

# Threats from the Dark Side – A Dark Web Tour from a PCI DSS Perspective

Christopher Strand, Chief Risk and Compliance Officer  
Cybersixgill



# Agenda



A Dark Web Tour from a PCI DSS perspective

How threat intelligence is used against you: techniques and tactics used on the dark web to exploit critical and sensitive data.

How payment data and systems are targeted, used, and sold by the criminal underground.

How PCI DSS v4.0 helps to counter the problem in the dark web environment to prevent threat actors from exploiting systems and data.

# The Attack Trend Has Been Changing



**14+ Billion**

Global Data Records  
Lost Since 2013

**40.4+ Billion**

Global Data Records  
Exposed in 2021

*Source: Tenable's 2021 Threat Landscape Retrospective (TLR) report*

# Signal to Noise Ratio of Data Protection



# The Levels of Dark Web Cyber Intelligence

Bad actors use cyber threat intelligence (CTI) to create opportunities throughout cyberspace. Accessing various underground sources for continually assembling attacks and hiding their tracks



## Clear Web

Paste sites (e.g. pastebin),  
Reddit, 8chan, NVD, Twitter  
(secondary+direct), GitHub  
(Secondary+direct)

## Deep Web

Open and closed (invite-  
only) forums, markets,  
credit card markets, paste  
sites and IRC channels

## Dark Web

Open and closed (invite-  
only) forums, markets,  
credit card markets, paste  
sites and IRC channels,  
Dread, Zeronet

## Social Messaging

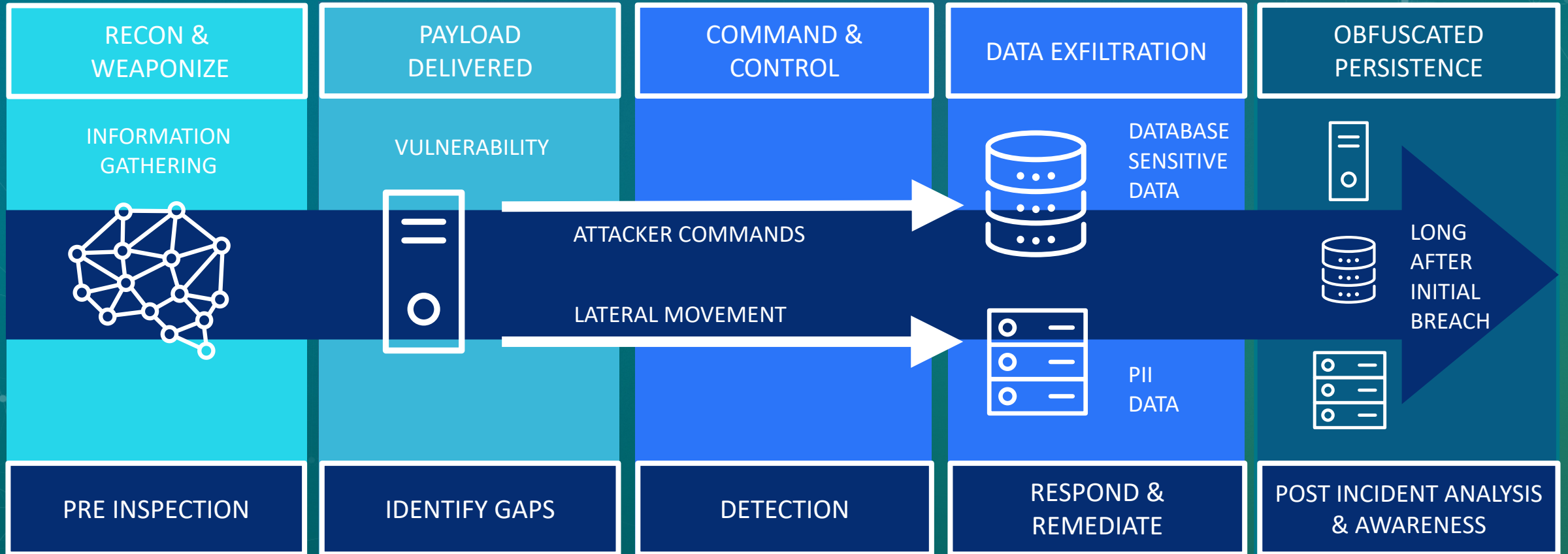
Open and closed (invite-  
only) groups and  
channels on **Telegram**,  
**Discord** and **QQ**, **ICQ**

# In a Dark Web Minute

Organizations today swim in data. We performed an exercise to feel the 'Pulse of the Underground' - what happens in the deep and dark web in a minute. The results were staggering.



