Acronis

#CyberFit Academy
Cyber Protect Cloud

Cloud Tech Associate – Advanced Security + EDR (Endpoint Detection and Response)

#CyberFit

#CyberFit

Acronis

#CyberFit

Cyber Protect Cloud

Introductions

Meet your **Instructor**

Steve Brining

Cybersecurity Evangelist – Cyber Protect

Tempe, Arizona (USA)

English

Steve.Brining@acronis.com

Steve honed his skills for over 25 years as a cybersecurity expert at PatchLink, McAfee, BeyondTrust and other technology companies. Mr. Brining holds a Masters in Business Administration in E-Business and Masters in Science in Technology and Innovation Management with specialization in Cybersecurity and is a Commanding Officer in the Arizona Army National Guard.

Learning Objectives

- The need for EDR
- Understand technical aspects of the Advanced Security Pack + EDR (Focus on the EDR portion)
- How to provision, setup and navigate EDR for a client

Course Modules

1. EDR Use Case
2. High Level Overview
3. What is EDR? How If Differs from Prevention Technologies
4. How Attacks Happen and How To Respond To Them
5. Challenges for Todays Security: The Need for EDR

Course Modules

6. MSP Challenges with Current EDR Solutions
7. Advanced Security + EDR Specific Overview: Problems Address by Advanced Security + EDR
8. How To Provision, Setup and Navigate

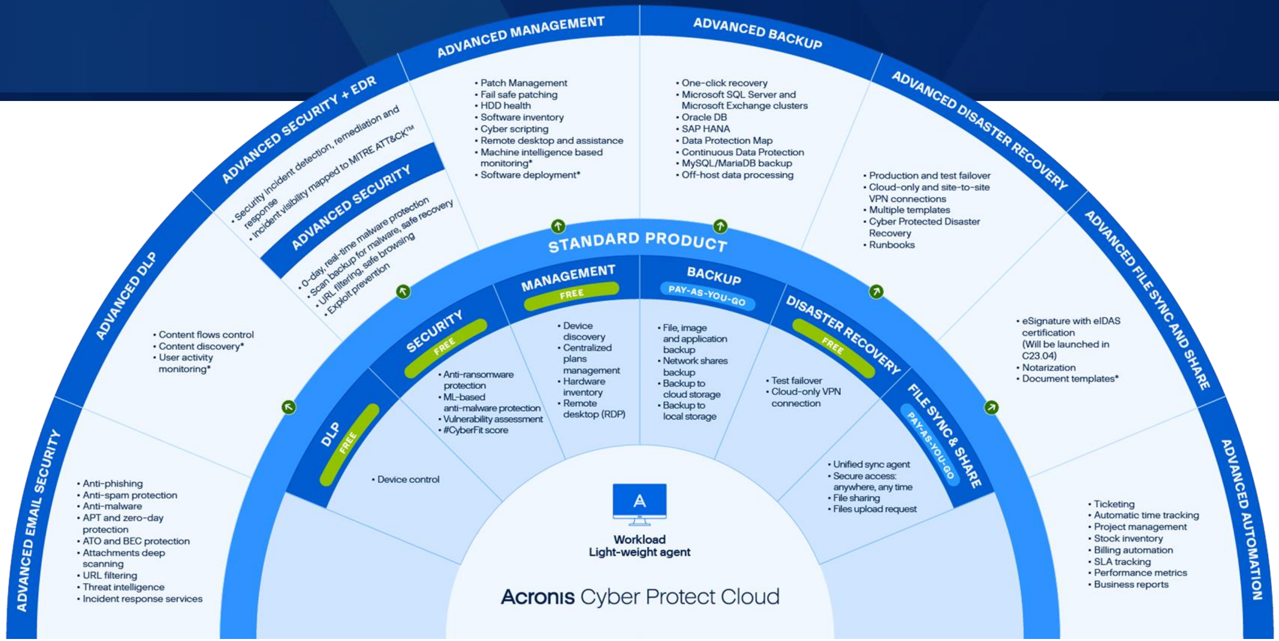
Acronis

#CyberFit

Cyber Protect Cloud

High Level Overview

Add advanced packs:
Security, Backup, Disaster Recovery, Email Security, File Sync and Share, Management, DLP, and **now EDR**



ADVANCED EMAIL SECURITY
- Anti-phishing
- Anti-spam protection
- Anti-malware
- APT and zero-day protection
- ATO and BEC protection
- Attachments deep scanning
- URL filtering
- Threat intelligence
- Incident response services

ADVANCED DLP
- Content flows control
- Content discovery*
- User activity monitoring*

ADVANCED SECURITY + EDR
- Security incident detection, remediation and response
- Incident visibility mapped to MITRE ATT&CK™

ADVANCED SECURITY
- 0-day, real-time malware protection
- Scan backup for malware, safe recovery
- URL filtering, safe browsing
- Exploit prevention

ADVANCED MANAGEMENT
- Patch Management
- Fail safe patching
- HDD health
- Software inventory
- Cyber scripting
- Remote desktop and assistance
- Machine intelligence based monitoring*
- Software deployment*

ADVANCED BACKUP
- One-click recovery
- Microsoft SQL Server and Microsoft Exchange clusters
- Oracle DB
- SAP HANA
- Data Protection Map
- Continuous Data Protection
- MySQL/MariaDB backup
- Off-host data processing

ADVANCED DISASTER RECOVERY
- Production and test failover
- Cloud-only and site-to-site VPN connections
- Multiple templates
- Cyber Protected Disaster Recovery
- Runbooks

ADVANCED FILE SYNC AND SHARE
- eSignature with eIDAS certification (Will be launched in C23.04)
- Notarization
- Document templates*

ADVANCED AUTOMATION
- Ticketing
- Automatic time tracking
- Project management
- Stock inventory
- Billing automation
- SLA tracking
- Performance metrics
- Business reports

STANDARD PRODUCT

DLP FREE
- Device control

SECURITY FREE
- Anti-ransomware protection
- ML-based anti-malware protection
- Vulnerability assessment
- #CyberFit score

MANAGEMENT FREE
- Device discovery
- Centralized plans management
- Hardware inventory
- Remote desktop (RDP)

BACKUP PAY-AS-YOU-GO
- File, image and application backup
- Network shares backup
- Backup to cloud storage
- Backup to local storage

DISASTER RECOVERY FREE
- Test failover
- Cloud-only VPN connection

FILE SYNC & SHARE PAY-AS-YOU-GO
- Unified sync agent
- Secure access: anywhere, any time
- File sharing
- Files upload request

Workload
Light-weight agent

Acronis Cyber Protect Cloud

* Coming soon

Optimize for every workload

Rapidly launch services

Consolidate vendors

Acronis

#CyberFit

Cyber Protect Cloud

EDR Use Case – Missed Patch / Forgot To Patch

Use Case EDR – Missed Patch/Forgot To Patch

Patch Preventing Attackers to Remotely Execute Code on Web Application Targeted Not Applied:

- Bad bug – can mess with system anywhere in the world
- Attacker performing reconnaissance
- Sent http request with malicious code tucked in content-type header
- Run queries to give better sense of some database structure and how many records
- SQL command to identify general details of data tables and select a sample of records from a database
- CWE of say Improper Input Validation as example

Use Case EDR – Missed Patch/Forgot To Patch

Patch Preventing Attackers to Remotely Execute Code on Web Application Targeted Not Applied:

- Next Stop: Upload “web shells” to gain access to a web server
- Positioned to collect credentials (thus access to back-end databases)
- (ex…Break into a building: easier to do if a resident leaves first floor window unlocked and you manage to steal employee IDs)

Use Case EDR – Missed Patch/Forgot To Patch

Patch Preventing Attackers to Remotely Execute Code on Web Application Targeted Not Applied:

- Next Stop: run series of SQL commands to find valuable data
- Getting that data is one thing: getting it undetected is another
- Store stolen data in temporary files (and if large compress and break into manageable sizes)
- Attacker keep transmissions small to avoid suspicion
- After exfiltrating, delete the compressed files to minimize the trail
- Attacker deep enough: could use existing encrypted communication channels to send queries and commands (look like normal activity)

Use Case EDR – Missed Patch/Forgot To Patch

Patch Preventing Attackers to Remotely Execute Code on Web Application Targeted Not Applied:

- Attacker setup many servers in many countries: use encrypted login protocols to mask involvement. Wipe server log files every day.
  - Access system via Swiss IP Address. Use stolen username and password for service account to get to a database.
  - Query database for specific info and store in output files
  - Create compressed file archive of results: copy to different directory and download
  - Data in hands of attacker: delete the archive
  - Perform over several weeks and get a lot of information to extort

Use Case EDR – Missed Patch/Forgot To Patch

Patch Preventing Attackers to Remotely Execute Code on Web Application Targeted Not Applied:

- Imagine patch not available (zero day) in this scenario: CVE could be in NIST NVD (attackers aware of issue)
- Items to ponder?
  - Sensitive fields plaintext stored or encrypted?
  - Databases segmented?
  - File integrity monitoring?
  - Using long-expired security certificates?

Use Case EDR – Missed Patch/Forgot To Patch

Patch Preventing Attackers to Remotely Execute Code on Web Application Targeted Not Applied:

- Imagine client data has high profile targets (CXX) and intelligence gathering (PII is leverage)

Acronis

#CyberFit

Cyber Protect Cloud

What is EDR? How It Differs From Prevention Technologies

What is EDR? How Differ From Prevention Technologies

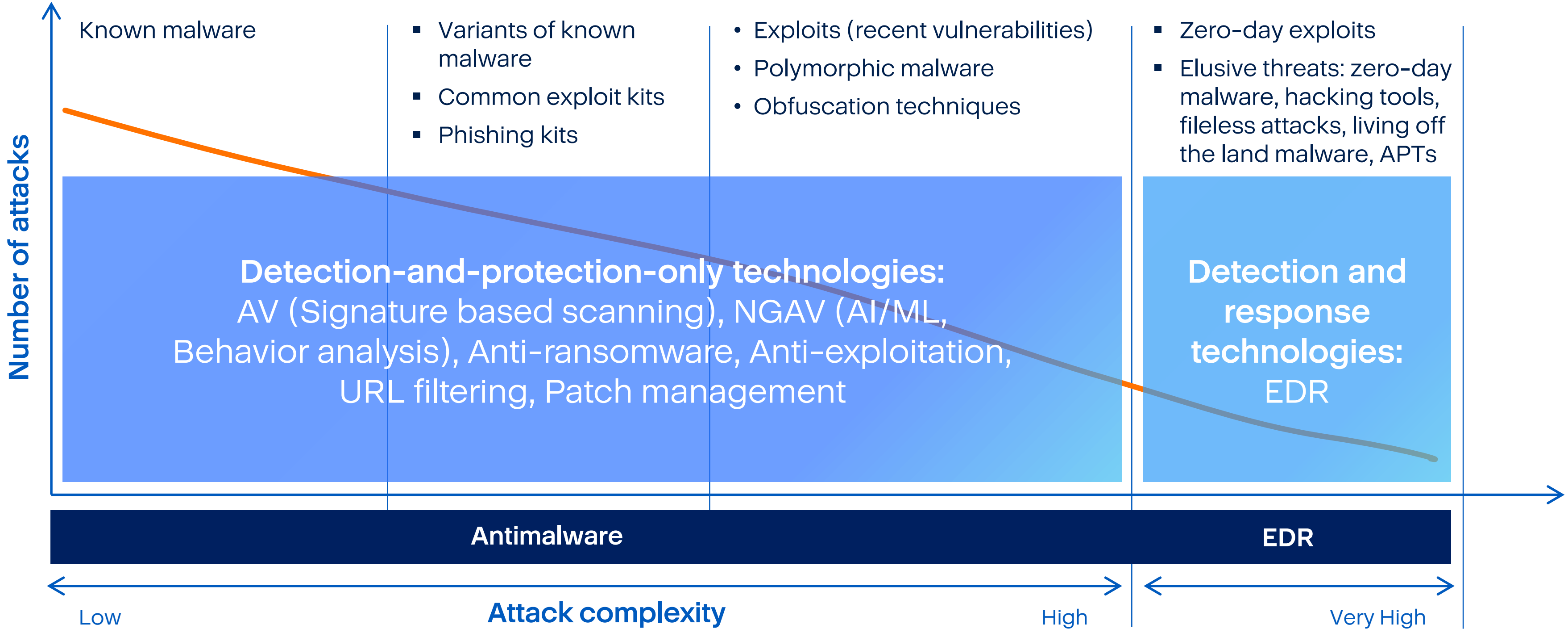
Event Correlation Security Platform

- **Capable of Identifying Advanced Threats or In-Progress Attacks**
  - Collects workload events
  - Correlates with machine learning and security analytic algorithms to highlight security incidents
- **Two Main Advantages**
  - Incident Investigation
  - Incident response (containment and remediation)
- **Records activities/events taking place on endpoints/workloads**
  - **Visibility to uncover incidents otherwise invisible**

Next step – Antimalware vs EDR

Category	Antimalware	EDR
Focus	Block/prevent attack	Post-incident detection and response
Detection Technology	Detects and stops **“known bad”** files, processes or behaviors	Detects **“intent”** by correlating a series of actions an attacker performs to be successful at achieving its objective
Visibility into attacks	Low – shows only detected and blocked threats.	High –broader scope of incidents and maps steps of the attack to show: • How did it get in? • How did it hide its tracks? • What did it harm? • How did it spread?
Response capabilities	Automatically blocks “known bad” processes and quarantines threats	Provides a multitude of response capabilities to: • Contain the incident at the endpoint • Investigate security incidents • Provide remediation

