CimTrak Integrity Suite

Integrity, Trust, and Resiliency Enterprise-Wide

ALL SECURITY ISSUES START WITH A CHANGE

CIMCOR

DISA Strategic Objective

The current environment of great power competition requires our agency to deliver capability to the warfighter with a velocity of action to win. We must evolve our organizational design and operating processes to align with:

1. next-generation capabilities
2. defend against new cyberspace threats
3. increase lethality for our warfighters while ensuring the best value.

Bottom Line: CimTrak Integrity Suite of products can help with all three of these objectives.

CimTrak Solves Critical Issues for Customers

CIMCOR

COVERING TODAY

- THE PROBLEM WE ARE SOLVING
- BENEFITS
- DEMO
- ZERO TRUST ALIGNMENT
- HOW THIS FITS THE DISA INITIATIVES
- NEXT STEPS
- PROCUREMENT PROCESS & VEHICLES

Achieving Visibility Via Integrity

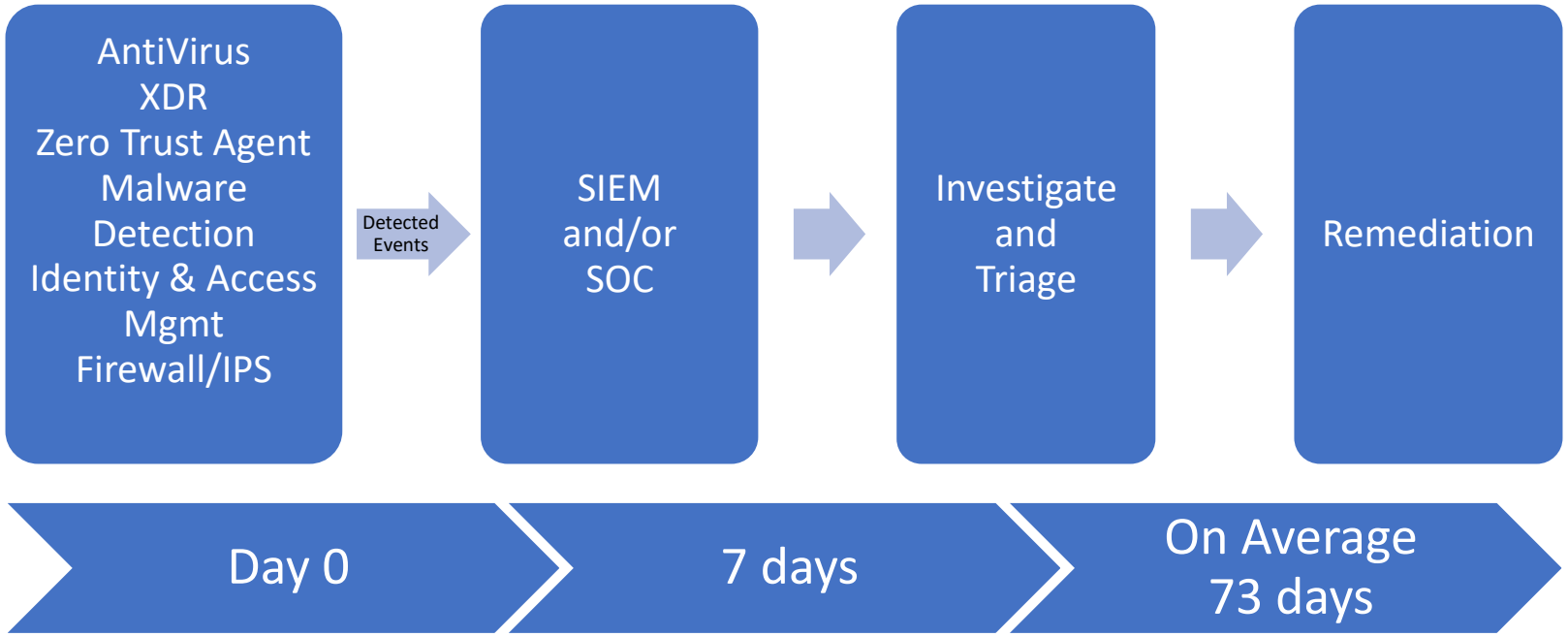
THE CIMTRAK INTEGRITY SUITE

CimTrak detects and prevents unwanted and unexpected changes (malicious and/or circumvented) in real-time to critical IT infrastructure and provides a path to remediate and roll back to create a trusted, secure, and resilient infrastructure at scale…