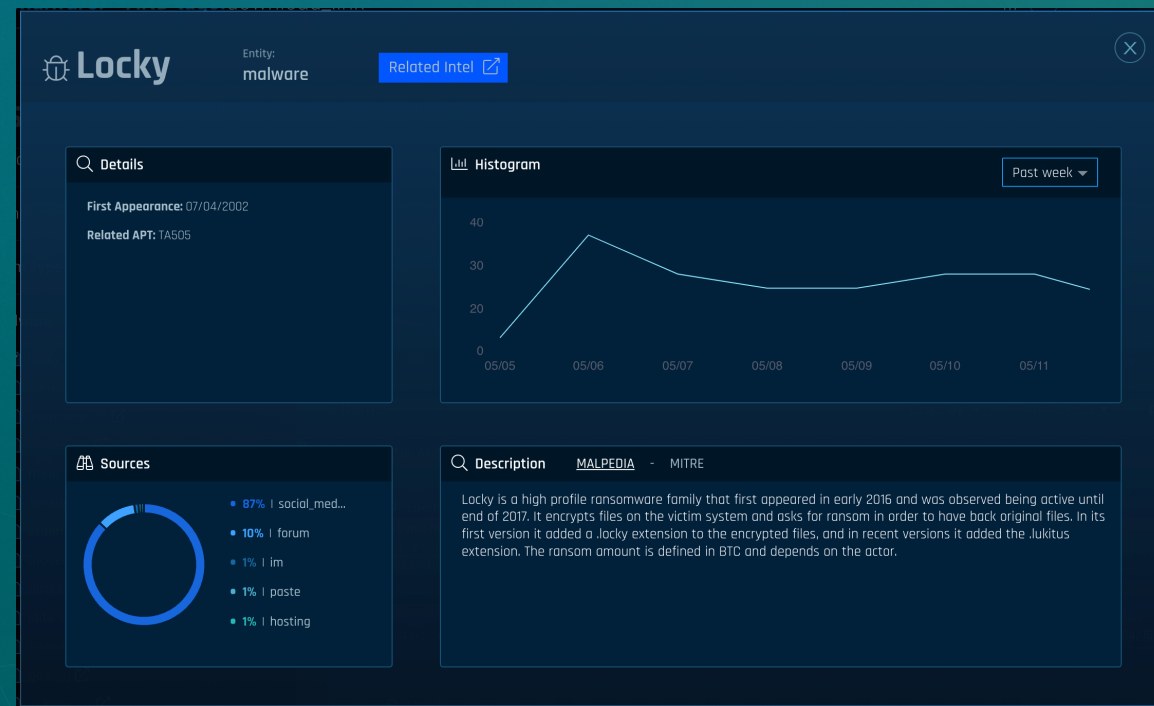
# Attackers utilize preemptive and proactive techniques for exploits



