ALARM GOES OFF
Grab phone

SLACK
Check Slack for incidents

EMAIL
Check email for tickets/incidents

NEWS
Quick scan of the news

CYBER NEWS
Quick scan of cyber security specific news/alerts (combating WSJ effect)
Incident POTENTIAL COMPROMISE

Employee downloaded a malicious file from their personal email account.

When I review the incident the questions I ask the team are as follows...

1. Does the employee have administrative access?
2. Do they have access to critical or sensitive data?
3. Did you review other activity associated with the account?
4. Did the malware exploit a vulnerability?

How many other assets have the same vulnerability?  
Check Tenable.io/Tenable.SC

What other vulnerabilities does this asset have?  
Check Tenable.io/Tenable.SC

Is a patch available for the vulnerability?  
Check Tenable.io/Tenable.SC

Do any of our other detection/protection mechanisms mitigate the vulnerability?  
Check Tenable.io/Tenable.SC

Do any of our other detection/protection mechanisms mitigate the vulnerability?  
Check Tenable.io/Tenable.SC

Do we need to send out a corporate communication?  
Check Tenable.io/Tenable.SC

Do we need to inform employees, vendors, partners, etc.?  
Check Tenable.io/Tenable.SC

Predictive Prioritization
<table>
<thead>
<tr>
<th>CERT Attack Vectors</th>
<th>MITRE Attack Vectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attrition</td>
<td>Initial Access</td>
</tr>
<tr>
<td>Email/Phishing</td>
<td>Execution</td>
</tr>
<tr>
<td>Improper Usage</td>
<td>Persistence</td>
</tr>
<tr>
<td>Loss or Theft</td>
<td>Privilege Escalation</td>
</tr>
<tr>
<td>Other</td>
<td>Defense Evasion</td>
</tr>
<tr>
<td>Removable Media</td>
<td>Credential Access</td>
</tr>
<tr>
<td>Spoofing</td>
<td>Discovery</td>
</tr>
<tr>
<td>Unknown</td>
<td>Lateral Movement</td>
</tr>
<tr>
<td>Web</td>
<td>Collection</td>
</tr>
<tr>
<td></td>
<td>Exfiltration</td>
</tr>
<tr>
<td></td>
<td>Command &amp; Control</td>
</tr>
</tbody>
</table>

- **Incident**: POTENTIAL COMPROMISE
- **IDENTIFY**
- **PROTECT**
- **DETECT**
- **RESPOND**
- **RECOVER**
<table>
<thead>
<tr>
<th></th>
<th>Question</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>How many other assets have the same vulnerability?</td>
<td>Check Tenable.io/Tenable.SC</td>
</tr>
<tr>
<td>2</td>
<td>How many of our those assets are considered critical?</td>
<td>Check Tenable.io/Tenable.SC (asset tagging/grouping – now our source of truth)</td>
</tr>
<tr>
<td>3</td>
<td>How many are of those assets are externally facing?</td>
<td>Check Tenable.io/Tenable.SC (asset tagging/grouping)</td>
</tr>
<tr>
<td>4</td>
<td>Is an exploit available or what is the likelihood of an exploit?</td>
<td>Threat intelligence/Tenable VPR Priority Rating (VPR)</td>
</tr>
<tr>
<td>5</td>
<td>What is the ease of exploitation?</td>
<td>Predictive Prioritization</td>
</tr>
<tr>
<td>6</td>
<td>Is a patch available for the vulnerability?</td>
<td>Check Tenable.io/Tenable.SC</td>
</tr>
<tr>
<td>7</td>
<td>Do we have any threat intel indicating prevalence or targeting for this</td>
<td>Tenable VPR</td>
</tr>
<tr>
<td></td>
<td>malware or vulnerability?</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Do any of our other detection/protection mechanisms mitigate the vulnerability?</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Do we need to send out a corporate communication?</td>
<td></td>
</tr>
<tr>
<td>Incident</td>
<td>CRITICAL VULNERABILITY</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------</td>
<td></td>
</tr>
<tr>
<td><strong>IDENTIFY</strong></td>
<td><strong>PROTECT</strong></td>
<td><strong>DETECT</strong></td>
</tr>
<tr>
<td>CERT Attack Vectors</td>
<td>Attrition</td>
<td>Email/Phishing</td>
</tr>
<tr>
<td>MITRE Attack Vectors</td>
<td>Initial Access</td>
<td>Execution</td>
</tr>
</tbody>
</table>

*RECOVER*
AUDITS

SOC 2
Service Organization Control (must have for SaaS providers)

CLIENT SITE VISITS
contractual program spot audits

SARBANES OXLEY

EVIDENCE REQUESTS
FINDINGS TO ADDRESS:

