



IT NATION™

SECURE

hosted by  CONNECTWISE

ConnectWise MDR™

True Managed Endpoint Protection



IT NATION™

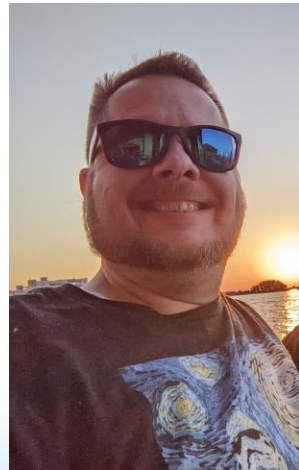
SECURE

Presenters

Rob DeBok (DeeeeeeeBok)

Software Training Consultant

- 9 years with ConnectWise
- Upcycle/repurpose
- Love helping partners



Rich Tourville

Sr. Sales Engineer, Security

- Specialist in Cybersecurity
- 12+ Years Industry Knowledge
- 4+ years Cybersecurity



Security NIST Mapping

	Identify	Protect	Detect	Respond	Recover
Risk Assessment	✓				
Vulnerability Management	✓				
Identify Assessment	✓				
MDR		✓	✓	✓	✓
Co-Managed SIEM			✓	✓	
SaaS Security			✓	✓	
BCDR					✓
Incident Response Service					✓
Secure Internet Access	✓	✓	✓	✓	
Secure Private Access		✓	✓	✓	
Identity and Access Mgmt		✓		✓	

Agenda

- Intro to MDR (managed detection and response)
- SOC (security operations center)
- EDR (endpoint detection and response) technologies
- Other resources

Managed Detection & Response (MDR)

What is it?



IT NATION™ **SECURE**

Managed Detection and Response (MDR)

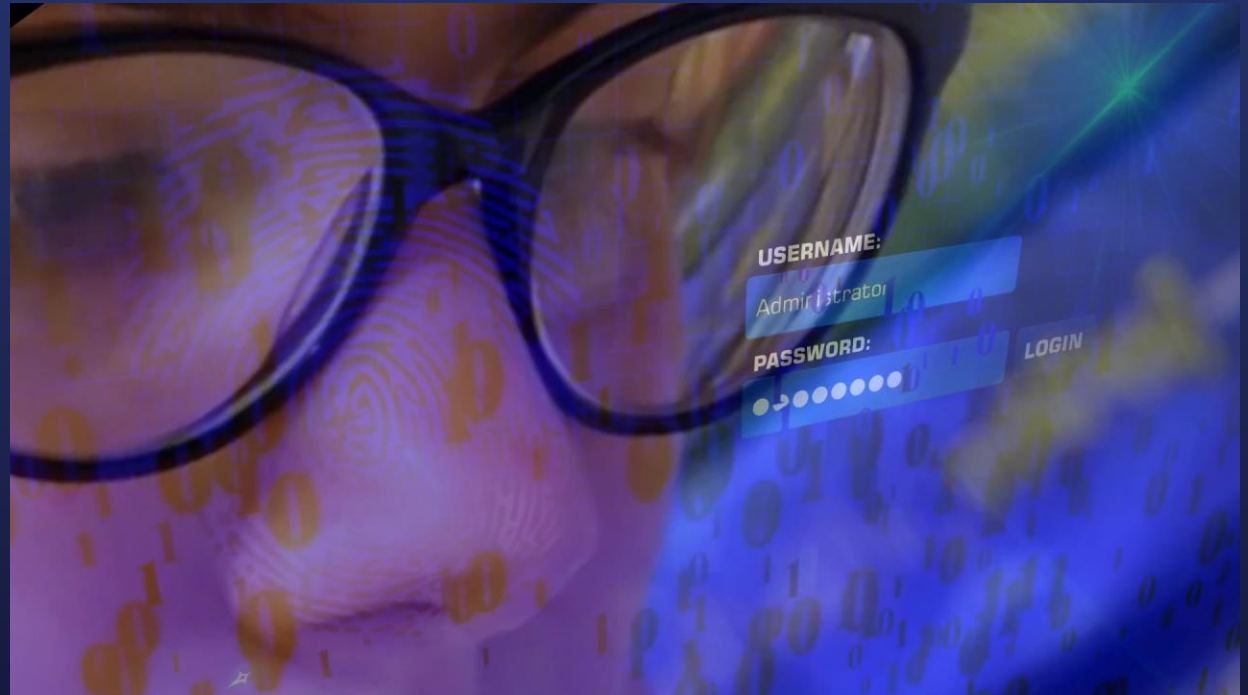
 SentinelOne®

OR

Bitdefender®

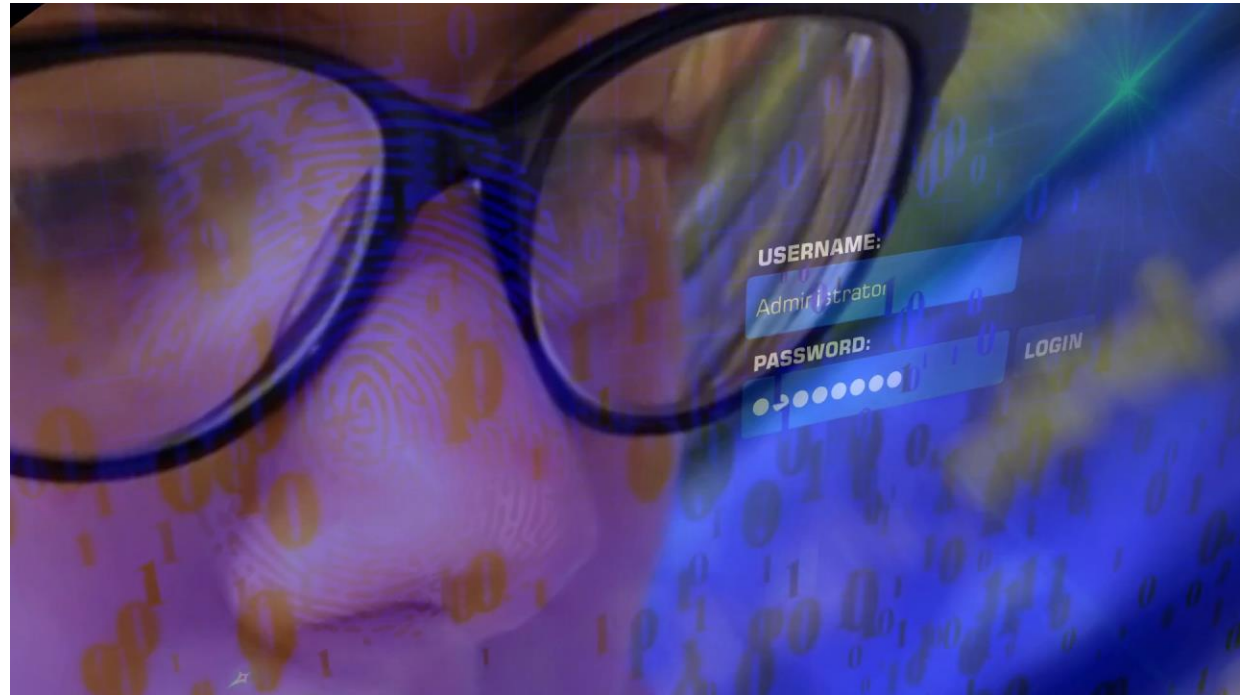


ConnectWise SOC
Services™



Managed Detection and Response (MDR)

- Proactive Security Monitoring
- Expert Security Analysis
- Compliance Support



Security Operations Center (SOC)

What is it?