PRE AND POST SECURITY CONTROLS RESPONSIBLE FOR PREVENTING AN EXPLOIT

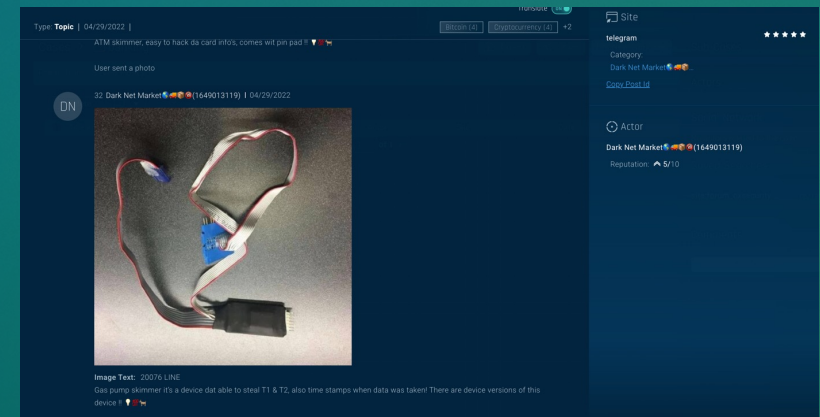
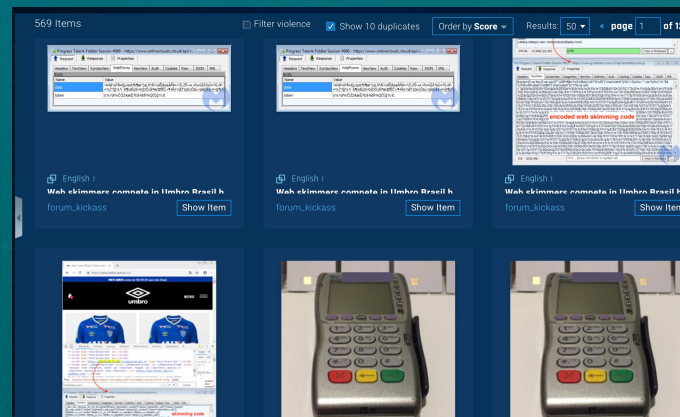
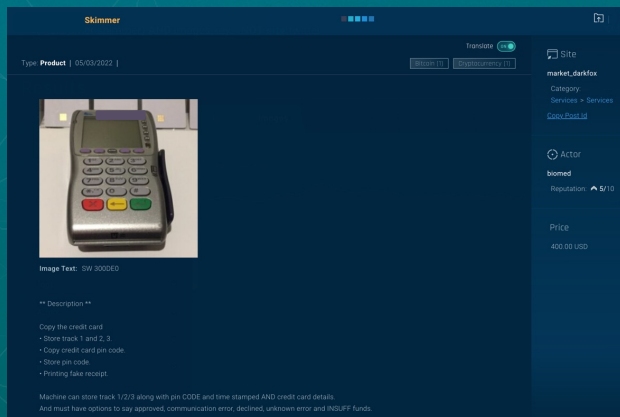
# Financial Sector System Targeting Escalates with Market Changes

Dark Web examples showing escalation of financial and payment system related targeting