How EDR helps to protect against more threats



Known malware

- Variants of known malware
- Common exploit kits
- Phishing kits

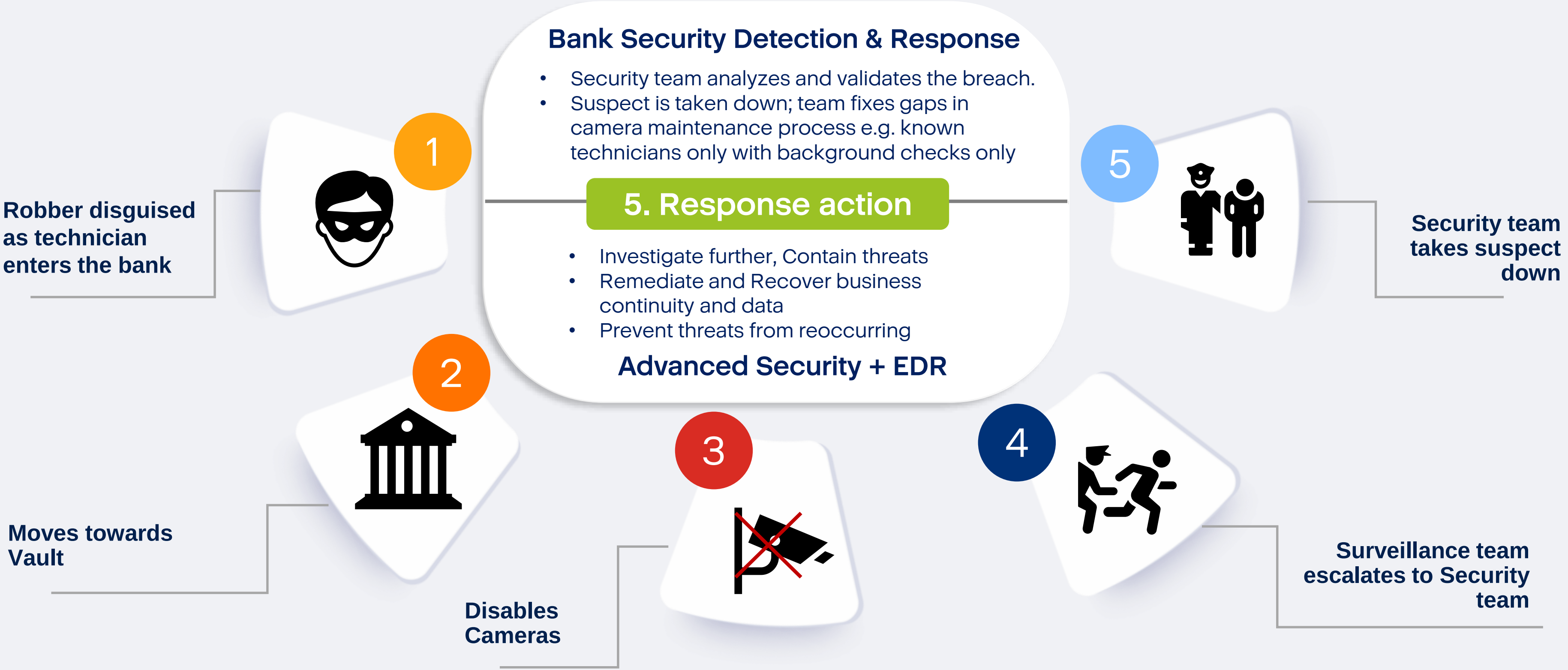
- Exploits (recent vulnerabilities)
- Polymorphic malware
- Obfuscation techniques

- Zero-day exploits
- Elusive threats: zero-day malware, hacking tools, fileless attacks, living off the land malware, APTs

Detection-and-protection-only technologies:
AV (Signature based scanning), NGAV (AI/ML, Behavior analysis), Anti-ransomware, Anti-exploitation, URL filtering, Patch management

Detection and response technologies:
EDR

Short EDR story – a bank robbery



Bank Security Detection & Response

- Security team analyzes and validates the breach.
- Suspect is taken down; team fixes gaps in camera maintenance process e.g. known technicians only with background checks only

5. Response action

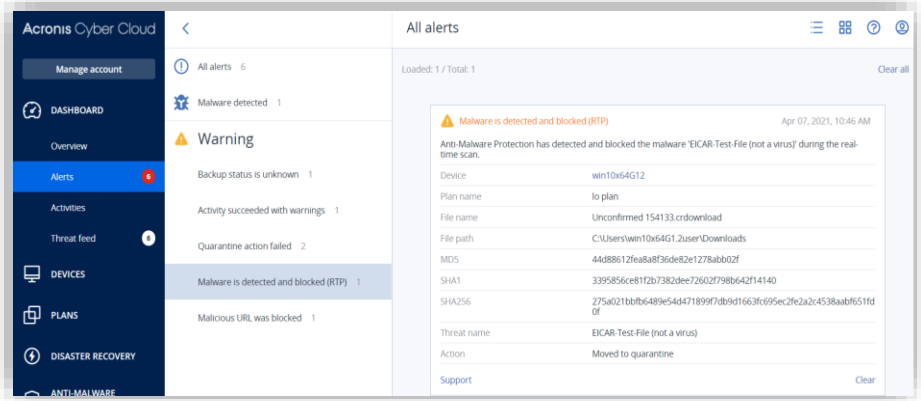
- Investigate further, Contain threats
- Remediate and Recover business continuity and data
- Prevent threats from reoccurring

Advanced Security + EDR

1. **Robber disguised as technician enters the bank**
2. **Moves towards Vault**
3. **Disables Cameras**
4. **Surveillance team escalates to Security team**
5. **Security team takes suspect down**

Better to Best

Advanced Security Pack



All alerts 6

Malware detected 1

Warning

Backup status is unknown 1

Activity succeeded with warnings 1

Quarantine action failed 2

Malware is detected and blocked (RTP) 1

Malicious URL was blocked 1

Loaded: 1 / Total: 1 Clear all

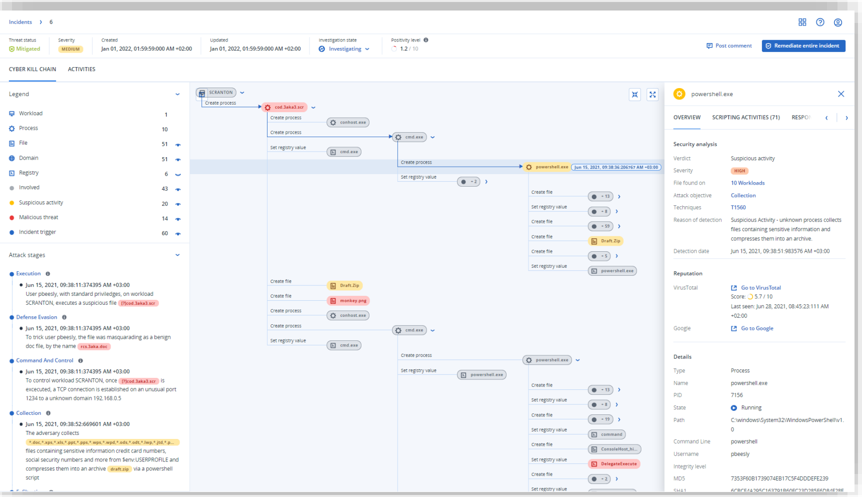
Malware is detected and blocked (RTP) Apr 07, 2021, 10:46 AM

Anti-Malware Protection has detected and blocked the malware 'EICAR-Test-File (not a virus)' during the real-time scan.

Device	win10x64G12
Plan name	lo plan
File name	Unconfirmed 154133.crdownload
File path	C:\Users\win10x64G1.2user\Downloads
MD5	44d88612fea8a8f36de82e1278abb02f
SHA1	3395856ce81f2b7382dee72602f798b642f14140
SHA256	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
Threat name	EICAR-Test-File (not a virus)
Action	Moved to quarantine

Support Clear

Advanced Security + EDR Pack



Threat status	Severity	Created	Updated	Investigation state	Positivity level
Mitigated	MEDIUM	Jan 01, 2022, 01:59:59:000 AM +02:00	Jan 01, 2022, 01:59:59:000 AM +02:00	Investigating	1.2 / 10

Legend

Workload	1
Process	10
File	51
Domain	51
Registry	6
Involved	43
Suspicious activity	20
Malicious threat	14
Incident trigger	60

Attack stages

Execution
- Jun 15, 2021, 09:38:11:374395 AM +03:00
  User pbeesly, with standard priviledges, on workload SCRANTON, executes a suspicious file [?]cod.3aka3.scr

Defense Evasion
- Jun 15, 2021, 09:38:11:374395 AM +03:00
  To trick user pbeesly, the file was masquarading as a benign doc file, by the name rcs.3aka.doc

Command And Control
- Jun 15, 2021, 09:38:11:374395 AM +03:00
  To control workload SCRANTON, once [?]cod.3aka3.scr is excecuted, a TCP connection is established on an unusual port 1234 to a unknown domain 192.168.0.5

Collection
- Jun 15, 2021, 09:38:52:669601 AM +03:00
  The adversary collects *.doc,*.xps,*.xls,*.ppt,*.pps,*.wps,*.wpd,*.ods,*.odt,*.lwp,*.jtd,*.p... files containing sensitive information credit card numbers, social security numbers and more from $env:USERPROFILE and compresses them into an archive draft.zip via a powershell script

powershell.exe

Security analysis

Verdict	Suspicious activity
Severity	HIGH
File found on	10 Workloads
Attack objective	Collection
Techniques	T1560
Reason of detection	Suspicious Activity - unknown process collects files containing sensitive information and compresses them into an archive.
Detection date	Jun 15, 2021, 09:38:51:983576 AM +03:00

Reputation

VirusTotal	Go to VirusTotal Score: 5.7 / 10 Last seen: Jun 28, 2021, 08:45:23:111 AM +02:00
Google	Go to Google

Details

Type	Process
Name	powershell.exe
PID	7156
State	Running
Path	C:\windows\System32\WindowsPowerShell\v1.0
Command Line	powershell
Username	pbeesly
Integrity level	
MD5	7353F60B1739074EB17C5F4DDDEFE239

#CyberFit Academy

#CyberFit

Section Summary

1 EDR collects workload events and uses data analytic techniques like AI and ML to detect suspicious system behavior. Two main advantages is incident investigation and incident response. A benefit is having visibility to uncover incidents otherwise invisible.

2 Prevention and detection work hand in hand and cover different parts of the threat landscape. While prevention is great at stopping attacks from starting, EDR uncovers the intention of an attacker analyzing benign and suspicious events. Every sequence of events is analyzed to understanding if the events might lead to bad intent.

Acronis

#CyberFit

Cyber Protect Cloud

How Attacks Happen and How To Respond To Them

How Attacks Happen and How To Respond

Reconnaissance	Gather information about the target
Weaponize	Create malware or malicious payloads
Delivery	Work on access/infecting first workload (Phishing email example)
Exploitation (Detonation)	Malicious code executed. Discover other devices connected to further infiltrate: learn more vulnerabilities
Installation	Privilege escalation. Install in network
Command and Control (C2)	Track, monitor and guide deployed “weapons” and tool stacks (Obfuscation or DoS). Move laterally
Action/Monetize	Execute objective (weeks/months). Data exfiltration, encryption, supply chain attacks, triple extortion

Incident investigation and response framework

Example:

1. Event classification

- Tier 1 Analyst **monitors** for events that merit attention:
  - User activity
  - Network events
  - Signals from security tools

EDR solutions do this automatically and create incidents, getting SP to step 3.

2. Prioritization, investigation and triage

- Tier 1 Analysts:
  - **prioritizes** the most important alerts:
  - **investigates** them
- True security incidents are passed to Security team

EDR solutions do this automatically and create incidents, getting SP to step 3.

3. Containment and recovery

- During a true security incident, the race is on to:
  - Gather data to **identify the source** of the attack
  - **Contain it**
  - **Recover data and restore system operations**.

Most EDR solutions can contain but none have true data recovery capabilities

4. Prevention of additional attacks

- Security staff work to:
  - **Identify** broad **security gaps** related to the attack
  - Plan **mitigation steps to prevent additional attacks**.

5. Assessment and audit

- SP staff must:
  - Asses attack evolution
  - Determine mitigation steps
  - Gather additional forensic data
  - Draw final conclusions and recommendations

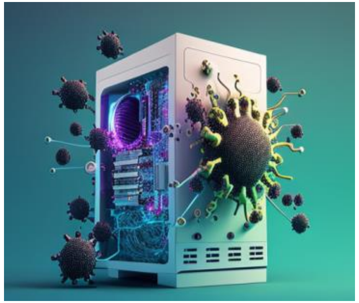
Acronis

#CyberFit

Cyber Protect Cloud

Challenges for Todays Security: The Need for EDR

The need for EDR



Advanced attacks can only be countered with advanced security

More than 60% of breaches **involve some form of hacking**

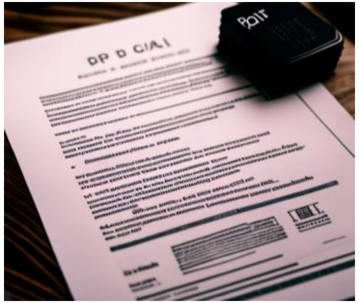
On average, it takes organizations **207 days to** identify a breach

Addressing breach impact is inevitable to ensure continuity

70 days to contain a breach

USD 4.35 million – average total cost of a data breach

76% of security and IT teams struggle with **no common view** over applications and assets



For many – compliance is essential

Regulations require organizations to **report security incidents** within a strict time-frame – e.g. 72 hours for GDPR

70% of breaches involve PII (post-incident analysis required for reporting for regulatory purposes)

Sources: “Data Breach Investigations Report’, Verizon, 2022”; “Cost of data breach report”, 2022, IBM Security & Ponemon Institute; “Costs and Consequences of Gaps in Vulnerability Response,” ServiceNow, 2020, Investigation or Exasperation? The State of Security Operations”, iDC

The Need for EDR

Prevention alone cannot ensure 100% protection from advanced threats

When prevention fails, SPs can be left in the dark by existing endpoint security solution.

