ANOMALI

# Executive Order on Improving the Nation's Cybersecurity

July 8, 2021

Stewart Wright – Director of Federal Sales: swright@anomali.com

Aaron Dee – Federal Sales Engineer: adee@anomali.com

Jason Burosh – VP of Sales Federal/East/Canada: jburosh@anomali.com

# Executive Summary

On May 12, 2021, President Biden signed an Executive Order to improve America's cybersecurity in the wake of major cyberattacks, such as SolarWinds. Although this Executive Order only applies to the federal government and federal government systems. It can also be applied to thousands of government contractors that provide IT goods and services to the US government.

While many of the cybersecurity provisions have not been written yet and will need to be drafted and commented on, we at Anomali believe strengthening the cybersecurity of our nation begins with cyber resilience.

To achieve a state of resilience, organizations need to elevate their Security Posture by taking a holistic approach to cybersecurity. To be resilient, a security strategy needs to include global, actionable intelligence that provides:

- Relevant Intelligence at Scale
- Precision Attack Detection
- Optimized Response across Security Ecosystems

## Relevant Intelligence at Scale

Threat intelligence, including global trends as well as locally observed incidents and vulnerabilities, is critical to any organization’s effort to establish a resilient IT infrastructure. But because of the cost to acquire intelligence, insufficient team skills to cultivate relevancy, and the inability to operationalize, many organizations’ security strategies lack this critical capability.

Anomali takes intelligence and makes it relevant to what matters, giving CISOs the power to monitor global cybersecurity risks, detect potential attacks and perform investigations required to determine gaps in security coverage. Anomali provides relevant intelligence at scale that:

- Helps security teams thoroughly understand global cyberthreats

- Provides increased visibility to monitor global trends to identify relevant cybersecurity risks
- Enables secure collaboration with internal teams and external suppliers, partners, and industry peers

## Precision Attack Detection

When it comes to detecting threats, the accuracy of the intelligence used in the detection process is critical. If the detection model is riddled with false positives, detection alerts are useless. If the severity scoring is off – the anticipated impact of a threat will not align with the reality of an attack.

Anomali's threat detection capabilities are fueled by constantly curated global intelligence that is used to detect threats at scale. This provides analysts with the data required to investigate the root cause of an attack and enables them to immediately respond.  Anomali provides precision attack detection that:

- Continuously evolves with the ever-changing global threat landscape to help accurately detect threats with pinpoint precision
- Integrates automated enrichments that increase the fidelity of intelligence to deliver more accurate detection of threats in an environment
- Provides a seamless workflow of human created and automated investigation between Security Operations, Threat Intelligence, and Incident Response functions to increase the accuracy of threat detections

## Optimized Response across Security Ecosystems

When under attack, security teams need to make decisions fast. Anomali allows security teams to effectively respond to attacks by giving them the tools and actionable intelligence needed to make informed decisions. Anomali helps provide an optimized response for security teams by:

- Providing relevant global intelligence at their fingertips to make quick informed decisions
- Enabling visualization of threat actor trends, attack activity, and relevance that enable analysts to prioritize investigations and effectively respond

- Automating response that enhances security posture after an identified breach and helps protect from future attacks

Anomali helps organizations achieve cyber resilience. We are committed to helping the federal government, its agencies and its suppliers become cyber resilient to meet the objectives of the Executive Order and defend against today's sophisticated cyber threats.

# Anomali Overview

The Anomali Threat Intelligence Management platform was purpose built to ingest and correlate threat data, information, and intelligence to make it actionable and drive effective cyber security decisions. It is a platform that automates detection, prioritization, and analysis of the most relevant threats facing organizations. By incorporating machine learning, automation, intelligence sharing, and an expansive partner ecosystem, Anomali empowers security teams to leverage threat intelligence for increased insights and definitive response to physical and cyber-attacks – while integrating with existing security defenses and workflows of your teams. Anomali helps organizations:

- Identify targeted threats to the organization
- Automate detection and analysis of threats
- Improve response with insights into threat actors and behaviors
- Save time and resources by reducing impact of attacks
- Allow for collaboration between internal and external groups
- Enhance security posture to prevent future attacks

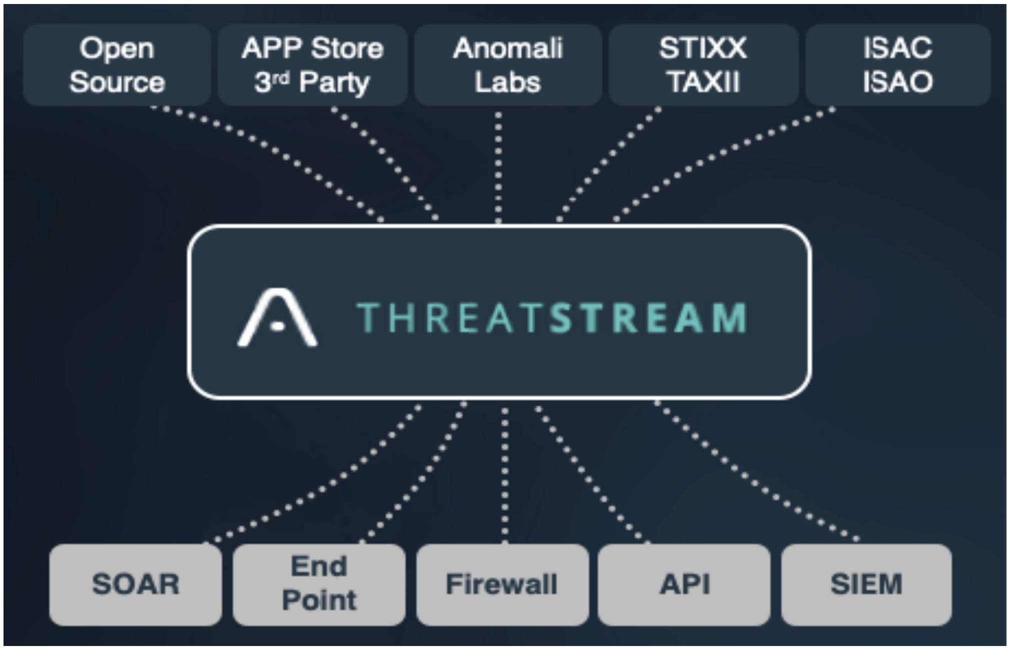
Anomali's security suite is composed of three main components: ThreatStream, Anomali Lens, and Anomali Match:

## ThreatStream

ThreatStream is a Threat Intelligence Management Platform that automates the collection and processing of raw data and transforms it into actionable threat intelligence to enable security teams to quickly investigate security incidents. With ThreatStream, analysts  can collect, contextualize, and risk rank complex, high-volume indicators with machine learning to prioritize alerts and guide security strategy.

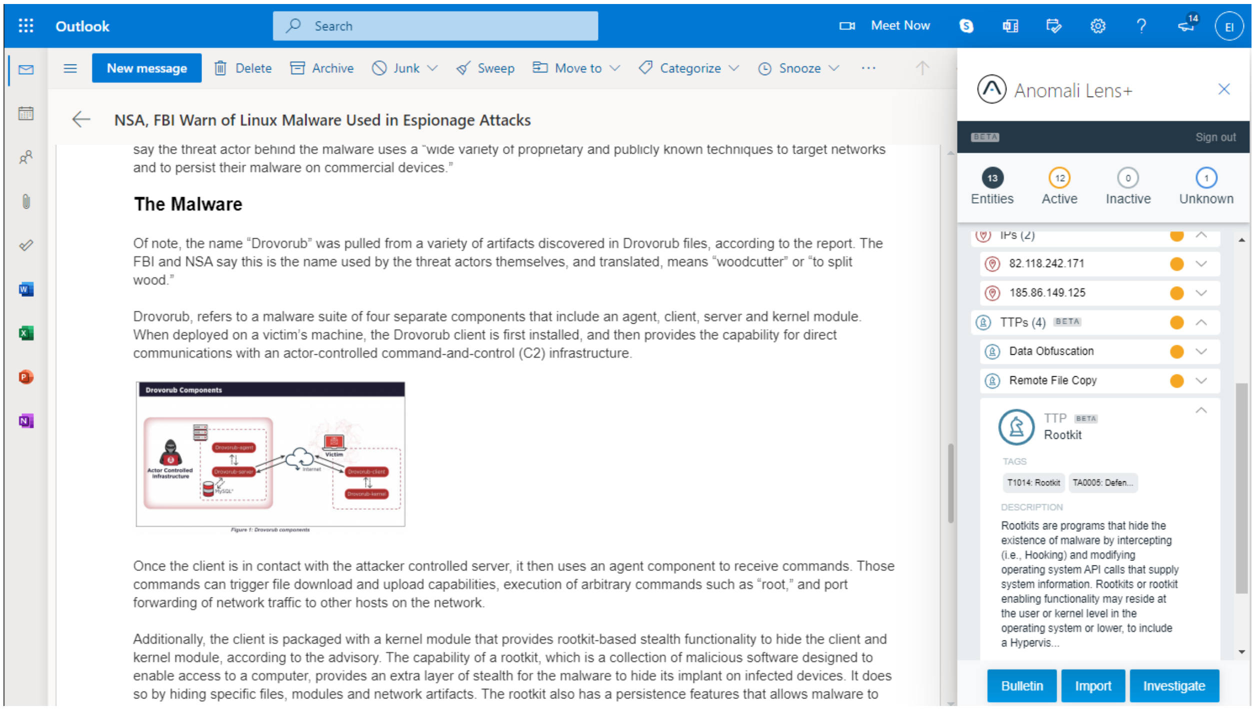
ThreatStream enables security teams to:

- Map threat intelligence to threat models (Actor Profiles, Campaigns, and TTPs)
- Aggregate OSINT, 3rd party premium feeds, Anomali Labs Research, and ISAC data (e.g. DHS AIS, CISCP, and more)
- Automate workflows for quicker analyst insights
- Securely share and collaborate threat intelligence with trusted partners
- Integrate with SIEMs, Data Lakes (Splunk, Elastic, Devo, etc.), Firewall, Endpoint, Proxy, IDS, API, Orchestration Tools, Ticketing Systems, and more



## Anomali Lens

Anomali Lens is a powerful  extension that helps operationalize threat intelligence by automatically scanning digital content to identify relevant threats and streamline the lifecycle of researching and reporting on them.Lens enables threat and security analysts to make faster and more accurate decisions. By providing instant access to strategic and tactical intelligence from within any web browser, Office 365, or Microsoft Word - analysts at all levels can quickly analyze content from a cyber intelligence perspective and instantly answer the most pertinent questions, i.e., “what am I looking at, and have we been impacted?”



NSA, FBI Warn of Linux Malware Used in Espionage Attacks

say the threat actor behind the malware uses a "wide variety of proprietary and publicly known techniques to target networks and to persist their malware on commercial devices."

**The Malware**

Of note, the name "Drovorub" was pulled from a variety of artifacts discovered in Drovorub files, according to the report. The FBI and NSA say this is the name used by the threat actors themselves, and translated, means "woodcutter" or "to split wood."

Drovorub, refers to a malware suite of four separate components that include an agent, client, server and kernel module. When deployed on a victim's machine, the Drovorub client is first installed, and then provides the capability for direct communications with an actor-controlled command-and-control (C2) infrastructure.

*Figure 1: Drovorub components*

Once the client is in contact with the attacker controlled server, it then uses an agent component to receive commands. Those commands can trigger file download and upload capabilities, execution of arbitrary commands such as "root," and port forwarding of network traffic to other hosts on the network.

Additionally, the client is packaged with a kernel module that provides rootkit-based stealth functionality to hide the client and kernel module, according to the advisory. The capability of a rootkit, which is a collection of malicious software designed to enable access to a computer, provides an extra layer of stealth for the malware to hide its implant on infected devices. It does so by hiding specific files, modules and network artifacts. The rootkit also has a persistence features that allows malware to

13 Entities 12 Active 0 Inactive 1 Unknown

IPs (2)
82.118.242.171
185.86.149.125
TTPs (4) BETA
Data Obfuscation
Remote File Copy

TTP BETA
Rootkit

TAGS
T1014: Rootkit TA0005: Defen...

DESCRIPTION
Rootkits are programs that hide the existence of malware by intercepting (i.e., Hooking) and modifying operating system API calls that supply system information. Rootkits or rootkit enabling functionality may reside at the user or kernel level in the operating system or lower, to include a Hypervis...

## Anomali Match

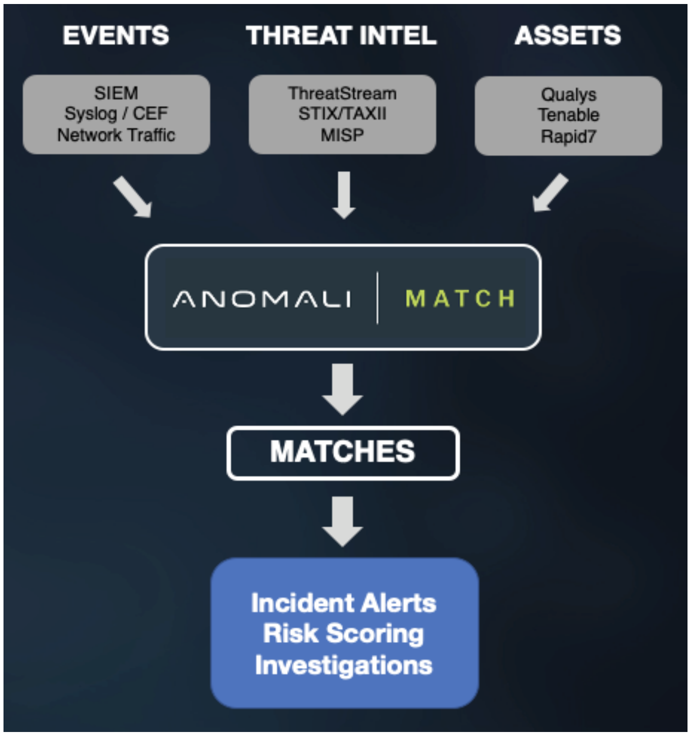
Match is an intelligence-driven extended detection and response solution that helps organizations quickly identify and respond to threats in real-time. Match correlates current and historic metadata against ALL active threat intelligence to expose previously unknown threats.

With Match, organization's can:

- Evaluate exposure to current and historical threats (5+ years' worth of log data)
- Operationalize ALL of the ACTIVE threat intelligence available to you (600+ million IOCs)
- Automatically tie indicator matches to threat models (e.g. CVEs and MITRE ATT&CK)
- Review assets with known CVEs and associate to Anomali Match rules and alerts
- Prioritize analysts' work with high-fidelity alerts
- Review timeline of incidents and anatomy of attacks

- Automatically detect and alert on traffic to DGA domains with 90%+ accuracy

Anomali Match automatically correlates ***all*** active threat intelligence against all current and historic event data. Matchis the only threat intelligence solution integrating this capability, and further complements the SIEM/EDR/Data Lake by increasing your historical visibility and helps leverage ALL of the active threat intelligence in your database to quickly identify any existing or lingering threats in your environment.



## Dedicated Account Management

Anomali's dedicated resources provide embedded support that becomes an extension of our customer's teams, as well as advocates for our customer's needs within Anomali. Embedded Anomali resources assist with deployment, planning, planning, design, integration, and success during the course of the engagement. Additionally, Anomali's embedded resources understand all aspects of the customer environment and provide onsite/remote assistance, as required. By working closely with the customer, embedded resources develop intimate knowledge and a personalized support relationship with our customer's security teams.

We appreciate the opportunity to work with your team regarding your Threat Intelligence Platform and maturing your cyber security program.  Below you will find Biden's Executive Order (EO) on Improving the Nation's Cybersecurity and how the Anomali Platform addresses the specific initiatives outlined by the administration.

# Sec. 2.  Removing Barriers to Sharing Threat Information

## Section A – Intelligence Sharing

(a)  The Federal Government contracts with IT and OT service providers to conduct an array of day-to-day functions on Federal Information Systems.  These service providers, including cloud service providers, have unique access to and insight into cyber threat and incident information on Federal Information Systems.  At the same time, current contract terms or restrictions may limit the sharing of such threat or incident information with executive departments and agencies (agencies) that are responsible for investigating or remediating cyber incidents, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and other elements of the Intelligence Community (IC).  Removing these contractual barriers and increasing the sharing of information about such threats, incidents, and risks are necessary steps to accelerating incident deterrence, prevention, and response efforts and to enabling more effective defense of agencies' systems and of information collected, processed, and maintained by or for the Federal Government.