Bottom Line: **CimTrak Reduces Dwell Time & Increases Resiliency**

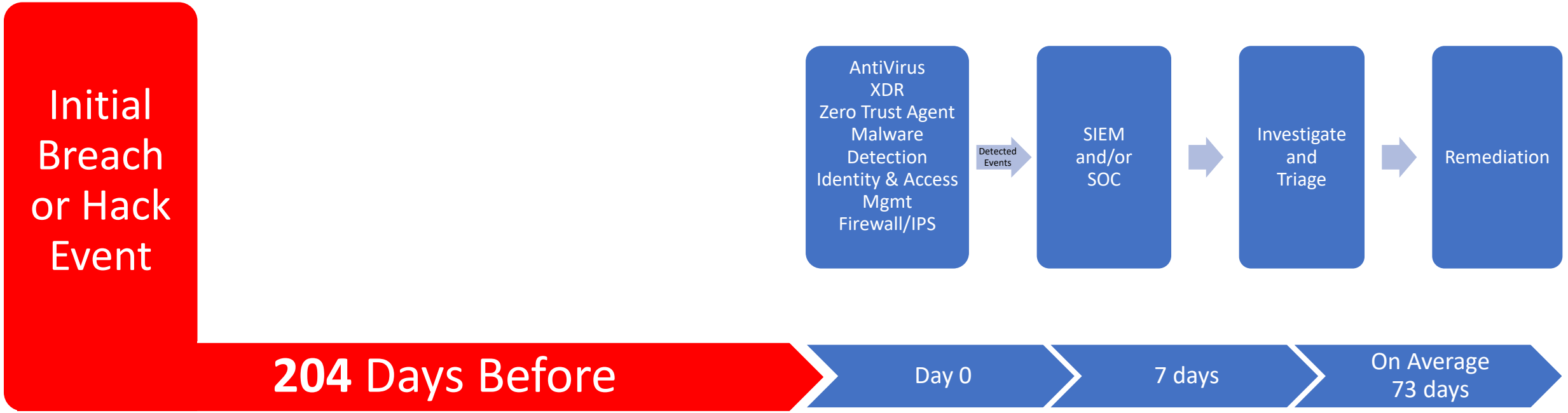
- Multiple Patents on Technology
- CDM Approved Products List

Rethinking Secure Patterns & Prioritizing Focus



Source: IBM Poneman Report 2023

Rethinking Secure Patterns & Prioritizing Focus



Source: IBM Poneman Report 2023

Rethinking Secure Patterns & Prioritizing Focus

CIMCOR

Initial Breach or Hack Event

NEFARIOUS DWELL TIME
- Preparation
- Modification
- Privilege Escalation
- Exfiltration

AntiVirus
XDR
Zero Trust Agent
Malware Detection
Identity & Access Mgmt
Firewall/IPS

Detected Events

SIEM and/or SOC

Investigate and Triage

Remediation

204 Days Before

Day 0

7 days

On Average 73 days

Source: IBM Poneman Report 2023

Rethinking Secure Patterns & Prioritizing Focus

CIMCOR

Initial Breach or Hack Event

NEFARIOUS DWELL TIME
- Preparation
- Modification
- Privilege Escalation
- Exfiltration

AntiVirus
XDR
Zero Trust Agent
Malware Detection
Identity & Access Mgmt
Firewall/IPS

Detected Events

SIEM and/or SOC

Investigate and Triage

Remediation

204 Days Before

Day 0

7 days

On Average 73 days

UNDER-REPRESENTED RISK
- **Unaddressed**
- **Unidentified**
- **Unaccounted**

Source: IBM Poneman Report 2023

Rethinking Secure Patterns & Prioritizing Focus

CIMCOR

Initial Breach or Hack Event

NEFARIOUS DWELL TIME
- Preparation
- Modification
- Privilege Escalation
- Exfiltration

AntiVirus
XDR
Zero Trust Agent
Malware Detection
Identity & Access Mgmt
Firewall/IPS

