n-dimension solutions

The Importance of Cybersecurity Monitoring for Utilities

www.n-dimension.com

Cybersecurity threats against energy companies, including utilities, have been increasing at an alarming rate. A comprehensive approach to ensuring cyber protection is essential and should include cybersecurity monitoring as a standard element. But not all cybersecurity solutions are created equal. Many offer 24 x 7 vigilance and alerts but alert data alone does not increase security posture. Alerts need to analyzed and distilled in a timely fashion. The data needs to be reviewed by knowledgeable security experts who can recommend appropriate actions to improve security posture. Without these additional elements, a cybersecurity monitoring program losses value and critical information can be missed exposing the utility to risk. If timely and appropriate actions are not taken, the utility can remain vulnerable to cyber threats. For utilities with limited IT/OT resources and security expertise, a cybersecurity monitoring solution that combines alerts, intelligent threat analysis, actionable data and reports and access to security experts to guide them in improving their security posture offers the best solution.

Cybersecurity Monitoring Defined

Cybersecurity monitoring has become a key element in the layered security architecture of most enterprise-class networks. It can be used to provide 24 x 7 monitoring of both internal and perimeter networks, detecting and alerting on a range of potential cyber threats. Most cybersecurity monitoring solutions also include reports about the threats detected but there is a wide variance on the level of analysis and distilling of the data reported which in translates to a wide range of real value provided to customers.

Why Cybersecurity Monitoring is Essential

There are some key reasons cybersecurity monitoring has evolved from a “nice-to-have” option to serve a more critical role. For utilities companies, the key reasons are:

- **Increase in Cyber Threats Against Utilities of All Sizes**
  There is news almost daily about energy companies, including utilities, being hacked or vulnerabilities discovered in various software and systems that create risk to the company, its customers and its partners.

  Below are news headlines, which represent just a few examples of recent media coverage:

"U.S. Utility's Control System hit by Advanced Cyber Attack – DHS"

"DHS Warns of Serious Cyber Threat to Critical U.S. Infrastructure"

"U.S. Orders Electric Utilities to Secure Sites From Attack"

"NSA Worries Hackers May Shut Down Utilities"

"Hacking Gets Physical: Utilities at Risk for Cyber Attacks"

Hacking industrial control systems has become one of the highest visibility threats – by the Department of Homeland Security, Department of Energy and other agencies, as it represents a critical target that could affect thousands or millions of people and businesses with devastating affects from just the click of a mouse. Without knowing and understanding what is happening in your utility network, it would be virtually impossible to prevent such cyber attacks.

- **NERC CIP/FERC Cybersecurity Requirements**
  Critical infrastructure energy companies that are moving towards compliance with NERC CIP standards or need to meet them, have requirements. Under the current CIP-007-3a R6 (NERC CIP version 3) and in the future with NERC CIP version 5, the standard specifies that cyber incidents such as malicious communications and/or malware, need to be monitored.

  Noteworthy is that NERC identified that CIP-007 is the most frequently violated standard as shown in the figure below.