IT NATION™ **SECURE**

Top Challenge: Bridging the Talent Gap

2.7-million-
person talent gap

Dwell time and
operational
downtime

Setting up your own
SOC can cost \$2-
4M

Alert fatigue

Cybersecurity tools
can generate 100s
to 1,000s of alerts

Speed to address
issues

ConnectWise Partners Have Deployed
Security To More Than

34,000 SMBs

ConnectWise SOC
Services™ is a team
dedicated to:

- Security monitoring
- Threat intelligence
- Incident response
- Vulnerability management
- Compliance

94.3% of
alerts and events handled by SOC on behalf
of ConnectWise Partners in 2022

ConnectWise SOC Services

200+

Security professionals

Capabilities for threat triage and analysis, log review, threat hunting, research, and incident response



- Our systems ingest more than 70B security events per day
- Analyze more than 3M events per month
- Incident Response as a Service (CWIRT)
- ConnectWise Cybersecurity Research Unit (CRU)



"We've been in competitive situations where people have agreed to talk to us because we're now seen as security specialists—a step up in terms of business services compared with being just another IT company. Our peers haven't been able to do this as effectively, or at all. Investing in all the training, knowledge, and products to build a security specialism from the ground up would be a major struggle, but the ConnectWise SOC gives us that capability."

James Ratcliff, Managing Director, Ratcliff IT

















EDR

Endpoint Detection and Response Technologies



IT NATION™ **SECURE**

Traditional Anti-Virus vs. EDR

	Legacy AV	EDR
Signature Based Detection		
Behavior Based Protection		
Centralized Management		
Automated Response		
Protects Endpoints		
Device Control		
Network Control		

