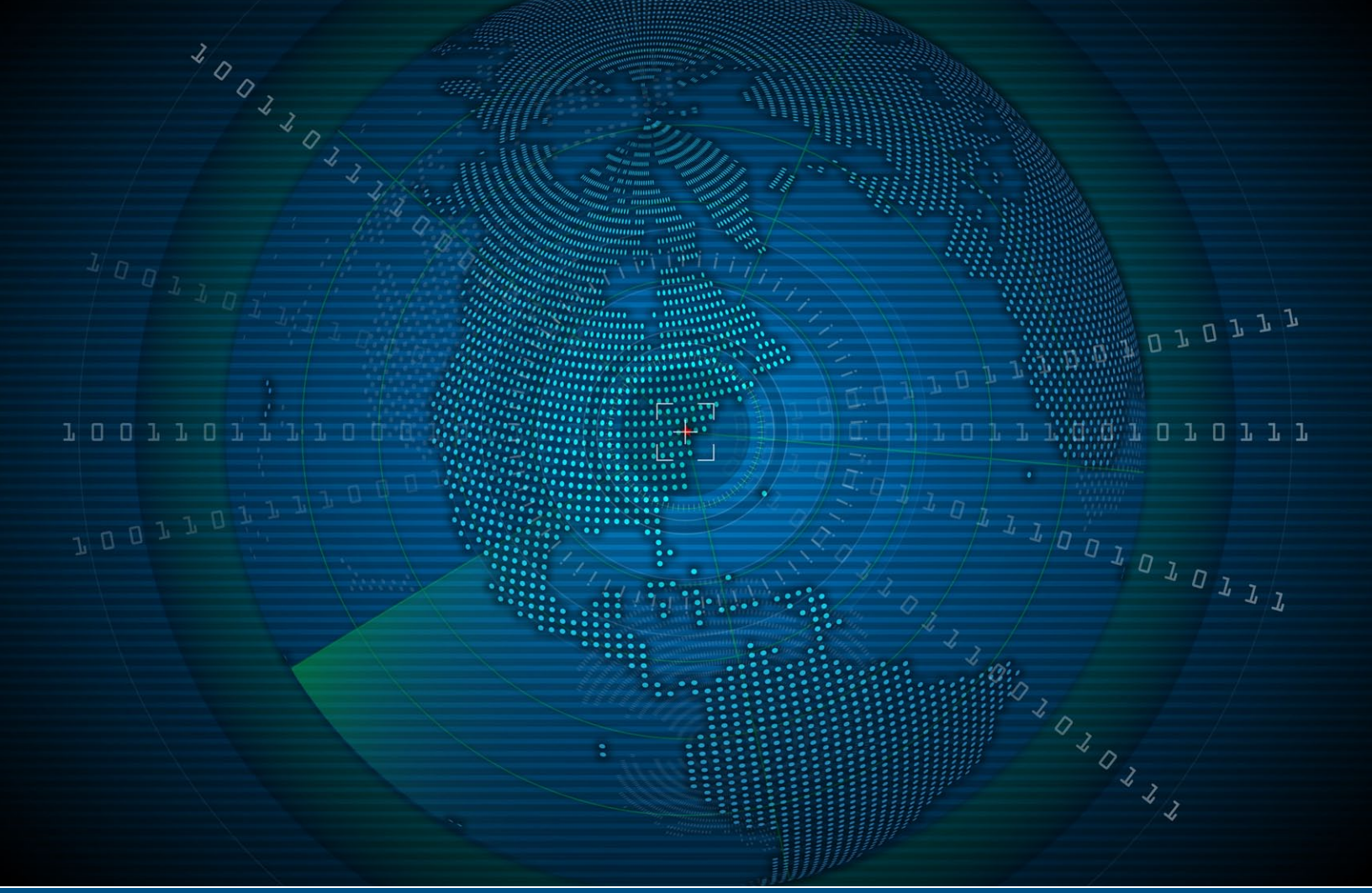


US-CERT Year in Review

United States Computer Emergency Readiness Team

CY 2012

Homeland Security

US-CERT Year in Review

United States Computer Emergency Readiness Team

CY 2012

What's Inside

Welcome

The United States Computer Emergency Response Team (US-CERT) is a 24x7 operational entity focused on collecting and analyzing data and disseminating the information to federal agencies, state and local partners, domestic and international organizations. The US-CERT mission, vision, and goals are as follows:

US-CERT Mission:

Improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans.

