-case basis, in organizational silos, and through channels of escalation. Analysts at the front lines perform low-level case management, while more skilled workers build detection and hunt tools, manage ingestion pipelines, and conduct incident response. Too often, teams and critical data are siloed and disconnected from one another, and across the workforce there are significant disparities in skillsets, scope of work, and role expectations.

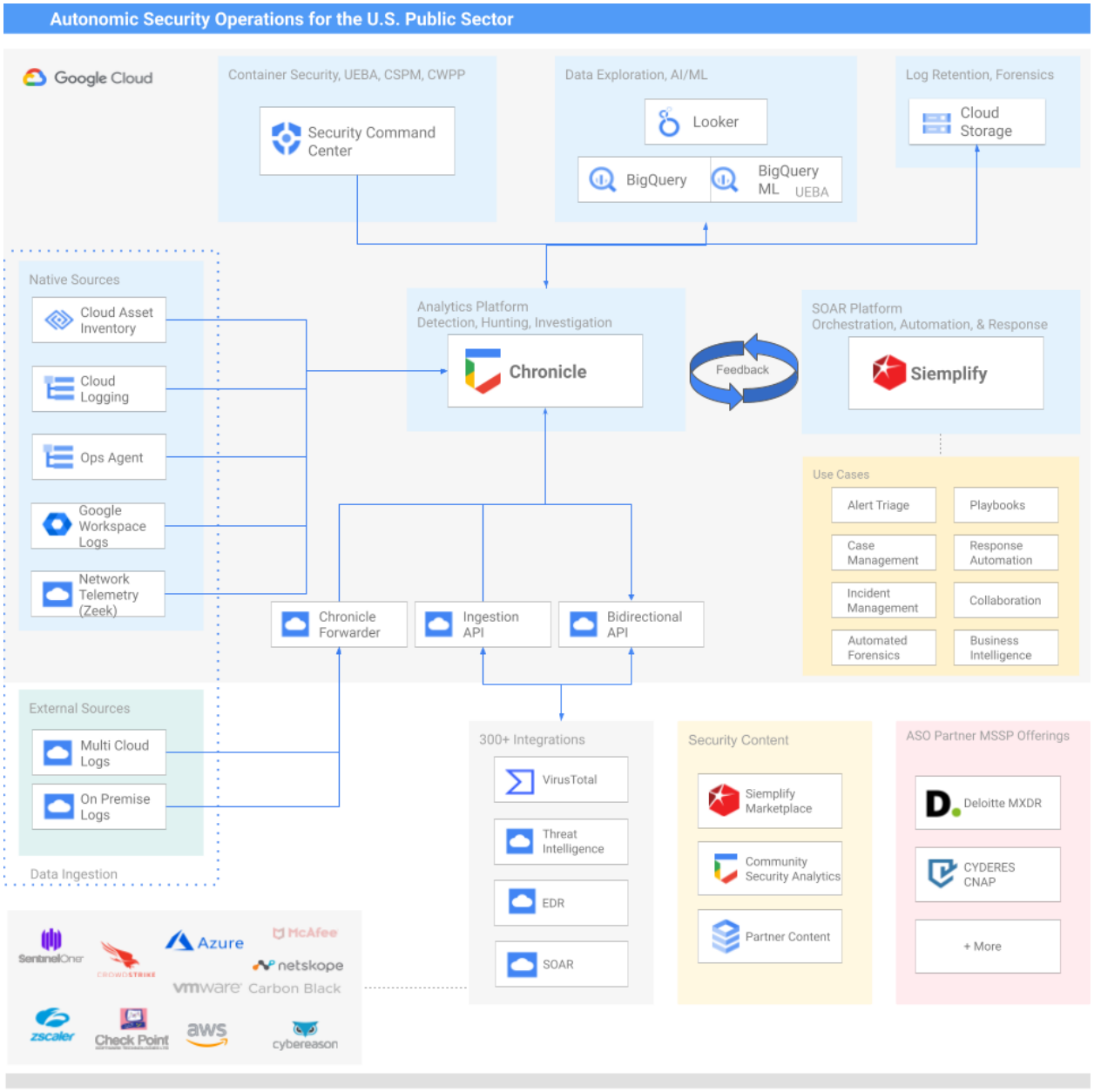
As a result, the traditional security model too often lacks the agility and scalability that defenders need to counter attackers. An excess of alerts generated by an excess of technologies challenges analysts to identify and investigate genuine threats. Most analyst time is spent manually integrating and correlating data from multiple systems, and wading through false alerts, rather than identifying and countering real intrusions. Defenders suffer from alert fatigue and burnout, while legitimate threats continue to penetrate their organization's defenses. As enterprise IT infrastructures have become more complex, with the increased reliance on hybrid and multi-cloud environments, data volumes continue to grow,

pressure on security teams continues to increase, and the need for greater visibility, agility and scalability becomes more critical.