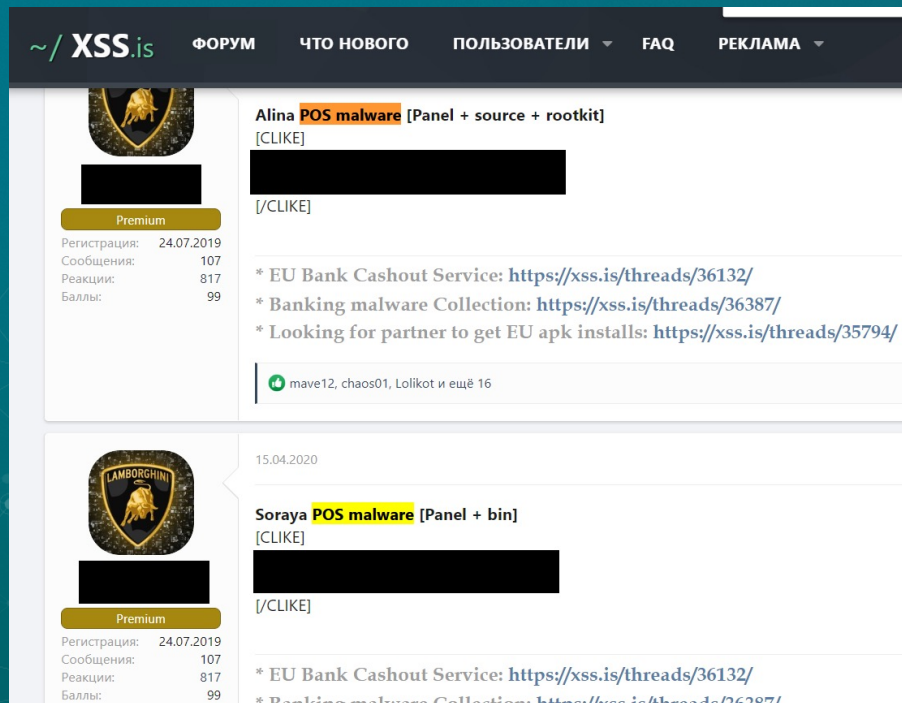


# Payment Related Data with Personal Information in Scope and Value Continues to Grow

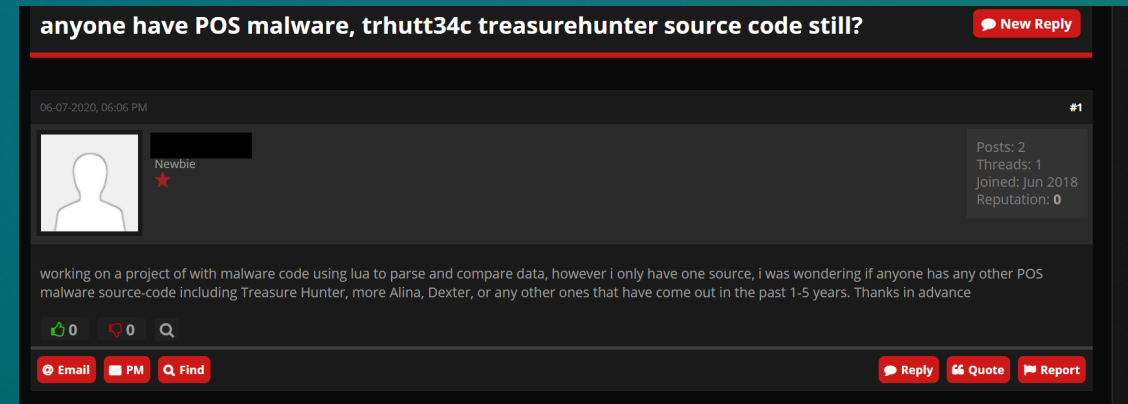
Dark Web examples showing targeting financial data via system security gaps



# Dark Web Forum Payment System Targeting



The screenshot shows a forum thread on XSS.is. The forum has a dark header with navigation links: "/ XSS.is", "ФОРУМ", "ЧТО НОВОГО", "ПОЛЬЗОВАТЕЛИ", "FAQ", and "РЕКЛАМА". The thread title is "Alina POS malware [Panel + source + rootkit] [CLIKE]". The user profile for "Alina" is visible, showing a premium status, registration date of 24.07.2019, 107 messages, 817 reactions, and 99 points. The thread content includes a redacted section, followed by links to other threads: "\* EU Bank Cashout Service: https://xss.is/threads/36132/", "\* Banking malware Collection: https://xss.is/threads/36387/", and "\* Looking for partner to get EU apk installs: https://xss.is/threads/35794/". The thread is replied to by "mave12, chaos01, Lolikot и ещё 16".



The screenshot shows a forum thread on XSS.is with the title "anyone have POS malware, trhutt34c treasurehunter source code still?". The thread is posted by a user named "Newbie" on 06-07-2020 at 06:06 PM. The user profile for "Newbie" is visible, showing a status of "Newbie", 2 posts, 1 thread, joined in Jun 2018, and a reputation of 0. The thread content includes the text: "working on a project of with malware code using lua to parse and compare data, however i only have one source, i was wondering if anyone has any other POS malware source-code including Treasure Hunter, more Alina, Dexter, or any other ones that have come out in the past 1-5 years. Thanks in advance". The thread has 0 replies, 0 likes, and 0 views. The thread is replied to by "Newbie".



# Find and Protect ALL Payment Related Data

**Imminent** | Compromised Credit Cards (partial) | Status: Treatment Required | Actions

Sixgill discovered 2 Cybersixgill compromised credit cards published in the underground. The preview below highlights the top five records - please click the "Export to CSV" button to download the full list of affected cards.

Trigger: **Assets** | 12/6/2021, 9:33:17 AM | **Traced** | **Compromised Accounts**

[Export to CSV](#)

BIN	Text	Date	Site	Actor
375000	3790001   United Kingdom   [REDACTED] DEBIT, PREPAID   10/25   Yes   Christopher ..   53017-5237   Chesterfield   Y   : CHEQUE   No   No   No   No   No   \$50.00	2021-12-06T09:05:40	cc_market_cwunion	Admin
370276	3702760   United States   [REDACTED]   CREDIT, [REDACTED]   10/23   Yes   Annette ..   94555   PITTSBURG   Yes   Yes   Yes   No   Yes   Yes   No   \$20.00	2021-12-06T09:05:26	cc_market_cwunion	Admin

2 records are in a "Traced" state. 2 records are in a "Treatment Required" state.

Traced and more records are in a "Treatment Required" state.