Attackers take advantage of situation to move inside the network

Adversaries can be inside your network for weeks and return

Due to silent failure of prevention layers, attackers often create back doors (allow to return at will)

Most cases: SPs learns about breach from third party, such as law enforcement, clients or suppliers

SPs lack the visibility needed to effectively monitor workloads

Incident is finally discovered, SP can spend months trying to remediate incident -- Lacks visibility required to see and understand exactly what happened, how it happened and how to fix it — only to see attacker return within a matter of days

Access to actionable intelligence is needed to respond to an incident

If vendor fails to fully scope an incident, remediation effort may fail to eradicate an attacker’s foothold in environment

Inappropriate remediation can be protracted and costly

SPs can spend weeks trying to discern what actions to take

MSPs need wide pallet of investigation, remediation and (disaster) recovery actions to restore business operations fast and prevent future attacks

Section Summary

1 Attackers run attacks in certain steps to achieve objectives. When incidents happen service providers need a resilience plan. Threats are becoming more frequent and complex (requiring advanced security controls). Compliancy is another driver: many impose strict requirements to responsd to security incidents.

2 Attackers often create backdoors to be able to return at will. When incidents get uncovered, time is not on your side and can take awhile to scope and remediate an incident.

Acronis

#CyberFit

Cyber Protect Cloud

SP Challenges with Current EDR Solutions

MSP challenges with current EDR solutions

Existing EDR solutions require a high-level of security expertise – e.g. SOC team or MDR services

Lack of security professionals, especially in MSP space

- Cybersecurity workforce gap is 3.1 million
- 84% of organizations are experiencing **security skills shortage**
- Security analysts are hard to find and expensive

MDR or SOC as-a-service is expensive

- **$5-10 mil/year** to build a SOC team
- Majority of MSP don't use MDR, nor do they have a SOC team

Incident analysis is time consuming

- EDR products by nature are creating alert fatigue
- **2 - 6 hours per incident** for security analysts to investigate
- High cost for MSPs
- **32 hours** to contain an incident, **120 hours** to recover business operations

Compliance forces MSPs to report breaches within a strict timeframe

- Compliance forces MSPs to report incident to clients within a strict timeframe (e.g. 72 hours for GDPR)
- If MSPs don't understand or validate incidents, they will be **forced to abandon** the product

Few EDR vendors with MSP management capabilities

- Bitdefender, ESET, Sophos, SentinelOne present in the MSP space
- Only a few have **MSP-management platform capabilities**

What makes a good EDR solution?

1-10-60 rule, according to security professionals and researchers

	Detect	Investigate	Respond
Ideal	< 1 min	< 10 min	< 60 min
Reality	Detection times are hard to measure	Investigation takes 2-6 hours for skilled security staff	Over 32 hours for containment Over 120 hours for business recovery

Crowdstrike: global-security-attitude-survey-takeaways-2019, Splunk: sec-conf2019, Acronis surveys

Section Summary

1 With the shortage of qualified cyber security professionals, this is a challenge for SP's. Even with staff, incident investigation can be time consuming due to manual investigative work. Compliancy forces SP's to report breaches with strict timelines.

2 When an attack is in progress, you have an average of one minute to detect, 10 minutes to understand/investigate it and one hour to contain it (1-10-60 rule). In reality these timelines are not met and thus one needs a solution that is fast, easy and efficient to use.

Acronis

#CyberFit

Cyber Protect Cloud

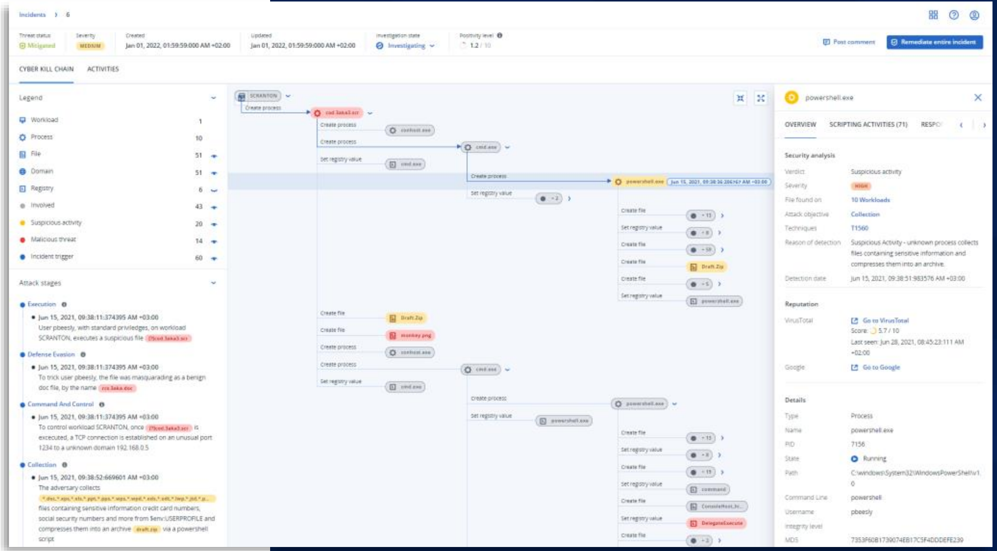
Advanced Security + EDR

Specific Overview: Problems Addressed

Advanced Security + Endpoint Detection and Response (EDR)

DETECT, and **RESPOND** to advanced attacks that sneak past other endpoint defenses with minimal investigation efforts and with pre-integrated **IDENTIFY, PROTECT**, and **RECOVER** capabilities.

- ✓ **Continuity at the speed of business** with protection across NIST, including recovery & backup
- ✓ **Minutes-not-hours detection and incident analysis** across MITRE ATT&CK®
- ✓ **Rapid turn-on and scale** with an SP-class platform


Incidents › 6

Threat status: Mitigated | Severity: MEDIUM | Created: Jan 01, 2022, 01:59:59:000 AM +02:00 | Updated: Jan 01, 2022, 01:59:59:000 AM +02:00 | Investigation state: Investigating | Positivity level: 1.2 / 10

CYBER KILL CHAIN | ACTIVITIES

Legend

Workload	1
Process	10
File	51
Domain	51
Registry	6
Involved	43
Suspicious activity	20
Malicious threat	14
Incident trigger	60

Attack stages

Execution
- Jun 15, 2021, 09:38:11:374395 AM +03:00
  User pbeesly, with standard priviledges, on workload SCRANTON, executes a suspicious file !?lcod.3aka3.scr

Defense Evasion
- Jun 15, 2021, 09:38:11:374395 AM +03:00
  To trick user pbeesly, the file was masquarading as a benign doc file, by the name rcs.3aka.doc

Command And Control
- Jun 15, 2021, 09:38:11:374395 AM +03:00
  To control workload SCRANTON, once !?lcod.3aka3.scr is executed, a TCP connection is established on an unusual port 1234 to a unknown domain 192.168.0.5

Collection
- Jun 15, 2021, 09:38:52:669601 AM +03:00
  The adversary collects *.doc,*.xps,*.xls,*.ppt,*.pps,*.wps,*.wpd,*.ods,*.odt,*.lwp,*.jtd,*.p... files containing sensitive information credit card numbers, social security numbers and more from $env:USERPROFILE and compresses them into an archive draft.zip via a powershell script

powershell.exe

OVERVIEW | SCRIPTING ACTIVITIES (71) | RESPO

Security analysis

Verdict	Suspicious activity
Severity	HIGH
File found on	10 Workloads
Attack objective	Collection
Techniques	T1560
Reason of detection	Suspicious Activity - unknown process collects files containing sensitive information and compresses them into an archive.
Detection date	Jun 15, 2021, 09:38:51:983576 AM +03:00

Reputation

VirusTotal	Go to VirusTotal Score: 5.7 / 10 Last seen: Jun 28, 2021, 08:45:23:111 AM +02:00
Google	Go to Google

Details

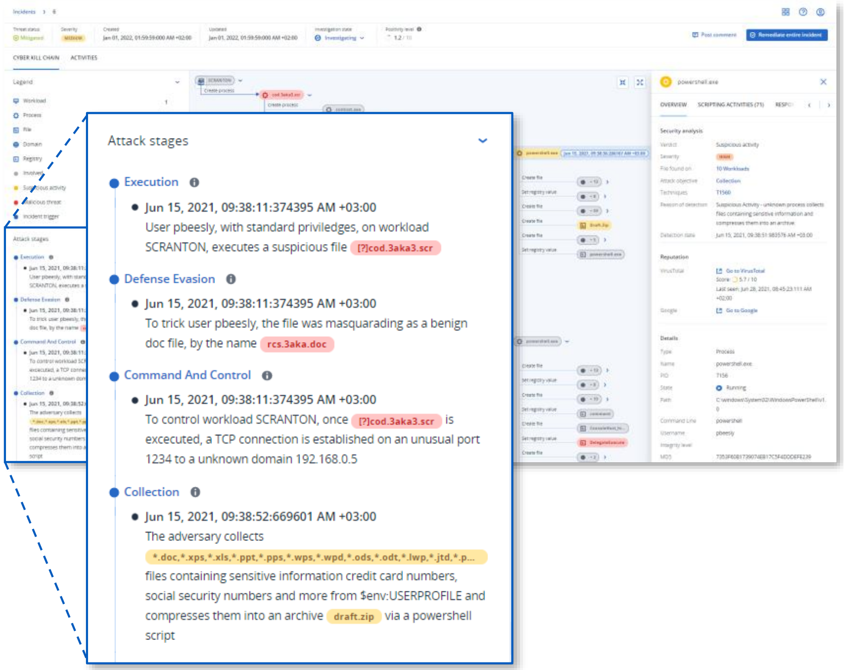
Type	Process
Name	powershell.exe
PID	7156
State	Running
Path	C:\windows\System32\WindowsPowerShell\v1.0
Command Line	powershell
Username	pbeesly
Integrity level	
MD5	7353F60B1739074EB17C5F4DDDEFE239

Analyze attacks in minutes to unlock rapid response

Leverage automated, human-friendly interpretation of attacks and prioritized visibility

Enable team to effortlessly analyze attacks with ease and speed:

- **Gain complete visibility into the attack chain –** attack evolution mapped to MITRE framework (industry-standard)
  - How did it get in?
  - How did it hide its tracks?
  - How did it cause harm?
  - How did it spread?
- **Save money and time, removing need for** rigorous trainings or highly skilled personnel doing operational tasks
- Get **prioritized visibility of suspicious activities** across endpoints – rather than flat list of all alerts
- **Focus threat hunting** using an emerging threat intelligence feed to search for IoCs



Attack stages

● Execution

- Jun 15, 2021, 09:38:11:374395 AM +03:00
  User pbeesly, with standard priviledges, on workload SCRANTON, executes a suspicious file [?]cod.3aka3.scr

● Defense Evasion

- Jun 15, 2021, 09:38:11:374395 AM +03:00
  To trick user pbeesly, the file was masquarading as a benign doc file, by the name rcs.3aka.doc

● Command And Control

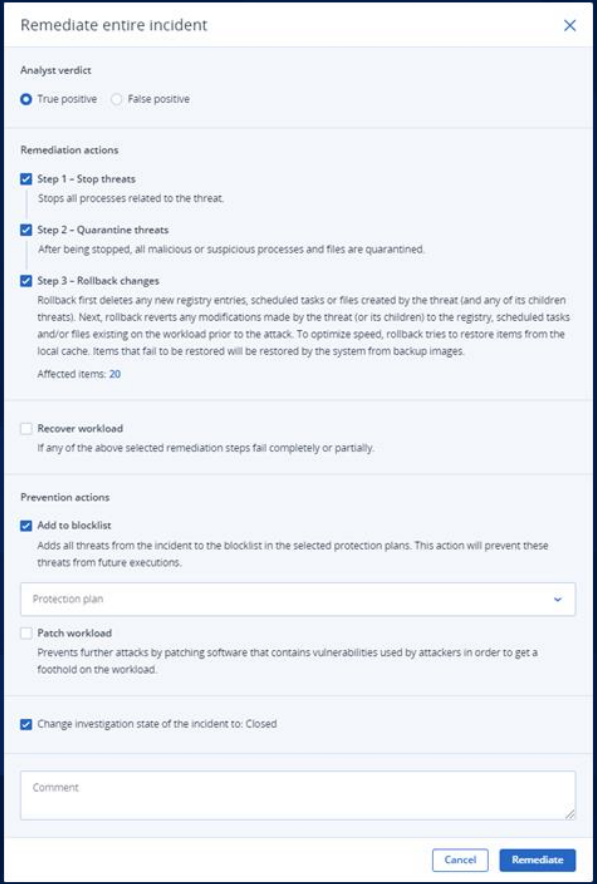
- Jun 15, 2021, 09:38:11:374395 AM +03:00
  To control workload SCRANTON, once [?]cod.3aka3.scr is excecuted, a TCP connection is established on an unusual port 1234 to a unknown domain 192.168.0.5

● Collection

- Jun 15, 2021, 09:38:52:669601 AM +03:00
  The adversary collects *.doc,*.xps,*.xls,*.ppt,*.pps,*.wps,*.wpd,*.ods,*.odt,*.lwp,*.jtd,*.p... files containing sensitive information credit card numbers, social security numbers and more from $env:USERPROFILE and compresses them into an archive draft.zip via a powershell script

Stop the breach: ensure business continuity

Succeed where point solutions fail. Unlock full power of platform with integrated capabilities across NIST framework



Remediate entire incident

Analyst verdict

● True positive ○ False positive

Remediation actions

☑ **Step 1 – Stop threats**

Stops all processes related to the threat.

