opentext™ | Cybersecurity

Product Flyer

ArcSight cyDNA for Government Agencies

National threat awareness and adversary signal analytics for cross-agency visibility.

Why ArcSight cyDNA?

National Threat Awareness

- Identify Threat Actors
- Protect Critical Infrastructure
- Zero-Touch Global Coverage

Cross-Agency Models

- Cross-Agency Visibility
- Adversary Pattern Recognition

Simplified Security

- External Perspective
- Amplify Existing Infrastructure
- Threat Prioritization

What are the biggest cybersecurity risks to government organizations today? The answer is an ever-growing list which includes:

- Nation-State Actors
- Cybercriminal Organizations
- Hacktivists
- Insider Threats
- Cyber mercenaries

Government agencies are prime targets for cyber-attacks due to their strategic importance and the potential for political or monetary gains. Malicious actors target government institutions to gather intelligence, disrupt operations, or compromise sensitive data for espionage, financial gain, or sabotage purposes. The ramifications of threat actors compromising your defenses and obtaining what they're after would be staggering.

A breach of government systems can have far-reaching consequences, potentially undermining the stability of a nation. A successful cyber-attack on these sectors can lead to significant disruptions, economic losses, and can even threaten public safety. Unfortunately, government sectors face unique challenges when defending against attacks:

1. **Scale and Complexity:** Government cybersecurity faces the challenge of protecting vast and complex networks spread across multiple agencies, departments, and critical infrastructure sectors. Coordinating and securing diverse systems, devices, and applications while ensuring interoperability and compliance with regulations is a complex undertaking.
2. **Siloed Detection and Response:** Many government entities operate with independent security systems and information silos, making it challenging to detect and respond to threats across organizational boundaries. The lack of centralized visibility and coordination leads to delayed incident response, inefficient resource allocation, and missed opportunities for early detection and mitigation.
3. **Limited Attribution Capabilities:** Determining the identity, motives, and origins of attackers can be complex and time-consuming. Sophisticated adversaries employ proxy servers, compromised systems, or false flags to obfuscate their true identities and locations. An inability to attribute attacks to attackers can hinder response efforts, making it difficult to coordinate appropriate countermeasures, pursue legal action, or engage in diplomacy.
4. **Fragmented Attack Visibility:** Without a comprehensive understanding of attack patterns and methodologies utilized by threat actors, governments may struggle to develop targeted countermeasures.
5. **Insufficient Utilization of Threat Intelligence:** It is difficult to correlate unwieldy threat intelligence feeds against the vast volumes of network traffic generated by government agencies. The sheer scale can overwhelm existing systems, leading to delays, incomplete analysis, or missed indicators of potential threats.

What if there was a way for government agencies to address these challenges, view attacks on their organization as a whole, and see who's behind them? With ArcSight cyDNA by OpenText, you can do just that. ArcSight cyDNA is a SaaS-based adversary signal analytics technology that provides a global view of divisions being targeted and

how attacks are being carried out. It unmasks adversarial behavior, discovers early signs of attack, and outlines sophisticated attack paths being used. Once your covered space is established, you'll receive timely and relevant intelligence, all without costly physical infrastructure or the collection of event logs.

National Threat Awareness

ArcSight cyDNA extends your visibility to "FarSpace", beyond the borders of your firewalls, to reveal malicious traffic to and from your networks. When you've identified and submitted the IP ranges, CIDR blocks and ASNs you want included under your covered space, you'll be able to discover, define, and contextualize adversarial internet signaling directed your organization. ArcSight cyDNA's single-platform visibility provides awareness and valuable insights across complex—and often siloed—operating environments.

Knowing who is behind attacks is an important factor in understanding why they're attacking. With cyDNA's threat actor attribution, you can see beyond digital disguises and reveal the true origins of attacks. ArcSight cyDNA provides vital intelligence that helps governments understand motives, capabilities, and tactics of their adversaries. Identifying threat actors allows governments to tailor their response strategies, allocate resources effectively, and develop countermeasures against future attacks. A signals-based analysis provides enhanced details for context, attack techniques, and actor motivations to build accurate adversary profiles.

Benefits for National Threat Awareness:

- **Identify Threat Actors**—Discern the origin of malicious activity based on context, motives, and techniques employed.
- **Protect Critical Infrastructure**—View adversarial traffic activity directed at disrupting water, electricity, gas, and other critical public infrastructure.

Figure 1. ArcSight cyDNA showing organization's (red) outbound data sent to adversarial (grey) destinations

- **Zero-Touch Global Coverage**—Identify areas of your global organization under cyberattack without setting up additional infrastructure or collecting event logs.