# How the PCI DSS v4.0 Helps to Counter Growing Attacks from the Dark Web



Vulnerability and Gap Prioritization

## PCI DSS v4.0 Requirement 6.3:

- Can help to uncover outlying gaps and vulnerabilities that attackers are capitalizing on and exploiting
- Will help to continually measure the real risk of any vulnerabilities across your enterprise
- Will ensure that the right priority is applied to the right vulnerabilities with measurable enforcement

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
<b>Defined Approach Requirements</b>	<b>Defined Approach Testing Procedures</b>	<p><b>Purpose</b></p> <p>Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.</p> <p><b>Good Practice</b></p> <p>Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy.</p> <p>When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution.</p> <p>An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.</p> <p><i>(continued on next page)</i></p>
6.3.1 Security vulnerabilities are identified and managed as follows:	6.3.1.a Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.	
<ul style="list-style-type: none"> <li>New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).</li> <li>Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.</li> </ul>	6.3.1.b Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	
<ul style="list-style-type: none"> <li>Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.</li> <li>Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.</li> </ul>		
<b>Customized Approach Objective</b>		
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
<b>Applicability Notes</b>		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
<b>Defined Approach Requirements</b>	<b>Defined Approach Testing Procedures</b>	<b>Purpose</b>
<p><b>6.3.1</b> Security vulnerabilities are identified and managed as follows:</p> <ul style="list-style-type: none"> <li>• New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).</li> <li>• Vulnerabilities are assigned a risk ranking based on industry best practices and consideral potential impact.</li> </ul>	<p><b>6.3.1.a</b> Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.</p>	<p>Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.</p>
<ul style="list-style-type: none"> <li>• Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk critical to the environment.</li> </ul>	<p><b>6.3.1.b</b> Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and</p>	
<ul style="list-style-type: none"> <li>• Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.</li> </ul>		<p><b>Good Practice</b></p> <p>Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment methodology.</p> <p>When an entity is assigning its risk rankings, it should consider using a formal, objective, repeatable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution.</p>
<b>Customized Approach Objective</b>		<p>An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.</p> <p><i>(continued on next page)</i></p>
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
<b>Applicability Notes</b>		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

industry-recognized sources for security vulnerability information

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
<p><b>Defined Approach Requirements</b></p> <p><b>6.3.1</b> Security vulnerabilities are identified and managed as follows:</p> <ul style="list-style-type: none"> <li>• New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).</li> <li>• Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.</li> <li>• Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.</li> <li>• Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.</li> </ul>	<p><b>Defined Approach Testing Procedures</b></p> <p><b>6.3.1.a</b> Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.</p> <p><b>6.3.1.b</b> Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.</p>	<p><b>Purpose</b></p> <p>Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.</p> <p><b>Good Practice</b></p> <p>Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy.</p> <p>When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution.</p> <p>An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.</p> <p><i>(continued on next page)</i></p>
<p><b>Customized Approach Objective</b></p> <p>New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.</p>		
<p><b>Applicability Notes</b></p> <p>This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.</p>		

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
<b>Defined Approach Requirements</b>	<b>Defined Approach Testing Procedures</b>	<b>Purpose</b>
<p><b>6.3.1</b> Security vulnerabilities are identified and managed as follows:</p> <ul style="list-style-type: none"> <li>New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).</li> <li>Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.</li> <li>Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.</li> <li>Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.</li> </ul>	<p><b>6.3.1.a</b> Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.</p> <p><b>6.3.1.b</b> Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and</p>	<p>Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.</p>
		<b>Good Practice</b>
		<p>Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy.</p> <p>When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution.</p>
		<p>In an organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally,</p>
		<p>vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.</p> <p><i>(continued on next page)</i></p>
<b>Customized Approach Objective</b>		
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
<b>Applicability Notes</b>		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