US-CERT Vision:

Be a trusted global leader in cybersecurity - collaborative, agile, and responsive in a complex environment.

US-CERT Goals:

In the upcoming year US-CERT will:

- Improve onsite and remote assistance capabilities to provide rapid and comprehensive operational support to our public and private partners;
- Partner with physical first responders to integrate physical and cyber information sharing and response processes; and
- Increase outreach to public, private, and international partners.

US-CERT 2012 Accomplishments

- Transitioned to a key role as a fully integrated element of the National Cybersecurity and Communications Integration Center (NCCIC) providing critical information and analysis feeds needed to perform their mission;
- Provided key support to public and private sector partners to respond to and mitigate current cyber intrusions and cyber risks;
- Developed the Advanced Malware Analysis Center (AMAC) to analyze malware threat data;
- Improved our International outreach and coordination to share cyber intrusion, detection, analysis, and mitigation strategies with our international partners; and
- Improved and expanded our outreach to our domestic public and private sector partners to share indicators and coordinate responses to domestic cyber events.

US-CERT Provides Assistance to a Partner

To enhance the Nation's cybersecurity posture, US-CERT actively partners with public and private sector entities. These partners include, but are not limited to, private sector critical infrastructure owners and operators, academia, federal agencies, Information Sharing and Analysis Centers (ISAC), state and local partners, and domestic and international organizations.