Legacy Security Operations Workflow

<table>
<tr><td colspan="2">Security Architects, Infrastructure, Project Teams (DevOps)</td><td colspan="3">Security Engineers, Tooling Engineers, Content Creators, Threat Researchers</td><td>Tier 1 Analyst</td><td>Tier 2 Analyst</td><td>Tier 3 Analyst</td></tr>
<tr><td colspan="2">Data Collection</td><td colspan="2">Enrichment</td><td>Detection</td><td>Triage</td><td>Investigation</td><td>Response</td></tr>
<tr><td>Threat Modeling</td><td colspan="4">SIEM</td><td>Case Management</td><td>Case Management</td><td>Incident Management</td></tr>
<tr><td>Endpoint Logs</td><td>Network Logs</td><td>Vulnerabilities</td><td>Log Aggregation</td><td>Retrospective Queries</td><td>Basic Investigation</td><td>Deep Investigations</td><td>Incident Response</td></tr>
<tr><td>Application Logs</td><td>Cloud Logs</td><td>Curated Signals (EDR, NDR, UEBA)</td><td colspan="2">Correlation, Dashboards & Analytics</td><td>Basic Remediation</td><td>Intermediate Remediation</td><td>Threat Hunting</td></tr>
<tr><td>Asset Inventory</td><td>All Relevant Logs</td><td>Threat Intelligence</td><td>Rule-based Detections</td><td>Model-based Detections</td><td>Basic Knowledge</td><td>Intermediate Knowledge</td><td>Advanced Knowledge</td></tr>
<tr><td colspan="2">Coverage % of Threats</td><td colspan="3">Mean Time To Detect (MTTD)</td><td colspan="3">Mean Time To Respond (MTTR)</td></tr>
<tr><td colspan="8">Software & Service Supply Chain – MSSPs, Systems Integrators, ISVs, Internal Customers, and all other partners</td></tr>
</table>

To help the U.S. Federal departments and agencies meet the requirements of the EO and OMB M-21-31, Google has assembled a cloud native solution architecture to modernize threat management. From left to right, the architecture covers data collection, analytics and decision making, with a feedback loop across these functions and across every connector. This stack is extensible–offering over 300 third party integrations–can be built to consume any and all security data, operates at cloud-scale, and is mostly running on managed services at a cost-efficiency that makes petabyte-scale data ingestion feasible.



ASO provides capabilities that are modular, extensible, and scalable, and which provide cloud-scale power and significant cost, productivity, and process improvements over legacy tooling. The extensibility of cybersecurity tools is particularly important, as many organizations are likely to retain some pre-existing tooling that they rely upon to process cybersecurity data. ASO supports multi- and hybrid-cloud environments and can be used in tandem with non-GCP security tools.

Building the Technology Stack

The EO requires log collection, aggregation, retention, exporting, Security Orchestration (SOAR), User and Entity Behavior Analytics (UEBA), container security, Endpoint Detection and Response, and makes additional recommendations regarding alignment to best practices. This requires departments and agencies to implement comprehensive systems for managing high-volume security event logs across multiple systems and sources, and making them readily usable through centralized access and analytics.

To understand how departments and agencies can leverage ASO to achieve the requirements of the EO, ASO capabilities are mapped against OMB M-21-31 requirements below. When reviewing the mapping, departments and agencies should evaluate the people and process changes that will be required to support a modernization of the technology stack. We discuss these in more detail later in the paper.

Event Logging Tier 1 - Basic Requirements

The EL1 “basic” requirements prepare agencies to make the foundational investments in centralized logging to support a modern threat detection infrastructure with SOAR and SIEM capabilities. Agencies are directed to meet these requirements by August 27, 2022 one year after the publication of OMB M-21-31, which include:

- **Basic logging** covering the highest criticality (level 0) events, in accordance with the minimum data elements, time standards, and formats;
- **Event forwarding**, in near real time, to a centralized SIEM and other analytical workflows;
- **Protections and validations** for log information including encryption, verification, access restrictions, access logs and audits, backups, integrity verification, alerts, and monitoring;
- **Passive DNS logging** of all DNS queries, including those made over encrypted connections, with accompanying analytics that allow for rapid identification of the source host;
- **Provision of log access to CISA and FBI** upon request, in accordance with formats, means, and timelines specified by the agencies, which may include near real time access;
- **Threat hunting and incident response playbooks** that leverage the new logs, to inform implementation of those capabilities at higher tiers;
- **Planning for user behavioral analytics** to allow for early detection of malicious behavior to inform implementation of those capabilities at higher tiers; and
- **Basic centralized access** through aggregation by an agency component-level Enterprise Log Manager (ELM).

Collecting Logs of Security and DNS Events

ASO brings together a number of Google Cloud’s security capabilities to help agencies quickly meet these needs and build the foundation for their threat detection systems.

At its core, it is supported by Google Cloud Logging, a fully-managed logging service that allows its users to to store, search, analyze, monitor, and alert on logging data and events from a range of sources including hybrid cloud systems. Google Cloud's operations suite provides agents for collecting logs, which can be configured to support parsing of log files from third party applications. The service includes log storage, a user interface, and an API that provides for programmatic management.

Google Cloud Logging can also be integrated with Google Cloud DNS, our resilient, reliable, and low-latency DNS service that also supports managed DNSSEC and both public and private zones. Here, DNS logs are recorded for every DNS query received from VMs and inbound forwarding flows. These DNS logs can be viewed and exported along with other kinds of logs.

Centralizing Log Collection and Access

Event and DNS logs are forwarded to Chronicle in near-real-time to provide for centralized access, as required under OMB M-21-31.[4] The service is designed to provide easy-to-use security analytics to support requirements under EL1, while also integrating with a range of other security services, including both Google and third-party offerings, to provide advanced capabilities.

Chronicle is a specialized layer on top of core Google infrastructure, designed for organizations to privately retain, analyze, and search the massive amounts of security and network telemetry that they generate. It normalizes, indexes, correlates, and analyzes the data to provide instant analysis and context on risky activity. By making security activity data from your organization, third-parties, and curated intelligence feeds available through a single platform, using Chronicle can free up security analysts to focus on the most critical security tasks, empowered, not encumbered, by the data at their fingertips.

The service's pricing structure is also designed to respond to agencies' needs for ensuring cost-effectiveness while ramping up security. Many of its competitors base their pricing models based on data volume, disincentivizing the broad-based logging contemplated under OMB M-21-31. In contrast, Chronicle's pricing is based upon seats, meaning that costs grow linearly with the size of the agency and not exponentially, with rapid increases in log collection. Accordingly, while OMB M-21-31 establishes distinct and cold storage requirements, agencies could opt for active storage for the full retention term without incurring additional cost.