**vulnerabilities considered to be a high-risk or critical to the environment**

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
<b>Defined Approach Requirements</b>	<b>Defined Approach Testing Procedures</b>	<p><b>Purpose</b></p> <p>Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.</p> <p><b>Good Practice</b></p> <p>Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy.</p> <p>When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution.</p> <p>An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.</p> <p><i>(continued on next page)</i></p>
6.3.1 Security vulnerabilities are identified and managed as follows:	6.3.1.a Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.	
<ul style="list-style-type: none"> <li>New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).</li> <li>Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.</li> </ul>	6.3.1.b Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	
<ul style="list-style-type: none"> <li>Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.</li> <li>Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.</li> </ul>		
<b>Customized Approach Objective</b>		
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
<b>Applicability Notes</b>		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
<b>Defined Approach Requirements</b>	<b>Defined Approach Testing Procedures</b>	<b>Purpose</b>
<p><b>6.3.1</b> Security vulnerabilities are identified and managed as follows:</p> <ul style="list-style-type: none"> <li>New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).</li> <li>Vulnerabilities are assigned a risk ranking based on industry best practices and their potential impact.</li> <li>Risk rankings identify, at a minimum, vulnerabilities considered to be a critical to the environment.</li> <li>Vulnerabilities for bespoke and custom third-party software (for example, cloud systems and databases) are covered.</li> </ul>	<p><b>6.3.1.a</b> Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.</p> <p><b>6.3.1.b</b> Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with this requirement.</p>	<p>Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.</p> <p><b>Good Practice</b></p> <p>Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment methodology. When an organization is assigning its risk rankings, it should consider using a formal, objective, and consistent methodology that accurately portrays the severity of the vulnerabilities pertinent to the environment and translates to an appropriate and consistent priority for resolution.</p>
<b>Customized Approach Objectives</b>		<b>Good Practice</b>
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		<p>An organization's processes for managing vulnerabilities should be integrated with other organizational processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.</p> <p><i>(continued on next page)</i></p>
<b>Applicability Notes</b>		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

**New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed**

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
<b>Defined Approach Requirements</b>	<b>Defined Approach Testing Procedures</b>	<p><b>Purpose</b> Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.</p> <p><b>Good Practice</b> Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution.</p> <p>An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.</p> <p><i>(continued on next page)</i></p>
6.3.1 Security vulnerabilities are identified and managed as follows:	6.3.1.a Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.	
<ul style="list-style-type: none"> <li>New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).</li> <li>Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.</li> </ul>	6.3.1.b Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	
<ul style="list-style-type: none"> <li>Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.</li> <li>Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.</li> </ul>		
<b>Customized Approach Objective</b>		
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
<b>Applicability Notes</b>		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
<b>Defined Approach Requirements</b> <b>6.3.1</b> Security vulnerabilities are identified and managed as follows: <ul style="list-style-type: none"> <li>New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).</li> <li>Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.</li> <li>Risk rankings identify, at a minimum, vulnerabilities considered to be a critical to the environment.</li> <li>Vulnerabilities for bespoke and custom third-party software (for example, cloud systems and databases) are covered.</li> </ul>	<b>Defined Approach Testing Procedures</b> <b>6.3.1.a</b> Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.  <b>6.3.1.b</b> Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	<b>Purpose</b> Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.  <b>Good Practice</b> Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy.
<b>Customized Approach Objective</b> New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		When an entity is assigning its risk rankings, it should consider using a formal, objective, methodology that accurately portrays the vulnerabilities pertinent to the environment and translates to an appropriate resolution priority for resolution.
<b>Applicability Notes</b> This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.  <i>(continued on next page)</i>

This requirement is not achieved by, nor is it the same as, vulnerability scans

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
<b>Defined Approach Requirements</b>	<b>Defined Approach Testing Procedures</b>	<b>Purpose</b>
<p><b>6.3.1</b> Security vulnerabilities are identified and managed as follows:</p> <ul style="list-style-type: none"> <li>• New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).</li> <li>• Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.</li> </ul>	<p><b>6.3.1.a</b> Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.</p>	<p>Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.</p>
<ul style="list-style-type: none"> <li>• Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.</li> <li>• Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.</li> </ul>	<p><b>6.3.1.b</b> Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.</p>	
<b>for a process to actively monitor industry sources</b>		<b>Good Practice</b>
		<p>Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy.</p>
		<p>When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution.</p>
<b>Customized Approach Objective</b>		<p>An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.</p> <p><i>(continued on next page)</i></p>
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
<b>Applicability Notes</b>		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
<b>Defined Approach Requirements</b>	<b>Defined Approach Testing Procedures</b>	<p><b>Purpose</b></p> <p>Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.</p> <p><b>Good Practice</b></p> <p>Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy.</p> <p>When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution.</p> <p>An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.</p> <p><i>(continued on next page)</i></p>
<p><b>6.3.1</b> Security vulnerabilities are identified and managed as follows:</p> <ul style="list-style-type: none"> <li>• New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).</li> <li>• Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.</li> </ul>	<p><b>6.3.1.a</b> Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.</p>	
<ul style="list-style-type: none"> <li>• Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.</li> <li>• Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.</li> </ul>	<p><b>6.3.1.b</b> Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.</p>	
<b>Customized Approach Objective</b>		
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
<b>Applicability Notes</b>		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
<b>Defined Approach Requirements</b> <b>6.3.1</b> Security vulnerabilities are identified and managed as follows: <ul style="list-style-type: none"> <li>New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).</li> <li>Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.</li> <li>Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk critical to the environment.</li> <li>Vulnerabilities for bespoke and custom, an third-party software (for example operating systems and databases) are covered.</li> </ul>	<b>Defined Approach Testing Procedures</b> <b>6.3.1.a</b> Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.  <b>6.3.1.b</b> Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	<b>Purpose</b> Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.  <b>Good Practice</b> Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy.
<b>Customized Approach Objective</b> New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.	<p style="text-align: center;"><b>Processes should support ongoing evaluation of vulnerabilities</b></p>	When an organization is assigning its risk rankings, it should consider using a formal, objective, methodology that accurately portrays the vulnerabilities pertinent to the system and translates to an appropriate remediation priority for resolution.
<b>Applicability Notes</b> This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.  <i>(continued on next page)</i>

