GameChanger

Transformation Through Technology

GENERAL DYNAMICS
C4 Systems

Cybersecurity: Knowing Who & What is on Your Network

Today, cybersecurity goes beyond passwords and firewalls. Modern cyber attacks are advanced viruses and malware with the ability to penetrate a network's outer layer of defense. General Dynamics C4 Systems takes a layered security technology approach to create defense in depth to manage and mitigate their clients' risk, protecting customer's networks from every possible angle.

And that protection is particularly important when those networks are responsible for protecting some of the most sensitive information in the world, and are prime targets for attackers. It's the history, expertise, and reliability of General Dynamics that has made the company a premier government systems developer and integrator of security management infrastructures for more than forty years.

General Dynamics C4 Systems, a division of General Dynamics Corp. based in Scottsdale, Ariz., comes from a background of developing trusted products and solutions that deliver at the highest assurance level.

"Building trusted systems with multiple components isn't a cookie-cutter skill set, it's more of an art form," says Bill Ross, Vice President of Federal Systems and Cyber Solutions, with General Dynamics C4 Systems. "When you look at the whole information assurance and cybersecurity landscape, there isn't one widget that's going to effectively solve the problem. As a solution provider, you've got to take a very broad view of the technology and standards available in the space and be seen as a trusted integrator that can deliver secure solutions."

A starting point for many government agencies today is to achieve a level of situational awareness, so they can effectively measure their security posture and reinforce it from that point. General Dynamics helps agencies develop an understanding of their current security stance – a baseline –so that they can recognize when elements on their networks have changed or when that baseline is no longer being met. But situational awareness is just a starting point; layered on top of that baseline are tools that can automate security tasks and actions to save on valuable resources and respond to security events in real time.

Developing cybersecurity solutions for government customers requires technology building blocks tailored to an organization's mission and objectives that can support information assurance for data in transit and data at rest, as well as measure and report identity and assess non-person entities. The areas that General Dynamics offers security solutions include:

- Identity Management
- Credential Management
- Attribute Management
- Policy Management
- Information Assurance Metadata Management
- Configuration Management
- Audit Management
- Key Management
- Privilege Management
- Cyber Net Ops

General Dynamics realizes that no customer wants to take a rip-and-replace approach to their cybersecurity infrastructure, and so the company works with an organization's existing technology architecture to strengthen its security posture and resiliency. Often, once effectiveness is measured, security solutions can be applied in an incremental fashion to boost reliability. General Dynamics also understands the importance of leveraging products that implement open, standards-based protocols and specifications, to ensure solution interoperability and longevity.

To help government agencies deliver on mission goals, General Dynamics believes it's important to first determine if three basic questions can be answered: Who is on your network? What non-person entities are on your network? And what are they doing on your network?

"Those three simple questions are harder to answer than one would initially think," says Ross. "But if they can't be answered with confidence then there's no basis for mission assurance. When people can't affirmatively answer those questions, they realize there's more work to be done."