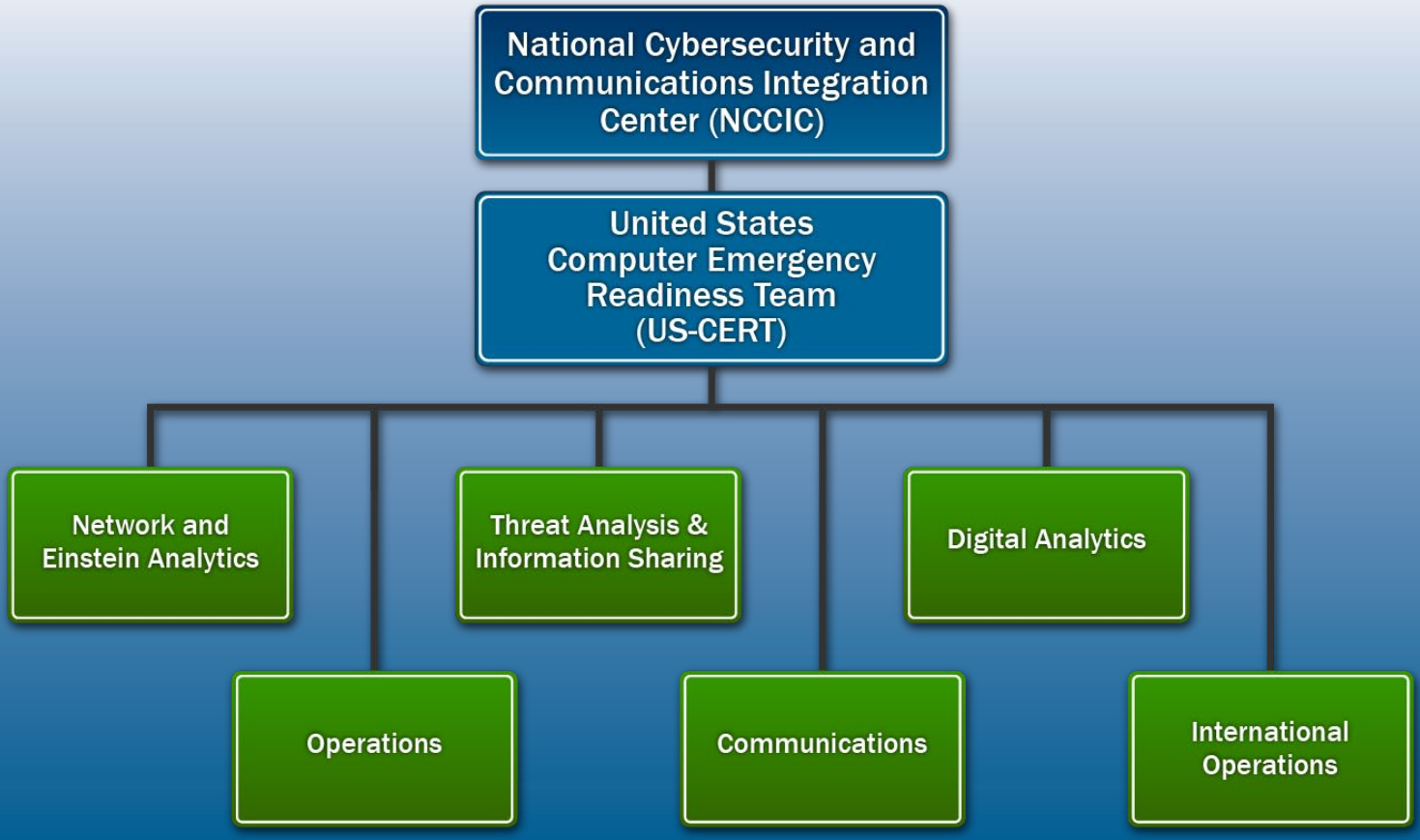
Case Study

In 2012, a partner asked US-CERT to provide technical assistance related to an intrusion event. US-CERT provided an on-site team to review the technical data in order to develop mitigation strategies and recommendations to prevent future events of similar nature.

During the course of the review, US-CERT determined that the partner did not realize the full extent of the intrusion. Due to the partner's reliance on standard intrusion detection and analysis procedures focused on single machines and servers, they were unaware that a nation state was conducting a series of large scale intrusions. Originally, they believed they were experiencing concurrent large scale intrusions from multiple single actors.