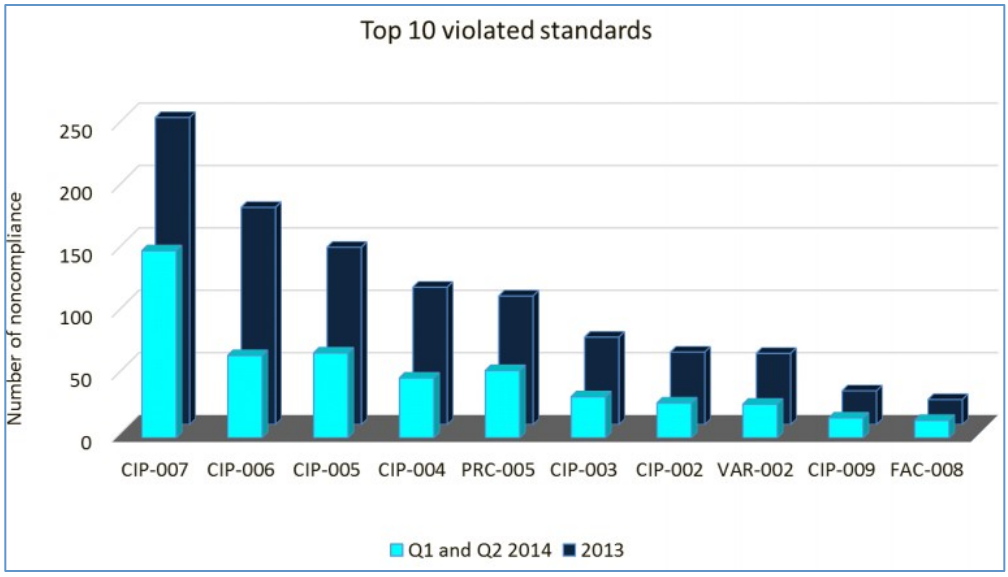


Figure 1: Source – NERC "Top 10 violated NERC CIP standards, 2013, Q1 and Q2 2014"

- **Complex Nature of Cybersecurity Incidents and Lack of Cyber Threat Knowledge**
  Cybersecurity within utilities is relatively new when compared to other industries such as banking and retail. Advanced methods of cyber attacks can bypass firewalls at the network perimeter and compromise systems in disguise without leaving noticeable traces. These cyber intrusion attempts need to be detected, identified and addressed quickly before they result in a security incident. In addition, the lack of cybersecurity knowledge and skills combined with overwhelming workload pressures already on IT/OT personnel, make it difficult for them to address cyber intrusion attempts quickly and appropriately. Moreover, the addition of technologies such as server virtualization, mobile devices (smart phones, tables, laptop computers, etc.), smart grid applications (smart meters, distribution automation, etc.) and cloud services, add to the complexity of cybersecurity protection. Without understanding the details of cyber intrusion attempts via different means, a cybersecurity monitoring program could be rendered ineffective.

- **False Sense of Security**
  Many companies have a false sense of security when they have an Internet-facing firewall in place. Even a high-end firewall or Unified Threat Management system that is monitoring entry to a network perimeter many not provide adequate protection for critical infrastructures. Oftentimes, these security devices can be bypassed…easily. Normally security systems that protect the perimeter do not provide protection of the interior network, and therefore, do not detect intrusion attempts to/from systems within the network. Also, many believe that Mac and Linux-based operating systems are secure and as a result, do not deploy protection mechanisms for these systems thereby making them vulnerable to cyber attacks. These are some of the reasons why NERC CIP and other cybersecurity best practices recommend defense-in-depth cybersecurity monitoring and protection.

- **Essential Element Identified by NIST**
  The "Framework for Improving Critical Infrastructure Cybersecurity" published by NIST was in response to President Obama's Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity". The EO calls for creation of a framework that provides a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to manage cybersecurity risks for the processes, information, and systems involved in the delivery of critical infrastructure services.

  One of the five core functions identified in the NIST Framework is "Detect". Detect specifies the timely discovery of anomalous cybersecurity activity and events on an ongoing basis. It also includes the ability to assess cybersecurity events and to verify the effectiveness of protective measures in place, identifying potential areas of risk.

  The NIST Framework is consistent with the NIST SP800-61 "Security Incident Handling Guide," which specifies that one of first steps is to detect and analyze cybersecurity events. Without knowing threats exist and understanding them, a utility's cybersecurity incident handling program cannot provide adequate protection.