Detected Events

SIEM and/or SOC

Investigate and Triage

Remediation

204 Days Before

Day 0

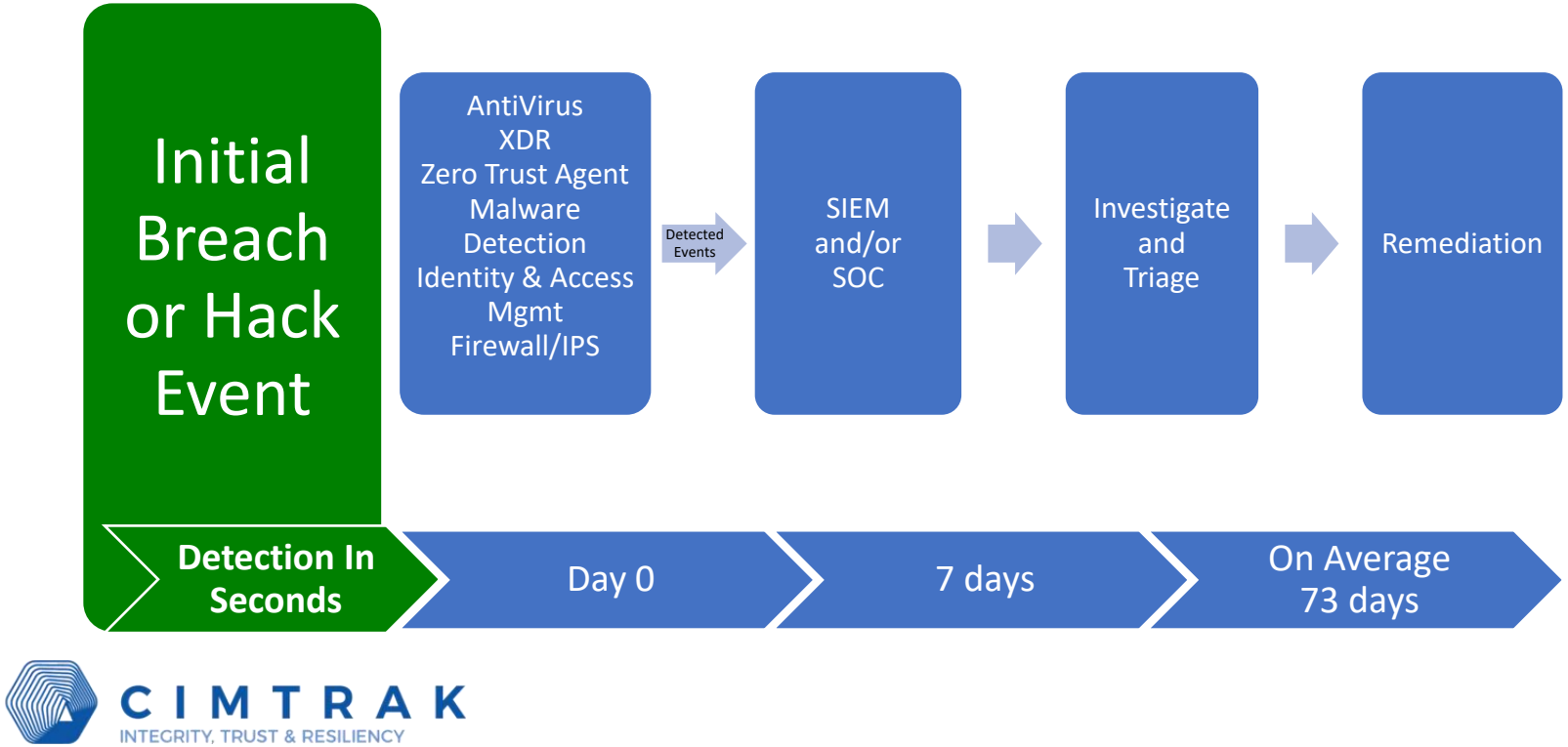
7 days

On Average 73 days

BOTTOM LINE: All of the Time, Energy, and Money invested in these well known, commonly used, enterprise tools DID NOT provide the protection and security their customers were expecting.

Source: IBM Poneman Report 2023

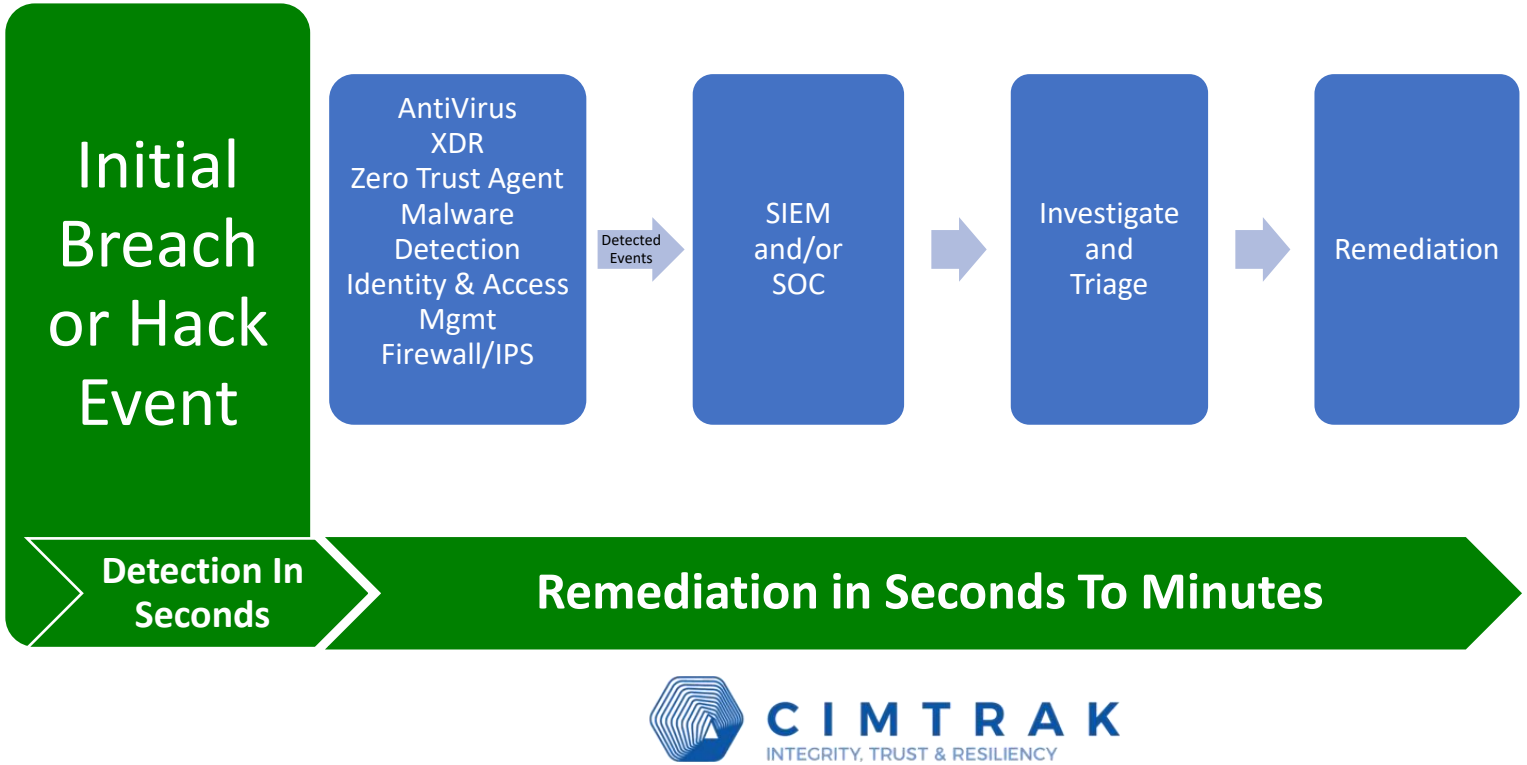
Rethinking Secure Patterns & Prioritizing Focus