➔ The Anomali platform is a cloud based service that provides collection and aggregation of active threat intelligence, scoring and prioritization of indicators, and maps indicators to threat model entities such as actors, campaigns, TTPs, vulnerabilities, and more.  As real-time intelligence is ingested into the platform, we help organizations operationalize prioritized intelligence to raise awareness of active threats.  By leveraging active threat intelligence at scale, we can help decrease time to detect and respond to active threats.  The Anomali platform also uses machine learning and automation to improve analyst workflow, create efficiencies for SOC and IR teams, and even integrate with ticketing and SOAR platforms for automated response efforts.

## Section C – Cybersecurity prevention, detection, response

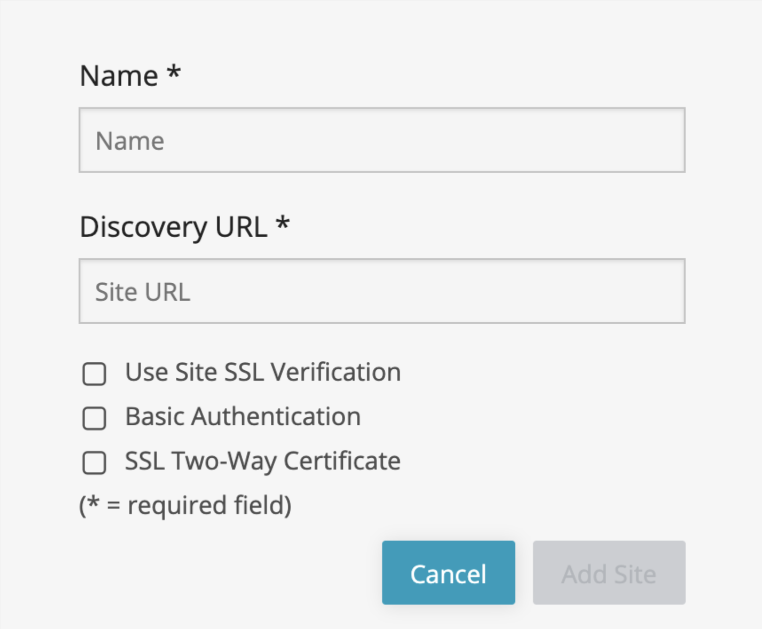
(c) The recommended contract language and requirements described in subsection (b) of this section shall be designed to ensure that:

(i) service providers collect and preserve data, information, and reporting relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control, including systems operated on behalf of agencies, consistent with agencies' requirements;

➔ Anomali ThreatStream automates and accelerates the process of collecting all relevant global threat data, giving you the enhanced visibility that comes with diversified, specialized intelligence sources, without increasing administrative load. ThreatStream curates external threat intelligence from over 120+ OSINT sources, ISACs and trusted circles (such as DHS, AIS, CISCP, NCFTA, MS-ISAC and others), as well as Premium intelligence feeds. Anomali Lens extends the ability to collect unstructured data provided through multiple formats including online threat bulletins, email, .csv files and pdf's.

(ii) service providers share such data, information, and reporting, as they relate to cyber incidents or potential incidents relevant to any agency with which they have contracted, directly with such agency and any other agency that the Director of OMB, in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, deems appropriate, consistent with applicable privacy laws, regulations, and policies;

- ➔ ThreatStream is the leading global threat sharing platform for ISACs, ISAOs, industry groups, holding companies, and other threat intel sharing communities seeking to power secure collaboration. The ISAC organization(s) has a unique threat sharing community portal leveraging the ThreatStream platform. Community members have access to 'Trusted circles' where they can collaborate and share relevant information via the secure, cloud-based portal. Anomali customers also have access to API and STIX/TAXII for programmatic access and automation. Community training is also available via online, self-paced courses.



Name *

Name

Discovery URL *

Site URL

□ Use Site SSL Verification
□ Basic Authentication
□ SSL Two-Way Certificate

(* = required field)

(iii) service providers collaborate with Federal cybersecurity or investigative agencies in their investigations of and responses to incidents or potential incidents on Federal Information Systems, including by implementing technical capabilities, such as monitoring networks for threats in collaboration with agencies they support, as needed; and

- ➔ ThreatStream provides continuous, updated intelligence that is scored and prioritized for your organization. Anomali manages the intelligence and downstream integrations so that you can manage active threats and incident response. If there are matches to external threat intelligence in your network and host-based logs — you can leverage the investigations and enrichments in our platform to optimize workflow and create efficiencies for the SOC and IR team. ThreatStream also has industry-leading integrations with ticketing and SOAR platforms to further automate manual tasks and response. After customers identify a threat, investigate, add artifacts, determine root cause, and remediate — they can optionally create a new threat bulletin sharing their investigation and known bad indicators of compromise back out to their trusted circles and sharing communities.

(iv) service providers share cyber threat and incident information with agencies, doing so, where possible, in industry-recognized formats for incident response and remediation.

➔ Anomali participates with organizations such as OASIS (STIX/TAXII standards) and MITRE (MITRE ATT&CK) to develop and support industry-recognized frameworks. Our platform integrates with these common frameworks to leverage best practices and allow our customers to not only assist with investigation efforts — but also share information back out to their trusted communities leveraging standard formats.

## Section F - Reporting on Cyber Attacks

(f) It is the policy of the Federal Government that:

(i) information and communications technology (ICT) service providers entering into contracts with agencies must promptly report to such agencies when they discover a cyber incident involving a software product or service provided to such agencies or involving a support system for a software product or service provided to such agencies;

- *As a cloud-based service — we scan our software and promptly report any cyber incidents. For third-party products — the Anomali platform automatically ingests new indicators and threat bulletins as they become available — adding that data to your threat intelligence repository. We also score and prioritize active intelligence and operationalizing that data to your downstream security products such as SIEM, Firewalls, EDR, Web proxies, and more. For example — when the Sunburst backdoor threat bulletins from Microsoft and Mandiant were published — we automatically imported the threat bulletins and indicators of compromise into ThreatStream. Customers that also had Anomali Match were immediately alerted if there were any historical matches in their historical metadata — automating the threat hunting and investigation efforts.*

(ii) ICT service providers must also directly report to CISA whenever they report under subsection (f)(i) of this section to Federal Civilian Executive Branch (FCEB) Agencies, and CISA must centrally collect and manage such information;

- When new threat bulletins and IOCs are ingested into the platform - all of that information is available to our community members. Some of our customers take that data and create specific threat bulletins with additional information that they share back out to their trusted communities and ISACs. By leveraging our threat bulletin and reporting capabilities you can customize what types of information to share depending on your audience. For example - you can share actor, TTP, and tactical indicators to an analyst team, and high-level information to management. Threat bulletins can be shared and disseminated via the ThreatStream platform leveraging multiple formats including email, pdf, .csv, and STIX TAXII.

## Section H – Certifications and Contractual Requirements

(h) Current cybersecurity requirements for unclassified system contracts are largely implemented through agency-specific policies and regulations, including cloud-service cybersecurity requirements. Standardizing common cybersecurity contractual requirements across agencies will streamline and improve compliance for vendors and the Federal Government.

- ➔ The Anomali platform is hosted in AWS and we adhere to best practices and cybersecurity requirements. Anomali has a SOC Type II certification and is currently in the process of FedRamp certification. Our solution has multiple deployment options (SaaS, On-prem, Air gap) and can also be hosted in AWS GovCloud, IBM Azure, and other cloud platforms.

  Anomali's portfolio of Threat Intelligence Management solutions are fully in accordance with NIST guidelines referenced in the Executive Order on Cybersecurity Section 3 Subsection B.