EDR/MDR

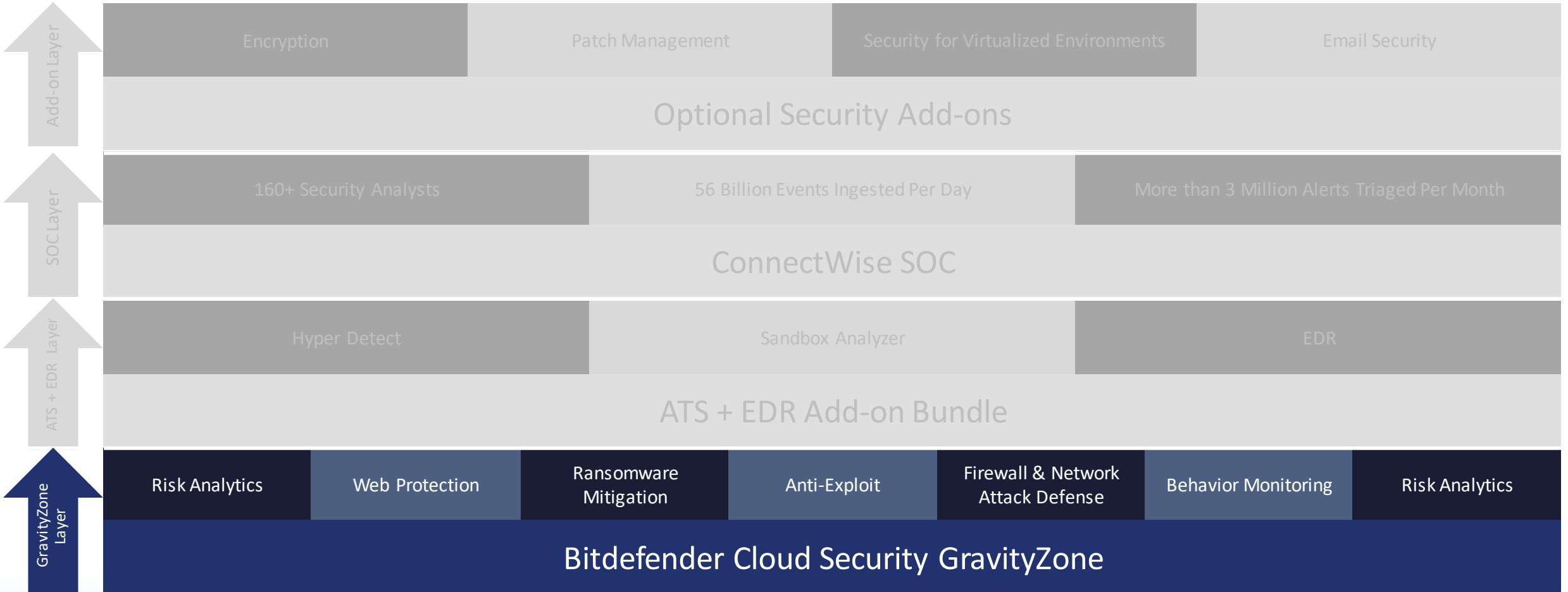
Bitdefender



IT NATION™ **SECURE**

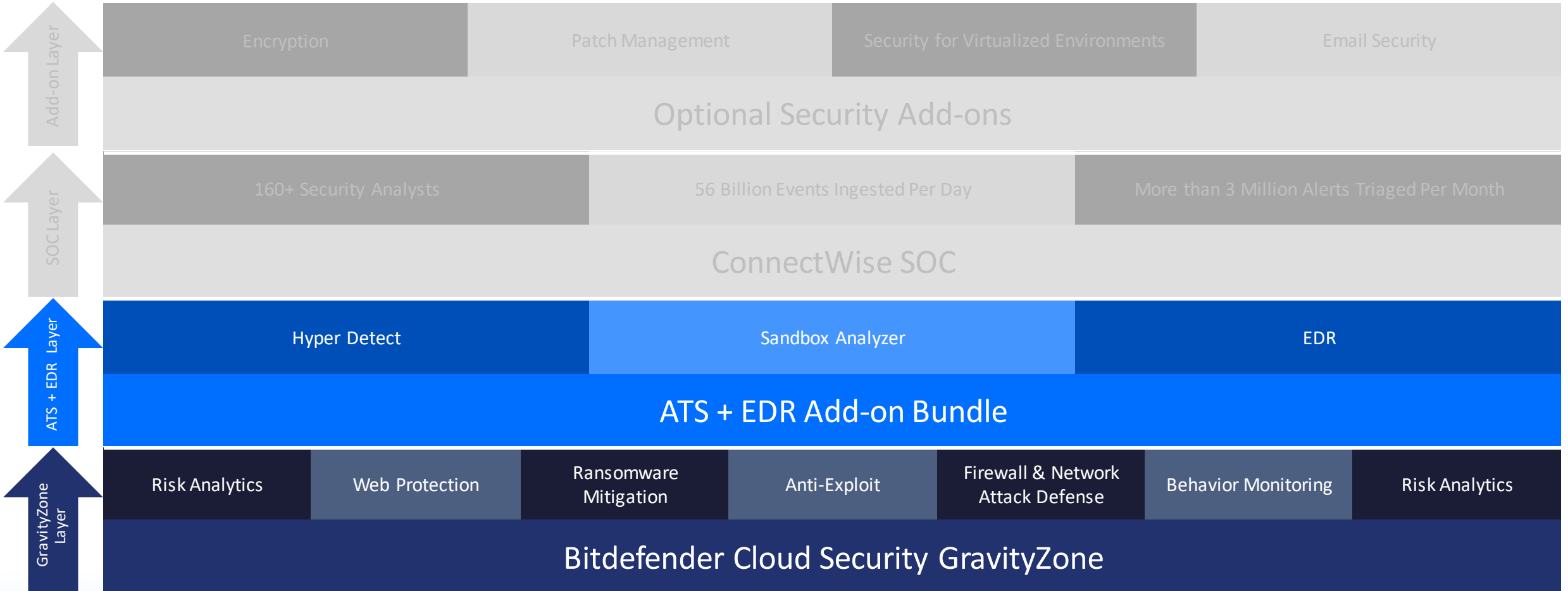
The Bitdefender Platform

Bitdefender®



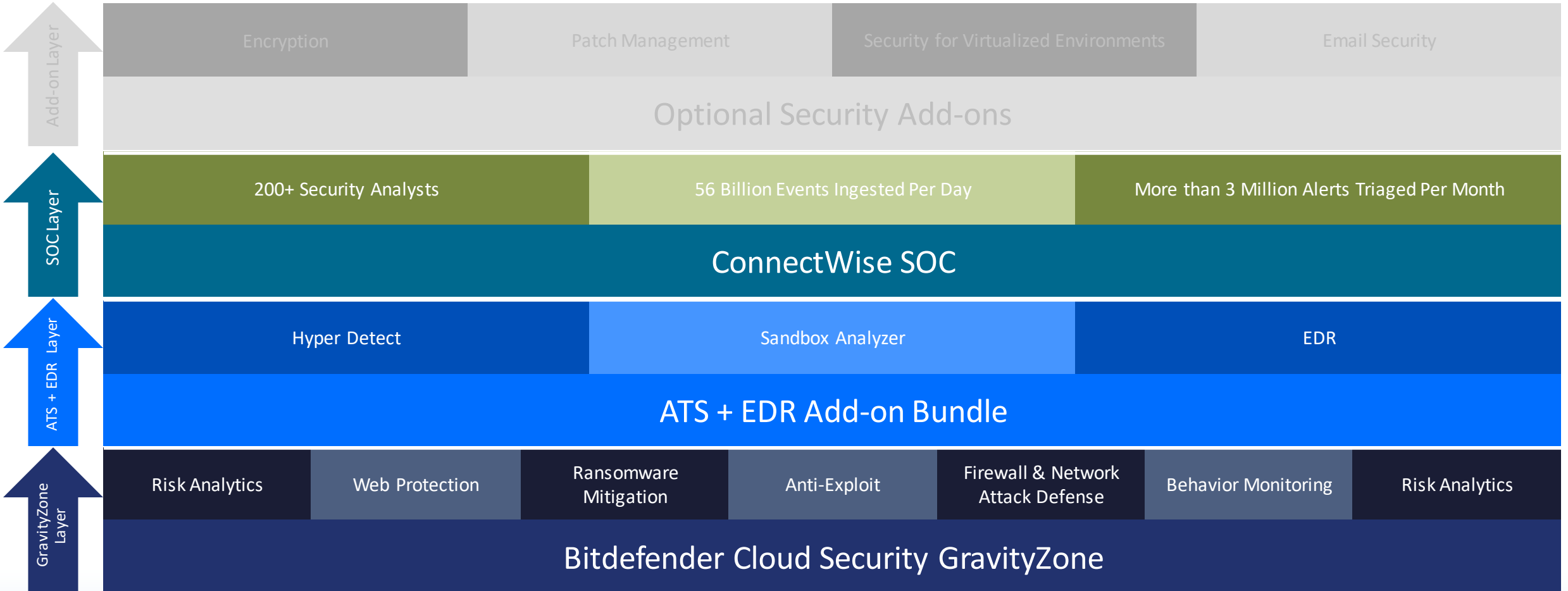
The Bitdefender Platform

Bitdefender®



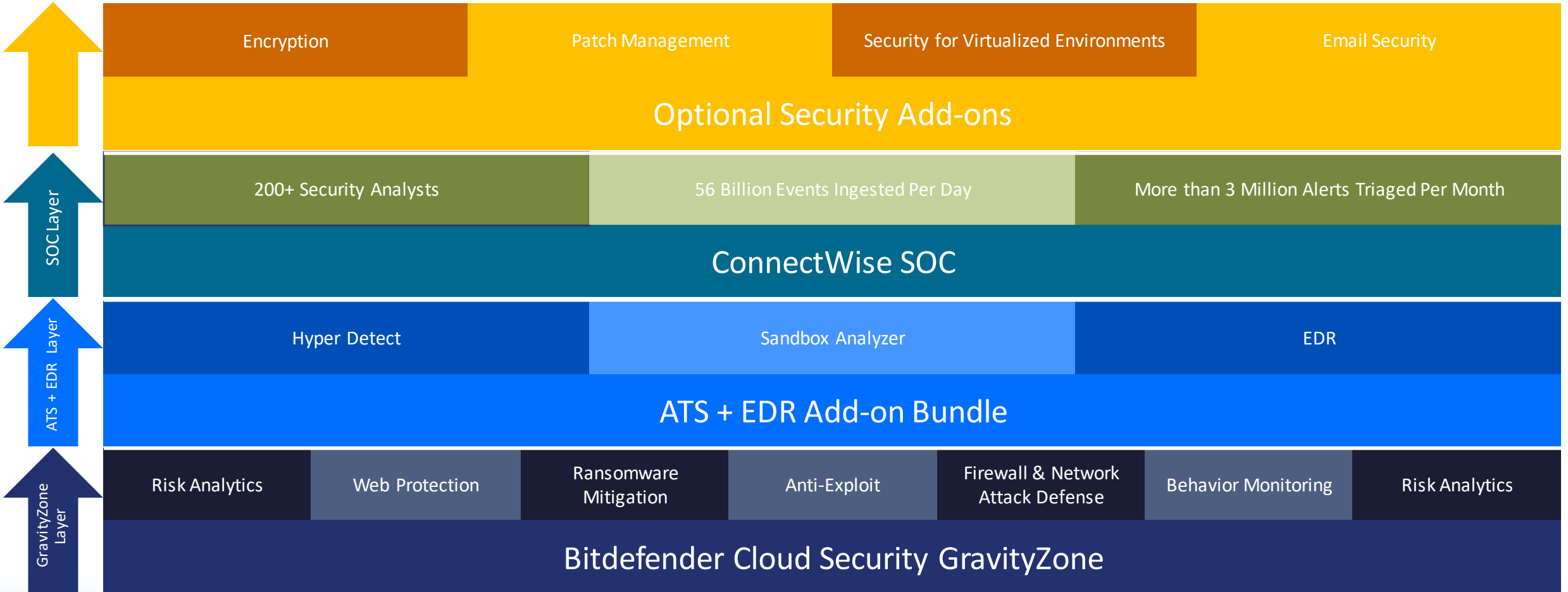
The Bitdefender Platform

Bitdefender®



The Bitdefender Platform

Bitdefender®



- More
- Network
- Patch Inventory
- Installation Packages
- Tasks
- Tags Management
- Risk Management
- Security Risks
- Companies View
- Policies**
- Configuration Profiles
- Assignment Rules
- Integrity Monitoring Rules
- Reports
- Ransomware Activity
- Integrity Monitoring Events
- Quarantine

- General
- Antimalware
- Sandbox Analyzer
- Firewall
- Network Protection**
- General
- Content Control**
- Web Protection
- Network Attacks
- Patch Management
- Device Control
- Integrity Monitoring
- Relay
- Exchange Protection
- Encryption
- Incidents Sensor

Back

Web Access Control Settings

Scheduler Categories Exclusions

Web Rules

Block All | Allow All

Ads:	Allow	News:	Allow
Advice:	Allow	Occult:	Block
Alcohol:	Block	Online Dating:	Allow
Astrology:	Allow	Online Payment:	Allow
Auto:	Allow	Online Photo:	Allow
Blogs:	Allow	Online Shopping:	Allow
Business:	Allow	Pets:	Allow
Computers and Software:	Allow	Pharmacy:	Block
Education:	Allow	Pornography:	Block
Entertainment:	Allow	Portals:	Allow
File Sharing:	Allow	Radio Music:	Allow

Save Cancel

- Assessment Rules
- Integrity Monitoring Rules
- Reports
 - Ransomware Activity
 - Integrity Monitoring Events
- Quarantine
 - Computers and VMs
 - Exchange Servers
- Companies
 - Custom Fields
- Accounts
 - User Activity
- Sandbox Analyzer**
 - Manual Submission
- Email Security
- Configuration

Sandbox Analyzer

Submit a sample

Search:

Search sample name or hash

Search

ConnectWise SOC Sandbox

Hide filters

Analysis Result

- Clean
- Infected
- Unsupported

Severity Score



High Medium Low

From 100 to: 0

Submission Type

- Manual