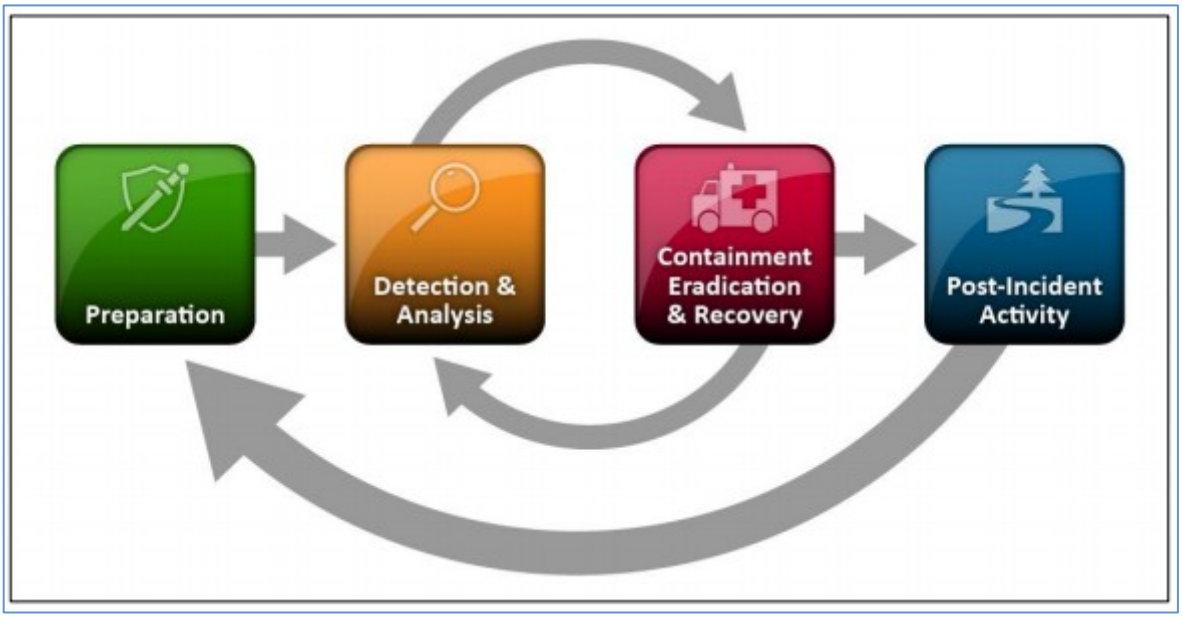


Figure 2: Source - NIST Sp800-61r2, Security Incident Handling Guide

N-Sentinel Cybersecurity Monitoring for Utilities

N-Sentinel is a comprehensive, cybersecurity monitoring program specifically designed to meet the needs of utilities. It includes a sensor placed nonintrusive to network traffic, within the utility's network. It delivers 24 x 7 monitoring of an internal and/or perimeter network for intrusion attempts.

With cloud-based cyber threat intelligence, N-Sentinel quickly identifies and analyzes threats. A team of utility industry, cybersecurity experts oversee and augment the threat data analysis and reporting process and bring add their utility industry knowledge. Customers receive an in-depth report, in plain English, that provides a clear description of threats and the level of risk each represents. With these insights, IT/OT are armed with the knowledge and can take appropriate and immediate action when necessary.

Customers that need some additional guidance can contact a cybersecurity expert who can review their security report and recommend next steps in how to remediate and/or improve their security posture. Cybersecurity experts are available for consultation via phone and/or email for this personalized help. This level of service and accessibility to cyber experts is an unmatched value in the utility industry.

After spending more than a decade delivering cybersecurity for energy companies, N-Dimension developed the N-Sentinel Cyber Security Monitoring Program based on real-life customer experiences and feedback plus requests from Municipal Utilities, Joint Action Agencies and Rural Electric Cooperatives. In some cases, these entities already had cybersecurity monitoring in place but lacked insights into the alerts thereby rendering them unable to take appropriate action. They requested help from our in-house cybersecurity experts to help them find and correct issues on their networks to reduce cyber risk. They even asked for our assistance in interpreting other vendors' cybersecurity monitoring reports, as they were hard to interpret unless you were a security expert and they lacked guidance in how to fix problems. Most of the other vendors' reports were merely event logs and much of what was "reported" was general noise and not real issues the utilities needed to be concerned about.

With the introduction of an N-Sentinel sensor in the network, along with the suite of services around it we deliver the data in a way that's easy to understand and is actionable. Plus cybersecurity experts are available to answer any questions and provide guidance. With the N-Sentinel program, you have a trusted cybersecurity expert ready to help improve your security posture.