Protecting Logs through Encryption, Role-Defined Access, Audit Logging, and More

ASO also integrates a range of protections to ensure the privacy and security of logging data. All data is encrypted, by default, in transit and at rest. Agencies can also choose to use customer-managed encryption keys (CMEK) and key access justifications, which offer an additional level of security by preventing access even by Google administrators, unless the key is provisioned by the customer.

For logs hosted on GCP-native services, access can be managed through IAM permissions and roles, which are designed to provide granular access control based upon role-specific needs. IAM also supports the creation of even more granular access through control policies to resources based on attributes like device security status, IP address, resource type, and date/time. IAM is also designed to

[4] In addition, Chronicle supports ingestion and normalization of many other data sets. For more information about supported data sets, please see our Reference Guide.

automatically create audit logs that can cover administrative activities (by default) as well as all access to log files (where enabled by the agency customer), as well as to support alerts which can be based upon changes to relevant metrics (e.g., errors or latency) or to create alerts where specific logged events occur.

Providing As-Needed Access to Partner Agencies

In addition to securely managing access by personnel within an agency, IAM can also be used to support cross-agency use cases as needed. In particular, the roles and accompanying permissions could be leveraged to provide as-needed access to DHS CISA and FBI to support their respective mandates for cross-agency security and national security more broadly.

Supporting Planning for Threat Hunting, Incident Response, and Behavioral Analysis

OMB M-21-31 recognizes that logging itself is not an end-goal, but rather should be used to support other activities that are essential to a modern security environment including threat hunting, incident management, and behavioral analysis. To these ends, it requires agencies to develop playbooks and undertake other preparatory work to support these activities at higher event logging tiers.

Similarly, we regard data ingestion and aggregation in Chronicle as an intermediate step to unlocking the advanced capabilities that are enabled by the platform and its integrations across these areas. Because these services are already integrated into the platform, agencies can anticipate and plan for these requirements without having to onboard hosts of new tools, allowing them to more easily build out their playbooks and transition across levels.

In 2022, Google Cloud also acquired Siemplify, a leading Security Orchestration Automation and Response ("SOAR") platform, which is integrated as part of Chronicle to enable customers to do even more with their security data, going beyond typical SIEM and toward extended detection and response tooling, enabling detection and response at the speed and scale of modern environments. While agencies are not required to make full use of Siemplify's capabilities at EL1, the service offers pre-build playbooks for common use cases that can support planning for these activities. These default playbooks also come with an easy-to-use editor that allows agencies to customize them to their needs.

Event Logging Tier 2 - Intermediate Requirements

Under Event Logging Tier 2 (EL2), agencies will need to adhere to additional requirements with respect to which logs are retained, their structure, security, access and more. OMB 21-31 provides agencies with eighteen months to comply with the additional intermediate requirements specified in Event Logging Tier 2 (EL2) by February 27, 2022. The requirements set forth under EL2 are cumulative, so agencies should also ensure that they continue to meet the EL1 requirements and the following additional requirements, which include:

- **Intermediate Logging**, expanded to include Level 1 and 2 criticality logs, adhering to the formats and timeframes as set forth in OMB M-21-31;
- **Publication of standardized log structure**, provided to CISA and published on data.gov;
- **Provisions for the inspection of data**, which call for agencies to work with CISA to log certain additional fields if they perform full traffic monitoring or otherwise log the available metadata;

- **Intermediate centralized access**, including new requirements for log visibility;
- **Monitoring potential disruptions** to log health, and
- **Adherence to zero-trust principles** of least privilege and reduced attack surface.*Supporting Intermediate Logging*

Google Cloud Logging allows for customization of its robust logging, reporting, and auditing capabilities to comply with and cover all of the log categories contemplated in OMB M-21-31.

Reporting Standardized Logging Schemas

Agency administrators using Google Cloud Logging can customize design patterns for exporting logging data. This includes specifying which logs are exported and log format schemas. Best practices for scenario-type exporting also provide detailed diagrams to assist with reporting and provide documentation for implementing and reporting structured logging designs, which can help agencies craft the required publication schema. Additionally, our partners can support U.S. Federal agencies' requirements to develop log schema documentation.

Storing Data in Clear Text

ASO enables authorized personnel to access data and metadata from Appendix C in clear text. This is true regardless of whether it is being stored in Google Cloud Storage, Google Cloud Logging, or Chronicle.

Inspection of Encrypted Data

OMB M-21-31 leaves it up to each agency whether to perform full traffic inspection. However, it provides that if full traffic is inspected through active proxies, then additional fields should be logged, as set forth in Appendix C. Alternatively, agencies are encouraged to log the metadata that is available to them. Our logging solutions can support agencies efforts with respect to traffic inspection and the storage of related metadata, irrespective of which option they pursue under the EO.

Adhering to Zero Trust Principles

While OMB M-21-31 does not set forth specific zero trust requirements, it generally instructs agencies to adhere to zero trust principles for activities carried out under the memo and related guidance by CISA and OMB. Such recent guidance includes OMB's Federal Zero Trust Strategy set forth in M-22-09 and CISA's Zero Trust Maturity Model. Both documents draw concepts from Google's BeyondCorp whitepapers, which set down the marker for our zero trust vision and journey starting nearly 10 years ago. Google Cloud strongly supports the efforts within the U.S. Federal Government to embrace zero trust as part of their cybersecurity modernization process, which we believe will provide agencies the strongest security, when implemented properly.