ArcSight cyDNA's enhanced visibility of your global operating environment provides key benefits for security operations. The ability to expose and block imminent threats before they gain a foothold is extremely important, especially for government agencies. Early detection and prevention can significantly mitigate the potential damage inflicted by cyber threats. By identifying and neutralizing threats in their early stages, government organizations can prevent unauthorized access to sensitive data, protect critical infrastructure, and safeguard national security. Ultimately, exposing imminent cyber-attacks before they gain traction allows government agencies to maintain a proactive cybersecurity posture, safeguarding both public and private interests from devastating consequences.

Cross-Agency Models

Security analytics across multiple agencies can play a crucial role in validating findings and enhancing the accuracy of threat assessments. ArcSight cyDNA combines and cross-references internet signals, patterns, and indicators of compromise, allowing agencies to identify commonalities and corroborate findings, strengthening the validity of their assessments. This multidimensional approach helps identify blind spots, uncover hidden connections, and reduce false positives for the organization overall.

Benefits for Agencies:

- **Cross-Agency Visibility**—Single-platform visibility for multiple security environments to help determine if threats are crossing domains, sectors, and nations.
- **Adversary Pattern Recognition**—Verify threats across single, cross, and conjoined sectors to distinguish between general or targeted attacks.

With the ability to see adversarial traffic to, from and between multiple agencies, cyDNA can identify anomalous activities, suspicious connections, and coordinated attacks that traverse traditional security boundaries. It leverages sophisticated threat intelligence feeds and anomaly detection techniques to identify attack patterns spanning government agencies and sectors. This allows for early

> **"I have spent a day in briefings to be told what [ArcSight cyDNA] has shown me in 5 minutes."**
>
> EU official

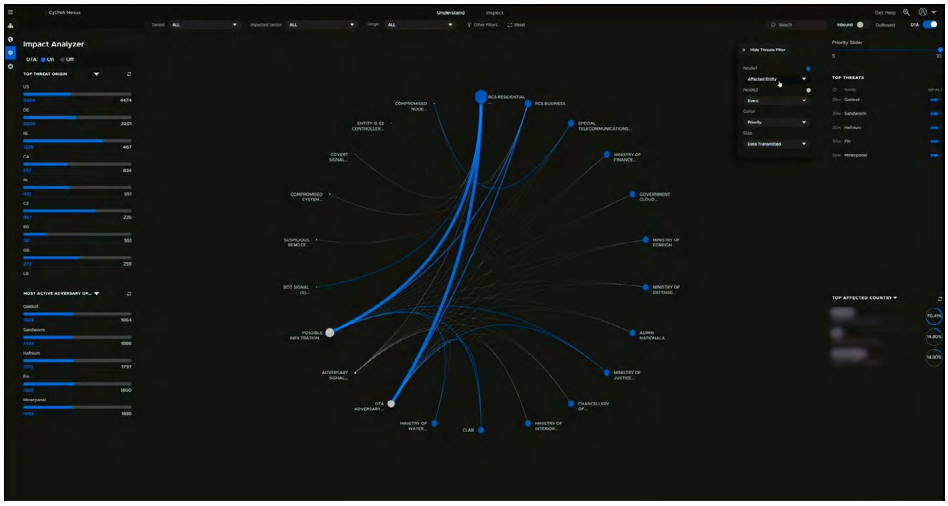

Figure 2. ArcSight cyDNA showing the affected agencies within a government organization

detection, prompt response, and coordinated mitigation efforts, empowering security organizations to collaborate effectively, share critical information, and defend against threats that transcend organizational silos. By validating the collective insights of multiple agencies, governments can make more informed decisions, allocate resources effectively, and develop robust strategies to counter emerging threats.

Simplified Security

ArcSight cyDNA's "outside-in" approach to security offers several advantages to organizations with a large global footprint. It assesses the organization's security posture from an external perspective, discovering entry points, and eliminating blind spots in traditional SOC tools. As an added benefit, it is deployed without the need for additional hardware and requires minimal effort for integration. It is delivered as a plug-and-play SaaS service, with tailored insights based on each environment's unique set of incoming and outgoing internet signals.

ArcSight cyDNA easily co-exists with existing security investments, and can even increase the ROI in many situations. Combined with the insights from cyDNA, organizations can supercharge their SIEM effectiveness, alerting security teams to security situations before traditional rules and thresholds would have been triggered. Overall, it delivers better defense against threats, reduced response times, and an enhanced security posture.

Simply put, being able to see the threats that are active in your environment allows you to allocate resources, implement controls, and prioritize efforts on the most significant risks. It allows you to take a proactive and targeted approach to mitigating risks, reducing the likelihood of successful attacks, and protecting your critical assets from evolving threats.

Benefits for Security Operations Center:

- **External Perspective**—Bird's-eye view of adversarial activity directed at the organization.
- **Amplify Existing Infrastructure**—Augment existing security infrastructure and increases the ROI of SIEM, XDR, MDR, and more.
- **Threat Prioritization**—Identify threats posing the most significant risk to the organization.

Learn more at
www.arcsight.com

761-000110-002 | O | 10/23 | © 2023 Open Text