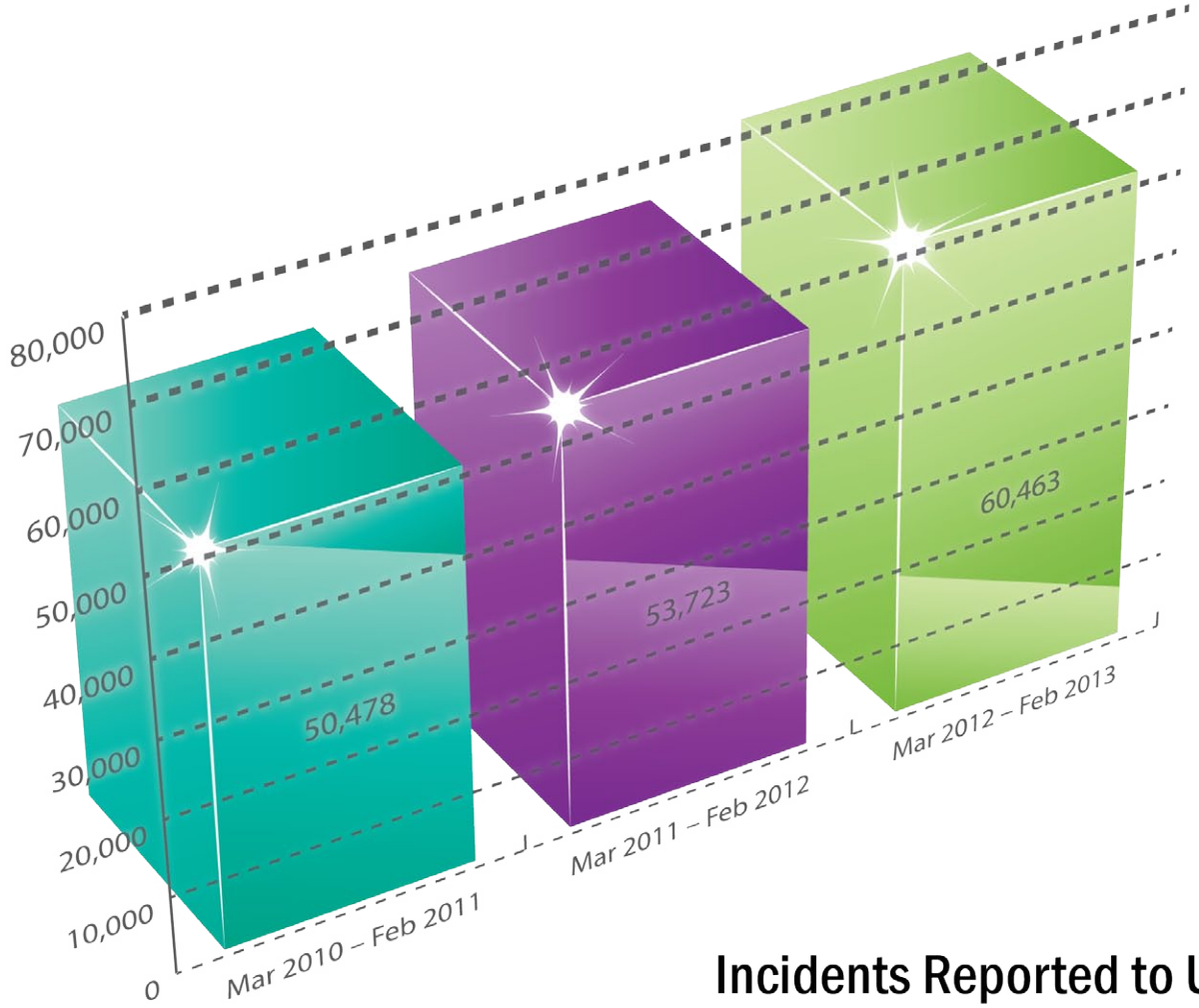
US-CERT identified the full scope of the intrusion activity and provided a detailed, in-depth analysis document that focused on mitigation strategies with four specific controls the partner could use to deal more effectively with the intrusion. The partner accepted US-CERT's recommendations and implemented the strategies to reduce their risk and exposure to the cyber vulnerabilities in question.

Using these controls, the partner was able to reduce the time between initial intrusion detection and initial response from 30 days to 45 minutes. Additionally, the partner made significant progress determining the difference between single and multiple intrusion events and those that were conducted by non-state and state actors.



US-CERT Organization

US-CERT is the National Cybersecurity and Communications Integration Center's (NCCIC) 24 hour operational cyber arm. US-CERT provides NCCIC with critical information and analysis feeds needed to perform their mission. Along with the National Coordinating Center (NCC) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), US-CERT is a key component for the NCCIC.