As zero trust underpins Google Cloud's overall security approach, we build zero trust capabilities into a number of our products that can help agencies adhere to this guidance. For example, for logs hosted on GCP-native services, access can be managed through Identity and Access Management (IAM) permissions and roles, which are designed with the concept of least privilege at their core. Rather than using basic roles, IAM uses granular controls to grant limited predefined or custom roles at the smallest

scope needed. It also encourages the creation of separate trust boundaries between application components, recommending that distinct service accounts be established on a per-service basis, with only the required permissions for each service account.

Providing Intermediate Centralized Access

EL2 requires that logs classified as Criticality Level 0 and Criticality Level 1 are accessible and visible for the highest-level security operations at the head of each agency, and that Criticality Levels 2 are retained, at a minimum, at component level. Role-based access can be managed through IAM, Chronicle also provides additional visibility and insights through the use of dashboards, which can allow agency administrators to better understand and make use of their data.

Monitoring Log Health

The same dashboards that facilitate access to logs, can also be configured to monitor the health status of log sources and give insights into potential data-stream disruptions. Alerts can also be configured to fire when disruptions occur. Because log health data is also integrated to Chronicle, teams can monitor log health through a single interface, making it easier to detect and manage log health in real time.

Event Logging Tier 3 - Advanced Requirements

Finally, agencies are required to comply with the advanced logging requirements of Event Logging Tier 3 (EL3) by August 27, 2022, two years from OMB M-21-31's publication. By the time they reach EL3, agencies must have comprehensive logging systems and related toolings in place, and leverage those technology investments to undertake security activities like threat hunting and incident response that they have prepared for during the earlier phases. To these ends, EL3 agencies must meet the following additional requirements:

- **Advanced logging**, covering all categories set forth in OMB 21-31;
- **Implementation of SIEM and SOAR capabilities**, to execute on agency playbooks for threat hunting and industry response;
- **User behavior monitoring**, that leverages artificial intelligence and machine learning to identify potentially compromises or malicious activities;
- **Application container security**, operations and management; and
- **Advanced centralized access** for logs across all criticality levels.

Supporting Comprehensive Logging

Google Cloud Logging provides robust logging capabilities that can cover all of the events contemplated in OMB 21-31. It also allows logs to be configured so that they comply with the required formats set forth in the memo.

Using SOAR and SIEM Tools To Execute on Threat Hunting and Incident Response Playbooks

At EL3, agencies are required to deploy the playbooks for threat hunting and incident response that they built across EL1 and EL2. As noted above, Siemplify includes playbooks that cover common security use cases that can both help support agencies' planning for these activities. Because these playbooks are

designed to use the platform's leading SOAR capabilities, as well as Chronicle's rich security analytics, agencies can more easily transition from planning to execution. In doing so, the integrated platform brings together vast troves of data and many security tools to empower analysts without overwhelming them.

Events within the platform are presented through a case management interface that ingests all relevant logs and applies logic to group them into threat-centric cases to streamline review by analysts and allow them to make better and faster decisions and reduce alert fatigue. Cases are designed to automatically highlight the most important data about a potential threat, as well as to enrich logging data with other helpful information. They also allow analysts to easily research the entities involved to gain a fuller picture of the threat and better carry out threat hunting or incident response.

Just as it streamlines analysis, the platform also empowers analysts to respond to threats with a single-click, which can include initiating a coordinated response in the case of an identified breach or blocking an executable where malicious activity is detected.

Detecting Potential Compromises and Threats with AI/ML

Security Command Center Premium can provide user and entity behavior analytics out-of-box through its threat detection suite. This data can also be natively ingested into Chronicle to give security teams a single security platform to triage and investigate, as well as to provide analysis and insights into a host of behavioral signals. The data can also be integrated into Siemplify, to streamline case management with respect to potential compromises or automate responses.

Integration of Container Security Information

Container Threat Detection data can also be ingested into Chronicle and Siemplify in order to continuously monitor the state of Container workloads in runtimes. This process includes evaluating all changes and remote access attempts to detect runtime attacks in near-real time. The service leverages several detection capabilities, including suspicious binaries and libraries, and uses natural language processing to detect malicious bash scripts. Chronicle supports the ingestion of logs at various layers of containerized infrastructure, so container-related events can also be managed through the same interface, streamlining analyst work.

Supporting Advanced Centralized Access

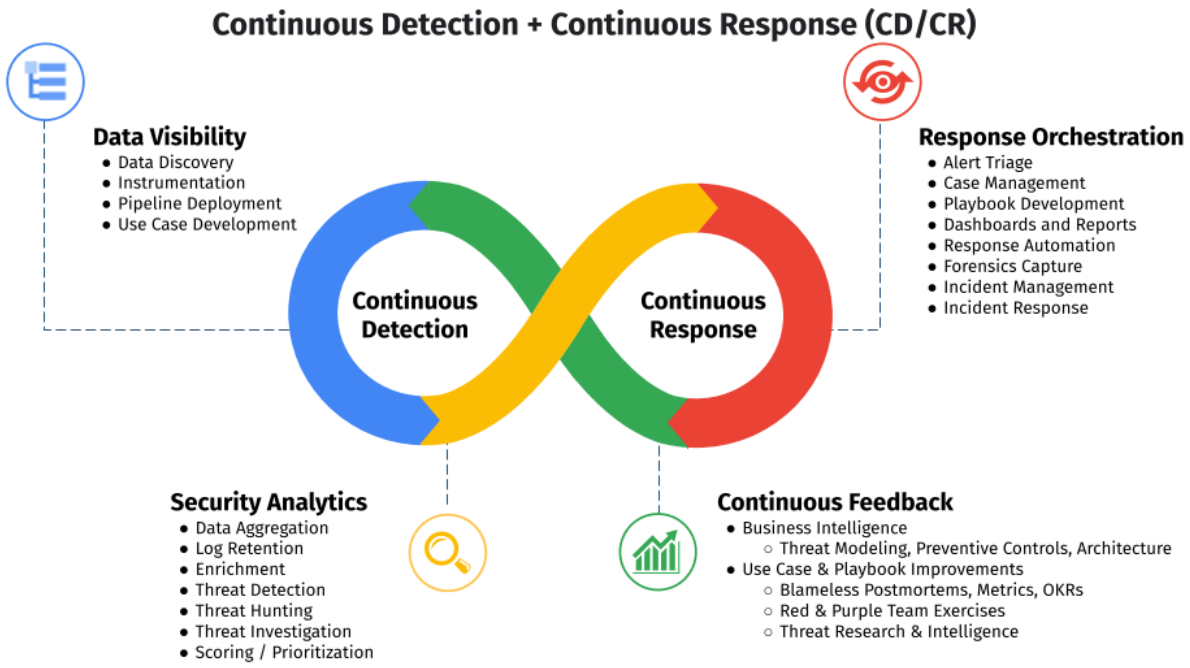
The same features discussed at EL2 can be used to manage role-based access to logs across all criticality levels.