☑ **Step 2 – Quarantine threats**

After being stopped, all malicious or suspicious processes and files are quarantined.

☑ **Step 3 – Rollback changes**

Rollback first deletes any new registry entries, scheduled tasks or files created by the threat (and any of its children threats). Next, rollback reverts any modifications made by the threat (or its children) to the registry, scheduled tasks and/or files existing on the workload prior to the attack. To optimize speed, rollback tries to restore items from the local cache. Items that fail to be restored will be restored by the system from backup images.

Affected items: 20

□ **Recover workload**

If any of the above selected remediation steps fail completely or partially.

Prevention actions

☑ **Add to blocklist**

Adds all threats from the incident to the blocklist in the selected protection plans. This action will prevent these threats from future executions.

Protection plan

□ **Patch workload**

Prevents further attacks by patching software that contains vulnerabilities used by attackers in order to get a foothold on the workload.

☑ Change investigation state of the incident to: Closed

Comment

Stop the breach: ensure business continuity

Select the actions you want to take, and respond with a single click.

Identify

inventory and data classification: better understand attack surface

Protect

threat feed, forensic insights, data protection map, patch management, blocking analyzed attacks, and policy management to reduce risks

Detect

continuous monitoring using automated behavioral and signature-based engines, URL filtering, threat intelligence feed, event correlation and MITRE ATT&CK

Respond

rapid investigation, forensic data collection, endpoint isolation, killing processes, quarantining threats, and attack-specific rollbacks to limit the impact.

Recover

best-of-breed backup and disaster recovery for true business continuity

An EDR solution built for MSPs

Challenge

Incident analysis requires extensive expertise

Understanding how an attack happened and how to prevent it from happening again requires extensive security expertise (many MSPs lack the resources to facilitate)

Investigation takes several hours

Even skilled security staff requires 2-6 hours to investigate incidents

Long time to contain and recover from incident

It takes 32 hours to contain an incident and 130 hours to recover business operations

Solution

Gain an easy-to-understand interpretation of attacks

- Enable team **regardless of security expertise** to understand and respond to incidents
- Get end-to-end visibility into attacks

Reduce investigation time

Shorten time spent on incident analysis from hours to minutes.

Remediate incident quickly and return to productivity

Leverage unmatched array of responses, including investigation, threat remediation, data and system recovery and preventive measures that thwart future threats

Section Summary

1. Acronis Advanced Security + EDR combines the power of threat prevention and detection with the ability to analyze attacks within minutes and respond fast via a centralized way to investigate, remediate, prevent and recover.

2. Attacks are mapped to the MITRE framework to provide visibility to attacks such as how did they get in, hide their tracks, cause harm and spread. Investigation time goes to a few minutes as opposed to 2-6 hours per incident.

Section Summary

3

Threats can be isolated to an affected workload and remediated by killing malware processes and rollback of system files done by the attack. Acronis provides the ability to select different actions desired to take with a single click helping you respond faster to attacks.

Acronis

#CyberFit

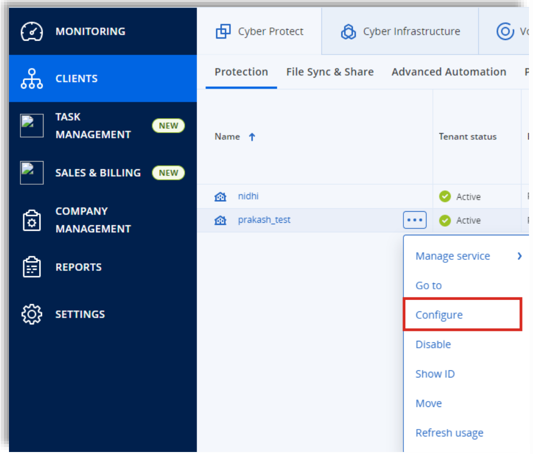
Cyber Protect Cloud

Advanced Security + EDR: How To Provision, Setup and Configure

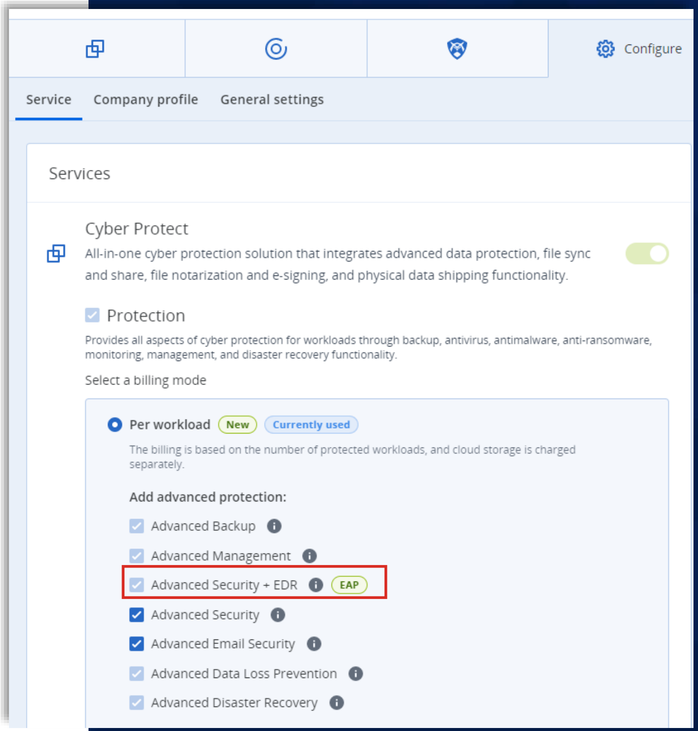
Provision in One Click

Can be enabled at tenant level

Pick configuration at tenant level



Name ↑	Tenant status
nidhi	Active
prakash_test	Active



Services

Cyber Protect

All-in-one cyber protection solution that integrates advanced data protection, file sync and share, file notarization and e-signing, and physical data shipping functionality.

☑ Protection

Provides all aspects of cyber protection for workloads through backup, antivirus, antimalware, anti-ransomware, monitoring, management, and disaster recovery functionality.

Select a billing mode

● Per workload New Currently used

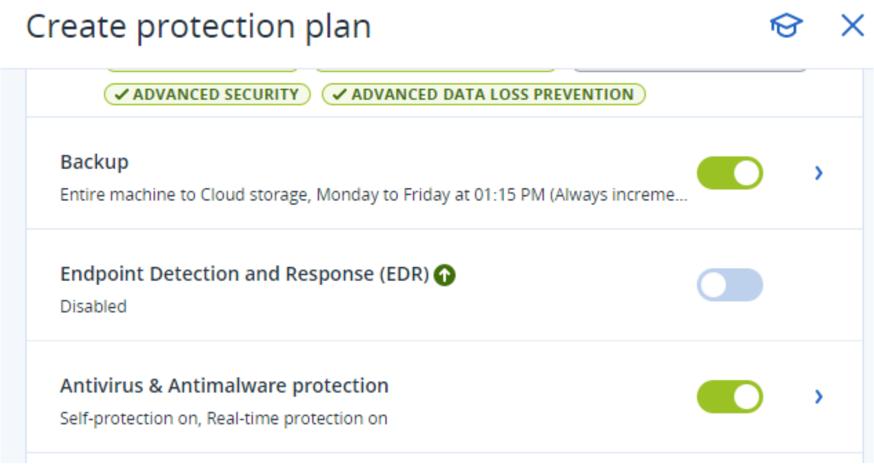
The billing is based on the number of protected workloads, and cloud storage is charged separately.

Add advanced protection:

- ☑ Advanced Backup
- ☑ Advanced Management
- ☑ Advanced Security + EDR EAP
- ☑ Advanced Security
- ☑ Advanced Email Security
- ☑ Advanced Data Loss Prevention
- ☑ Advanced Disaster Recovery

Enable features in 1-2 clicks

Enable EDR in protection plan (only workloads you want)



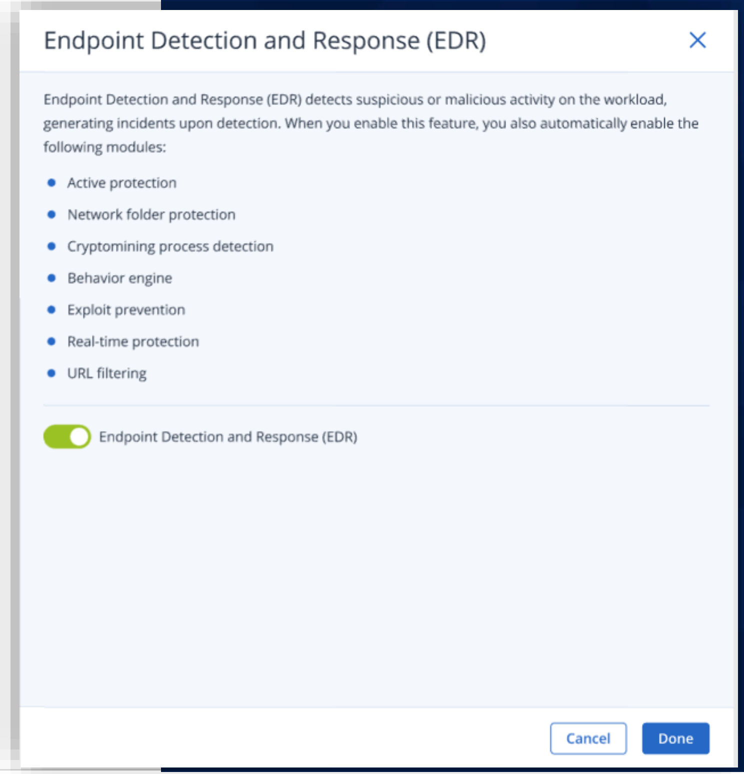
Create protection plan

✓ ADVANCED SECURITY ✓ ADVANCED DATA LOSS PREVENTION

Backup
Entire machine to Cloud storage, Monday to Friday at 01:15 PM (Always increme...

Endpoint Detection and Response (EDR)
Disabled

Antivirus & Antimalware protection
Self-protection on, Real-time protection on



Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) detects suspicious or malicious activity on the workload, generating incidents upon detection. When you enable this feature, you also automatically enable the following modules:

- Active protection
- Network folder protection
- Cryptomining process detection
- Behavior engine
- Exploit prevention
- Real-time protection
- URL filtering

Endpoint Detection and Response (EDR)

Acronis

Video

Provisioning and Enabling Advanced Security + EDR for Tenant

Acronis

#CyberFit

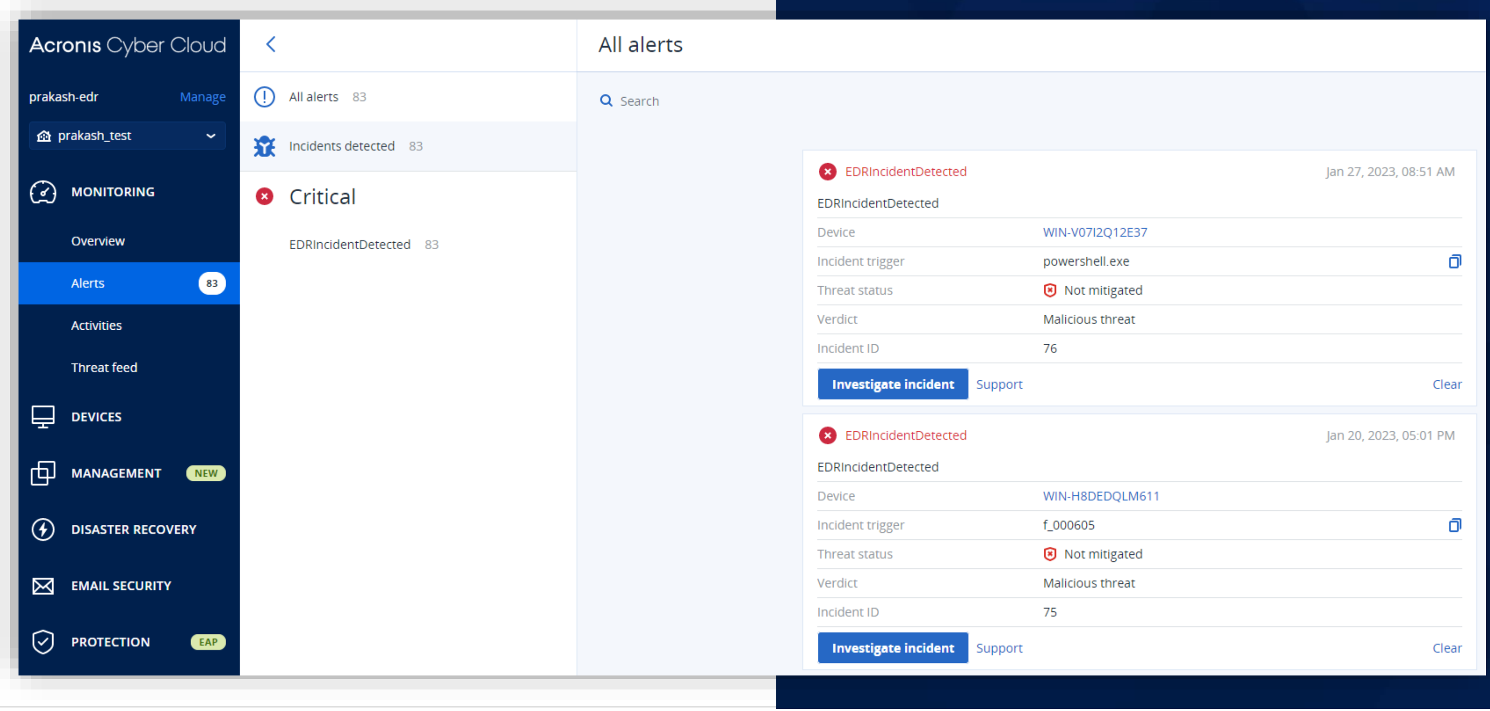
Cyber Protect Cloud

Advanced Security + EDR: Alerts, Incident Management and Investigation

Incident alerts

Receive in console or (email) alerts when incidents are detected

Alerts



EDRIncidentDetected Jan 27, 2023, 08:51 AM

EDRIncidentDetected

Device	WIN-V07I2Q12E37
Incident trigger	powershell.exe
Threat status	Not mitigated
Verdict	Malicious threat
Incident ID	76