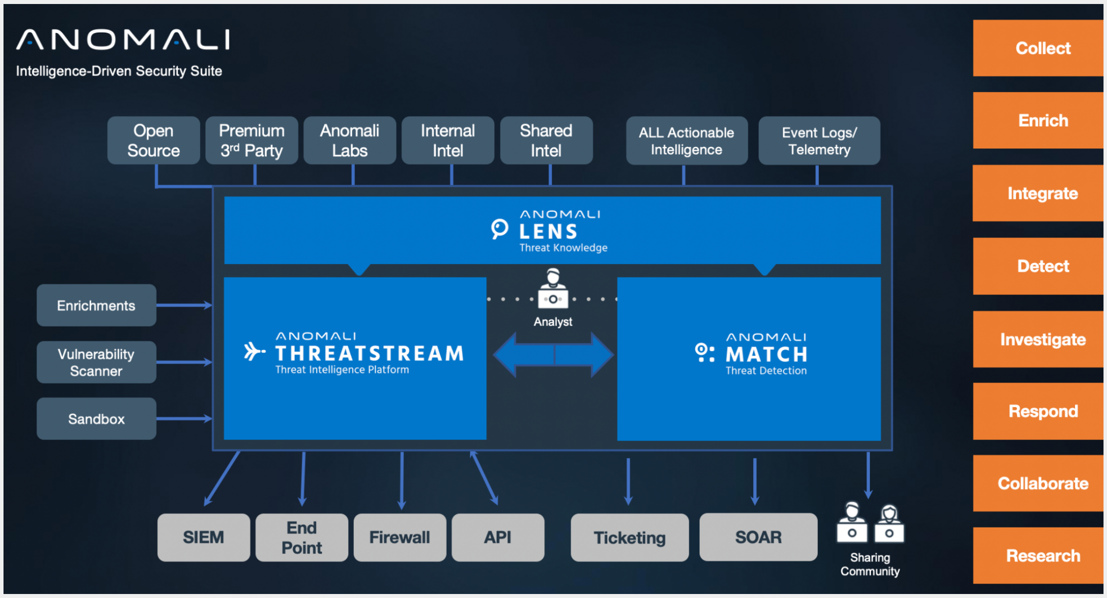
  Detailed compliance information for all Anomali solutions can be found in Section B - Cloud Technology, Zero Trust, NIST Standards.

# Sec. 3. Modernizing Federal Government Cybersecurity

## Section A – Increasing Threat Visibility

(a) 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, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

➔ Anomali is the World leading SaaS Threat Intelligence Platform. We help our customers centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks.  ThreatStream includes security best practices and is a fundamental element of a mature cyber security program.  We collect relevant intelligence, score/prioritize/enrich the data, actively maintain downstream integrations leveraging active intel, provide workflow and investigations tools to create efficiencies across your teams, provide ticketing and SOAR integrations for automated response, and allow you to share information securely with ISACs and trusted circles.



# Section B – Cloud Technology, Zero Trust, NIST Standards

(b) Within 60 days of the date of this order, the head of each agency shall:

(i) update existing agency plans to prioritize resources for the adoption and use of cloud technology as outlined in relevant OMB guidance;

➔ The Anomali platform is the only native cloud offering in the TIP (Threat Intelligence Platform) space. We are the market leader and innovator defining where TIP and XDR is going in the future. That continues to be a differentiator allowing unparalleled scalability and an overall lower cost of ownership for our customers.

(ii) develop a plan to implement Zero Trust Architecture, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance, describe any such steps that have already been completed, identify activities that will have the most immediate security impact, and include a schedule to implement them; and

➔ The zero trust architecture includes:

- Enhanced Identity and Access Management
- Implement Least Privilege at the Firewall
- Log and Analyze Security Events — match with active threat intel

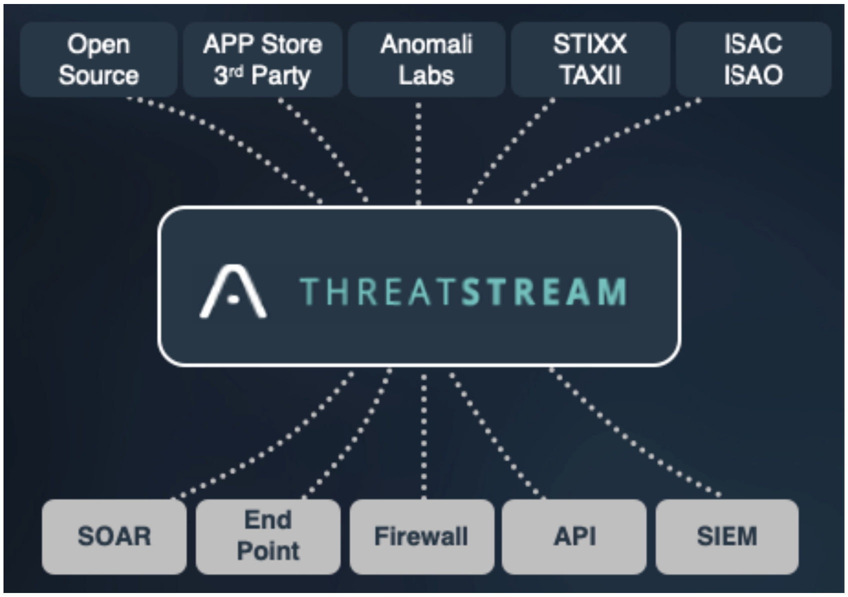
Anomali is a SaaS solution with multi-factor authentication and granular role-based access control. You can limit IP addresses where users are allowed to log into the platform. ThreatStream can assist with scoring intelligence and integrating into your SIEM environment to match logs against active threat intelligence. Match can also provide greater visibility across historical logs and leverage external threat intelligence at scale. This helps match new intelligence against ‘historical logs’ during the time frame when these newly discovered IOCs were active.

The following section outlines how the Anomali Platform offerings ThreatStream, Lens and Match accomplish these objectives and map to National Institute of Standards and Technology (NIST) standards and guidelines as referenced in Executive Order Section 3 Subsection B.

## Anomali ThreatStream NIST Compliance

In accordance with NIST guidelines referenced in the Executive Order on Cybersecurity Section 3 Subsection B, Anomali is proud to announce that Anomali ThreatStream is compliant with NIST SP 800-53 Rev. 5 control: **RA-10 Threat HUNTING.** RA-10 requires organizations to establish and maintain a cyber threat hunting capability to: Search for indicators of compromise in organizational systems; and detect, track, and disrupt threats that evade existing controls; and employ the threat hunting capability [Assignment: organization-defined frequency]. Anomali ThreatStream is a best in class Threat Intelligence Management Platform that empowers analysts to accelerate threat hunting activities with targeted threat intelligence to investigate relevant threats. With ThreatStream, analysts can collect, contextualize, and risk rank complex, high-volume indicators with automated machine-learning to prioritize alerts and guide security strategy and threat hunting initiatives. ThreatStream can:

- Map threat intelligence to threat models (Actors, Attack Patterns, Campaigns, Courses of Action, Identities, Incidents, Infrastructure, Signatures, Intrusion Sets, Malware, Threat Bulletins, Tools, TTPs, Vulnerabilities)
- Aggregate OSINT, Anomali Labs Research, premium Flashpoint Intelligence and ISAC data (e.g. US-CERT DHS AIS, CISCP, and more)
- Automate workflows for quicker analyst insights
- Securely share and collaborate threat intelligence with trusted partners
- Integrate with SIEMs (e.g. Splunk), AI/FPC (e.g. NetWitness), Firewalls, Endpoint, Proxy, IDS, API, Orchestration Tools, Ticketing Systems, and more



*Note: Below you will find the cited NIST SP 800-52 Rev. 5 control*

NIST SP 800-53 Rev. 5 Control: RA-10 THREAT HUNTING Control:

a) Establish and maintain a cyber threat hunting capability to:

   1. Search for indicators of compromise in organizational systems; and

   2. Detect, track, and disrupt threats that evade existing controls; and

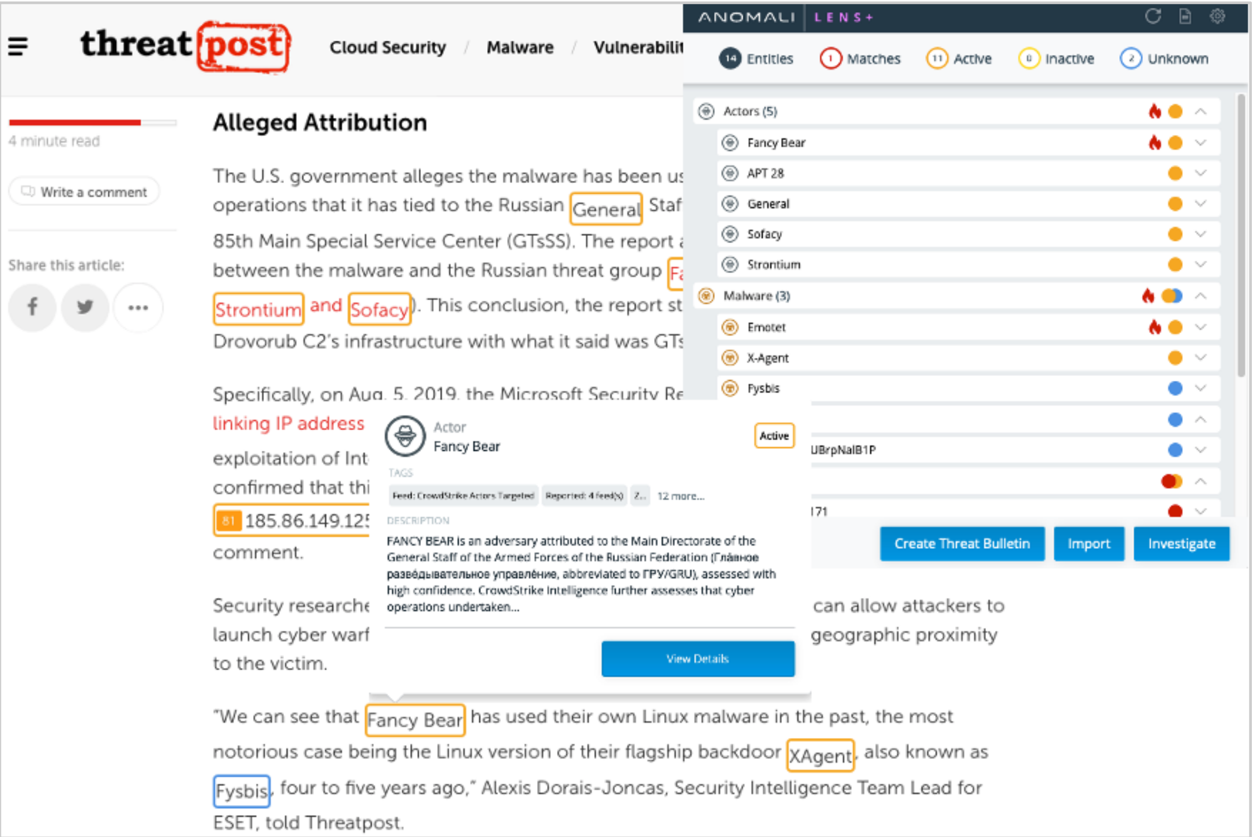
b) Employ the threat hunting capability [Assignment: organization-defined frequency].

Discussion: Threat hunting is an active means of cyber defense in contrast to traditional protection measures, such as firewalls, intrusion detection and prevention systems, quarantining malicious code in sandboxes, and Security Information and Event Management technologies and systems. Cyber threat hunting involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. Indicators of compromise include unusual network traffic, unusual file changes, and the presence of malicious code. Threat hunting teams leverage existing threat intelligence and may create new threat intelligence, which is shared with peer organizations, Information Sharing and Analysis Organizations (ISAO), Information Sharing and Analysis Centers (ISAC), and relevant government departments and agencies.

Link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

## Anomali Lens+ NIST Compliance

In accordance with NIST guidelines referenced in the Executive Order on Cybersecurity Section 3 Subsection B, Anomali is proud to announce that Anomali Lens+ is compliant with NIST SP 800-53 Rev. 5 control: **AU-13 Monitoring for Information Disclosure - Control Enhancements section 2: Monitoring for Information Disclosure | REVIEW OF MONITORED SITES.** AU-13 requires organizations to review the list of open-source information sites being monitored. Anomali Lens+ enables threat and security analysts to make faster and more accurate decisions. By providing instant access to strategic and tactical intelligence from any web browser, analysts at all levels can quickly analyze content from a cyber intelligence perspective by instantly answering the most pertinent questions, i.e., “what am I looking at, and have we been impacted?”



Alleged Attribution

The U.S. government alleges the malware has been us
operations that it has tied to the Russian General Staf
85th Main Special Service Center (GTsSS). The report a
between the malware and the Russian threat group Fa
Strontium and Sofacy). This conclusion, the report st
Drovorub C2's infrastructure with what it said was GTs

Specifically, on Aug. 5, 2019, the Microsoft Security Re
linking IP address
exploitation of Int
confirmed that thi
185.86.149.125
comment.

Security researche … can allow attackers to
launch cyber warf … geographic proximity
to the victim.

FANCY BEAR is an adversary attributed to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (Гла́вное разве́дывательное управле́ние, abbreviated to ГРУ/GRU), assessed with high confidence. CrowdStrike Intelligence further assesses that cyber operations undertaken...

“We can see that Fancy Bear has used their own Linux malware in the past, the most notorious case being the Linux version of their flagship backdoor XAgent, also known as Fysbis, four to five years ago,” Alexis Dorais-Joncas, Security Intelligence Team Lead for ESET, told Threatpost.

*Note: Below you will find the cited NIST SP 800-52 Rev. 5 control*

NIST SP 800-53 Rev. 5 Control: AU-13 Monitoring for Information Disclosure – Control Enhancements section 2: Monitoring for Information Disclosure | REVIEW OF MONITORED SITES

Review the list of open-source information sites being monitored [Assignment: organization-defined frequency].

Discussion: Reviewing the current list of open-source information sites being monitored on a regular basis helps to ensure that the selected sites remain relevant. The review also provides the opportunity to add new open-source information sites with the potential to provide evidence of unauthorized disclosure of organizational information. The list of sites monitored can be guided and informed by threat intelligence of other credible sources of information.

Link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

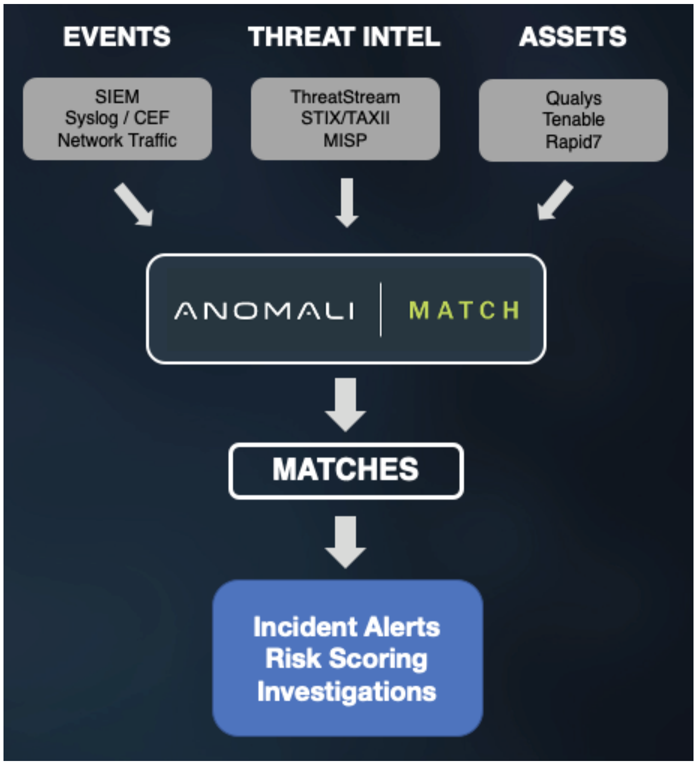
## Anomali Match NIST Compliance

In accordance with NIST guidelines referenced in the Executive Order on Cybersecurity Section 3 Subsection B, Anomali is proud to announce that Anomali Match is compliant with **NIST SP 800-53 Rev. 5 control: PM-16 THREAT AWARENESS PROGRAM – Control Enhancements section 1: THREAT AWARENESS PROGRAM | AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE**

**. PM-16** requires organizations to employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information. Anomali Match is an extended detection and response solution purpose-built to automate and decrease time to detection and ability to respond. Anomali Match correlates current and historic metadata against ALL active threat intelligence to expose previously unknown threats. Anomali Match is built to share Threat Intelligence within Trusted Circles (private/public) as well as ISAC/ISAO.