Modernizing the Security Operations Workflow

A modern and agile security-operations practice is not siloed and task-focused and reactive. Its workflow is not linear and reliant on escalations across tiered groups of analysts. Instead, modern security workflows should be closely aligned with key technology and operating elements of the broader enterprise. Achieving this closer collaboration will provide fuller visibility into IT assets and workloads, as well as foster closer relationships to and better communications with project teams across the organization that are building or deploying software, or managing infrastructure and IT operations.

Closer collaboration and coordination by security teams with the rest of the agency reduces the risk of limited visibility and lack of context into relevant cybersecurity and IT data.

By modernizing both technology and workflows, security-operations teams can achieve Continuous Detection and Continuous Response (CD/CR), wherein they can–rapidly, and in an automated fashion–access and analyze all of the relevant IT data and cyber telemetry that the enterprise possesses. There is a need to effectively prioritize threat events and appropriately assign resources depending on the severity. A successful operation will increasingly automate routine and highly manual tasks, giving security teams more time and ability, for example, to engage in proactive threat hunting, which was added in 2020 to NIST SP-800-53 as a security best practice.



In modern threat management practices, the workflow is structured to enable the continuous improvement of detection and response functions. Many times, ineffective security operations are a result of the failure to properly support, empower, and incentivize talent with the right business processes and technical resources. Knowing what this continuous loop looks like for your organization will help you identify gaps and realign your analysts to a model that makes the most sense for your organization. Business processes are aligned to the particulars of your organization and teams are structured where they best fit.

How can departments and agencies ensure that their Security Operations practices and workflows evolve and continually improve? As departments and agencies assess their maturity across the key areas of the OMB Event Logging tiers and the CD/CR model, the following questions can provide useful guidance.

- Which one of these core processes do we perform today?

- How would we rank the maturity of this practice?
- Where can we radically improve our capabilities here? Is it with people, process, technology, or a combination of them?
- Who performs these functions? Where can we expand their reach?
- If we're not performing these functions, where are they being done? Who are the key players, do we have close alignment with them?
    - E.g. If your team is completely disconnected from the teams that handle data collection, and you have a use case that is missing key data from instrumentation, can you identify who drives this today? Do you have alignment? If you have a way to solve a visibility gap by deploying a set of instrumentation, how can you focus on continual improvement?
- Can we align Objectives and Key Results (OKRs) to these functions both from a team-level to the role expectations?
- What are the metrics we're capturing across each function?
- Where can we upskill our analysts to take on more ownership of the pipeline?

Empowering the Cybersecurity Workforce

In addition to the modernization of technology tools and business processes, ASO calls for a parallel transformation of agencies' security workforce. In the longer term, we believe that this transformation of the productivity of cybersecurity personnel, as well as efforts to deepen diversity in the cybersecurity workforce can help address today's critical shortages of skilled cybersecurity talent.

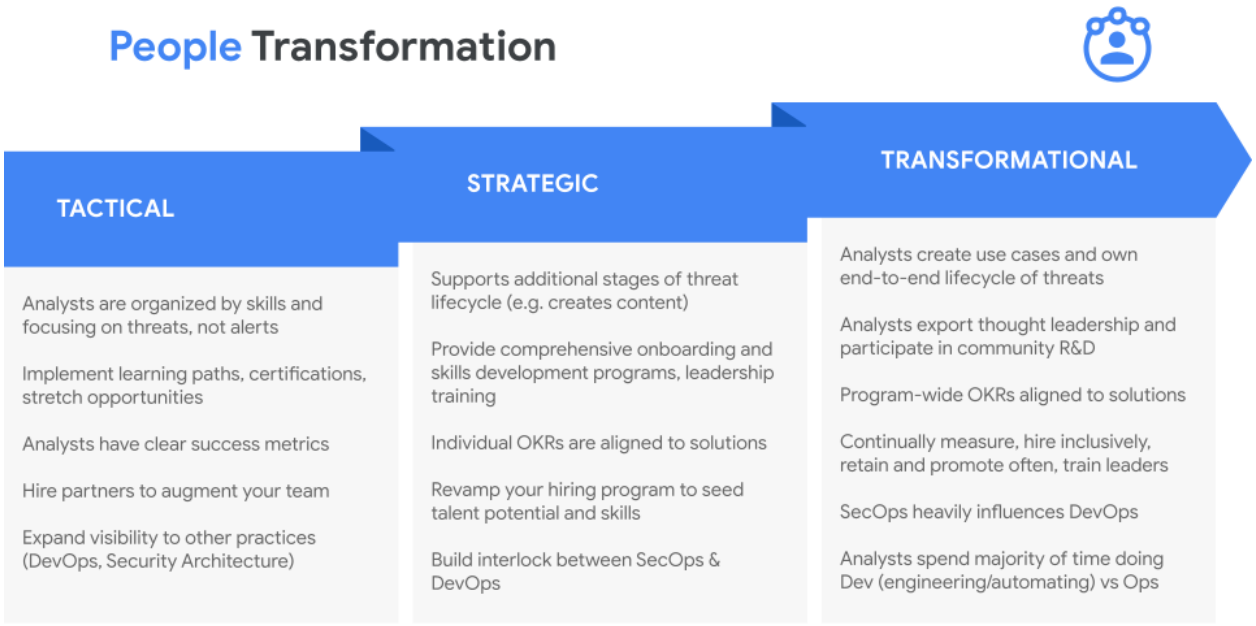
Current estimates project that 3.5 million cybersecurity jobs will be unfilled by 2021, and more than half of Chief Information Security Officers expect the problem to worsen.[5] U.S. Public Sector agencies are particularly challenged to recruit, train, and retain the cyber workforce they need for the future. The human capital challenges that the U.S. Public Sector faces, extend beyond just a global shortage of technical talent. Many public sector employees are motivated by a deep commitment to public service and to the mission of their agencies, but with a growing number of roles to fill it is essential to be able to continue to attract and retain new talent. That has become increasingly difficult when public sector agencies must compete with a competitive private sector talent market across dimensions including work-life balance and flexibility; salaries and benefits; coaching and development; career advancement; and access to modern technology tools.[6]