CIMTRAK
INTEGRITY, TRUST & RESILIENCY

Source: IBM Poneman Report 2023

Rethinking Secure Patterns & Prioritizing Focus



CIMTRAK
INTEGRITY, TRUST & RESILIENCY

Source: IBM Poneman Report 2023

Achieving Visibility Via Integrity

CIMCOR

HOW DOES CIMTRAK ADD VALUE TO THE ENTERPRISE?

- CimTrak identifies unauthorized and unexpected changes in seconds.
- CimTrak has modes of operation that prevent changes entirely from happening.
- CimTrak can immediately remediate & restore changes manually or automatically.
- CimTrak's ease of use allows it to be deployed and operational in just an hour.
- CimTrak simplifies IT audits by providing forensic evidence for compliance mandates.
- CimTrak can scale to the most demanding environments.
  - On Prem & In-Cloud
    - Example: Zoom Video Communications (Globally)

Why CimTrak Is Vitally Important

MGM

Started with social engineering, later deploying ransomware. **Server Monitoring** would have detected the introduction of malicious executables, alerting security teams before encryption and damage occurred

SolarWinds

Hackers injected malicious code into Orion software, impacting over 18,000 customers. **Code monitoring** would have detected unauthorized code changes and alerted administrators before deployment.

As an Orion customer, **Server Monitoring** for unexpected changes would have identified and alerted Security teams that something was going on.

Equifax

This breach exposed 143 million's personal data by exploiting a web app vulnerability that was not fixed. **Configuration Monitoring** would have detected unauthorized changes, notifying Equifax to patch and prevent the massive data theft.

Colonial Pipeline

The attack leveraged ransomware after compromising an unused VPN. **Active Directory Monitoring** would have notified admins to disable the account stopping lateral movement and disrupted fuel delivery from ever happening.

Ukraine Power Grid

Began with spear phishing, installing malware that altered system files. **Monitoring Installed Software** & **SCADA Monitoring** would have detected unauthorized changes, alerting operators to block the attack before disruption caused over $200 million in damages

World Class Tools Didn't Help, CimTrak Could...

CimTrak Solves Critical Issues for Customers

CRITICAL CAPABILITIES

- **PROTECT** system from unauthorized changes in real-time
- **DETECT** malicious and circumvented changes to critical systems immediately
- **RECOVER** & roll back to previous trusted baselines manually or automatically
- **ENFORCE** regulatory compliance that requires integrity monitoring (FIM)
- **REDUCE COST** of security operations & compliance audit preparation, inspection, assessment, & reporting