EDRIncidentDetected Jan 20, 2023, 05:01 PM

EDRIncidentDetected

Device	WIN-H8DEDQLM611
Incident trigger	f_000605
Threat status	Not mitigated
Verdict	Malicious threat
Incident ID	75

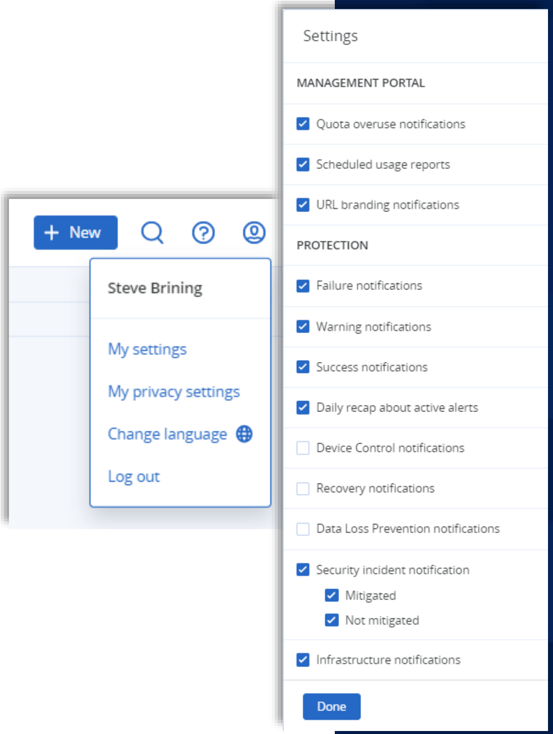
Incident alerts

Receive in console or (email) alerts when incidents are detected

Settings for Alerts

When logged in go to "*My Settings*" in upper right

Edit notifications and select what security incident notifications desired and click done



Settings

MANAGEMENT PORTAL

- ☑ Quota overuse notifications
- ☑ Scheduled usage reports
- ☑ URL branding notifications

PROTECTION

- ☑ Failure notifications
- ☑ Warning notifications
- ☑ Success notifications
- ☑ Daily recap about active alerts
- ☐ Device Control notifications
- ☐ Recovery notifications
- ☐ Data Loss Prevention notifications
- ☑ Security incident notification
  - ☑ Mitigated
  - ☑ Not mitigated
- ☑ Infrastructure notifications

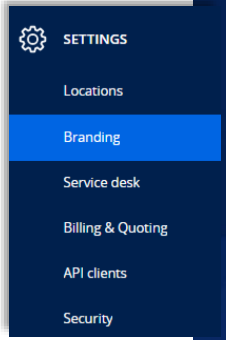
Done

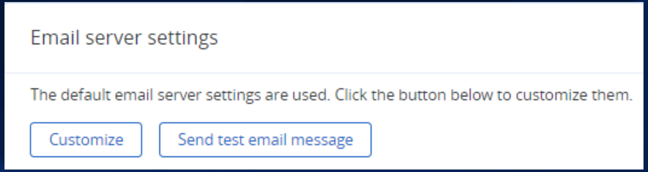
Incident alerts

Make sure email settings at parent level is setup correctly

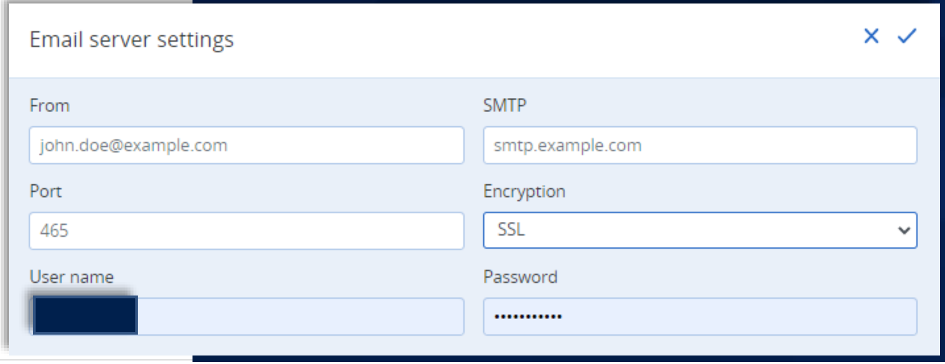
Setting Email Server Settings

- At partner level go to “Settings” and then “Branding”
- Scroll down to “Email Server Settings” and then “Customize”
- Enter proper credentials
- Good idea to hit the “Send test email message” (ensure emails go through for notifications and alerts)




Email server settings

The default email server settings are used. Click the button below to customize them.

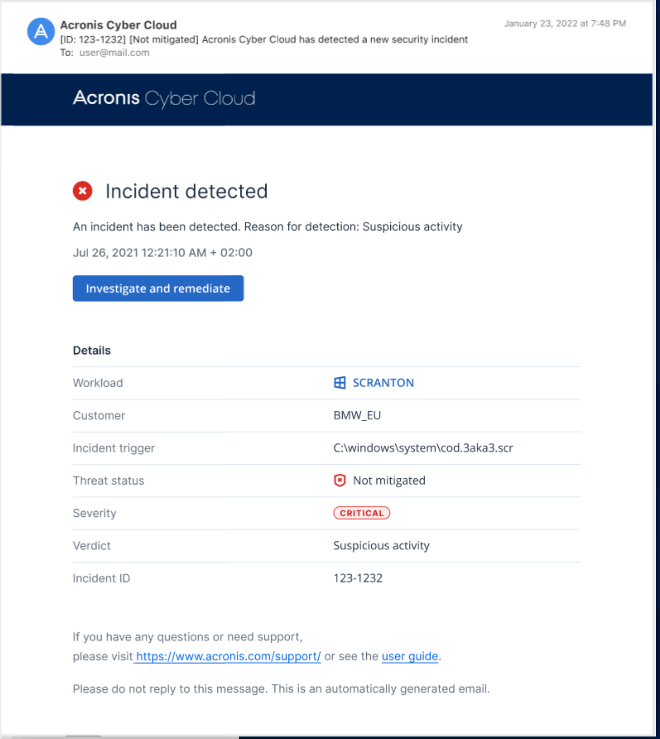

Email server settings

From	SMTP
john.doe@example.com	smtp.example.com
Port	Encryption
465	SSL
User name	Password
[redacted]	•••••••••••

Incident alerts

Receive in console or (email) alerts when incidents are detected

Email alerts



Acronis Cyber Cloud
[ID: 123-1232] [Not mitigated] Acronis Cyber Cloud has detected a new security incident
To: user@mail.com

January 23, 2022 at 7:48 PM

Acronis Cyber Cloud

Incident detected

An incident has been detected. Reason for detection: Suspicious activity

Jul 26, 2021 12:21:10 AM + 02:00

Details

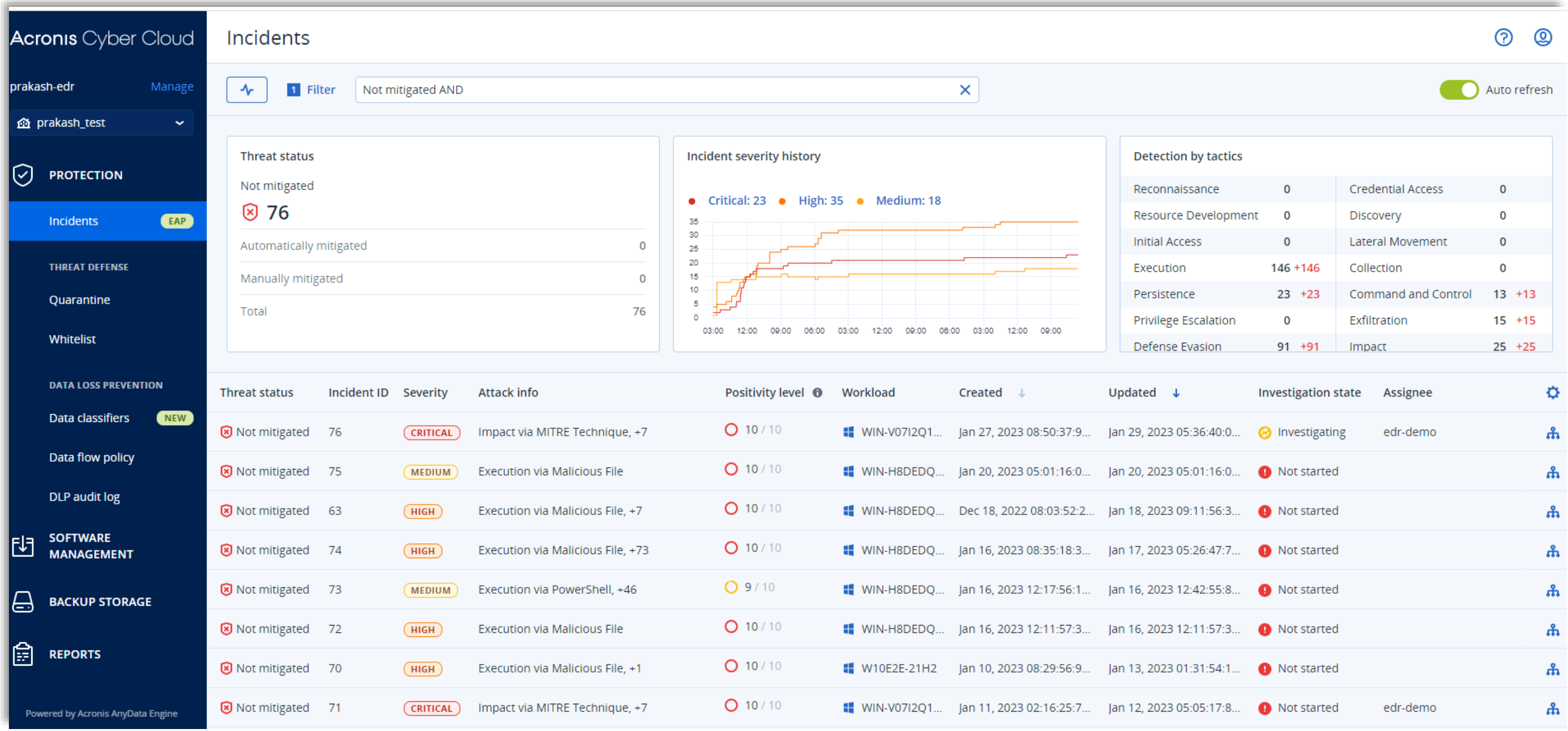
Workload	SCRANTON
Customer	BMW_EU
Incident trigger	C:\windows\system\cod.3aka3.scr
Threat status	Not mitigated
Severity	CRITICAL
Verdict	Suspicious activity
Incident ID	123-1232

If you have any questions or need support,
please visit https://www.acronis.com/support/ or see the user guide.

Please do not reply to this message. This is an automatically generated email.