With the right tools and a reimagining of the business process of threat detection, analysts can focus on higher-value-added activities and problem solving. Departments and agencies don't need everyone in the world to become a data scientist or an engineer, but they should discourage the legacy assembly-line approach to detection and response and restructure team members around a common framework that will give them the ability to leverage their creativity and curiosity. Many defenders join the government for the mission–to serve the public and protect the nation. Let's empower them to

[5] Harvard Business Review, The Public-Private Partnership That's Working to Make New York City a Global Hub of Cybersecurity Talent.
[6] For a deeper exploration of the challenges to U.S. Federal cybersecurity hiring see the Cyberspace Solarium Commission Report, Strategic Objective #4.

solve the kinds of challenges they signed up for, and provide the opportunities for growth, impact, and innovation that can fuel their careers.

Fully harnessing the benefits of this approach will require changes to how security teams are structured and incentivized. This is essential for a number of reasons. First, OMB M-21-31 proposes a significant shift in how much security data is made available to security teams, making an equivalent shift in the number of security personnel costly and impractical. Second, given the ongoing workforce shortages, even with a mandate to significantly increase cybersecurity related hiring, many key cybersecurity roles would inevitably go unfilled. To those ends we propose a parallel three-phase people transformation, that reorients security analysts away from narrowly-focused tactical responsibilities, toward more creative, empowered, and impactful problem solving and influence within the enterprise.



Departments and agencies should consider some practical and concrete steps they can take to make progress on people reforms within their security operations teams.

As a first step, people managers should start thinking about how to re-align objectives and key results (OKRs) and performance metrics for security operations teams. For example, rewarding analysts based on how many cases they have resolved fails to address the proliferation of false alerts and analyst burnout. On the other hand, an analyst who helps develop detection use cases and identifies the signals needed to cut down false positives is reducing toil, driving productivity gains, and shifting the security operating model. If you can instill and reward curiosity, critical thinking, and creativity in the minds of the analysts closest to the threats, you may find that your staff discovers clever ways to develop solutions to problems that go beyond day-to-day tactical responsibilities.

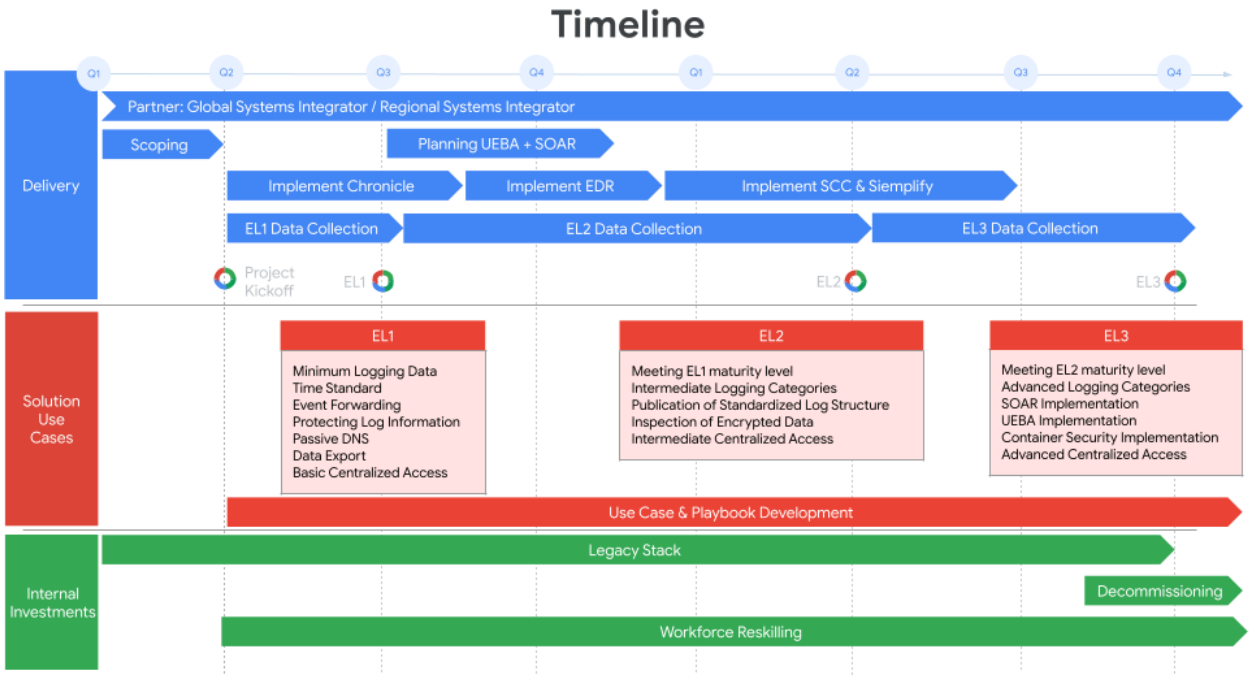
Second, not all agencies have the benefit of a dedicated SOC. Depending on where your security organization is in its journey, capable security partners can be critical to improving your threat management – from providing advisory, consulting, and staff augmentation services to ingesting all of your cybersecurity data and owning the entire detection and response workflow (e.g. MSSPs). There isn't a one-size-fits-all approach for every organization to achieve Continuous Detection and Continuous Response. While ASO envisions aspirational team structures, process maps, and technology architectures, these are all reference concepts. As a partner, Google Cloud will help you assess your current level of maturity, define a target state, and develop a plan for driving security transformation across technology, process, and workforce.