Use Case Demo

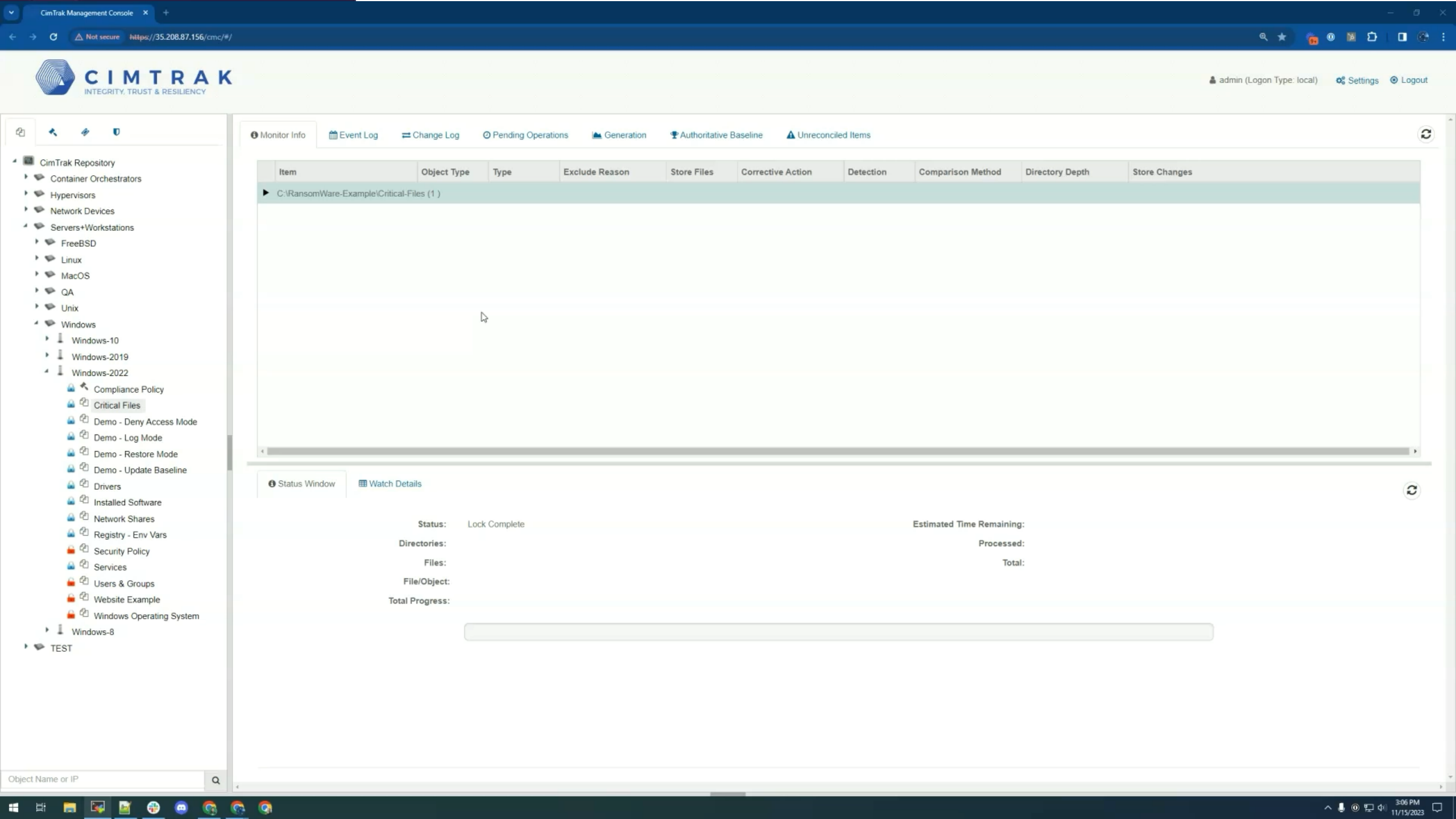
Ransomware

CIMTRAK IS AN EARLY WARNING SYSTEM FOR RANSOMWARE

Demo Link

https://www.loom.com/share/7d00397881f24adb8f6c36bef67bbd54?sid=7984d58c-c31d-4da0-b307-b56a398bf148

CIMCOR


CimTrak Management Console
Not secure https://35.208.87.156/cmc/#/
CIMTRAK
INTEGRITY, TRUST & RESILIENCY
admin (Logon Type: local)
Settings
Logout
CimTrak Repository
Container Orchestrators
Hypervisors
Network Devices
Servers+Workstations
FreeBSD
Linux
MacOS
QA
Unix
Windows
Windows-10
Windows-2019
Windows-2022
Compliance Policy
Critical Files
Demo - Deny Access Mode
Demo - Log Mode
Demo - Restore Mode
Demo - Update Baseline
Drivers
Installed Software
Network Shares
Registry - Env Vars
Security Policy
Services
Users & Groups
Website Example
Windows Operating System
Windows-8
TEST
Object Name or IP
Monitor Info
Event Log
Change Log
Pending Operations
Generation
Authoritative Baseline
Unreconciled Items
Item
Object Type
Type
Exclude Reason
Store Files
Corrective Action
Detection
Comparison Method
Directory Depth
Store Changes
C:\RansomWare-Example\Critical-Files (1)
Status Window
Watch Details
Status:
Lock Complete
Directories:
Files:
File/Object:
Total Progress:
Estimated Time Remaining:
Processed:
Total:
3:06 PM
11/15/2023

