Which domains are used by Cyber Crucible?

_General

Created by Kyle Nehman, last modified on Apr 10, 2024

Beyond just pinging the domains used by Cyber Crucible to make sure that your endpoint can reach all of the correct network address, the Cyber Crucible Agent installer includes a test argument that ensures a valid TLS/SSL connection can be made in both directions to all required servers.

Untitled-20240410-185719.png
Simply add `--test-connection` to the installer execution, making sure to still include group id(s) and OAuth tokens that are necessary to perform authentication. Seen above is a screenshot showing the only modification needed to the provided .bat script, and a successful output.

Attachments:

▨ Untitled-20240410-185719.png (image/png)

Document generated by Confluence on May 18, 2026 19:44

Atlassian

_General

Created by Dennis Underwood, last modified by Kyle Nehman on Jun 12, 2025

Domain	Port	Protocol	Component	Producers of Traffic	Purpose	Certificate Validation/Revocation Domains (as of 1 May 2024)
dashboard.cybercrucible.com	443	HTTPS	Web Application	Users, typically assigned members of the IT, Security, and Compliance teams, who manage Cyber Crucible software. This web application is built on ReactJS.	This domain is tied to the administration panel for Cyber Crucible software. This admin panel is used to manage all licenses, and software agents. It is used to investigate and observe potential data or identity extortion incidents.	OCSP URL: http://r3.o.lencr.org CA URL/Issuer: http://r3.i.lencr.org
agent.tasking.rpp.cybercrucible.com	443	HTTPS	Windows Service	Cyber Crucible software agents use this domain. Users do not interact with this server, and this server is managed by a separate Federated ID allocation.	Cyber Crucible software agents use this domain to receive tasking, and submit data to the agent-specific REST server.	OCSP URL: http://r3.o.lencr.org CA URL/Issuer: http://r3.i.lencr.org

cognito-idp.us-west-2.amazonaws.com	443	HTTPS	Web Application	Users of the web application, or custom REST API calls by a client will produce traffic to the AWS Cognito service during login.	Cyber Crucible currently uses AWS Cognito for user pool and Federated Identity services, in support of software, REST API, and user oAuth 2.0 protected communications and user management.	CRL distribution URL: http://crl.r2m03.amazontrust.com/r2m03.crl OCSP URL: http://ocsp.r2m03.amazontrust.com CA URL/Issuer: http://crt.r2m03.amazontrust.com/r2m03.cer CRL distribution URL: http://crl.r2m02.amazontrust.com/r2m02.crl OCSP URL/Issuer: http://ocsp.r2m02.amazontrust.com CRL distribution URL: http://crt.r2m02.amazontrust.com/r2m02.cer

ransomwarerewind.auth.us-west-2.amazoncognito.com	443	HTTPS	Web Application	Users of the web application, or custom REST API calls by a client will produce traffic to the AWS Cognito service during login.	Cyber Crucible currently uses AWS Cognito for user pool and Federated Identity services, in support of software, REST API, and user oAuth 2.0 protected communications and user management.	CRL distribution URL: http://crl.r2m03.amazontrust.com/r2m03.crl OCSP URL: http://ocsp.r2m03.amazontrust.com CA URL/Issuer: http://crt.r2m03.amazontrust.com/r2m03.cer CRL distribution URL: http://crl.r2m02.amazontrust.com/r2m02.crl OCSP URL/Issuer: http://ocsp.r2m02.amazontrust.com CRL distribution URL: http://crt.r2m02.amazontrust.com/r2m02.cer

ransomwarerewind-agents.auth.us-west-2.amazoncognito.com (deprecated)	443	HTTPS	Windows Service	Cyber Crucible software agents use this domain. Users do not use this domain.	Cyber Crucible software agents use this domain, which is AWS Cognito, for user pool and Federated Identity services, in support of their OAuth 2.0 protected communications and software management.	CRL distribution URL: http://crl.r2m03.amazontrust.com/r2m03.crl OCSP URL: http://ocsp.r2m03.amazontrust.com CA URL/Issuer: http://crt.r2m03.amazontrust.com/r2m03.cer CRL distribution URL: http://crl.r2m02.amazontrust.com/r2m02.crl OCSP URL/Issuer: http://ocsp.r2m02.amazontrust.com CRL distribution URL: http://crt.r2m02.amazontrust.com/r2m02.cer