N-Sentinel Monitoring Program Overview

N-Sentinel Monitoring is offered as a managed security service; its key elements are:

- ✓ N-Sentinel Monitoring and Alerting Sensor(s)
- ✓ N-Sentinel Monitoring Monthly Report
- ✓ N-Sentinel Customer Portal
- ✓ Recommended Actions to Reduce Risk
- ✓ Utility Cyber Community Data
- ✓ Access to Trusted Cybersecurity Experts

- N-Sentinel Monitoring and Alerting Sensors

The N-Sentinel Monitoring program includes one or more sensors that are placed at a strategic location to monitor a utility's headend network, operation network and/or a specific network inside the utility. The sensor is typically placed behind a firewall and uses port mirroring (SPAN) functionality of the switch so that it is passive and does not interfere with normal network traffic. The N-Sentinel sensor has tens of thousands of signatures including but not limited to SCADA communication protocol intrusion signatures such as DNP3, Modbus and ICCP. The sensor will detect cybersecurity issues such as intrusion attempts by malware and viruses that may have gone undetected for a long time; it can alert unencrypted traffic that is confidential (such as customer account and credit card information).

Approximately two weeks after installation of the N-Sentinel sensor, one of our cybersecurity experts will analyze the event logs and work with the customer to tune the sensor. Two weeks later, event logs will be accessed and the first monthly report generated and provided to the utility.

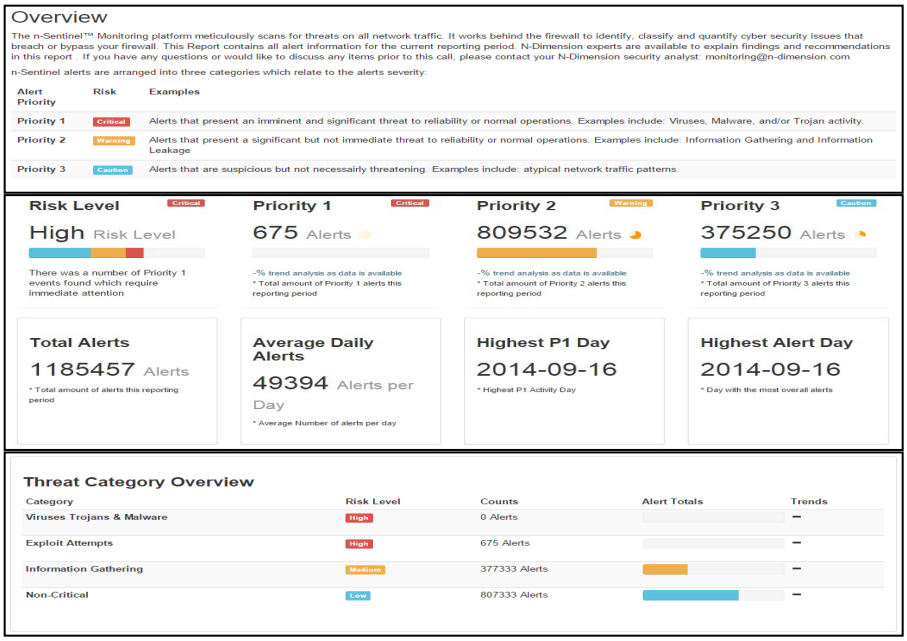
- **N-Sentinel Monitoring Monthly Report**

Reports are provided on a monthly basis and are emailed to utility personnel. Each report includes a summary of cyber incidents and issues (events) detected during the reporting period. The events are sorted by priority using levels 1 through 3, with Priority 1 being those incidents that are most critical, requiring immediate attention. The total number of events for each priority level is listed along with the details of the type of events for Priority 1 and 2. Next in the report is a summary of the major issues found, what they mean and what the utility can do to address them – in plain English.

Every month when the report is available, a cybersecurity expert schedules a phone call to review the report with utility personnel. These same trusted experts are available as needed as part of the N-Sentinel program, to answer questions via email or phone.

Following is a description of the main sections of the monthly report:

✓ Overview – This section contains a high-level summary of cybersecurity incidents detected in the utility's network during the reporting period.