- Evaluate exposure to current and historical threats (5+ years' worth of log data)
- Operationalize ALL of the ACTIVE threat intelligence available to you (400+ million IOCs)
- Automatically tie indicator matches to threat models (e.g. CVEs and MITRE ATT&CK)
- Review assets with known CVEs and associate to Anomali Match rules and alerts
- Prioritize analysts' work with high-fidelity alerts

- Review timeline of incidents and anatomy of attacks
- Automatically detect and alert on traffic to DGA domains with 90%+ accuracy



*Note: Below you will find the cited NIST SP 800-52 Rev. 5 control*

NIST SP 800-53 Rev. 5 Control:PM-16 THREAT AWARENESS PROGRAM – Control Enhancements section 1: THREAT AWARENESS PROGRAM | AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE

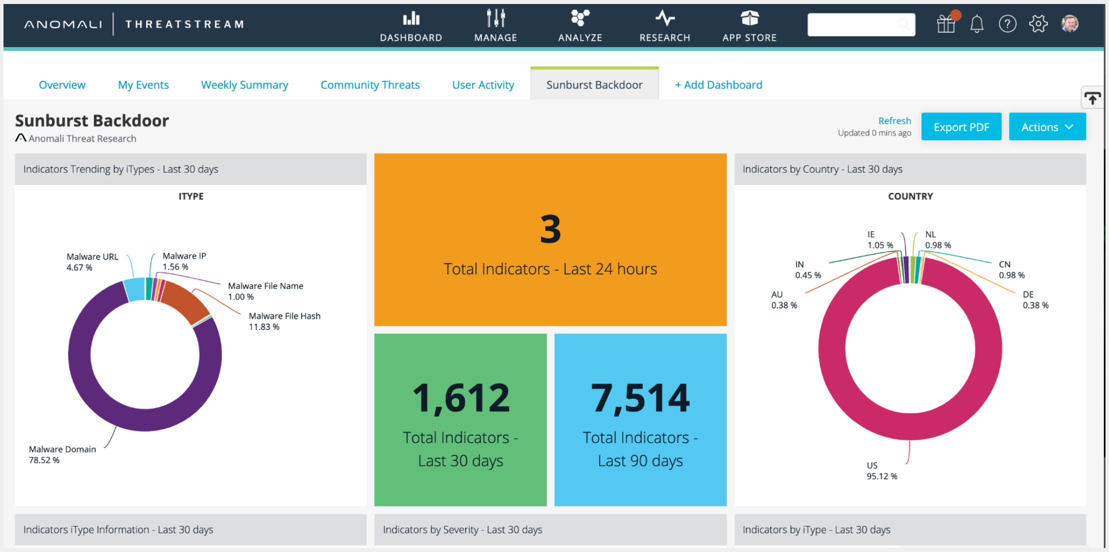
Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.

Discussion: To maximize the effectiveness of monitoring, it is important to know what threat observables and indicators the sensors need to be searching for. By using well-established frameworks, services, and automated tools, organizations improve their ability to rapidly share and feed the relevant threat detection signatures into monitoring tools.

Link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

(iii) provide a report to the Director of OMB and the Assistant to the President and National Security Advisor (APNSA) discussing the plans required pursuant to subsection (b)(i) and (ii) of this section.

➔ The Anomali platform comes with customizable dashboards, threat bulletin creation, as well as robust reporting tools that can be leveraged to create detailed reports. We also have role-based access control and user activity audit reports available in the platform.



## Section C – Using Cloud Technology to Defend

(c) As agencies continue to use cloud technology, they shall do so in a coordinated, deliberate way that allows the Federal Government to prevent, detect, assess, and remediate cyber incidents. To facilitate this approach, the migration to cloud technology shall adopt Zero Trust Architecture, as practicable. The CISA shall modernize its current cybersecurity programs, services, and capabilities to be fully functional with cloud-computing environments with Zero Trust Architecture. The Secretary of Homeland

Security acting through the Director of CISA, in consultation with the Administrator of General Services acting through the Federal Risk and Authorization Management Program (FedRAMP) within the General Services Administration, shall develop security principles governing Cloud Service Providers (CSPs) for incorporation into agency modernization efforts.  To facilitate this work:

➔ Anomali is a native cloud application hosted with AWS. S3SSE is enabled with maximum encryption ciphers to ensure the security of any data at rest.  As the CSP, AWS provides encryption of any data requiring transfer or transportation. Anomali utilizes S3SSE for all datastores. While at rest, all data is encrypted using 256 bit AES Encryption. In Transit, Anomali enforces the use of TLS tunnels and requires clients to use modern protocols and cipher suites to prevent interception or manipulation.  We support perfect forward secrecy and flag all authentication cookies as secure. We enable HSTS and enforce HTTPS for all communication, even to our public website.

All data that resides in the platform is owned by the customer and not shared by Anomali. You can enforce role-based access control for users in your organization - and leverage the TLP protocol for sensitive data and access/privileges.

We are currently working with customers to obtain an ATO on major DoD networks — and also in talks with our consultant, Anitian, on beginning the process for getting FedRamp certified.

## Section D – Multi-Factor Authentication

(d)  Within 180 days of the date of this order, agencies shall adopt multi-factor authentication and encryption for data at rest and in transit, to the maximum extent consistent with Federal records laws and other applicable laws.  To that end:

(i)  Heads of FCEB Agencies shall provide reports to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA on their respective agency's progress in adopting multifactor authentication and encryption of data at rest and in transit.  Such agencies shall provide such reports every 60 days after the date of this order until the agency has fully adopted, agency-wide, multi-factor authentication, and data encryption.

- ➔ Being a Native Cloud-based solution, Anomali offers Multi-factor authentication as well as data encryption in transit and at rest. Secure access to ThreatStream SaaS with SAASPASS multi-factor authentication (MFA) and secure single sign-on (SSO) and integrate it with SAML in no time and with no coding. User activity and audit reports are available ad-hoc or scheduled within the user interface of the platform.

(ii) Based on identified gaps in agency implementation, CISA shall take all appropriate steps to maximize adoption by FCEB Agencies of technologies and processes to implement multifactor authentication and encryption for data at rest and in transit.

- ➔ Anomali can help expedite the adoption of best practices, multi-factor authentication, and encryption using our SaaS platform

# Sec. 4. Enhancing Software Supply Chain Security

## Section A – Ensuring Integrity of Critical Software

(a) The security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions. The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended. The security and integrity of "critical software" — software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources) — is a particular concern. Accordingly, the Federal Government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software.

➔ The Anomali platform can assist with enhancing Software Supply Chain Security in the following areas:
- Establishing multi-factor, risk-based authentication and conditional access across the enterprise;
- Documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software;
- Employing encryption for data; and
- Monitoring operations and alerts and responding to attempted and actual cyber incidents

As malicious actor reports or threat bulletins containing information about third party software vendors are ingested in the platform - we import indicators which will automatically flow down to your downstream integrations to identify or block malicious activity. For example - as late breaking news comes out regarding threats - we will provide information on the available intel and also create dashboards in the platform to track that activity for our community members. The Anomali platform can also identify suspicious domain registrations that could be used for phishing attempts, and can also identify possible compromised credentials for third parties/supply chain monitoring.

# Sec. 6. Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents

## Section A – Developing Standardized Response Tactics

(a) The cybersecurity vulnerability and incident response procedures currently used to identify, remediate, and recover from vulnerabilities and incidents affecting their systems vary across agencies, hindering the ability of lead agencies to analyze vulnerabilities and incidents more comprehensively across agencies. Standardized response processes ensure a more coordinated and centralized cataloging of incidents and tracking of agencies' progress toward successful responses.

➔ Anomali's world class customer success organization is an extension of your team and meets with our customers on a bi-weekly cadence. We help identify the maturity of cyber threat intel programs and outline a path moving forward with continuous improvement. During the discovery phase, we identify gaps, create prioritized intelligence requirements that map to your business use cases, enable the appropriate feeds, integrate with your current products in the security stack, and start identifying SOPs and opportunities for automation.