Requirements and Testing Procedures		Guidance
6.3 Security vulnerabilities are identified and addressed.		
<b>Defined Approach Requirements</b>	<b>Defined Approach Testing Procedures</b>	<p><b>Purpose</b></p> <p>Classifying the risks (for example, as critical, high, medium, or low) allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.</p> <p><b>Good Practice</b></p> <p>Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy.</p> <p>When an entity is assigning its risk rankings, it should consider using a formal, objective, justifiable methodology that accurately portrays the risks of the vulnerabilities pertinent to the organization and translates to an appropriate entity-assigned priority for resolution.</p> <p>An organization's processes for managing vulnerabilities should be integrated with other management processes—for example, risk management, change management, patch management, incident response, application security, as well as proper monitoring and logging of these processes. This will help to ensure all vulnerabilities are properly identified and addressed. Processes should support ongoing evaluation of vulnerabilities. For example, a vulnerability initially identified as low risk could become a higher risk later. Additionally, vulnerabilities, individually considered to be low or medium risk, could collectively pose a high or critical risk if present on the same system, or if exploited on a low-risk system that could result in access to the CDE.</p> <p><i>(continued on next page)</i></p>
6.3.1 Security vulnerabilities are identified and managed as follows:	6.3.1.a Examine policies and procedures for identifying and managing security vulnerabilities to verify that processes are defined in accordance with all elements specified in this requirement.	
<ul style="list-style-type: none"> <li>New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).</li> <li>Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.</li> </ul>	6.3.1.b Interview responsible personnel, examine documentation, and observe processes to verify that security vulnerabilities are identified and managed in accordance with all elements specified in this requirement.	
<ul style="list-style-type: none"> <li>Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.</li> <li>Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.</li> </ul>		
<b>Customized Approach Objective</b>		
New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.		
<b>Applicability Notes</b>		
This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.		

# 6.3 In Practice Combined with Dark Web Intelligence to Find Outliers

Search for keywords, sites, actors Search Assistant Translate

## CVE-2021-31955

Windows Kernel Information Disclosure Vulnerability

### CVE Score Card

Dynamic Vulnerability Exploit Score	CVSS 3.1	CVSS 2.0
Current Score	3.65	Score 5.5
Highest Score	9.99	Published 6/8/2021
Previously Exploited	9.8	Modified 6/10/2021

Attributes Events Chart Github References

Attribute	Status
Anonymous	False
Exploit Kit	False
Metasploit	False
POC Exploit	True
Related Ransomware	True

**Results** 1 i

# 6.3 In Practice Combined with Dark Web Intelligence to Find Outliers

CVE-2020-0989	5.14	2.1	5.5
CVE-2020-16999	5.11	2.1	5.5
CVE-2020-10002	5.09	2.1	5.5
CVE-2020-4842	5.04	4	4.9
CVE-2019-1440	5.01	2.1	

An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1436.

## CVE-2019-1440 <sup>?</sup>

An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1436.

### CVSS Score Card

#### Dynamic Vulnerability Exploit Score

Current Score	0
Highest Score	5.01
Previously Exploited	2.5



#### CVSS 3.1

Score	N/A
Published	11/12/2019
Modified	11/13/2019

#### CVSS 2.0

Score	2.1
Published	11/12/2019
Modified	11/13/2019



# Vulnerability Prioritization Using Dark Web Intelligence (Windows EOL)

CVE-2017-0147 <sup>?</sup>

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to obtain sensitive information from process memory via a crafted packets, aka "Windows SMB Information Disclosure Vulnerability."