Overview

The n-Sentinel™ Monitoring platform meticulously scans for threats on all network traffic. It works behind the firewall to identify, classify and quantify cyber security issues that breach or bypass your firewall. This Report contains all alert information for the current reporting period. N-Dimension experts are available to explain findings and recommendations in this report . If you have any questions or would like to discuss any items prior to this call, please contact your N-Dimension security analyst: monitoring@n-dimension.com

n-Sentinel alerts are arranged into three categories which relate to the alerts severity:

Alert Priority	Risk	Examples
Priority 1	Critical	Alerts that present an imminent and significant threat to reliability or normal operations. Examples include: Viruses, Malware, and/or Trojan activity.
Priority 2	Warning	Alerts that present a significant but not immediate threat to reliability or normal operations. Examples include: Information Gathering and Information Leakage
Priority 3	Caution	Alerts that are suspicious but not necessarily threatening. Examples include: atypical network traffic patterns.

Risk Level (Critical): High Risk Level
There was a number of Priority 1 events found which require immediate attention

Priority 1 (Critical): 675 Alerts
-% trend analysis as data is available
* Total amount of Priority 1 alerts this reporting period

Priority 2 (Warning): 809532 Alerts
-% trend analysis as data is available
* Total amount of Priority 2 alerts this reporting period

Priority 3 (Caution): 375250 Alerts
-% trend analysis as data is available
* Total amount of Priority 3 alerts this reporting period

Total Alerts: 1185457 Alerts
* Total amount of alerts this reporting period

Average Daily Alerts: 49394 Alerts per Day
* Average Number of alerts per day

Highest P1 Day: 2014-09-16
* Highest P1 Activity Day

Highest Alert Day: 2014-09-16
* Day with the most overall alerts

Threat Category Overview

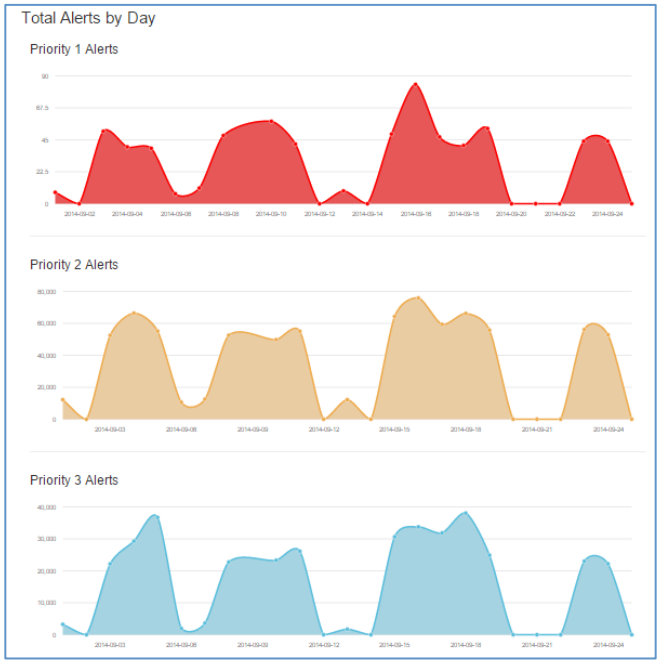
Category	Risk Level	Counts	Alert Totals	Trends
Viruses Trojans & Malware	High	0 Alerts		–
Exploit Attempts	High	675 Alerts		–
Information Gathering	Medium	377333 Alerts		–
Non-Critical	Low	807333 Alerts		–

✓ Community Analysis – This data offers the utility a comparison on the number and severity of threats they experienced during the reporting period, compared to the N-Sentinel Community. The N-Sentinel Community numbers aggregate all the utilities monitored by N-Sentinel and show average and median numbers.