- Endpoint Sensor

Submission Status

- Finished
- Pending Analysis
- Failed

ATT&CK Techniques (0 selected)

About

Search MITRE tag

- Abuse Elevation Control Mechanism: Bypass ...
- Access Token Manipulation: Create Process wi...
- Access Token Manipulation: Parent PID Spoofi...
- Accessibility Features

9 FEB 2023

Manual submission for ConnectWise SOC Sandbox

Clean

ULPAIGYKRIJA.7z

Manual submission at 15:52, 09 Feb 2023

Severity Score: 0

Files and Processes Involved: 3

Submitted from N/A

Environment: Cloud Sandbox

View

MD5: ULPAIGYKRIJA.7z - N/A

ATT&CK Techniques: Discovery - Query Registry ... Delete Entry

8 FEB 2023

Manual submission for ConnectWise SOC Sandbox

Clean

ConnectWise-assessment-utility_TKN4a279...

Severity Score:

Files and Processes

Submitted from

Environment:

View

FILE INFO

Threat Analysis:



No threat detected



ULPAIGYKRIJA.7z

The sample writes additional files on the system, which may be used in various ways, including ensuring persistence. The new files can be executables that continue the sample's actions or storage/configuration files that hold viable information for the sample.

[Copy MD5](#) | [Copy SHA256](#) | [View in VirusTotal](#)

SUBMISSION DETAILS

General info

Filename	ULPAIGYKRIJA.7z
Command Line	%PROFILE%\downloads\ULPAIGYKRIJA.7z
File Type	7z [archive]
File Size	112602 bytes
MD5	c080233fd8ce9e5cfe26a1b7ee6fb60b
SHA1	05b110de624652f203a7fa58cd9cb567f2f300e7
SHA256	c7aef54c550778bb70654773eb1671c185c614d87cacb2072e7657b6f527e590
SHA512	93dd6fd378fcc055fb1f24283a9eecf1a19a54002debc03b1b92a236f814f2fde58a91bff2db98d3402b1d17cf5cc90a4d472aea45f34146791ed7375009ae40
CRC32	308A20B
Submission Time	09.02.2023, 23:52:26
Analysis Time	5.87m

DETECTIONS

No threat detected

- Monitoring
- Dashboard
- Executive Summary
- Incidents**
 - Blocklist
 - Search
 - Custom Rules
- Threats Xplorer
- Network
 - Patch Inventory
 - Installation Packages
 - Tasks
 - Tags Management
- Risk Management
 - Security Risks