Incidents Reported to US-CERT

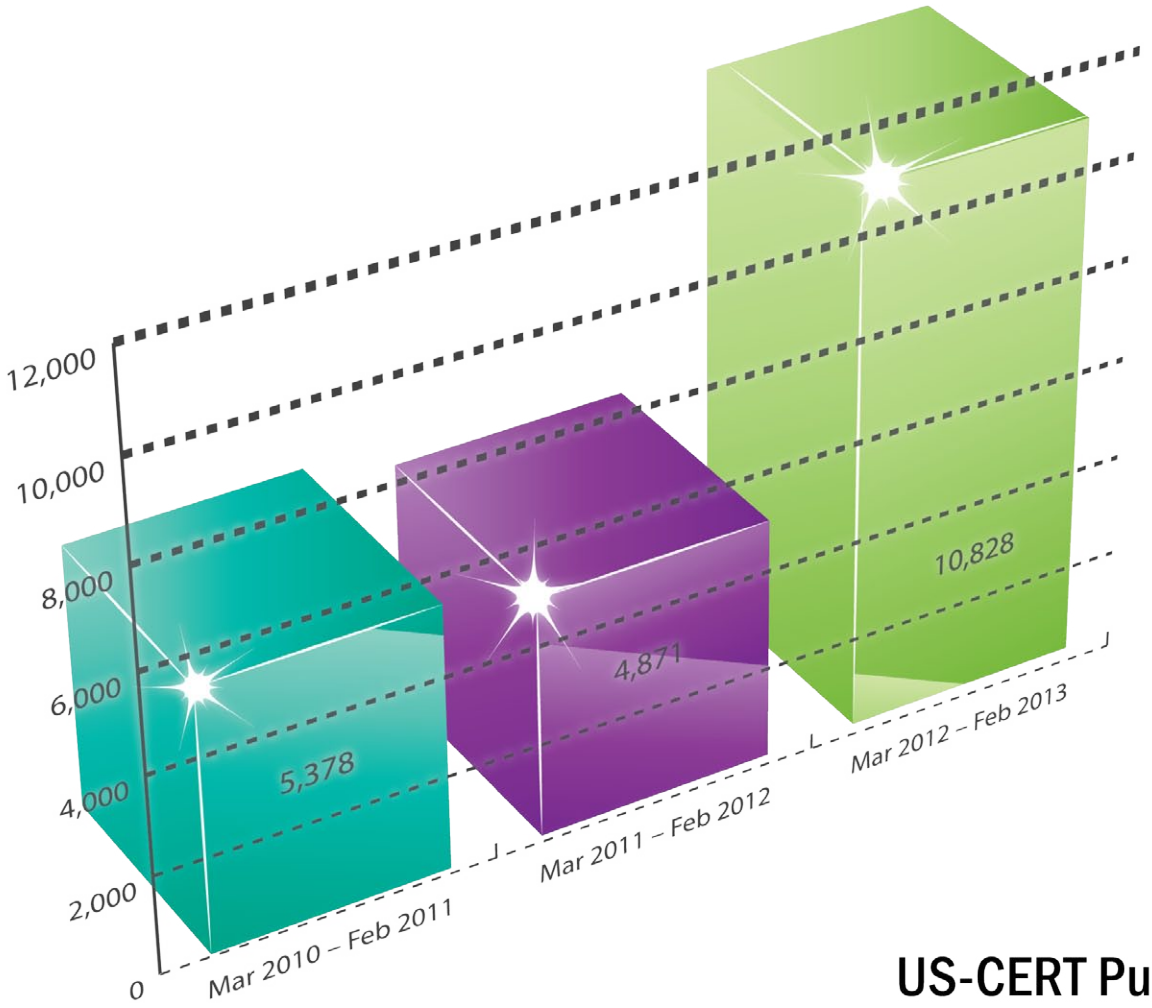
Critical Mission Activities, Key Initiatives, and Programs

US-CERT's critical mission activities include applying our analytic expertise to identify, correlate and, where possible, predict the behaviors and tactics of our adversaries. US-CERT also develops machine readable indicators and actionable mitigation approaches to promote collaborative response activities within our stakeholder communities. US-CERT's capabilities inform and enable US-CERT to provide critical on-site deployments when our partners request them in order to assist those partners with incident response activities.

US-CERT provides a unique vantage point at the intersection of civilian Federal government, law enforcement, the intelligence community, International partners, State and Local government and the private sector to detect, prevent and develop mitigation strategies against national-level cyber threats. Additionally, US-CERT has received increasing numbers of cyber incident reports during the past three years.