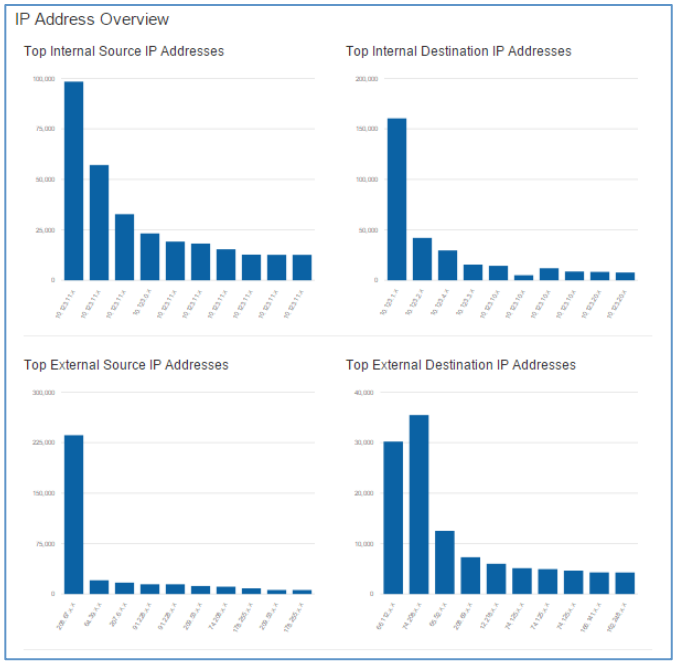
Community Analysis

	Utility		N-Sentinel Community			
Priority	Actual	Trend	Average	Average Trend	Median	Median Trend
Priority 1	11	22 % ↑	15	7 % ↑	11	22 % ↑
Priority 2	24	9 % ↑	12	20 % ↑	22	10 % ↑
Priority 3	17	21 % ↑	7	No Change	14	8 % ↑

- ✓ Total Alerts by Day – This section depicts the alert data in a graphical representation to offer an at-a-glance understanding of when intrusion attempts were the most frequent and what type they were throughout the month. The data can in identifying events that the utility may or may not have been aware of. For example, if a large number of intrusions happened on a particular date, the utility may be able to correlate that date to an event that happened on that day – a change or update to a firewall or switch configuration for example.



- ✓ IP Address Overview – This section shows the top internal and external source IP addresses that caused incidents as well the destination IP addresses. This can be useful in identifying a security issue, for example, if you see a lot of intrusion attempts going out to an external IP address you were unaware of, it could indicate an issue that needs to be addressed.



- ✓ Alert Overview – This section provides a high-level description of security incidents that have been detected, sorted by Priority levels and including alert ID, type of incident attempt (e.g. exploit, attempt, information gathering, etc.).