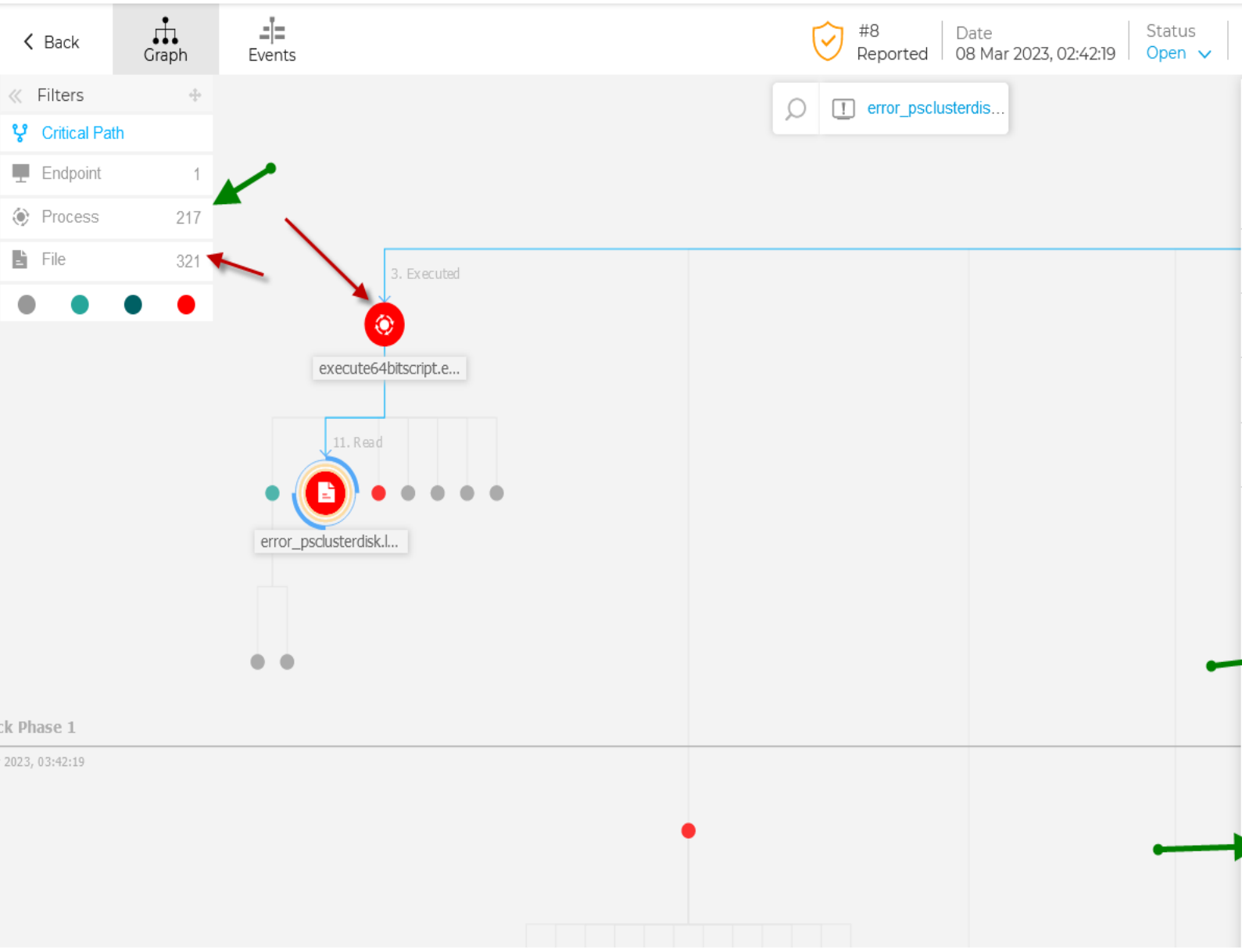
Extended Incidents Endpoint Incidents Detected Threats

Change Status Alert name Search for filenames, IP addresses, hostnames ...

ID	Date	Status	Severity Score	Priority	Action tak...	Company	Endpoint	Ale...	Assigned to
<input type="checkbox"/> Search..	Select...	Open, Investiga	100-30	Choose...	Choose...	All Compar	Search...		All Users
<input type="checkbox"/> #8	Updated at 10:00 on 8 Mar	Open	64	Unassigned	Reported	Autobros	JOOM	155	Unassigned
<input type="checkbox"/> #7	Updated at 02:27 on 8 Mar	Open	64	Unassigned	Reported	Autobros	JOOM	722	Unassigned
<input type="checkbox"/> #6	Updated at 08:45 on 6 Mar	Open	64	Unassigned	Reported	Autobros	SENSOR001	137	Unassigned
<input type="checkbox"/> #5	Updated at 01:57 on 6 Mar	Open	64	Unassigned	Reported	Autobros	SENSOR001	669	Unassigned
<input type="checkbox"/> #4	Updated at 11:45 on 4 Mar	Open	64	Unassigned	Reported	Autobros	SENSOR001	785	Unassigned
<input type="checkbox"/> #3	Updated at 07:59 on 2 Mar	Open	64	Unassigned	Reported	Autobros	SENSOR001	6	Unassigned
<input type="checkbox"/> #2	Updated at 07:12 on 2 Mar	Open	64	Unassigned	Reported	Autobros	SENSOR001	739	Unassigned
<input type="checkbox"/> #1	Created at 08:44 on 28 Feb	Open	67	Unassigned	Reported	Autobros	DESK-001	2	Unassigned
<input type="checkbox"/> #2	Updated at 13:33 on 20 Feb	Open	50	Unassigned	Reported	The Crafty G...	SOC-WINDOW...	5	Unassigned

9 items First Page < 1 of 1 > Last Page Show 20

- Monitoring
- Dashboard
- Executive Summary
- Incidents**
- Blocklist
- Search
- Custom Rules
- Threats Xplorer
- Network
- Patch Inventory
- Installation Packages
- Tasks
- Tags Management
- Risk Management
- Security Risks
- Companies View
- Policies
- Control Center
- More Profiles



#8 Reported | Date 08 Mar 2023, 02:42:19 | Status Open | Assignee Unassigned | Priority Unassigned

- Filters
- Critical Path
 - Endpoint 1
 - Process 217
 - File 321

error_psclusterdis...

error_psclusterdisk.log
File

ALERTS
1
File detected as **MALWARE** by analysis
Gen:Illusion.Veyron.16.3010100

INVESTIGATION
Network Presence
2 endpoints | First Seen On: 28 Feb 2023, 10:26

Further Analysis
Sandbox Analysis completed
[View Sandbox Analyzer Report](#)
VirusTotal | Google

REMEDIATION
No actions taken
Fix & Remediate
[Quarantine file](#)
Prevent
[Add file to Blocklist](#) [Add file as exception](#)

EDR/MDR

SentinelOne



IT NATION™ **SECURE**

ADVANCED SECURITY SERVICES

ConnectWise MDR

Powered by



Features and Benefits

Complete endpoint protection with 24/7 SOC services to detect, mitigate and remediate threats.