## 📊 CVE Score Card

### Dynamic Vulnerability Exploit Score

Current Score	<b>9.97</b>
Highest Score	<b>10</b>
Previously Exploited	<b>10</b>

### CVSS 3.1

Score	<b>5.9</b>
Published	<b>03/16/2017</b>
Modified	<b>06/20/2018</b>

### CVSS 2.0

Score	<b>4.3</b>
Published	<b>03/16/2017</b>
Modified	<b>06/20/2018</b>

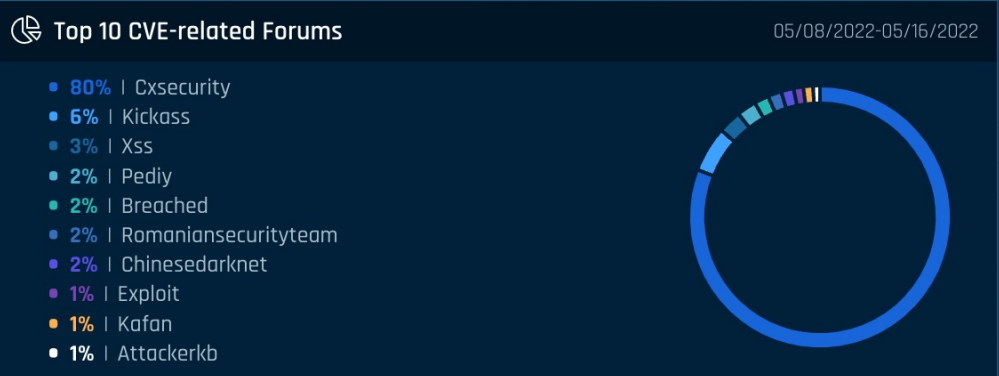
## Activity by Date

Date:



846 Items

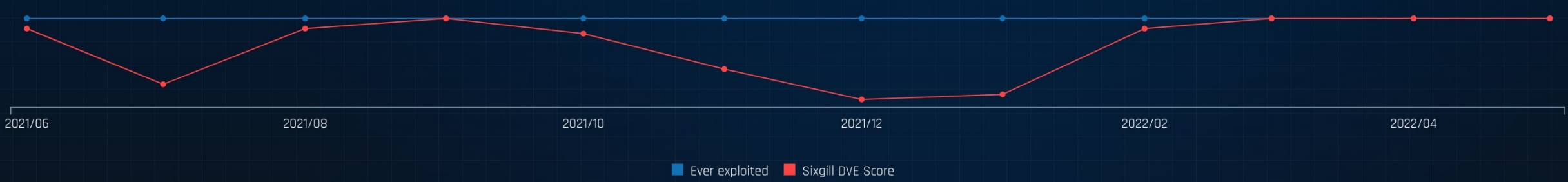
# Vulnerability Prioritization Using Dark Web Intelligence (Windows EOL)



Attributes Events Chart Github References

Date	Current Score	Previously Exploited Score	Description
05/14/2022	10	10	Mentioned on clear web twitter 9b0f46f45bc4a5475858d3845034b4e7d0eeff85
05/14/2022	10	10	Mentioned on twitter (highly regarded source with rank 4.0. 9b0f46f45bc4a5475858d3845034b4e7d0eeff85
05/13/2022	10	10	Mentioned on clear web twitter 4f646257d40062ee53a0c62c9f8be5c54ca3f1d1
05/13/2022	10	10	Mentioned on twitter (highly regarded source with rank 4.0. 4f646257d40062ee53a0c62c9f8be5c54ca3f1d1

Attributes Events Chart Github References



# Conduct Security Vulnerability Prioritization vs. Analysis

## Combine other sources like CTI with traditional VM

Integrate external sources and metrics to add risk measure to existing vulnerability management techniques

## Continually measure your risk

Continually assess CVE-related external risks to re-prioritize system patch management personnel and efforts

## Enrich your risk analysis

Incorporate broader threat intelligence from all depths of the web and uncover the real threat to your CDE

## Risk-based Vulnerability Prioritization



**Grazie!**  
**Thank You!**