Alert Overview

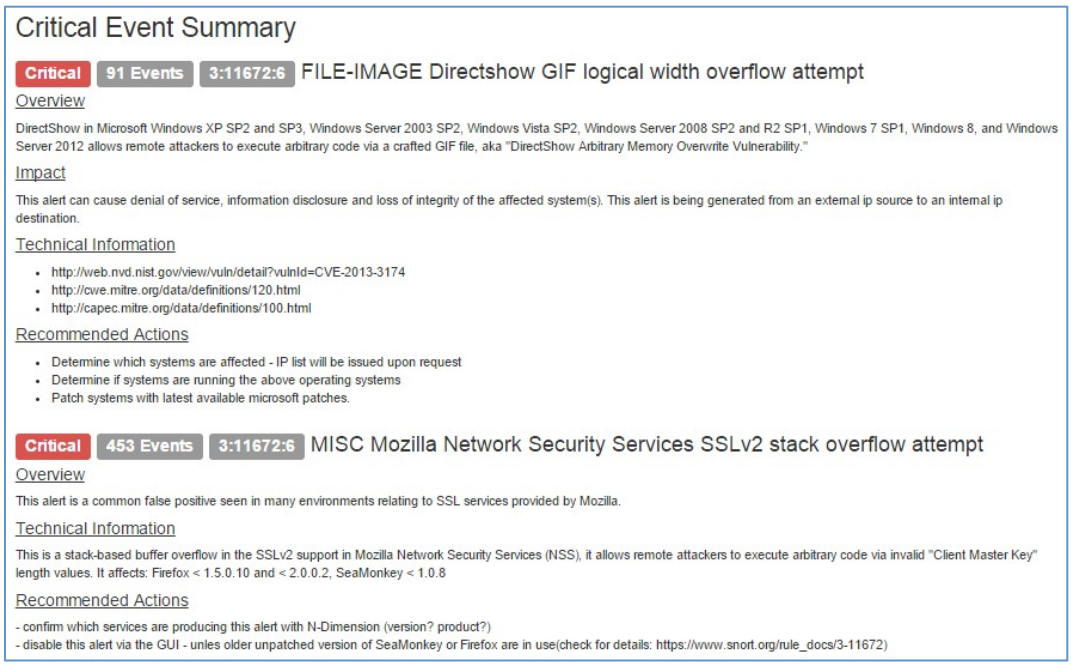
Priority 1 Alerts

Rank	Alert ID	Name	Total
1	3:11672:6	Exploit Attempts MISC Mozilla Network Security Services SSLv2 stack overflow attempt	453
2	1:27525:6	Exploit Attempts FILE-IMAGE Directshow GIF logical width overflow attempt	91
3	1:20883:10	Exploit Attempts FILE-OFFICE Microsoft Windows embedded packager object with .application extension bypass attempt	32
4	124:1:1	Exploit Attempts (smtp) Attempted command buffer overflow	42
5	3:19187:4	Exploit Attempts BAD-TRAFFIC TMG Firewall Client long host entry exploit attempt	21
6	3:15328:4	Exploit Attempts WEB-CLIENT Sun JDK image parsing library ICC buffer overflow attempt	1
7	1:20128:12	Exploit Attempts FILE-OFFICE Microsoft Office Invalid MSO-OGRAPH DataFormat buffer overflow attempt	1
8	1:26852:3	Exploit Attempts BROWSER-IE Microsoft Internet Explorer create-add range on DOM objects memory corruption attempt	1

Priority 2 Alerts

Rank	Alert ID	Name	Total
1	3:21355:3	Information Gathering BAD-TRAFFIC potential dns cache poisoning attempt - mismatched txid	238138
2	119:19:1	Non-critical Events (http_inspect) LONG HEADER	215431
3	129:15:1	Non-critical Events Reset outside window	109778
4	138:5:1	Information Gathering SENSITIVE-DATA Email Addresses	89239
5	139:1:1	Information Gathering (spp_sdf) SDF Combination Alert	40784

- ✓ Critical Event Summary – This section provides a detailed description of critical events detected and offers recommended actions.



Critical Event Summary

Critical | 91 Events | 3:11672:6 FILE-IMAGE Directshow GIF logical width overflow attempt

Overview

DirectShow in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, and Windows Server 2012 allows remote attackers to execute arbitrary code via a crafted GIF file, aka "DirectShow Arbitrary Memory Overwrite Vulnerability."

Impact

This alert can cause denial of service, information disclosure and loss of integrity of the affected system(s). This alert is being generated from an external ip source to an internal ip destination.

Technical Information

- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-3174
- http://cwe.mitre.org/data/definitions/120.html
- http://capec.mitre.org/data/definitions/100.html

Recommended Actions

- Determine which systems are affected - IP list will be issued upon request
- Determine if systems are running the above operating systems
- Patch systems with latest available microsoft patches.

Critical | 453 Events | 3:11672:6 MISC Mozilla Network Security Services SSLv2 stack overflow attempt

Overview

This alert is a common false positive seen in many environments relating to SSL services provided by Mozilla.

Technical Information

This is a stack-based buffer overflow in the SSLv2 support in Mozilla Network Security Services (NSS), it allows remote attackers to execute arbitrary code via invalid "Client Master Key" length values. It affects: Firefox < 1.5.0.10 and < 2.0.0.2, SeaMonkey < 1.0.8

Recommended Actions

- confirm which services are producing this alert with N-Dimension (version? product?)
- disable this alert via the GUI - unles older unpatched version of SeaMonkey or Firefox are in use(check for details: https://www.snort.org/rule_docs/3-11672)

- **N-Sentinel Customer Portal**
  Customers have a secure customer portal, accessible through an easy to use web-based graphical user interface. The portal provides administrative controls to setup who within the utility has rights to access the portal and receive reports; it provides a repository for N-Sentinel Monthly Reports; it offers visibility into Utility Cyber Community Data; and it has a database of useful tips, information and articles about cyber threats and remediation which customers can browse.