- Detect known and unknown threats leveraging the latest behavior-based technology
- Gain visibility into the root causes and origins of the threats, reverse the malicious operations of ransomware, and remediate them quickly

How ConnectWise MDR™ Works

Protect

Detect

Respond

Recover



Workstations
& Servers

WFH Employees

Cloud

Event
Logs

Analysis

SOC

contain and
Isolate Threats

SOC

Remediation

Recovery

Partner
Service
Desk

Approvals

End
Customer

- Containment: Stopping all processes related to the threat, encrypting and quarantining the threat and its executables.
- Isolation: Disconnecting from the network to prevent spread of malicious activity.
- Remediation: Deleting files and system changes created by the threat.
- Recovery: Restoring files and configurations that the threat had changed.

TECHNOLOGY

PEOPLE

PROCESS

SentinelOne: Industry Leading EDR



Platform ▾ Why SentinelOne? ▾ Services ▾ Partners ▾ Resources

SentinelOne is ranked #1 in MITRE Engenuity™ ATT&CK® Evaluation 2022 🏆

Want to learn why? 📍

#1 Again. The XDR Leader.

SentinelOne leads in the latest MITRE ATT&CK Evaluation with 100% prevention

- Leading analytic coverage.
- Leading visibility.
- Zero detection delays.

[GET A DEMO >](#)

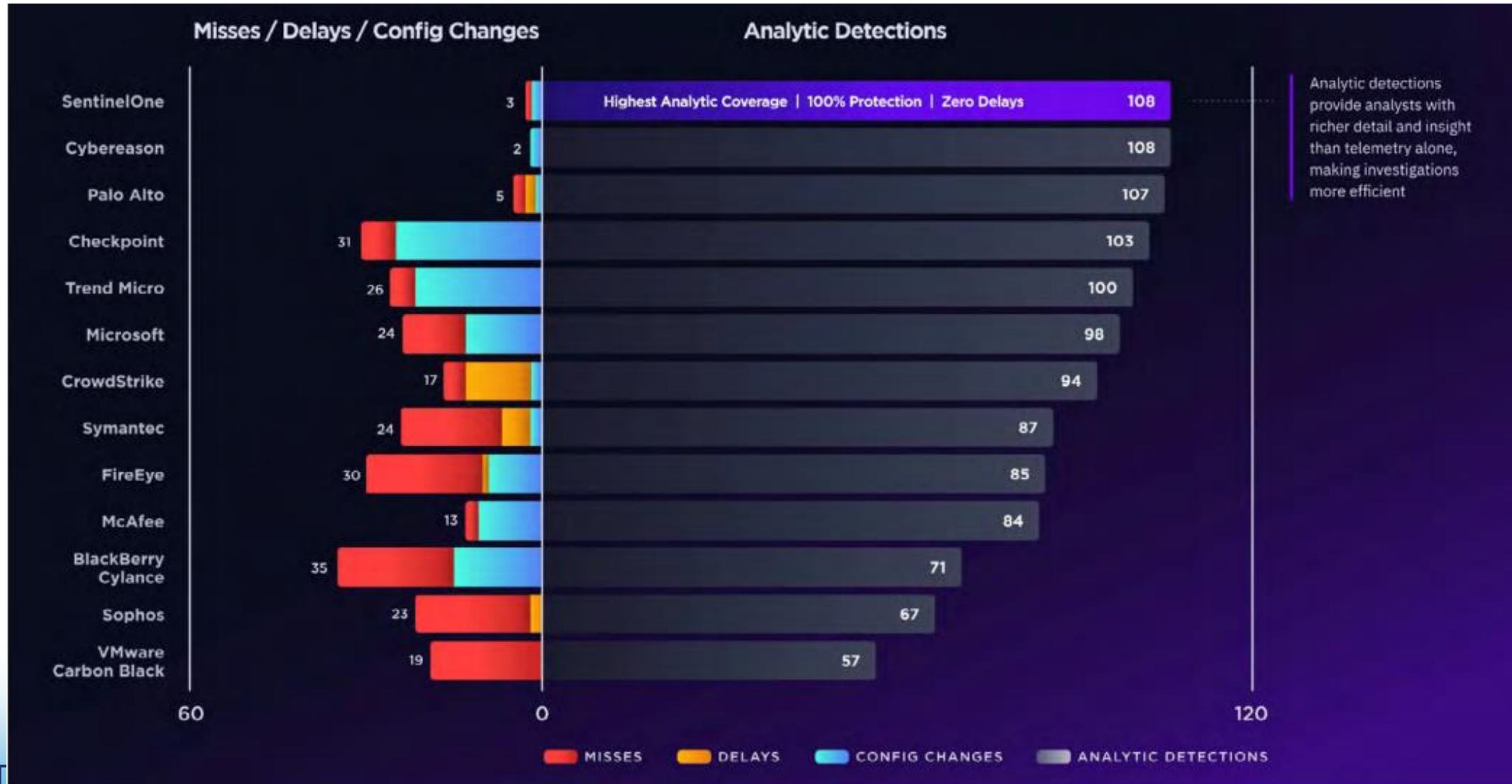


Wizard Spider & Sandworm 2022

Analytic Detections



SentinelOne: MITRE ATT&CK Evaluation Leader!



S1 Control

Provides security suite features to support agent consolidation



Firewall for all OSes



Bluetooth & BLE Control



Full Remote Shell for all OSes



USB Device Control



Unpatched Apps



ONE One Agent & Console



MITRE ATT&CK

S1 Complete EDR

Adds Deep Visibility™ Endpoint Detect & Respond

EDR Differentiators

- ✓ Combines enterprise features + ease-of-use
- ✓ Deeply coupled with Prevention enforcement
- ✓ MITRE ATT&CK™ technique searching
- ✓ ActiveEDR™ mark entire story as threat
- ✓ Built for massive data retention, scale, performance



ONE One Agent & Console










MITRE ATT&CK™

SENTINELS ENDPOINTS TAGS POLICY BLACKLIST EXCLUSIONS NETWORK CONTROL DEVICE CONTROL PACKAGES UPGRADE POLICY ACCOUNT INFO

Select filters... 

Load Filter Save Filter

Actions Group No Items Selected 50 Endpoints 50 Results Columns Export

<input type="checkbox"/>	Endpoint Name	Endpoint Tags	Account	Site	Last Logged In User	Group	Domain
<input type="checkbox"/>	 Tanja's MacBook Pro <small>Pending request</small>	N/A	TAM-DEMO	CarNet, Inc	Tanja	Default Group	N/A
<input type="checkbox"/>	 LAPTOP-4UVG6TP5	GM TEst : Key	TAM-DEMO	Flat Top Gym	njp61	Back Office	WORKGRO
<input type="checkbox"/>	 DESKTOP-Q3RPM5N	N/A	TAM-DEMO	Rich Training	icpou	Default Group	WORKGRO
<input type="checkbox"/>	 DESKTOP-9BH8KJ7	N/A	TAM-DEMO	ATX (Deleted)	hjmrt	Default Group	WORKGRO
<input type="checkbox"/>	 DESKTOP-0SIQPI6	N/A	TAM-DEMO	Dunder Mifflin	sentinel	Default Group	WORKGRO
<input type="checkbox"/>	 vmanage2	N/A	TAM-DEMO	SDConsulting	N/A	Manage Servers	WORKGRO
<input type="checkbox"/>	 vcontrol	N/A	TAM-DEMO	SDConsulting	N/A	Default Group	WORKGRO





APPLICATIONS

Beta



Select filters...