One area where the Anomali platform can assist with vulnerability and incident response procedures is how we leverage that data in Match. Match looks at historical logs up to 5+ years and ALL active threat intelligence for correlation or matches. It also looks at asset criticality and historical vulnerability information for that host. If there is a match to external, known bad indicators for that device — we can help prioritize the alerts based upon asset criticality and historical vulnerability information. If it is a critical asset and 'had' an open port/vulnerability that could be susceptible to that attack, that raises the priority of the alert. The device may have been patched recently… however, we care about the vulnerabilities at the time of the 'match' — not just what patch level the host is currently at today.

Based upon the type of indicator, severity, asset criticality and vulnerabilities - we can then take some automated actions streamlining the investigation/remediation process.

# Sec. 7. Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks

## Section A – Proactively Detect Threats

(a) The Federal Government shall employ all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks. This approach shall include increasing the Federal Government's visibility into and detection of cybersecurity vulnerabilities and threats to agency networks in order to bolster the Federal Government's cybersecurity efforts.

➔ **ThreatStream** leverages STIX 2.1 utilizing Anomali's threat model first approach. This gives us the ability to not only ingest IOCs such as IPs, Email, Hash, Domain, URL - but also threat model entities such as Actor, Campaign, TTP, **Vulnerabilities**, Course of action, and more. When intelligence feeds include vulnerability data and CVE information mapping back to the intelligence, we automatically make those associations for that data inside of ThreatStream.

**Anomali Match** leverages asset criticality and historical vulnerability data from your vuln management system to determine historical vulnerabilities on that host at the time we've detected activity to now known malicious indicators.  It is used in risk calculation and can help identify if the device was susceptible to the attack 'when' that activity occurred.

## Section B – Deploy Supporting Technologies

(b)  FCEB Agencies shall deploy an Endpoint Detection and Response (EDR) initiative to support proactive detection of cybersecurity incidents within Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response.

➔ Anomali is a  leader and innovator in the XDR market. We view XDR as an architecture and in terms of how enterprises can leverage it to maximize the performance of their overall security investment (people, technologies, services) to take action against threats at the fastest possible speed. As leaders in the threat intelligence market and with deference to the essential role that global threat intelligence plays in accelerating detection and response, we offer up the following working definition:

Organizations that run on top of XDR architectures are able to move closer to managing their security infrastructure as an integrated, unified platform. With XDR, Security Operations Centers (SOCs) can break silos to converge all security data and telemetry collected and generated by security technologies they've deployed (tech that includes firewalls, EDR, CASB, SIEM, SOAR, TIP etc.). With this information, they can generate strategic threat intelligence that empowers immediate threat detection, streamlined investigations, and high-performance, automated-response capabilities that isolate and mitigate threats before they escalate into costly and disruptive incidents.

# Sec. 8. Improving the Federal Government's Investigative and Remediation Capabilities

## Section A – Using Network and System Log Data

(a) Information from network and system logs on Federal Information Systems (for both on-premises systems and connections hosted by third parties, such as CSPs) is invaluable for both investigation and remediation purposes. It is essential that agencies and their IT service providers collect and maintain such data and, when necessary to address a cyber incident on FCEB Information Systems, provide them upon request to the Secretary of Homeland Security through the Director of CISA and to the FBI, consistent with applicable law.

➔ Anomali Match compliments your SIEM/Data Lake for automated threat hunting and greater visibility across historical data, active threat intelligence, and quickly identifies existing threats as new threat intelligence is available.

SIEMs have 2 limitations that Match helps overcome:

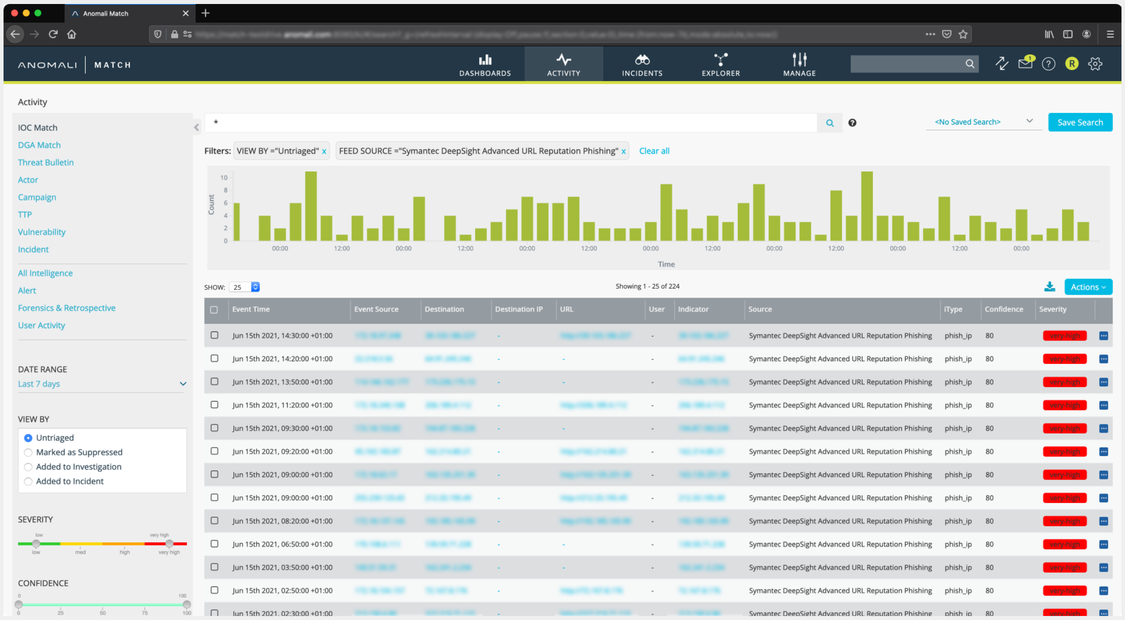
1. SIEMs have limited types of data, and limited historical data for online searching, pivoting, and threat hunting capabilities. Most customers have limited data online, and pick and choose which types of logs to send to the SIEM for security correlation. This is limited both by the resources of the

SIEM as well as the cost of sending more data, indexing, and storing historical data online.

Match can collect logs from SIEM, data lakes, syslog, CEF, network flow data, taps… giving you visibility for up to 5+ years of your network and host based log activity. We use machine learning and automation to automatically identify existing threats as new intelligence is ingested into the platform. This quickly detects active threats and bubbles up to your existing workflow process. You can search, pivot, and run reports against this data without impacting the resources in your SIEM environment. This not only increases your visibility, but optimizes workflow and creates efficiencies in the IR process.

2. SIEMs have a finite number of indicators they can correlate against the logs you have online. It varies based upon your configuration and product - and we typically see anywhere from 2-8 million IOCs that a SIEM can actively correlate against. The problem with this approach is:
    a. We have hundreds of millions of ACTIVE indicators in our platform today and it continues to grow exponentially. Customers are not seeing the ROI on the intelligence feeds they have available due to the limitations of current security products to leverage the volume of threat intelligence available. Match can operationalize ALL active threat intelligence so you can quickly determine what is relevant to you - and take appropriate actions. Essentially eliminating the gaps of visibility you have today in your SIEM environment.
    b. Filtering on high severity/high confidence indicators and limiting to 2-8 million IOCs not only limits visibility into potential active threats and dwell time - but it also creates more false positives for the SOC/IR team. If a high confidence, high severity indicator is ingested into the platform today - it will flow down to your SIEM for active correlation. However, if the ‘active’ time frame for that indicator was 10-14 months ago (in the case of Sunburst backdoor) all you would be doing is creating alerts to matches on those indicators ‘today’ not during the active time frame. This causes potential alert fatigue and wastes hours of analyst investigation time taking them away from detecting & remediating real threats.

Anomali Match first threat detection and response solution that automatically and continuously correlates ALL your logs against ALL active threat intelligence to expose previously unknown threats that have already penetrated your enterprise, resulting in faster Mean-Time-To-Detection (MTTD), reduced cost of security incidents, and more efficient security operations.