Across all industries, hiring, retaining, and promoting candidates from diverse backgrounds can drive significant benefits. Google believes that much of the strength of our business stems from building a workforce that is more representative of our users and a workplace that creates a sense of belonging. When compared to other industries, the cybersecurity profession is more representative of diverse populations, but diverse communities are still lacking representation in leadership positions. Recent studies from the International Information System Security Certification Consortium (ISC2) (Innovation Through Inclusion: The Multicultural Cybersecurity Workforce) and McKinsey analyze these challenges, finding that organizations with diverse leadership teams perform better both financially and in terms of corporate culture, while also adding to the overall confidence of an organization's security posture.

Adversaries have no organizational confines to adhere to and come from regions all across the globe. As they become increasingly persistent and sophisticated, the cybersecurity problems that defenders face require creative approaches to building defense in depth. The core element of transforming people in the modern security operations workforce is dependent on your ability to shift from an operations-centric workforce to a creative, solutions-oriented workforce. A diverse security workforce and leadership team can ensure you're looking at solving these challenges from all angles, fostering creative problem solving, and cultivating perspectives that would not be derived from homogenous environments. We're thrilled to see the public sector championing this approach with the White House Executive Order 13985 on Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce.

How to Achieve Autonomic Security Operations

To embark on this journey, we've partnered with industry leading transformation catalysts to invest in this multi-year journey alongside our U.S. Public Sector customers, and continue to expand on our trusted partners equipped to deliver ASO in the Public Sector. To achieve the full requirements of the Executive Order, a prototypical timeline may look as depicted below.



Deloitte

"Deloitte[7] is excited to collaborate with Google Cloud on their transformational Public Sector Autonomic Security Operations (ASO) solution offering. Deloitte has been recognized as Google Cloud's Global Services Partner of the Year for four consecutive years, and also as their inaugural Public Sector Partner of the Year in 2020. Our deep bench of more than 1,000 Google Cloud certifications, capabilities spanning the Google Cloud security portfolio, and decades of delivery experience in the Government & Public Sector (GPS) makes us well-positioned to help our clients undertake critical Security Operations Center (SOC) transformation efforts with Google Cloud ASO.

Today's GPS clients operate the most critical and complex digital environments in a high-risk and high-threat sector, while managing significant government cyber security compliance and oversight requirements. For these reasons it's important to choose strategic advisors with a demonstrated track record of innovation and helping GPS organizations achieve their operational goals across people, process, and technology - as discussed in Deloitte and Google Cloud's Future of the SOC papers that can be accessed here.

Complementing and enabling ASO's approach requires transformation of talent, operations, and technology. Deloitte delivers these three through our industry-leading cyber security and data analytics

[7] As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

frameworks driving state of the art SOC transformations. Specifically, Managed Extended Detection and Response (MXDR) by Deloitte combines an integrated, modular detection and response Software as a Service (SaaS) platform with managed security services including military-grade threat hunting, detection, response, and remediation capabilities. Furthermore, Deloitte and Google Cloud have jointly developed Predictive Analytics for Cyber in Enterprises (PACE™), a cloud-native analytics solution built on Google Cloud, which leverages Deloitte's industry-leading cyber risk quantification and reporting methodologies to help SOC's with persona-driven decision making. Coupled with Google Cloud's ASO strategy and solutioning, Deloitte leverages decades of experience to provide Executive Order and OMB compliant end-to-end cloud security, SOC, and digital transformation services designed to help elevate and modernize cyber threat management programs in the public sector." Chris Weggeman, Managing Director | GPS Cyber and Strategic Risk Google Cloud Cyber Alliance Leader, Deloitte & Touche LLP

CYDERES

"Cyderes shares Google Cloud Security's mission to transform security operations, and we are honored to co-develop the Autonomic Security Operations (ASO) solution for the public sector. As the #1 MSSP in the world (Cyber Defense Magazine's 2021 Top MSSPs List) with decades of advisory and technology experience detecting and responding to the world's biggest cyber threats, Cyderes is uniquely positioned to equip federal agencies and departments to go far beyond the requirements of the executive order to transform their security programs entirely via Google's unique ASO approach. As an original launch partner of Google Cloud's Chronicle our deep expertise will propel our joint offering to modernize security operations in the public sector, all with significant cost efficiency compared to competing solutions.