Incident management

Prioritized list of incidents



Filter: Not mitigated AND

Threat status

Not mitigated

76

Automatically mitigated	0
Manually mitigated	0
Total	76

Incident severity history

● Critical: 23 ● High: 35 ● Medium: 18

Detection by tactics

Reconnaissance	0		Credential Access	0	
Resource Development	0		Discovery	0	
Initial Access	0		Lateral Movement	0	
Execution	146	+146	Collection	0	
Persistence	23	+23	Command and Control	13	+13
Privilege Escalation	0		Exfiltration	15	+15
Defense Evasion	91	+91	Impact	25	+25

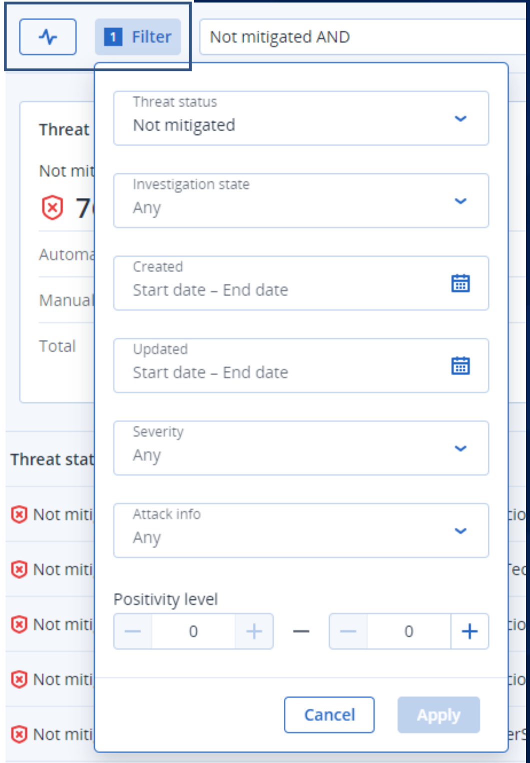
Threat status	Incident ID	Severity	Attack info	Positivity level	Workload	Created ↓	Updated ↓	Investigation state	Assignee
Not mitigated	76	CRITICAL	Impact via MITRE Technique, +7	10 / 10	WIN-V07I2Q1...	Jan 27, 2023 08:50:37:9...	Jan 29, 2023 05:36:40:0...	Investigating	edr-demo
Not mitigated	75	MEDIUM	Execution via Malicious File	10 / 10	WIN-H8DEDQ...	Jan 20, 2023 05:01:16:0...	Jan 20, 2023 05:01:16:0...	Not started	
Not mitigated	63	HIGH	Execution via Malicious File, +7	10 / 10	WIN-H8DEDQ...	Dec 18, 2022 08:03:52:2...	Jan 18, 2023 09:11:56:3...	Not started	
Not mitigated	74	HIGH	Execution via Malicious File, +73	10 / 10	WIN-H8DEDQ...	Jan 16, 2023 08:35:18:3...	Jan 17, 2023 05:26:47:7...	Not started	
Not mitigated	73	MEDIUM	Execution via PowerShell, +46	9 / 10	WIN-H8DEDQ...	Jan 16, 2023 12:17:56:1...	Jan 16, 2023 12:42:55:8...	Not started	
Not mitigated	72	HIGH	Execution via Malicious File	10 / 10	WIN-H8DEDQ...	Jan 16, 2023 12:11:57:3...	Jan 16, 2023 12:11:57:3...	Not started	
Not mitigated	70	HIGH	Execution via Malicious File, +1	10 / 10	W10E2E-21H2	Jan 10, 2023 08:29:56:9...	Jan 13, 2023 01:31:54:1...	Not started	
Not mitigated	71	CRITICAL	Impact via MITRE Technique, +7	10 / 10	WIN-V07I2Q1...	Jan 11, 2023 02:16:25:7...	Jan 12, 2023 05:05:17:8...	Not started	edr-demo

Incident management

Filtering and Toggling

Filter Settings

- Threat status
- Investigation status
- Created or Updated dates
- Severity level
- Attack Info
- Positivity level



Not mitigated AND

Threat status: Not mitigated

Investigation state: Any

Created: Start date – End date

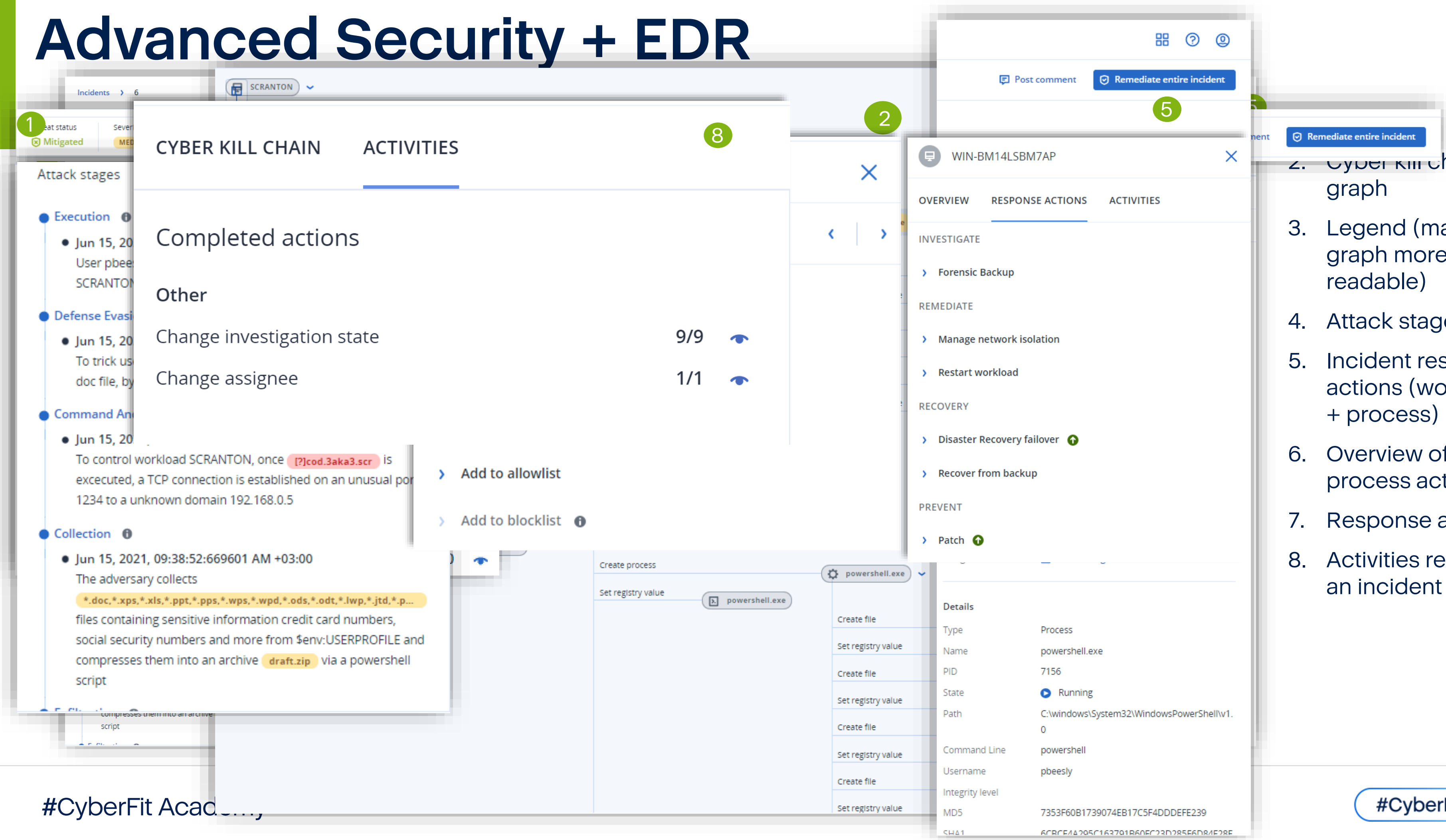
Updated: Start date – End date

Severity: Any

Attack info: Any

Positivity level: 0 – 0

Advanced Security + EDR



Attack stages

- Execution
  - Jun 15, 20
    User pbee
    SCRANTO
- Defense Evasi
  - Jun 15, 20
    To trick us
    doc file, by
- Command An
  - Jun 15, 20
    To control workload SCRANTON, once [?]cod.3aka3.scr is excecuted, a TCP connection is established on an unusual por 1234 to a unknown domain 192.168.0.5
- Collection
  - Jun 15, 2021, 09:38:52:669601 AM +03:00
    The adversary collects *.doc,*.xps,*.xls,*.ppt,*.pps,*.wps,*.wpd,*.ods,*.odt,*.lwp,*.jtd,*.p... files containing sensitive information credit card numbers, social security numbers and more from $env:USERPROFILE and compresses them into an archive draft.zip via a powershell script

Completed actions

Other

Change investigation state	9/9
Change assignee	1/1

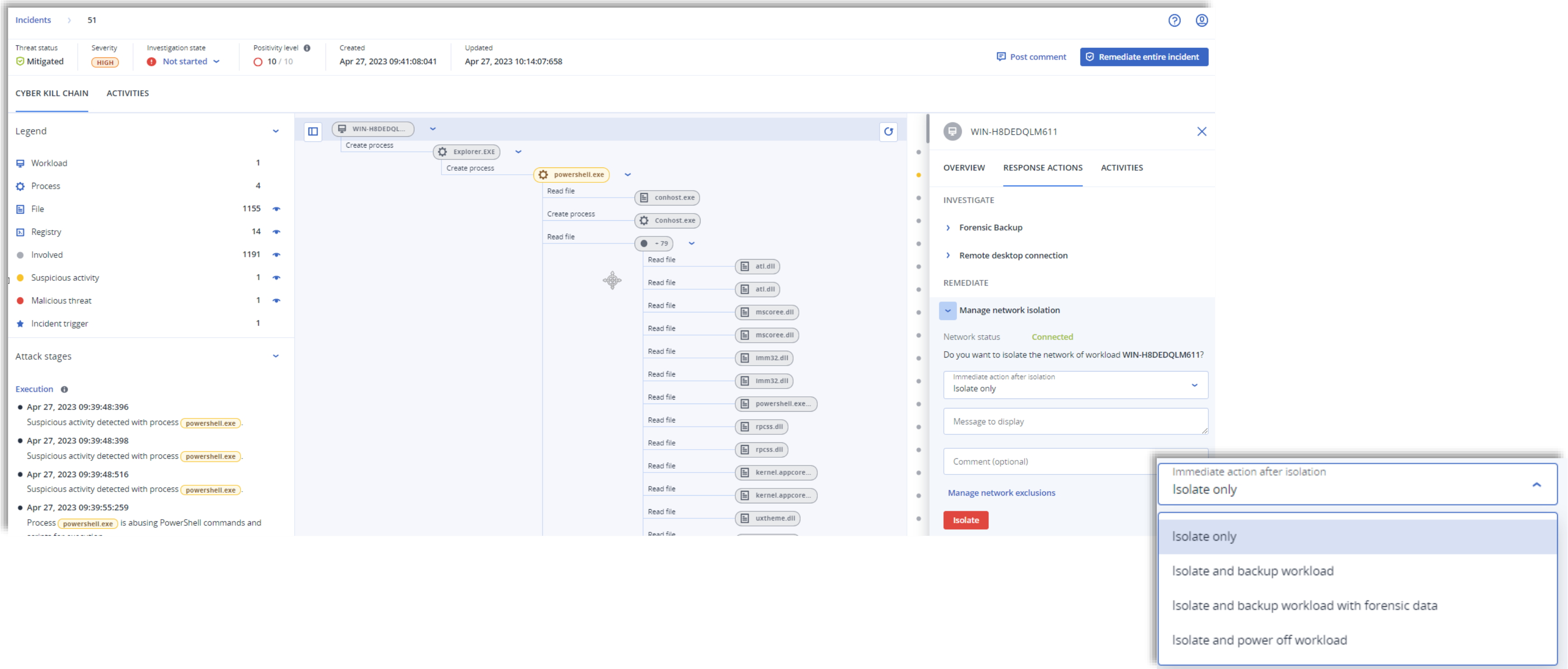
Details

Type	Process
Name	powershell.exe
PID	7156
State	Running
Path	C:\windows\System32\WindowsPowerShell\v1.0
Command Line	powershell
Username	pbeesly
Integrity level	
MD5	7353F60B1739074EB17C5F4DDDEFE239
SHA1	6CBCF4A295C163791B60FC23D285F6D84F28E

2. Cyber kill chain graph
3. Legend (make graph more readable)
4. Attack stages
5. Incident response actions (workload + process)
6. Overview of process activities
7. Response actions
8. Activities related to an incident

Incident response

Isolate Workload



Incidents › 51

Threat status: Mitigated
Severity: HIGH
Investigation state: Not started
Positivity level: 10 / 10
Created: Apr 27, 2023 09:41:08:041
Updated: Apr 27, 2023 10:14:07:658

Post comment | Remediate entire incident

CYBER KILL CHAIN | ACTIVITIES

Legend

Workload	1
Process	4
File	1155
Registry	14
Involved	1191
Suspicious activity	1
Malicious threat	1
Incident trigger	1

Attack stages

Execution

- Apr 27, 2023 09:39:48:396
  Suspicious activity detected with process powershell.exe.
- Apr 27, 2023 09:39:48:398
  Suspicious activity detected with process powershell.exe.
- Apr 27, 2023 09:39:48:516
  Suspicious activity detected with process powershell.exe.
- Apr 27, 2023 09:39:55:259
  Process powershell.exe is abusing PowerShell commands and

WIN-H8DEDQLM611

OVERVIEW | RESPONSE ACTIONS | ACTIVITIES

INVESTIGATE
- Forensic Backup
- Remote desktop connection

REMEDIATE
- Manage network isolation

Network status: Connected

Do you want to isolate the network of workload **WIN-H8DEDQLM611**?