Low (0)
 Medium (0)
 High (1)
 Critical (9)
 No known risk (4,367)

10 applications 50 Results [Export](#)



Type	Name	Endpoint	Risk	Installed Date	Version	Publisher	Size
App	openssl	awkwardmc	Critical	Apr 26, 2023 2:25 AM	3.0.2-0ubuntu1.9	Ubuntu Developers <ubuntu-...	2.00 MB
App	openssl	TCG-JELLYFISH	Critical	Apr 25, 2023 4:12 PM	3.0.2-0ubuntu1.9	Ubuntu Developers <ubuntu-...	2.00 MB
App	Microsoft SQL Server 2016 (...)	gjs-z6-g4	Critical	Nov 11, 2020 2:13 PM	N/A	Microsoft Corporation	N/A
App	Veeam Backup & Replication	gjs-z6-g4	Critical	Nov 11, 2020 2:23 PM	10.0.1.4854	Veeam Software Group GmbH	N/A
App	VLC media player	HParks-PC	Critical	Oct 11, 2020 3:48 PM	2.2.4	VideoLAN	120.41 KB
App	Microsoft SQL Server 2019 (...)	mssql	Critical	Aug 31, 2021 1:50 PM	N/A	Microsoft Corporation	N/A
App	Microsoft SQL Server 2016 (...)	vspc	Critical	Mar 29, 2022 9:53 AM	N/A	Microsoft Corporation	N/A
App	Microsoft SQL Server 2019 (...)	vmanage2	Critical	Jul 20, 2020 3:29 PM	N/A	Microsoft Corporation	N/A



Threat Status: MITIGATED

AI Confidence Level: MALICIOUS

Analyst Verdict: True Positive

Incident Status: Resolved



Identified Time May 12, 2023 13:49:28

Reporting Time May 12, 2023 13:49:28

Mitigation Actions taken: KILLED 100/100 QUARANTINED 11/11 REMEDIATED 84/84 ROLLED BACK 259/260

NETWORK HISTORY

First seen May 12, 2023 13:49:28
Last seen May 12, 2023 13:49:28

Only 1 time on the current endpoint
1 Account / 1 Site / 1 Group

Find this hash on Deep Visibility
[Hunt Now](#)

THREAT FILE NAME ExchangeRates2.ods

[Copy Details](#) [Download Threat File](#)

Path	\Device\HarddiskVolume2\S1DemoToolkit\Demo01\E...
Command Line Arguments	"-o" "C:\S1DemoToolkit\Demo01\ExchangeRates2.ods...
Process User	DESKTOP-3JCFUPD\sentinel
Publisher Name	N/A
Signer Identity	N/A
Signature Verification	NotSigned
Originating Process	soffice.exe
SHA1	0e03e2f71d07f5ab21720088858595d42bf1eec5

Initiated By	Agent Policy
Engine	Documents, Scripts
Detection type	Dynamic
Classification	Ransomware
File Size	15.46 KB
Storyline	C7A1D3266FBE433C
Threat Id	1683467534080618876

ENDPOINT

Real-time data about the endpoint:

DESKTOP-3JCFUPD
TAM-DEMO / Flat Top Gym / Test Group

At detection time:

Scope TAM-DEMO / Flat Top Gym / Test Gr
OS Version Windows 10 Enterprise Evaluation 19
Agent Version 21.7.5.1090

THREAT INDICATORS (13)

NOTES

XDR

Infostealer

Chrome's sensitive information was accessed
MITRE : Credential Access [T1555.003][T1552.001]

Post Exploitation

Process attempted to export a certificate on ADFS server
MITRE : Credential Access [T1606.002]
MITRE : Resource Development [T1588.004]

Evasion

A new root certificate was added
MITRE : Defense Evasion [T1553.004]

Process tampered with the Event Viewer logs
MITRE : Defense Evasion [T1070.001][T1562.001][T1562.002]

Indirect command was executed
MITRE : Defense Evasion [T1218][T1202]

General

Powershell execution policy was changed
MITRE : Execution [T1059.001]

User logged on
MITRE : Persistence [T1078]
MITRE : Defense Evasion [T1078]
MITRE : Privilege Escalation [T1078]
MITRE : Initial Access [T1078]





Threat Status: MITIGATED

AI Confidence Level: MALICIOUS

Analyst Verdict: True Positive

Incident Status: Resolved



Identified Time May 12, 2023 13:49:28

Reporting Time May 12, 2023 13:49:28

Mitigation Actions taken: KILLED 100/100 QUARANTINED 11/11 REMEDIATED 84/84 ROLLED BACK 259/260

Processes

DESKTOP-3JCFUPD

Search Process

Process	Pid	Date
soffice.bin (Exch...	2492	May 12, 2023 16:48:25
conhost.exe	980	May 12, 2023 16:48:26
cmd.exe (dtk.bat)	7664	May 12, 2023 16:48:26
forfiles.exe (dtk.b...	2192	May 12, 2023 16:48:26
cmd.exe (CLI inte...	8740	May 12, 2023 16:48:27
findstr.exe	6964	May 12, 2023 16:48:27
reg.exe (CLI inter...	7132	May 12, 2023 16:48:27

1 2 3 4 5 6

Export 38%



Load more (5/12)

Load more (5/50)

Showing all events for the current threat

Go to root

- All Events 700
- Files 494
- Registry 1
- Network Actions 4
- Processes 100
- Indicators 101