- **Recommended Actions to Reduce Risk**
  The Critical Event Summary, shown above, offers suggestion actions that can be taken to fix or reduce the risk associated with security events identified. These are suggestions from our team of cybersecurity experts based on the N-Sentinel Monitoring event log. The actions recommended can be as basic as updating software on a server or as complex as redesigning the network to improve its overall security posture.

- **Utility Cybersecurity Community Data**
  The N-Sentinel Monitoring program offers utilities access to anonymous cybersecurity data that is aggregated from other utilities. This data enables customers to compare how their utility compares with others in terms of cyber incidents such as number of Priority 1, 2 and 3 alerts, types of threats being identified, and types of devices affected by threats.

  N-Dimension cybersecurity analysts monitor the utility cyber community data to identify trends in numbers and types of threats targeting utilities enabling them to provide a timely alert to all customers about the threat and actions they can take to reduce their risk.

- **Access to Trusted Cybersecurity Experts**
  Each month, one of N-Dimension's cybersecurity experts will review the monthly report with utility personnel, focusing on the Priority 1 and 2 events and recommended actions. Our cybersecurity experts are always available to N-

Sentinel customers for phone and email support. On-site assistance is available upon request for an additional fee.

As trends emerge, usually over a period of several months, our cybersecurity experts can help identify potential risks in a utility's current network security defenses. Using the N-Sentinel report data along with a network diagram (as shared by utility), N-Dimension can provide the utility on ways in which they can improve their overall security posture.

Benefits of N-Sentinel Monitoring Program

- ✓ Monitoring – Identify intrusion attempts quickly – before they cause damage, access data, and/or proliferate. Acts as an additional layer of protection, oftentimes identifying threats that bypass other security defenses such as firewalls.
- ✓ Alerting – Timely alert when a critical, Priority 1 cyber incident is detected.
- ✓ Actionable Reports – Access to comprehensive information and data about detected cyber incidents and what actions you can take.
- ✓ Utility Cyber Community Data – Offers insights into how your utility's cybersecurity threat experience compares with others. It can provide utilities with early warning about cyber threats being launched against other utilities and actions to take to reduce risk.
- ✓ Trusted Cybersecurity Experts – Phone and email access to help in understanding threats and reports and who can provide guidance on remediation.
- ✓ Cloud-based Service – Once the N-Sentinel sensor is installed, software updates and maintenance are managed by N-Dimension, freeing IT/OT time for other projects.
- ✓ Customer Portal – The secure web-based portal provides access to your N-Sentinel data at any time. In addition it includes relevant articles and information about current cybersecurity related issues.
- ✓ Compliance – Contributes to meeting NERC CIP (CIP-007-3a R6), PCI Requirements (10 – Track and Monitor all access to network resources and card holder data), ISO-27002 (10.6 Network Security Management primarily)

N-Sentinel Monitoring Free Trial Offer

N-Dimension has learned from customers that there's nothing quite like experiencing N-Sentinel Monitoring for yourself. Most utilities find there's a lot going on in their network that they didn't know about – some good, some not so good. If you want to gain some visibility into what's going on in your network, contact us about a free trial and visit our website for more information.

About N-Dimension Solutions

N-Dimension Solutions addresses the critical need to protect critical energy infrastructures from the increasing the risk of cyber threats. As a result of protecting these networks, system reliability and safety increases, and energy infrastructure, data and assets are safeguarded from malicious activity and damages.

N-Dimension picks up where most cyber-security solutions leave off – at the vulnerable interconnections between information technology systems and critical infrastructure assets. Only N-Dimension offers a comprehensive solution for critical energy infrastructure operators.

N-Dimension is the exclusive cybersecurity partner of Hometown Connections, the utility services subsidiary of the American Public Power Association (APPA). The company is a member of the National Rural Electric Cooperative Association (NRECA), APPA and EDA.

Corporate Headquarters
9030 Leslie Street, Unit 300
Richmond Hill, Ontario
Canada L4B 1G2

Telephone: +1.905.707.8884
Toll Free: +1.866.837.8884

U.S. Headquarters
15305 Dallas Parkway
Suite 300
Addison, TX 75001

Email: sales@n-dimension.com
Web: www.n-dimension.com