In response to many of these incidents, US-CERT's key initiatives over the past year have included the development and implementation of the Advanced Malware Analysis Center (AMAC).

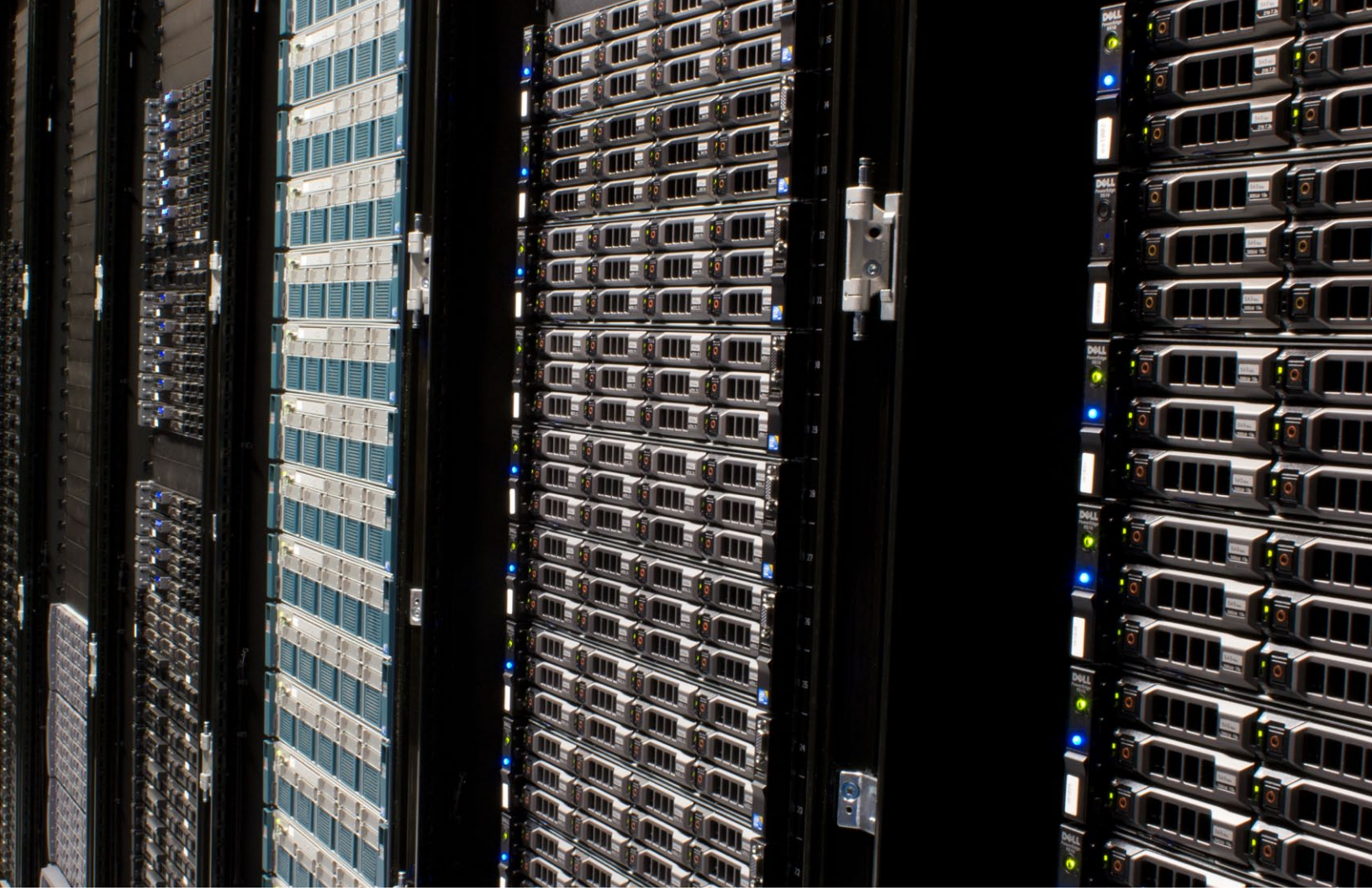
The AMAC enables US-CERT to analyze data related to malware threats targeted against the United States government's network space. The AMAC provides a segregated, closed, computer network system that is used to analyze computer network vulnerabilities and threats. US-CERT receives malicious code, submitted by AMAC, and analyzes the code or images to discover how to secure or defend computer systems against the threat. US-CERT publishes corrective action information in vulnerability and malware reports, as well as, alerts for use by partners.