Use Case Demo

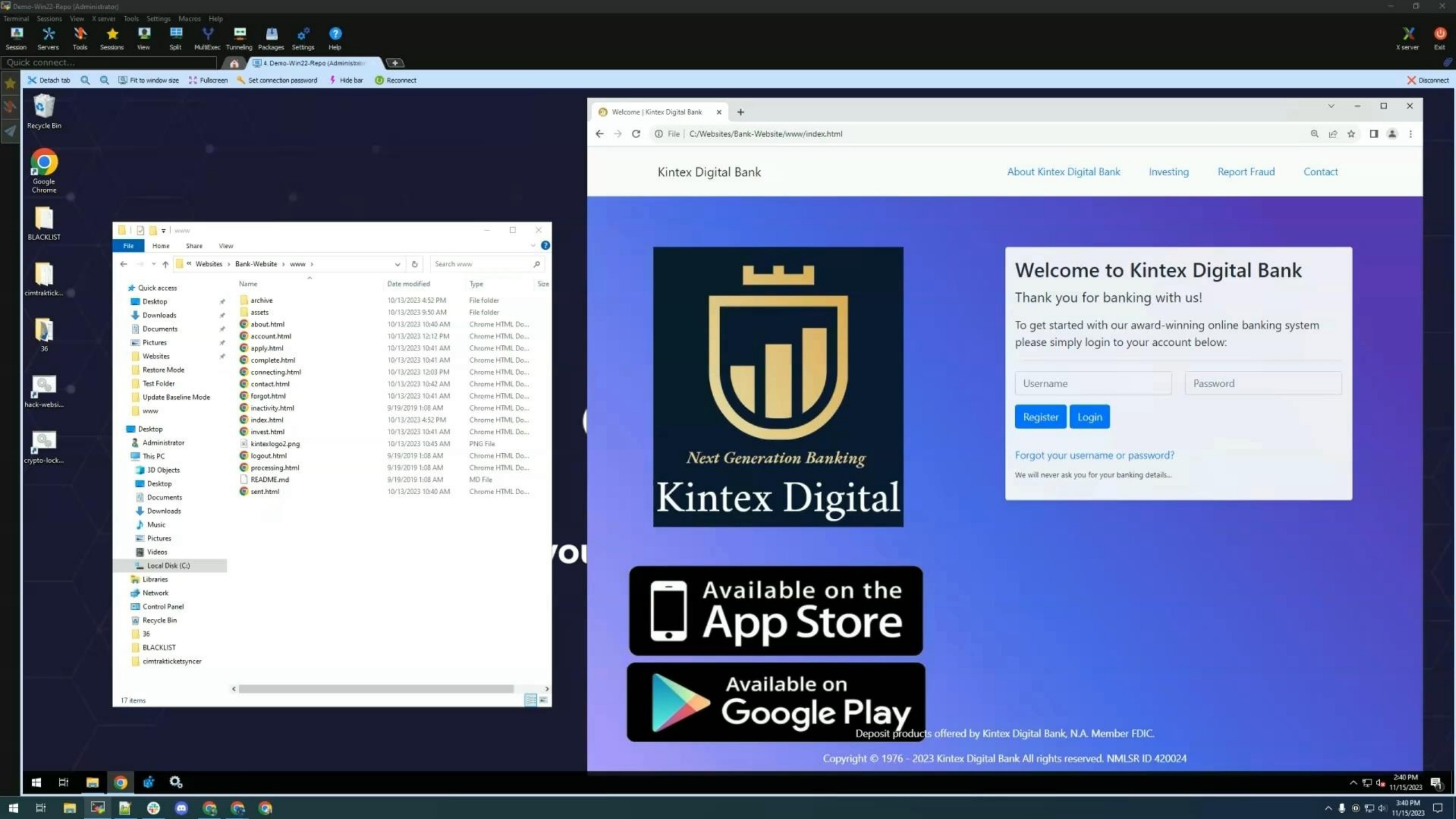
Website Defacement

CIMTRAK CAN PROTECT, DETECT, & RECOVER FROM MALICIOUS CHANGES AUTOMATICALLY

Demo Link

https://www.loom.com/share/9420f99fab5b4e4ab718eb06e0fc32ab?sid=3a850d86-a604-4982-933b-fde2e78cb02c