• BYOD Policies
• Security Strategy/Management
• Physical Security – staff passes
**SECURITY ASSESSMENT QUESTIONNAIRES (SAQs)**

<table>
<thead>
<tr>
<th>Ref</th>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS13.3</td>
<td>Please describe the process you follow for the validation and remediation of any findings identified as part of the penetration test</td>
<td>Remediation is tracked via a ticket which is created for each vulnerability/weakness discovered during the Pen Test. Progress is tracked to completion and subsequently the ticket(s) will be closed.</td>
</tr>
<tr>
<td>IS14</td>
<td>Please describe the process and output of all network vulnerability scans performed.</td>
<td>Vulnerability scans follow the Vulnerability Management Policy. See Policy for additional details.</td>
</tr>
<tr>
<td>IS14.1</td>
<td>Please confirm if your vulnerability scans cover: - all internal &amp; external network ranges on a monthly basis - cover all network components eg. switches, routers etc - be approved by an Approved Scanning Vendor where appropriate - devices not scanned are raised as issues</td>
<td>Sources of vulnerability findings are derived from both SecurityCenter and Tenable.io products to ensure complete coverage, including: 1. Nessus vulnerability scans 2. Nessus Network Monitor (NMM) continuous monitoring 3. Results of internal or third party penetration testing 4. Log Correlation Engine (LCE) events 5. Web applications scans 6. Vulnerabilities reported by the United States Computer Emergency Readiness Team (USCERT)</td>
</tr>
<tr>
<td>IS14.2</td>
<td>Please describe the controls operated regarding the remediation of any vulnerability scan findings</td>
<td>Discovered vulnerabilities are remediated based on vulnerability management policy. High and Critical vulnerabilities are given priority. These findings are considered proprietary and we are unable to distribute to customers.</td>
</tr>
</tbody>
</table>

**TABS**

- 7 tabs
- 130+ questions

**WE RECEIVED**

- 48 SAQs in Q4 2018 alone!

**SCREENSHOT**
d) Remove from service and the network any workstation, file, disk or other resource on which a virus, threat or security vulnerability is detected until the issue is resolved.

e) Maintain a periodic vulnerability testing of Supplier’s network, infrastructure and applications, regardless of dedicated or non-dedicated networks, and vulnerabilities are to be remediated in accordance with the following timetable:

- Critical Vulnerabilities within 72 hours of identification.
- High Vulnerabilities within 30 days of identification (CVSS of 7.0-10.0)
- Medium Vulnerabilities within 60 days of identification (CVSS of 4.0-6.9)
- Low Vulnerabilities within 90 days of identification (CVSS of 0.0-3.9.0)
### IT Risk - Security Assessment Questionnaire (SAQ)

Tenable Network Security, Inc. ("Tenable") has a responsibility to ensure all information associated with the company and our customers is appropriately protected during the handling, transmission, storage or processing by a third party organization.

This questionnaire is part of the Tenable risk review process for third parties, intended to identify and understand the control environment in place for managing the protection of information in external custody.

SAQ (this worksheet): Please answer all questions and provide relevant explanation or detail in the ‘Further Information’ column. Where necessary, please provide copies of, or extracts from, supporting policy or procedure documents.

Scope: This form is only required for companies that are not ISO or SOC 2 Type II compliant. For companies that are ISO or SOC 2 Type II compliant, please provide an attestation of your compliance along with a security whitepaper.

<table>
<thead>
<tr>
<th>1</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Company’s full legal name</td>
</tr>
<tr>
<td>1.2</td>
<td>Date of completion</td>
</tr>
<tr>
<td>1.11</td>
<td>Briefly outline the service that your company does (or will) provide to Tenable.</td>
</tr>
<tr>
<td>1.12</td>
<td>Briefly describe relevant systems/applications (in terms of the platforms, technologies, architecture).</td>
</tr>
<tr>
<td>1.13</td>
<td>List the physical locations where Tenable information will be stored.</td>
</tr>
<tr>
<td>1.2</td>
<td>Your name</td>
</tr>
<tr>
<td>1.3</td>
<td>Job title</td>
</tr>
<tr>
<td>1.4</td>
<td>E-mail address</td>
</tr>
<tr>
<td>1.5</td>
<td>Telephone number</td>
</tr>
</tbody>
</table>

### Basic Requirements

| 2.1 | Is your company certified to information security or auditing standards, such as ISO27001 or SSAE16 |
| 2.2 | Does your company have a documented process for responding to security incidents? |
| 2.11 | Does this process ensure that security incidents are reported through to the appropriate channels to Tenable? |
| 2.2 | Have you been independently audited in any other way? |
3rd Party Scorecards

Customer and Partner 3rd party vendor procurement and security assessment teams monitor our scores - so we must.
From the field:
Customer is looking for verification of proper security testing for vulns, exploits, etc. in our product. They don't need specific findings but an executive summary of how we test the security of our products.