Filters: VIEW BY ="Untriaged" x FEED SOURCE ="Symantec DeepSight Advanced URL Reputation Phishing" x Clear all

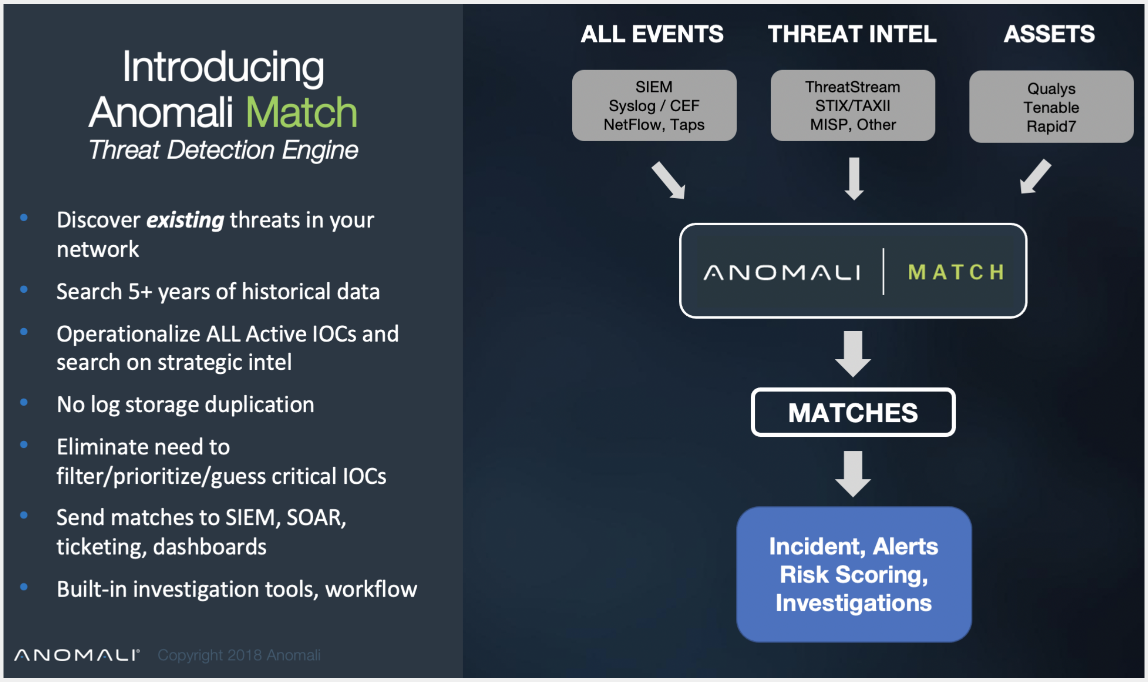
Showing 1 - 25 of 224

| ☐ | Event Time | Event Source | Destination | Destination IP | URL | User | Indicator | Source | iType | Confidence | Severity |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | Jun 15th 2021, 14:30:00 +01:00 | [redacted] | [redacted] | - | [redacted] | - | [redacted] | Symantec DeepSight Advanced URL Reputation Phishing | phish_ip | 80 | very-high |
| ☐ | Jun 15th 2021, 14:20:00 +01:00 | [redacted] | [redacted] | - | - | - | [redacted] | Symantec DeepSight Advanced URL Reputation Phishing | phish_ip | 80 | very-high |
| ☐ | Jun 15th 2021, 13:50:00 +01:00 | [redacted] | [redacted] | - | - | - | [redacted] | Symantec DeepSight Advanced URL Reputation Phishing | phish_ip | 80 | very-high |
| ☐ | Jun 15th 2021, 11:20:00 +01:00 | [redacted] | [redacted] | - | [redacted] | - | [redacted] | Symantec DeepSight Advanced URL Reputation Phishing | phish_ip | 80 | very-high |
| ☐ | Jun 15th 2021, 09:30:00 +01:00 | [redacted] | [redacted] | - | - | - | [redacted] | Symantec DeepSight Advanced URL Reputation Phishing | phish_ip | 80 | very-high |
| ☐ | Jun 15th 2021, 09:20:00 +01:00 | [redacted] | [redacted] | - | [redacted] | - | [redacted] | Symantec DeepSight Advanced URL Reputation Phishing | phish_ip | 80 | very-high |
| ☐ | Jun 15th 2021, 09:00:00 +01:00 | [redacted] | [redacted] | - | [redacted] | - | [redacted] | Symantec DeepSight Advanced URL Reputation Phishing | phish_ip | 80 | very-high |
| ☐ | Jun 15th 2021, 09:00:00 +01:00 | [redacted] | [redacted] | - | [redacted] | - | [redacted] | Symantec DeepSight Advanced URL Reputation Phishing | phish_ip | 80 | very-high |
| ☐ | Jun 15th 2021, 08:20:00 +01:00 | [redacted] | [redacted] | - | [redacted] | - | [redacted] | Symantec DeepSight Advanced URL Reputation Phishing | phish_ip | 80 | very-high |
| ☐ | Jun 15th 2021, 06:50:00 +01:00 | [redacted] | [redacted] | - | - | - | [redacted] | Symantec DeepSight Advanced URL Reputation Phishing | phish_ip | 80 | very-high |
| ☐ | Jun 15th 2021, 03:50:00 +01:00 | [redacted] | [redacted] | - | - | - | [redacted] | Symantec DeepSight Advanced URL Reputation Phishing | phish_ip | 80 | very-high |
| ☐ | Jun 15th 2021, 02:50:00 +01:00 | [redacted] | [redacted] | - | [redacted] | - | [redacted] | Symantec DeepSight Advanced URL Reputation Phishing | phish_ip | 80 | very-high |
| ☐ | Jun 15th 2021, 02:30:00 +01:00 | [redacted] | [redacted] | - | [redacted] | - | [redacted] | Symantec DeepSight Advanced URL Reputation Phishing | phish_ip | 80 | very-high |

## Section B – Recommendations and Requirements

(b) Within 14 days of the date of this order, the Secretary of Homeland Security, in consultation with the Attorney General and the Administrator of the Office of Electronic Government within OMB, shall provide to the Director of OMB recommendations on requirements for logging events and retaining other relevant data within an agency's systems and networks. Such recommendations shall include the types of logs to be maintained, the time periods to retain the logs and other relevant data, the time periods for agencies to enable recommended logging and security requirements, and how to protect logs. Logs shall be protected by cryptographic methods to ensure integrity once collected and periodically verified against the hashes throughout their retention. Data shall be retained in a manner consistent with all applicable privacy laws and regulations. Such recommendations shall also be considered by the FAR Council when promulgating rules pursuant to section 2 of this order.

➔ After defining which logs to collect in the SIEM, and how long to store that information — Match can help compliment the SIEM to collect/store anything else you are not sending to the SIEM. This increases visibility into logs you would not have otherwise had access to for threat hunting, searching, and reporting.  The logs are stored and maintained securely — and retains a pointer back to the raw log.



Introducing
Anomali Match
*Threat Detection Engine*

- Discover ***existing*** threats in your network
- Search 5+ years of historical data
- Operationalize ALL Active IOCs and search on strategic intel
- No log storage duplication
- Eliminate need to filter/prioritize/guess critical IOCs
- Send matches to SIEM, SOAR, ticketing, dashboards
- Built-in investigation tools, workflow

ALL EVENTS

SIEM
Syslog / CEF
NetFlow, Taps

THREAT INTEL

ThreatStream
STIX/TAXII
MISP, Other

ASSETS

Qualys
Tenable
Rapid7

ANOMALI | MATCH

MATCHES

Incident, Alerts
Risk Scoring,
Investigations

ANOMALI Copyright 2018 Anomali

## Section C – Establish Requirements and Policies

(c)  Within 90 days of receiving the recommendations described in subsection (b) of this section, the Director of OMB, in consultation with the Secretary of Commerce and the Secretary of Homeland Security, shall formulate policies for agencies to establish requirements for logging, log retention, and log management, which shall ensure centralized access and visibility for the highest level security operations center of each agency.

- ➔ Anomali Match can help determine the types of logs to be maintained and time periods to retain the logs in the SIEM - versus a larger superset of logs and metadata stored in Match. This typically helps save money on ingestion rates and long term storage in the SIEM/Data Lake - and also provides greater visibility, searching, reporting against historical logs - and allows you to operationalize ALL active intelligence.