CIMCOR


Demo-Win22-Repo (Administrator)
Terminal Sessions View X server Tools Settings Macros Help
Session Servers Tools Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
4. Demo-Win22-Repo (Administrator)
Detach tab Fit to window size Fullscreen Set connection password Hide bar Reconnect Disconnect
Recycle Bin
Google Chrome
BLACKLIST
cimtraktick...
36
hack-websi...
crypto-lock...
www
File Home Share View
Websites › Bank-Website › www ›
Search www
Quick access
Desktop
Downloads
Documents
Pictures
Websites
Restore Mode
Test Folder
Update Baseline Mode
www
Desktop
Administrator
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Libraries
Network
Control Panel
Recycle Bin
36
BLACKLIST
cimtrakticketsyncer
Name Date modified Type Size
archive 10/13/2023 4:52 PM File folder
assets 10/13/2023 9:50 AM File folder
about.html 10/13/2023 10:40 AM Chrome HTML Do...
account.html 10/13/2023 12:12 PM Chrome HTML Do...
apply.html 10/13/2023 10:41 AM Chrome HTML Do...
complete.html 10/13/2023 10:41 AM Chrome HTML Do...
connecting.html 10/13/2023 12:03 PM Chrome HTML Do...
contact.html 10/13/2023 10:42 AM Chrome HTML Do...
forgot.html 10/13/2023 10:41 AM Chrome HTML Do...
inactivity.html 9/19/2019 1:08 AM Chrome HTML Do...
index.html 10/13/2023 4:52 PM Chrome HTML Do...
invest.html 10/13/2023 10:41 AM Chrome HTML Do...
kintexlogo2.png 10/13/2023 10:45 AM PNG File
logout.html 9/19/2019 1:08 AM Chrome HTML Do...
processing.html 9/19/2019 1:08 AM Chrome HTML Do...
README.md 9/19/2019 1:08 AM MD File
sent.html 10/13/2023 10:40 AM Chrome HTML Do...
17 items
Welcome | Kintex Digital Bank
File | C:/Websites/Bank-Website/www/index.html
Kintex Digital Bank
About Kintex Digital Bank
Investing
Report Fraud
Contact
Next Generation Banking
Kintex Digital
Welcome to Kintex Digital Bank
Thank you for banking with us!
To get started with our award-winning online banking system please simply login to your account below:
Username
Password
Register
Login
Forgot your username or password?
We will never ask you for your banking details...
Available on the App Store
Available on Google Play
Deposit products offered by Kintex Digital Bank, N.A. Member FDIC.
Copyright © 1976 – 2023 Kintex Digital Bank All rights reserved. NMLSR ID 420024
2:40 PM 11/15/2023
3:40 PM 11/15/2023