agent.oauth.rpp.cybercrucible.com	443	HTTP	Windows Service	Cyber Crucible software agents use this domain. Users do not use this domain.	Cyber Crucible software agents use this domain for OAuth 2.0 protected communications and software management. This domain replaces the deprecated AWS Cognito OAuth url above.	
installerfiles.rpp.cybercrucible.com	443	HTTPS	HTTPS File Server	Cyber Crucible installation and update files (drivers, services, etc.)	Cyber Crucible's installation and update files are stored in this website. It is used to do initial agent installation as well as fetch files for any required updates.	OCSP URL: http://r3.o.lencr.org CA URL/Issuer: http://r3.i.lencr.org
ipv4.icanhazip.com	443	HTTPS	Windows Service	Cyber Crucible software agents use this domain.	Cyber Crucible software agents query this domain to correlate the IPv4 WAN address for an agent.	OCSP URL: http://r3.o.lencr.org CA URL/Issuer: http://r3.i.lencr.org
ipv6.icanhazip.com	443	HTTPS	Windows Service	Cyber Crucible software agents use this domain.	Cyber Crucible software agents query this domain to correlate the IPv6 WAN address for an agent.	OCSP URL: http://r3.o.lencr.org CA URL/Issuer: http://r3.i.lencr.org

r3.o.lencr.org	80	OCSP	Windows Service	Web application users and Cyber Crucible software agents both use this domain.	This domain is the Let’s Encrypt TLS certificate validation and revocation check (OCSP) check server. Without access to this server, agents and the web application communications may not work.	
rs.i.lencr.org	80	HTTP	Windows Service	Web application users and Cyber Crucible software agents both use this domain.	This domain is the Let’s Encrypt TLS Certificate Authority (CA) server, that is used by validate TLS certificates. Without access to this server, agents and the web application communications may not work.	
crl.r2m03.amazontrust.com	80	HTTP	Windows Service	Web application users and Cyber Crucible software agents both use this domain.	This domain is the Amazon Web Services (AWS) certificate validation and revocation check (CRL) server. Without access to this server, agents and web application users cannot gain validated credentials, to then access secured Cyber Crucible resources.	

crl.r2m02.amazontrust.com	80	HTTP	Windows Service	Web application users and Cyber Crucible software agents both use this domain.	This domain is the Amazon Web Services (AWS) certificate validation and revocation check (CRL) server. Without access to this server, agents and web application users cannot gain validated credentials, to then access secured Cyber Crucible resources.	
ocsp.r2m03.amazontrust.com	80	OCSP	Windows Service	Web application users and Cyber Crucible software agents both use this domain.	This domain is the Amazon Web Services (AWS) certificate validation and revocation check (OCSP) server. Without access to this server, agents and web application users cannot gain validated credentials, to then access secured Cyber Crucible resources.	

ocsp.r2.m02.amazontrust.com	80	OCSP	Windows Service	Web application users and Cyber Crucible software agents both use this domain.	This domain is the Amazon Web Services (AWS) certificate validation and revocation check (OCSP) server. Without access to this server, agents and web application users cannot gain validated credentials, to then access secured Cyber Crucible resources.	
crt.r2m03.amazontrust.com	80	HTTP	Windows Service	Web application users and Cyber Crucible software agents both use this domain.	This domain is the Amazon Web Services (AWS) TLS Certificate Authority (CA) server, that is used by validate TLS certificates. Without access to this server, agents and the web application cannot gain validated credentials, to then access secured Cyber Crucible resources.	

crt.r2m02.amazontrust.com	80	HTTP	Windows Service	Web application users and Cyber Crucible software agents both use this domain.	This domain is the Amazon Web Services (AWS) TLS Certificate Authority (CA) server, that is used by validate TLS certificates. Without access to this server, agents and the web application cannot gain validated credentials, to then access secured Cyber Crucible resources.	
v2-agent.tasking.ransomwarerewind.com (deprecated)	443	HTTPS	Windows Service	Cyber Crucible software agents use this domain. Users do not interact with this server, and this server is managed by a separate Federated ID allocation.	Cyber Crucible software agents use this domain to receive tasking, and submit data to the agent-specific REST server.	OCSP URL: http://r3.o.lencr.org CA URL/Issuer: http://r3.i.lencr.org