The growing frequency and sophistication of today's threats demands a proactive cybersecurity strategy to detect and respond to acute attacks that threaten our national and individual security. In addition, even with essential federal policies, agencies face the daunting task of implementing upgrades with limited resources from a cost and engineering perspective. Cyderes provides 24-7 people, processes, and technology to manage risk, detect threats, and respond to security incidents in real-time. With our proprietary cloud-native analytics platform custom built on Google Cloud's flagship security offering Chronicle, six global security operations centers, and one of the world's largest managed services focused engineering teams entirely dedicated to solving the most complex security problems, Cyderes is prepared to deliver mature security operations at 10x scale (see whitepaper).

Cyderes leverages Google ASO's adaptive, agile, and automated approach to enable clients' security operations to become an innate defense mechanism, or auto-immune system fighting advanced threats. Our industry leading Cloud Native Analytics Platform (CNAP) is custom built on GCP's infrastructure foundation layer for unmatched performance, scale, availability, and trust and compliance. Combined with our full 24/7 EMDR (Enterprise Managed Detection & Response) agencies can shift from reactive monitoring to proactive threat hunting with 24/7 detection, investigation, and remediation capabilities. This comprehensive human-led and machine-driven Security-as-a-Service solution yields the results needed for modern agencies – fast, consistent, and highly automated outcomes using custom playbooks to deliver true autonomic security operations to the public sector." - Robert Herjavec, CEO, CYDERES

Conclusion

EO 14028 and the accompanying OMB M-21-31 signaled the U.S. Federal Government's recognition that a comprehensive program for threat detection and response is critical to defending our Nation against the cybersecurity threats it faces. To these ends, they proposed a multi-year process for departments and agencies to mature their cybersecurity capabilities, expand the usability of security activity data, and strengthen capabilities to analyze data more effectively in order to hasten and improve threat detection and response.

Modernizing security operations and threat management will require departments and agencies to assess their current state, plan strategic investments, establish milestones, and identify resources. Detailed planning will be necessary to meet the timelines in OMB M-21-31. Some agencies will have the capabilities to build everything in-house with a predominantly open source-led approach. Other agencies may lack security operations maturity and need a guided approach in addition to a technology stack to achieve ASO. And finally, some will prefer to partner with managed security service providers (MSSPs) to have them run the organization's security workflows.

Autonomic Security Operations can help the US Federal Government and its myriad agencies advance their event logging capabilities in alignment with OMB maturity tiers. We also believe that ASO can help the US Federal Government and its agencies undertake a larger transformation of technology, process, and people, toward a model of continuous threat detection and response. In doing so, we believe that ASO can help address a number of challenges presently facing cybersecurity teams, from the global shortage of skilled workers, to the overproliferation of security tools, to poor cybersecurity situational awareness and analyst burnout caused by an increase of data without sufficient context or tools to automate and scale detection and response.

We believe that by embracing ASO, agencies can help agencies achieve:

- **10x technology**, through the use of cloud-native tools that help agencies meet event logging requirements in the near term, while powering a longer-term transformation in threat management;
- **10x process**, by redesigning workflows and using automation to achieve Continuous Detection and Continuous Response in security operations;
- **10x people**, by transforming the productivity and effectiveness of security teams and expanding their diversity; and
- **10x influence** across the enterprise through a more collaborative and data-driven approach to solving security problems between security teams and non-security stakeholders.

We look forward to working with the US Federal Government to support departments and agencies in their cybersecurity transformation.

Appendix

The table below details ASO support for the Logging Requirements set forth in the OMB M-21-31.

To see specific logging retention requirements per log category, please refer to Appendix C of M-21-31

Log Category	Criticality	Supports
Identity & Credential Management	0	✅
Privileged Identity & Credential Management	0	✅
Email Filtering, Spam, and Phishing	0	✅
Network Device Infrastructure: (For Devices with Multiple Interfaces: Interface MAC - If Correlated to the DeNAT IP Address)	0	✅
Network Device Infrastructure	0	✅
Network Device Infrastructure (General Logging)	0	✅
Network Device Infrastructure (Access, Authorization, and Accounting)	0	✅
Operating Systems - Windows Infrastructure and Operating Systems	0	✅
Operating Systems - MACOS (Or Other Apple Desktop and Server Operating Systems)	0	✅
Operating Systems – BSD (Linux)	0	✅
Cloud Environments (General Events)	0	✅
Cloud Environments (General Logging)	0	✅
Cloud AWS	0	✅
Cloud Azure	0	✅
Cloud GCP	0	✅
System Configuration and Performance	1	✅
Authentication and Authorization	1	✅
Email Filtering, Spam, and Phishing	1	✅

Antivirus and Behavior Based Malware Protection	1	✅
Network Device Infrastructure	1	✅
Network Device Infrastructure (for Devices with Multiple Interfaces: Interface MAC - If Correlated to the De- NAT IP Address)	1	✅
PKI Infrastructure	1	✅
Vulnerability Assessment	1	✅
Database Level	1	✅
Application Level	1	✅
Virtualization System	1	✅
Mobile (Smartphones and Tablets) EMM (UEM) / MTD Server Logs	1	✅
Mobile (Smartphones and Tablets) EMM (UEM) / MTD Agent Logs	1	✅
Container - Supply Chain	1	✅
System Configuration and Performance	2	✅
Email Filtering, Spam, and Phishing	2	✅
Data Loss Prevention	2	✅
Network Traffic	2	✅
Application Level	2	✅
Container - Image	2	✅
Container - Engine (Management / Orchestration)	2	✅
Container - OS	2	✅
System Configuration and Performance	3	✅
Email Filtering, Spam, and Phishing	3	✅
Mainframes	3	✅
Container - Cluster/Pod Events	3	✅