Immediate action after isolation: Isolate only

Message to display

Comment (optional)

Manage network exclusions

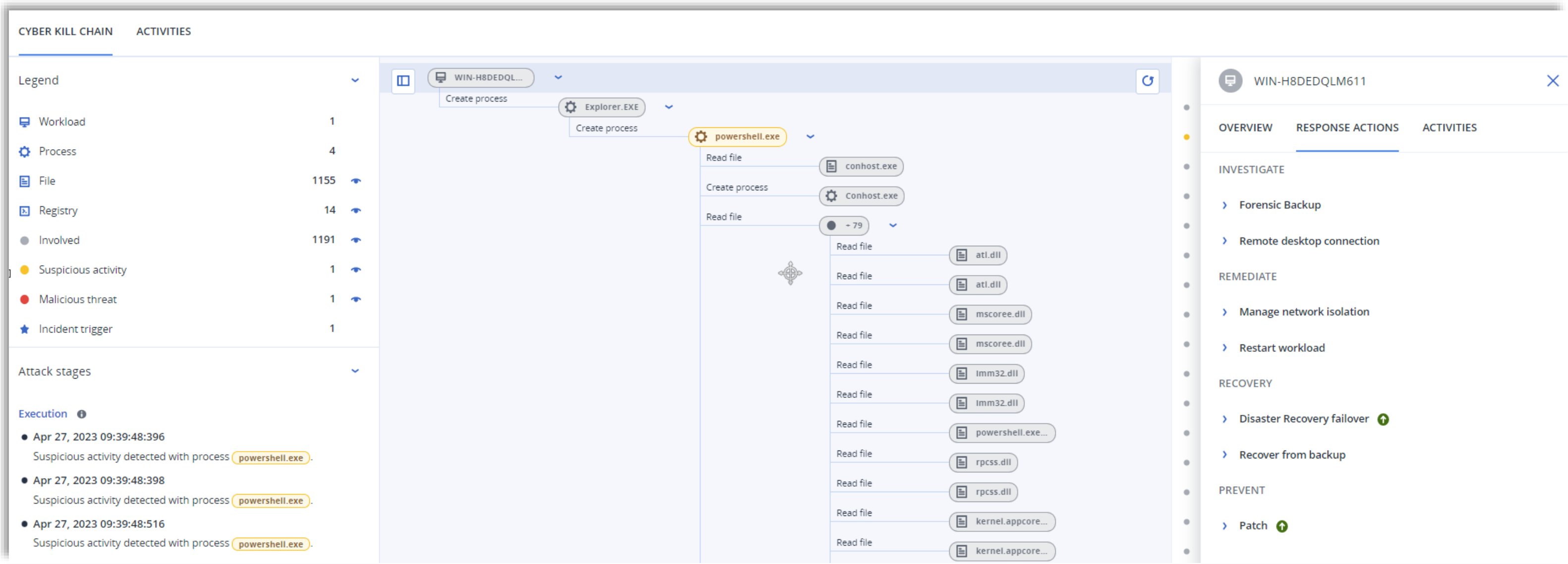
Isolate

Immediate action after isolation: Isolate only

- Isolate only
- Isolate and backup workload
- Isolate and backup workload with forensic data
- Isolate and power off workload

Incident response

Other Response Actions Depending on Incident



CYBER KILL CHAIN   ACTIVITIES

Legend

Workload	1
Process	4
File	1155
Registry	14
Involved	1191
● Suspicious activity	1
● Malicious threat	1
★ Incident trigger	1

Attack stages

Execution

- Apr 27, 2023 09:39:48:396
  Suspicious activity detected with process powershell.exe.
- Apr 27, 2023 09:39:48:398
  Suspicious activity detected with process powershell.exe.
- Apr 27, 2023 09:39:48:516
  Suspicious activity detected with process powershell.exe.

WIN-H8DEDQLM611

OVERVIEW   RESPONSE ACTIONS   ACTIVITIES

INVESTIGATE

- › Forensic Backup
- › Remote desktop connection

REMEDIATE

- › Manage network isolation
- › Restart workload

RECOVERY

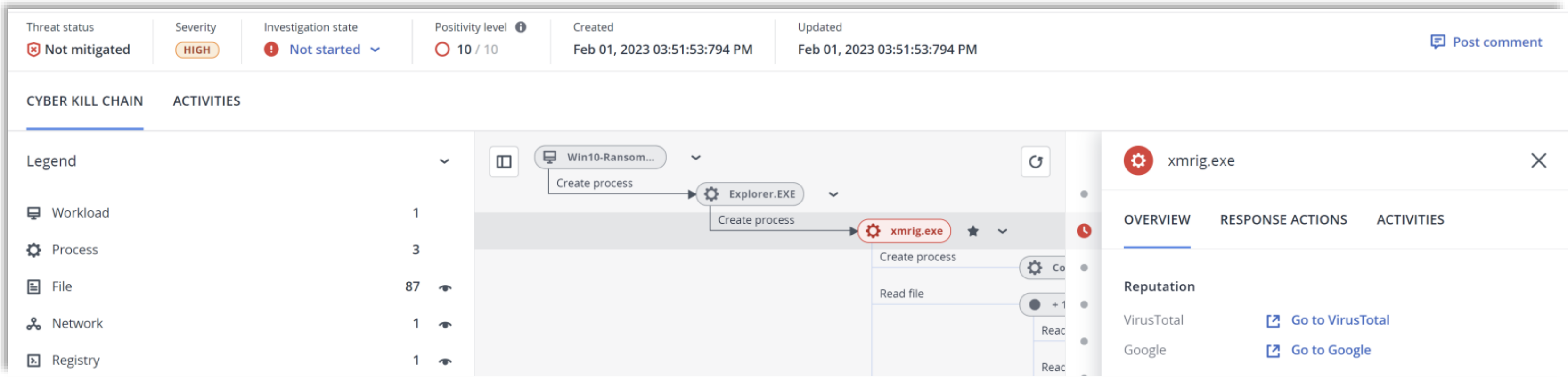
- › Disaster Recovery failover
- › Recover from backup

PREVENT

- › Patch

Incident response

Validate File – Virus Total



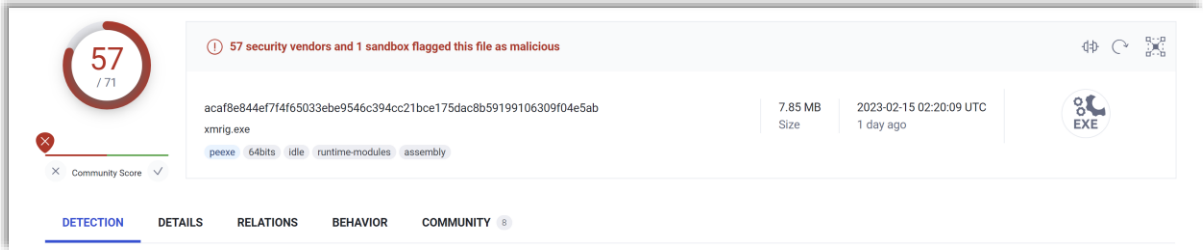
Threat status	Severity	Investigation state	Positivity level	Created	Updated
Not mitigated	HIGH	Not started	10 / 10	Feb 01, 2023 03:51:53:794 PM	Feb 01, 2023 03:51:53:794 PM

Legend

Workload	1
Process	3
File	87
Network	1
Registry	1

Reputation

VirusTotal	Go to VirusTotal
Google	Go to Google



57 / 71

57 security vendors and 1 sandbox flagged this file as malicious

acaf8e844ef7f4f65033ebe9546c394cc21bce175dac8b59199106309f04e5ab
xmrig.exe

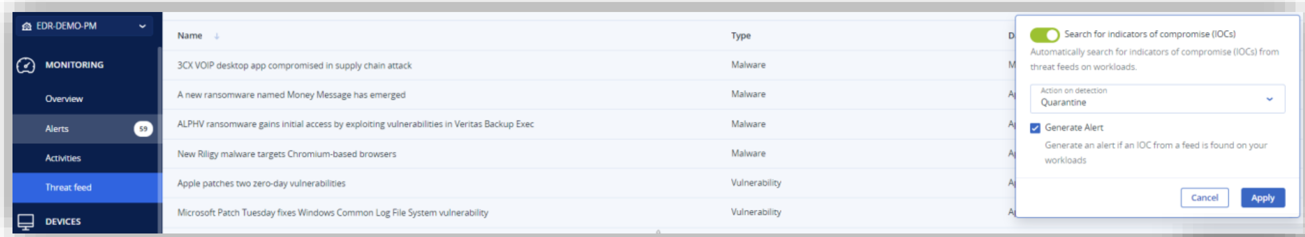
peexe 64bits idle runtime-modules assembly

7.85 MB
Size

2023-02-15 02:20:09 UTC
1 day ago

Search IoCs

Search Indicators of Compromise (IoCs) from “Threat feeds” on workloads



Name	Type	D
3CX VOIP desktop app compromised in supply chain attack	Malware	M
A new ransomware named Money Message has emerged	Malware	A
ALPHV ransomware gains initial access by exploiting vulnerabilities in Veritas Backup Exec	Malware	A
New Riligy malware targets Chromium-based browsers	Malware	A
Apple patches two zero-day vulnerabilities	Vulnerability	A
Microsoft Patch Tuesday fixes Windows Common Log File System vulnerability	Vulnerability	A

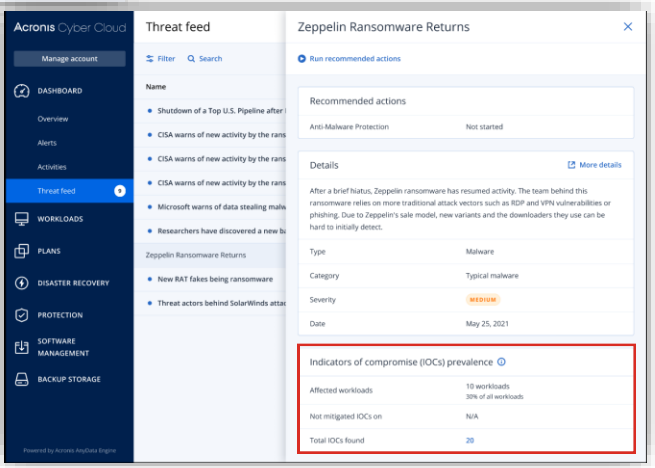
● Search for indicators of compromise (IOCs)

Automatically search for indicators of compromise (IOCs) from threat feeds on workloads.

Action on detection: Quarantine

☑ Generate Alert

Generate an alert if an IOC from a feed is found on your workloads



Name

- Shutdown of a Top U.S. Pipeline after I
- CISA warns of new activity by the rans
- CISA warns of new activity by the rans
- CISA warns of new activity by the rans
- Microsoft warns of data stealing malw
- Researchers have discovered a new ba

Zeppelin Ransomware Returns

- New RAT fakes being ransomware
- Threat actors behind SolarWinds attac

Zeppelin Ransomware Returns

Recommended actions

Anti-Malware Protection	Not started

Details

After a brief hiatus, Zeppelin ransomware has resumed activity. The team behind this ransomware relies on more traditional attack vectors such as RDP and VPN vulnerabilities or phishing. Due to Zeppelin's sale model, new variants and the downloaders they use can be hard to initially detect.

Type	Malware
Category	Typical malware
Severity	MEDIUM
Date	May 25, 2021

Indicators of compromise (IOCs) prevalence

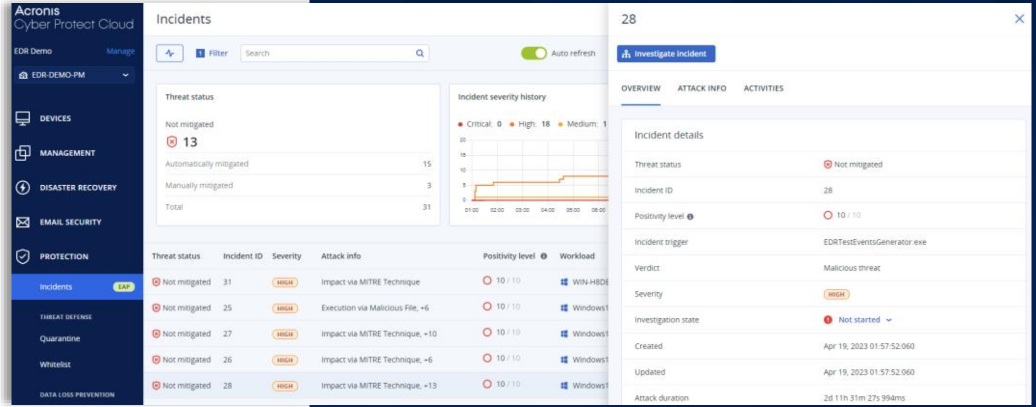
Affected workloads	10 workloads 30% of all workloads
Not mitigated IOCs on	N/A
Total IOCs found	20

Remediate Entire Event

Single platform and integration

1. Select Incident
2. Click “Investigate Incident

Click Remediate Entire Incident



Acronis
Cyber Protect Cloud

EDR Demo Manage

EDR-DEMO-PM

Incidents

Threat status

Not mitigated
13

Automatically mitigated	15
Manually mitigated	3
Total	31

Incident severity history

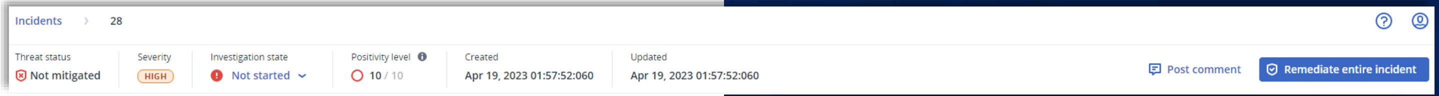
Critical: 0 High: 18 Medium: 1

Threat status	Incident ID	Severity	Attack info	Positivity level	Workload
Not mitigated	31	HIGH	Impact via MITRE Technique	10 / 10	WIN-H8DE
Not mitigated	25	HIGH	Execution via Malicious File, +6	10 / 10	Windows1
Not mitigated	27	HIGH	Impact via MITRE Technique, +10	10 / 10	Windows1
Not mitigated	26	HIGH	Impact via MITRE Technique, +6	10 / 10	Windows1
Not mitigated	28	HIGH	Impact via MITRE Technique, +13	10 / 10	Windows1