700 Items 50 Results Columns Export

Object Type	Event Type	Time	Attribute					
indicators	Behavioral Indicators	May 12, 2023 16:48:24	Indicator Name Remote Memory Free	Indicator Description N/A	Target Process Name lsass.exe	Target Process UID 762F21B16F216EF7	Source Process Name soffice.bin (ExchangeRate...	Source Process UID 63DECEE2C1CBC1
ip	IP Connect	May 12, 2023 16:48:24	Source IP 10.0.2.15	Source Port 50592	Destination IP 104.21.81.147	Destination Port 443	Protocol tcp	Source Process Name soffice.bin (Exchang
file	File Rename	May 12, 2023 16:48:24	Full Path \\registrymodifications.xcu	SHA1 037a03dbb7eef8b55463...	Source Process Name soffice.bin (ExchangeRate...	Source Process UID 63DECEE2C1CBC17E	Verified Status NotSigned	File Size 113071
file	File Rename	May 12, 2023 16:48:24	Full Path \\registrymodifications.xcu	SHA1 037a03dbb7eef8b55463...	Source Process Name soffice.bin (ExchangeRate...	Source Process UID 63DECEE2C1CBC17E	Verified Status NotSigned	File Size 113071
file	File Modification	May 12, 2023 16:48:24	Full Path \\registrymodifications.xcu	SHA1 037a03dbb7eef8b55463...	Source Process Name soffice.bin (ExchangeRate...	Source Process UID 63DECEE2C1CBC17E	Verified Status NotSigned	File Size 113071
file	File Creation	May 12, 2023 16:48:24	Full Path \\registrymodifications.xcu	SHA1 037a03dbb7eef8b55463...	Source Process Name soffice.bin (ExchangeRate...	Source Process UID 63DECEE2C1CBC17E	Verified Status NotSigned	File Size 113071
file	File Deletion	May 12, 2023 16:48:24	Full Path \\ExchangeRates20.ods	SHA1 d5eb50a5198410a8806f...	Source Process Name soffice.bin (ExchangeRate...	Source Process UID 63DECEE2C1CBC17E	Verified Status NotSigned	File Size 15322
file	File Deletion	May 12, 2023 16:48:24	Full Path \\lu249214ze5.tmp	SHA1 d5eb50a5198410a8806f...	Source Process Name soffice.bin (ExchangeRate...	Source Process UID 63DECEE2C1CBC17E	Verified Status NotSigned	File Size 15322
file	File Creation	May 12, 2023 16:48:24	Full Path \\ExchangeRates2.ods	SHA1 0e03e2f71d07f5ab21720...	Source Process Name soffice.bin (ExchangeRate...	Source Process UID 63DECEE2C1CBC17E	Verified Status NotSigned	File Size 15831
file	File Modification	May 12, 2023 16:48:24	Full Path \\lu249214zeb.tmp	SHA1 0e03e2f71d07f5ab21720...	Source Process Name soffice.bin (ExchangeRate...	Source Process UID 63DECEE2C1CBC17E	Verified Status NotSigned	File Size 15831



Threat Status: MITIGATED | AI Confidence L

Mitigation Actions taken: KILLED 102/102



Identified Time Apr 28, 2023 14:37:47

Reporting Time Apr 28, 2023 14:37:47


NETWORK HISTORY

First seen Apr 28, 2023 14:37:47
Last seen Apr 28, 2023 14:37:47


THREAT FILE NAME ExchangeRates2.ods

Path \Device\HarddiskVo
Command Line Arguments "-o" "C:\S1DemoTool
Process User DESKTOP-3JCFUPD
Publisher Name N/A
Signer Identity N/A
Signature Verification NotSigned
Originating Process soffice.exe
SHA1 30851f054cff19faabd8368d36d5f4ad2f08ffdd


Mitigation Actions




KILL
Stops all processes related to the threat



QUARANTINE
Encrypts and moves the threat and its executables




REMEDiate
Deletes all files and system changes created by the threat



ROLLBACK
Restores files and configurations that the threat changed

Mark as Resolved
 Add to Blacklist

 This action will apply only on this threat

* Analyst verdict: True Positive Suspicious

Apply

ENDPOINT

Real-time data about the endpoint:

At detection time:

NOTES

XDR

78]
[T1078]
on [T1078]
078]
Powershell execution policy was changed
MITRE : Execution [T1059.001]
Persistence
Application registered itself to become persistent
MITRE : Persistence [T1547.001]
MITRE : Privilege Escalation [T1547.001]
Application registered itself to become persistent via an autorun
MITRE : Persistence [T1547.001]
MITRE : Privilege Escalation [T1547.001]
Application registered itself to become persistent via scheduled task

Cybersecurity

ConnectWise Resources



IT NATION™ **SECURE**

ConnectWise Cybersecurity Center

<https://www.connectwise.com/cybersecurity-center>

Know the threat landscape, keep your customers and business safe



Cybersecurity Management Solutions



Our Philosophies



Trust Center



Partner Program



SOC Services



Education + Resources



Cybersecurity Management Solutions

No matter where you are in the cybersecurity services journey, ConnectWise offers the software, support, and solutions that are critical to protecting your clients and your business. Solutions are easy to deploy and

administer with licensing models that make sense for MSPs. Learn more about EDR, SIEM, risk assessment, cloud app security, security policy management, and a 24/7 SOC.

[Our Cybersecurity Solutions](#)

[Incident Response Service](#)

#ITNation



IT NATION

Partner Program Membership Levels

REGISTERED PARTNER Grow at your own pace



SELF-PACED JOURNEY

- Access to on demand education
- Brandable marketing assets
- Marketing automation platform
- Free fundamentals certification



STRATEGY

- Sales, marketing, tech readiness
- Optional internal assessment
- Implement CW cybersecurity/BCDR
- Pricing and bundling tips
- Free advanced certifications

ACCELERATE PARTNER Grow with expert guidance



MARKETING

- Dedicated marketing concierge
- Market Development Funds
- Earn Co-Op Funds on growth
- Ready to use campaigns and assets for clients & prospects
- Access to Subject Matter Experts for events



SALES

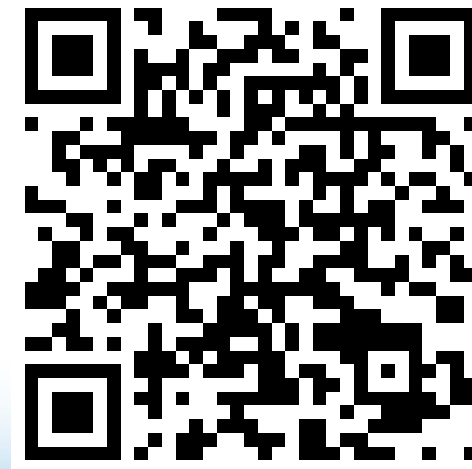
- Dedicated partner development manager
- Sales training for your team
- Sales framework coaching
- Access to pre-sales resources
- Co-Sell opportunities
- Sales debrief

Download the latest!



- Major MSP-focused hacks in 2022
- Emerging and continuing cyberattack trends
- Top ransomware methods of threat actors
- Action items for MSPs in 2023

<https://www.connectwise.com/resources/msp-threat-report-2023>



Next Steps

- Replace legacy AV with ConnectWise MDR
 - 24/7/365 monitored protection
 - Scale faster
- Leverage other features such as device control to close gaps
- Join the Partner Program
- Download the 2023 MSP Threat Report

—

Don't forget to fill out your

SESSION SURVEY

■

■

Q & A

Thank You

#ITNation