Proactive identification of security issues in our products, can you triage, assess and report mitigations and/or plans to address?
WHAT DO I NEED TO IDENTIFY CYBER EXPOSURE?

To combine all these things....
FOCUS ON WHAT MATTERS FIRST
1. possibility of loss or injury: PERIL
2. function of:
   ASSETS
   THREATS
   VULNERABILITIES
**static adjective**

\stat-ik \n
1. : pertaining to or characterized by a fixed or stationary condition
2. : showing little or no change
“Cyber Exposure is an emerging discipline for managing and measuring cybersecurity risk in the digital era. Cyber Exposure transforms security from static and siloed visibility into cyber risk to dynamic and holistic visibility across the modern attack surface.”
BUSINESS IMPACT ANALYSIS

Identify at a high level impact to key locations, personnel or systems given a disruption, considering the following:

- **FINANCIAL IMPACTS**
- **OPERATIONAL IMPACTS**
- **MANAGEMENT TOLERANCES**
- **RESOURCE DEPENDENCIES**
BIA: Critical Functions, Assets, Services

**BUSINESS CONTEXT**

- Client data and services
- External websites
- CRM
- Productivity suite
- Code repositories
- Key personnel & facilities
Key Risk Indicators (KRIs)

EXAMPLES WITH KPIs

1. Strategic information leak (G Suite)
   - VISIBILITY, CRITICAL EVENTS IDENTIFIED AND MONITORED, ACCESS CONTROLS

2. Tenable.io customer vulnerability data disclosure
   - VISIBILITY, VULNERABILITIES AND MISCONFIGURATIONS IN T.IO INFRASTRUCTURE

3. Loss of intellectual property (code repos)
   - ACCESS CONTROLS, CRITICAL EVENTS IDENTIFIED AND MONITORED

4. Damage to brand or reputation (external websites)
   - PENETRATION TESTS, WAS, VM, AMBIONICS

5. Sales information leakage (Salesforce)
   - VISIBILITY, CRITICAL EVENTS IDENTIFIED AND MONITORED, ACCESS CONTROL
## Asset Prioritization in the Public Sector

### National Risk Management Framework

- **IDENTIFY**
  - 3,300 electricity utilities in the U.S.
  - 32 EMCs in NC, 76 municipally owned
  - ~70% of customers get their electricity from IOUs

- **ANALYZE**
  - 16,000 publicly owned wastewater treatment plants in operation across the country
  - 87% of US are served by publicly owned water/waste
  - NC regulates 90+ Water/Sewer entities

- **PRIORITIZE**
  - 7,700 organizations provide public transportation in the U.S.

- **MANAGE**
  - There are 1,830,672 miles of oil and gas pipelines across the U.S.
  - 8 municipal gas systems in NC
  - Cross sector dependencies
Digital transformation has made asset and vulnerability identification DIFFICULT
Data science can measure elements that impact threat intent, capability, and opportunity:

- Threat recency
- Threat intensity
- Exploits available
- Previous attacks/TTPs
- Complexity
- Darkweb, forums, blogs, code repos
risk noun

1. : possibility of loss or injury : PERIL

2. : function of :
   : ASSETS
   : THREATS
   : VULNERABILITIES
7% of vulnerabilities had an exploit available

63% of vulnerabilities discovered in environments are CVSS 7+

12% of vulnerabilities disclosed in 2017 were CVSS 9+

Vulnerability Intelligence Report Tenable Research
If Everything Is Important — NOTHING IS

59% High or Critical
VPR

VULNERABILITY PRIORITY RATING

Leverages supervised machine learning algorithms to calculate the priority of a vulnerability based on the real threat posed.

Key Drivers include

- Threat Recency
- Threat Intensity
- Exploitability
- Vulnerability Age
- Threat Sources
WHAT DO I NEED TO IDENTIFY CYBER EXPOSURE?

To combine all these things....
FOCUS ON WHAT MATTERS FIRST
Leverage machine learning and threat intelligence to prioritize vulnerabilities based on real world risk

Prioritize assets based on indicators of business value and criticality

Focus First On What Matters Most

Prioritize based on importance of asset AND risks posed by vulnerabilities on the asset

VPR + ACR

VULNERABILITY PRIORITY RATING

ASSET CRITICALITY RATING

Assets and Vulnerabilities to Fix First
Recommended Workflows
Drill down into specific vulnerabilities and assets for business and technical context to enable more effective remediation.
**cyber risk** *noun*

1. : risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems

2. : function of :

---

**cyber exposure** *noun*

1. : an emerging discipline for managing and measuring cybersecurity risk

2. : function of :