ransomware-rewind-installation-files-64.s3.us-west-2.amazonaws.com (deprecated)	443	HTTPS	AWS S3 File Server	Cyber Crucible installer file location	Cyber Crucible's installer exe is located in an S3 bucket hosted at this domain. This domain is likely only accessed if using the script installer.	CRL distribution URL: http://crl.r2m03.amazontrust.com/r2m03.crl OCSP URL: http://ocsp.r2m03.amazontrust.com CA URL/Issuer: http://crt.r2m03.amazontrust.com/r2m03.cer CRL distribution URL: http://crl.r2m02.amazontrust.com/r2m02.crl OCSP URL/Issuer: http://ocsp.r2m02.amazontrust.com CRL distribution URL: http://crt.r2m02.amazontrust.com/r2m02.cer

installerfiles.ransomwarerewind.com (deprecated)	443	HTTPS	AWS S3 File Server	Cyber Crucible download and installers	Cyber Crucible's installation and update files are stored in this S3 bucket. It is used to do initial agent installation as well as fetch files for any required updates.	CRL distribution URL: http://crl.r2m03.amazontrust.com/r2m03.crl OCSP URL: http://ocsp.r2m03.amazontrust.com CA URL/Issuer: http://crt.r2m03.amazontrust.com/r2m03.cer CRL distribution URL: http://crl.r2m02.amazontrust.com/r2m02.crl OCSP URL/Issuer: http://ocsp.r2m02.amazontrust.com CRL distribution URL: http://crt.r2m02.amazontrust.com/r2m02.cer

v2-web.tasking.ransomwarerewind.com (deprecated)	443	HTTPS	Web Application	Users, typically assigned members of the IT, Security, and Compliance teams, who manage Cyber Crucible software. Custom REST API programs developed by customers will also use this domain.	This domain is the REST server which the ReactJS dashboard uses to dynamically create, retrieve, update, and delete relevant data from the web application.	OCSP URL: http://r3.o.lencr.org CA URL/Issuer: http://r3.i.lencr.org

How can I test connection to these domains?

How can I test connection to these domains?

Checking Certificate Chains

The following PowerShell script may be used to output the certificate chain obtained by a particular machine. This can be useful for debugging SSL issues or investigating the impact of an SSL firewall configuration.

Usage

On the PowerShell command line, call the script with the -TargetHost parameter. For example:

```
.\Get-SslCertificateChain.ps1 -TargetHost "agent.oauth.rpp.cybercrucible.com"
```

On yields the following output:

```
SSL Connection established to agent.oauth.rpp.cybercrucible.com:443
Certificate Chain:
  Leaf Certificate (Subject): CN=agent.oauth.rpp.cybercrucible.com
True
    - Subject: CN=agent.oauth.rpp.cybercrucible.com
      Issuer: CN=E7, O=Let's Encrypt, C=US
      Thumbprint: 2E401711BBC229F34B8A13D0233264CFBB155C82
      Valid From: 10/05/2025 06:06:01
      Valid To: 01/03/2026 05:06:00
    - Subject: CN=E7, O=Let's Encrypt, C=US
      Issuer: CN=ISRG Root X1, O=Internet Security Research Group, C=US
      Thumbprint: 3B73C17E3DF87CF3AA77F1389219EB5EDD519E7F
      Valid From: 03/12/2024 20:00:00
      Valid To: 03/12/2027 18:59:59
    - Subject: CN=ISRG Root X1, O=Internet Security Research Group, C=US
      Issuer: CN=ISRG Root X1, O=Internet Security Research Group, C=US
      Thumbprint: CABD2A79A1076A31F21D253635CB039D4329A5E8
      Valid From: 06/04/2015 07:04:38
      Valid To: 06/04/2035 07:04:38
```

How much data is produced by Cyber Crucible?

Created by Kyle Nehman on May 23, 2024

The data collected by the Cyber Crucible agent goes through multiple layers of filtering, in order to cut out noise from having too much raw telemetry. The raw data produced by the kernel sensors is trimmed down [**Filter #1**] to reduce both endpoint memory usage, and network bandwidth per-agent. Following that, the REST API will associate raw process/endpoint telemetry it receives to automated responses, such that the analyst can choose to view only relevant data [**Filter #2**].

Blank diagram-20240523-165941.png

As seen in the figure above, an average customer’s workstation endpoints may produce multiple gigabytes of raw sensor data over a 24hr span, whereas only a few megabytes of which will be relevant to a SOC alert if an attack is attempted.