US-CERT Publications

Other key initiatives include: US-CERT's International Outreach Program to share information with the National Cyber Response Centers of our foreign partners in a proactive and timely fashion; and, working groups such as the Joint Agency Cyber Knowledge Exchange (JACKE) and the Government Forum of Incident Response and Security Teams (GFIRST) to facilitate collaboration for detecting and mitigating threats to the .gov domain.

Through the use of such working groups, US-CERT encourages proactive and preventative security practices and conference presentations. US-CERT personnel regularly speak and present technical papers at FloCon, Blackhat, GFIRST, the MS-ISAC Annual Meeting, Federal Networks Conference, and the Symantec Government Symposium. US-CERT also shares detection, analysis, and mitigation information for our partners in key information sharing products such as Joint Indicator Bulletins (JIB), Early Warning and Indicators Notices (EWIN), Malware Initial Findings Reports (MIFR), and Malware Analysis Reports (MAR). US-CERT published increasing numbers of technical cyber reports during the past three years.



US-CERT is responsible for the National Cybersecurity Protection System's Einstein program, which provides an automated process for collecting, correlating, analyzing, and sharing computer security information across the Federal Government to improve the nation's cyber situational awareness.

EINSTEIN 1 uses an automated process to collect network flow information from voluntary participating federal executive agencies. Using this information, US-CERT can detect cyber threats and vulnerabilities and coordinate with the appropriate federal executive agencies to mitigate them. US-CERT shares this analysis, along with additional computer network security information, as appropriate, with both the public and private sectors, via the US-CERT web site at www.us-cert.gov.

EINSTEIN 2 augments, rather than replacing or reducing the current computer network security practices of participating federal executive agencies. It passively observes network traffic to and from participating federal executive agency networks and adds an intrusion detection system (IDS) capability that alerts when a pre-defined specific cyber threat is detected. US-CERT is then able to analyze cyber threat activity occurring across the federal Information Technology (IT) infrastructure. This results in improved computer network security situational awareness through the sharing of the information with individual federal executive agencies in an effort to reduce and prevent computer network vulnerabilities. EINSTEIN 2's network intrusion detection technology custom signatures, based upon known or suspected cyber threats, are derived from numerous sources such as: commercial or public computer security information; incidents reported to US-CERT; information from federal partners; or, independent analysis by US-CERT analysts.

US-CERT also manages the National Cyber Awareness System's (NCAS) National Vulnerability Database (NVD). The NVD is the U.S. Government's repository of standards-based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance.

US-CERT participates in the Protected Critical Infrastructure Information (PCII) program which enables private sector partners to voluntarily provide their privately held cyber data to create time sensitive indicator information about current anomalous and/or malicious cyber activity from across private partner networks. US-CERT provides anonymized data to mission partners that can be used to implement effective Computer Network Defense (CND) measures in response to the identified indicators.

US-CERT Contact Information

US-CERT assistance is readily available for all partners 24 hours a day.

US-CERT encourages all public and private sector partners to report suspicious cyber activity as soon as possible by using the US-CERT contact information below.

To contact US-CERT:

info@us-cert.gov
(888) 282-0870
www.us-cert.gov

To report a cyber incident to US-CERT online:
https://forms.us-cert.gov/report/

For PCII Data Submissions to US-CERT: www.dhs.gov/pcii

Homeland Security