28

Incident details

Threat status	Not mitigated
Incident ID	28
Positivity level	10 / 10
Incident trigger	EDRTestEventsGenerator.exe
Verdict	Malicious threat
Severity	HIGH
Investigation state	Not started
Created	Apr 19, 2023 01:57:52:060
Updated	Apr 19, 2023 01:57:52:060
Attack duration	2d 11h 31m 27s 994ms



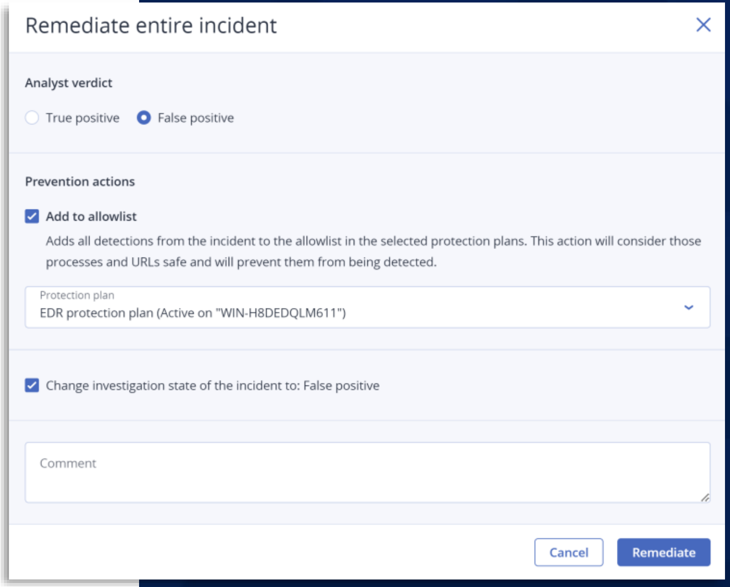
Incidents > 28

Threat status	Severity	Investigation state	Positivity level	Created	Updated
Not mitigated	HIGH	Not started	10 / 10	Apr 19, 2023 01:57:52:060	Apr 19, 2023 01:57:52:060

Remediate Entire Event

False Positive

- ✓ Option for allowlisting on selected protection plans
- ✓ Processes and URL's then marked safe
- ✓ Add comments and "remediate" to provide resolution.



Remediate entire incident

Analyst verdict

○ True positive ● False positive

Prevention actions

☑ Add to allowlist

Adds all detections from the incident to the allowlist in the selected protection plans. This action will consider those processes and URLs safe and will prevent them from being detected.

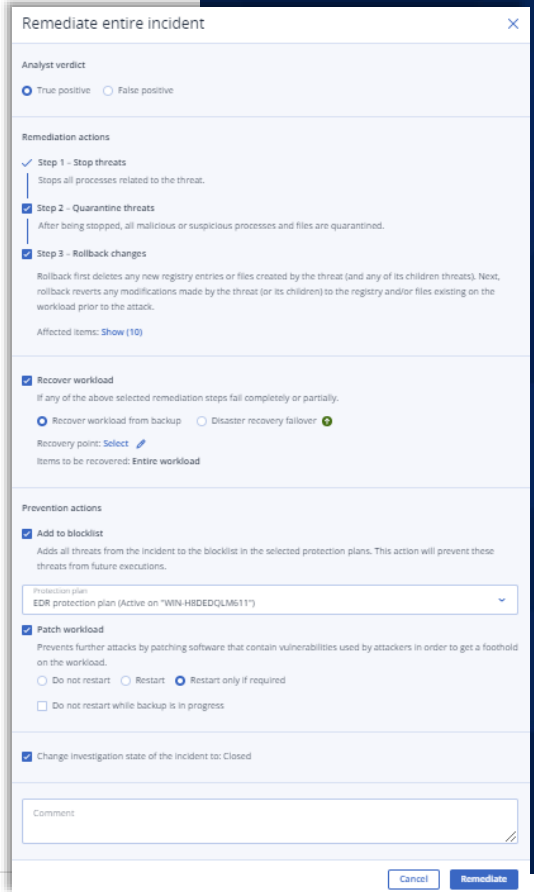
Protection plan: EDR protection plan (Active on "WIN-H8DEDQLM611")

☑ Change investigation state of the incident to: False positive

Remediate Entire Event

True Positive

- ✓ One-click button to remediate based on options selected
- ✓ All action options in one console and one agent



Remediate entire incident

Analyst verdict

● True positive ○ False positive

Remediation actions

✓ Step 1 – Stop threats

Stops all processes related to the threat.

☑ Step 2 – Quarantine threats

After being stopped, all malicious or suspicious processes and files are quarantined.

☑ Step 3 – Rollback changes

Rollback first deletes any new registry entries or files created by the threat (and any of its children threats). Next, rollback reverts any modifications made by the threat (or its children) to the registry and/or files existing on the workload prior to the attack.

Affected items: Show (10)

☑ Recover workload

If any of the above selected remediation steps fail completely or partially.

● Recover workload from backup ○ Disaster recovery failover

Recovery point: Select

Items to be recovered: **Entire workload**

Prevention actions

☑ Add to blocklist

Adds all threats from the incident to the blocklist in the selected protection plans. This action will prevent these threats from future executions.

Protection plan: EDR protection plan (Active on "WIN-H8DEDQLM611")

☑ Patch workload

Prevents further attacks by patching software that contain vulnerabilities used by attackers in order to get a foothold on the workload.

○ Do not restart ○ Restart ● Restart only if required

□ Do not restart while backup is in progress

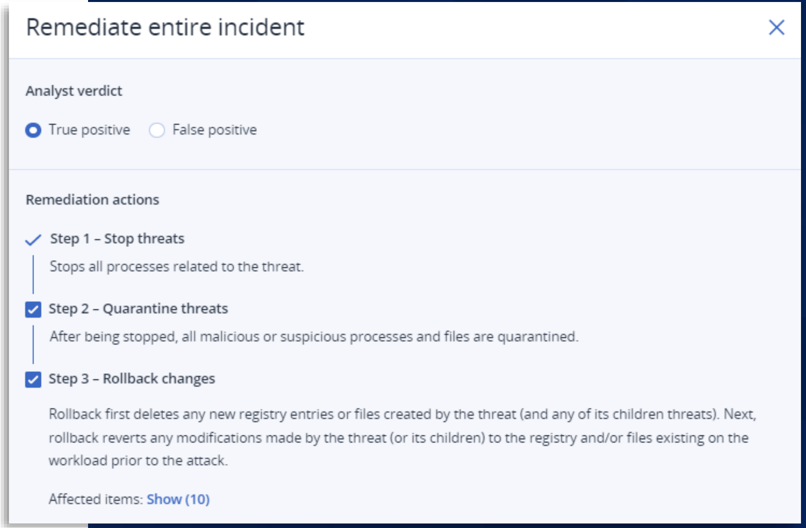
☑ Change investigation state of the incident to: Closed

Comment

Remediate Entire Event

Stop Breach: Ensure Continuity

- ✓ Contain Threats
- ✓ Remediate
  - Kill malware processes
  - Quarantine threats
  - Rollback changes
    - See affected files and registries
    - Attack specific rollback



Remediate entire incident

Analyst verdict

● True positive ○ False positive

Remediation actions

✓ Step 1 – Stop threats

Stops all processes related to the threat.

☑ Step 2 – Quarantine threats

After being stopped, all malicious or suspicious processes and files are quarantined.

☑ Step 3 – Rollback changes

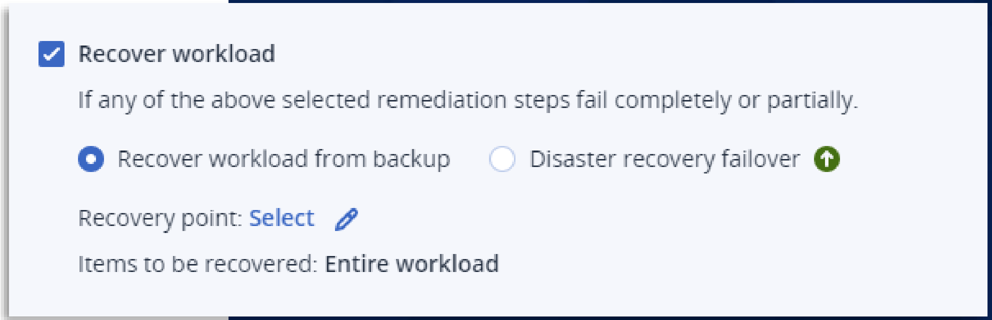
Rollback first deletes any new registry entries or files created by the threat (and any of its children threats). Next, rollback reverts any modifications made by the threat (or its children) to the registry and/or files existing on the workload prior to the attack.

Affected items: Show (10)

Remediate Entire Event

Stop Breach: Ensure Continuity

- ✓ **Recover workload**
  - If steps 1-3 fail or partially fail
- ✓ **Select recovery point (must have prior backup)**
- ✓ **Option for Disaster Recovery Failover**
  - Need recovery server setup prior
  - Need Advanced Disaster Recovery Pack



☑ Recover workload

If any of the above selected remediation steps fail completely or partially.

● Recover workload from backup ○ Disaster recovery failover

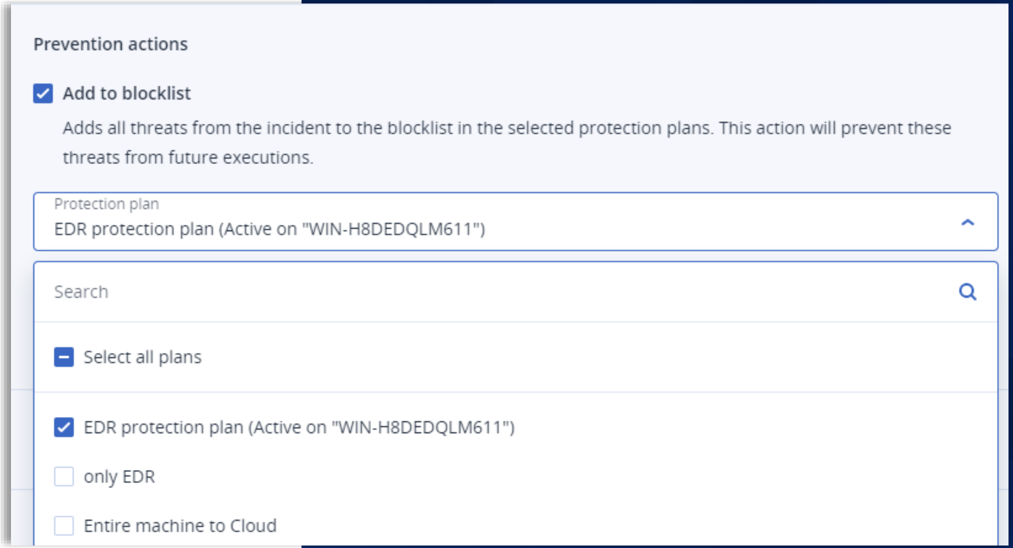
Recovery point: Select

Items to be recovered: **Entire workload**

Remediate Entire Event

Add to Blocklist

- ✓ Block threats from incidents based on selected protection plans
- ✓ Prevent from future execution



Prevention actions

☑ Add to blocklist

Adds all threats from the incident to the blocklist in the selected protection plans. This action will prevent these threats from future executions.

Protection plan: EDR protection plan (Active on "WIN-H8DEDQLM611")

Search

⊟ Select all plans

☑ EDR protection plan (Active on "WIN-H8DEDQLM611")

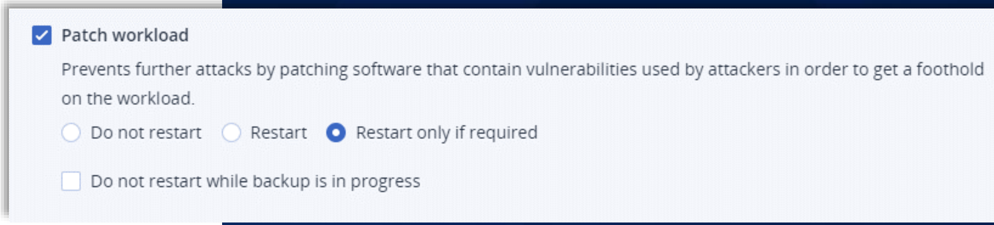
□ only EDR

□ Entire machine to Cloud

Remediate Entire Event

Patching, Closing and Starting Remediation

- ✓ **Patching options**
  - Patch based on protection plan workload belongs to
  - Advanced Management Pack
  - Restart options
- ✓ **Ensure performing vulnerability scans often for updates**
  - Changing investigation state
  - Start remediation based on options selected

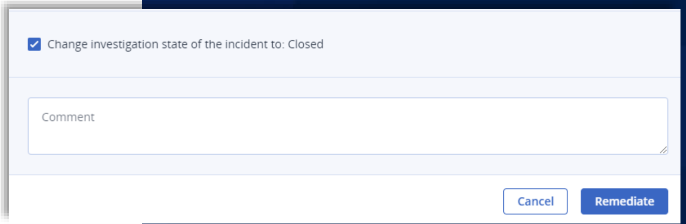


☑ Patch workload

Prevents further attacks by patching software that contain vulnerabilities used by attackers in order to get a foothold on the workload.

○ Do not restart ○ Restart ● Restart only if required

□ Do not restart while backup is in progress



☑ Change investigation state of the incident to: Closed

Comment

Acronis

Thank you for watching!

#CyberFit