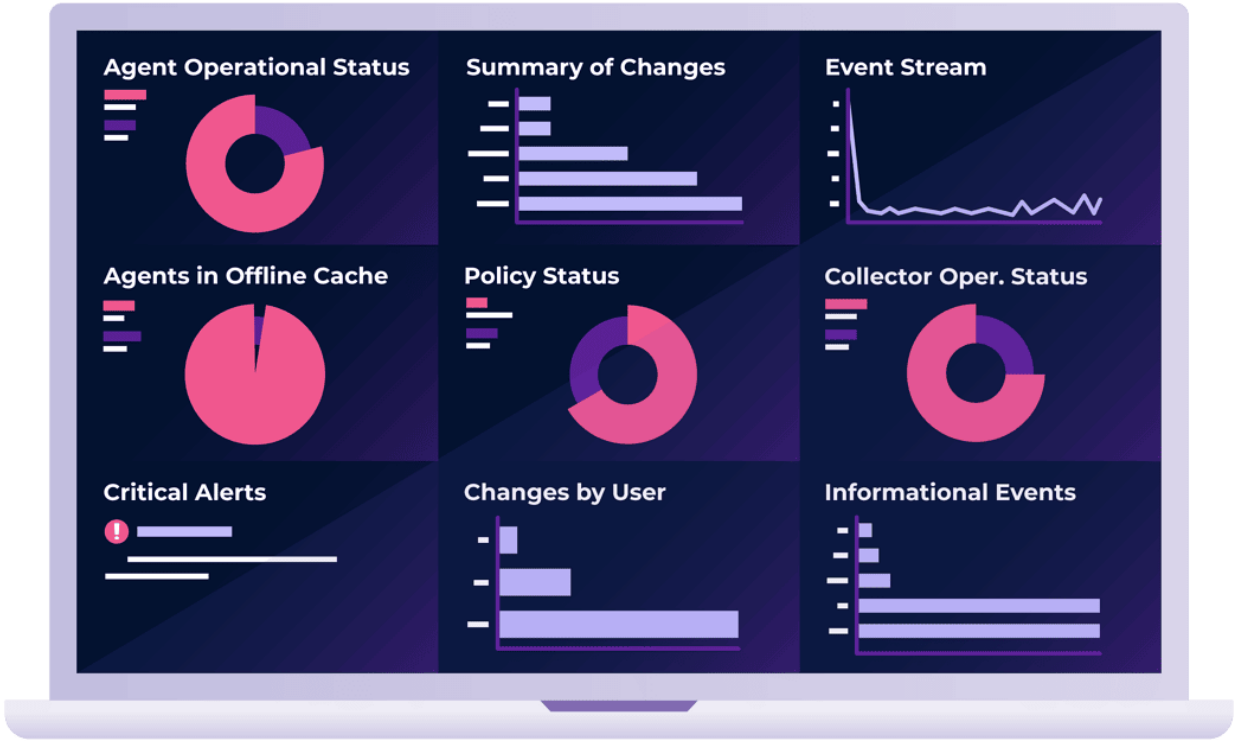
Use Case Demo

Network Device, Database, and ESXi Monitoring

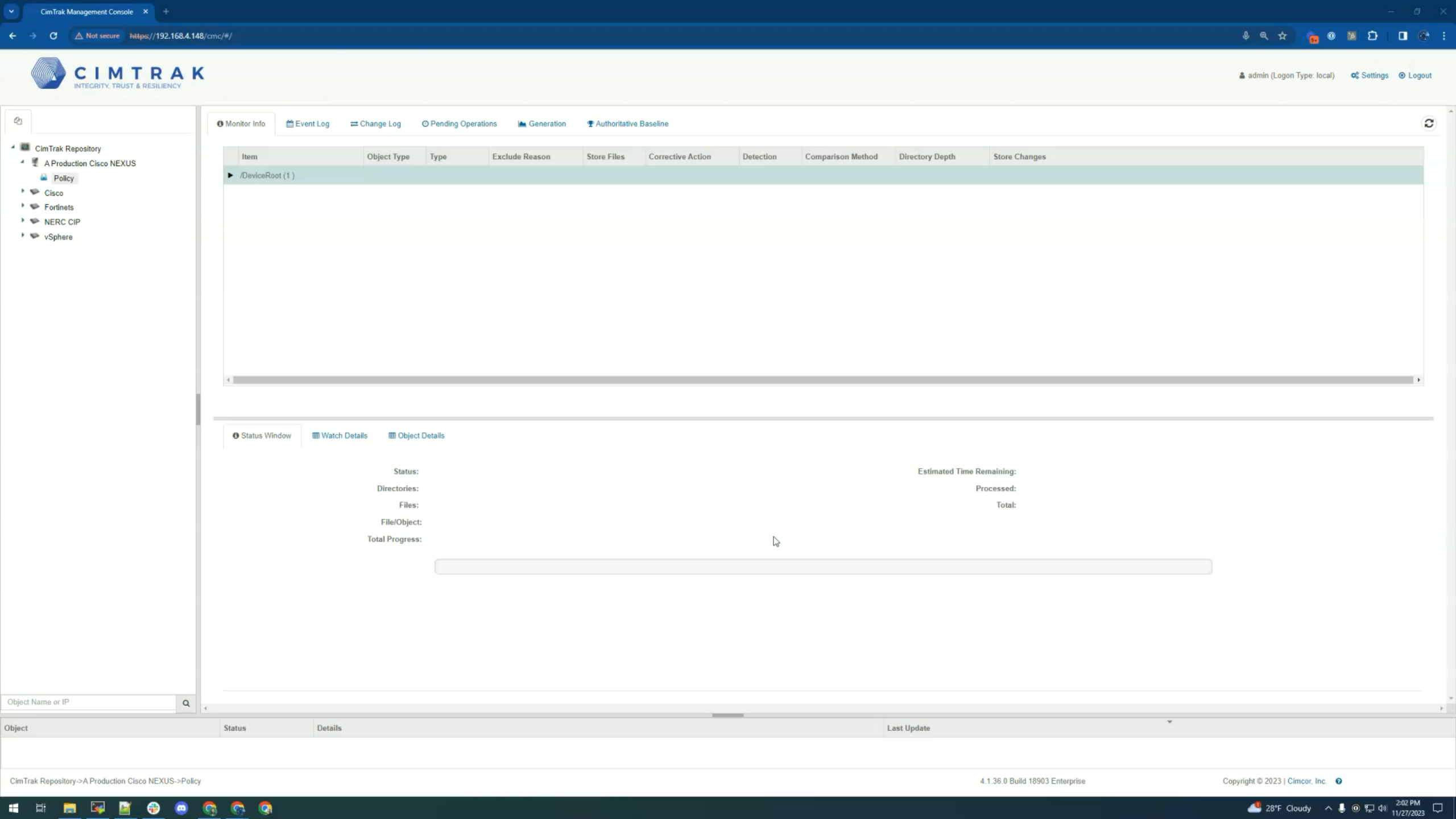
CIMTRAK CAN PROTECT, DETECT, & RECOVER FROM CHANGES TO NETWORK DEVICES, DATABASES, & HYPERVISORS

Demo Link

https://www.loom.com/share/1cc2cdc4592b46f19d5c44788e71cbcd?sid=db337be4-a060-4988-a8e4-943e37883100



CIMCOR


CimTrak Management Console
Not secure https://192.168.4.148/cmc/#/
CIMTRAK
INTEGRITY, TRUST & RESILIENCY
admin (Logon Type: local)
Settings
Logout
CimTrak Repository
A Production Cisco NEXUS
Policy
Cisco
Fortinets
NERC CIP
vSphere
Monitor Info
Event Log
Change Log
Pending Operations
Generation
Authoritative Baseline
Item
Object Type
Type
Exclude Reason
Store Files
Corrective Action
Detection
Comparison Method
Directory Depth
Store Changes
/DeviceRoot (1)
Status Window
Watch Details
Object Details
Status:
Directories:
Files:
File/Object:
Total Progress:
Estimated Time Remaining:
Processed:
Total:
Object Name or IP
Object
Status
Details
Last Update
CimTrak Repository->A Production Cisco NEXUS->Policy
4.1.36.0 Build 18903 Enterprise
Copyright © 2023 | Cimcor, Inc.
28°F Cloudy
2:02 PM
11/27/2023

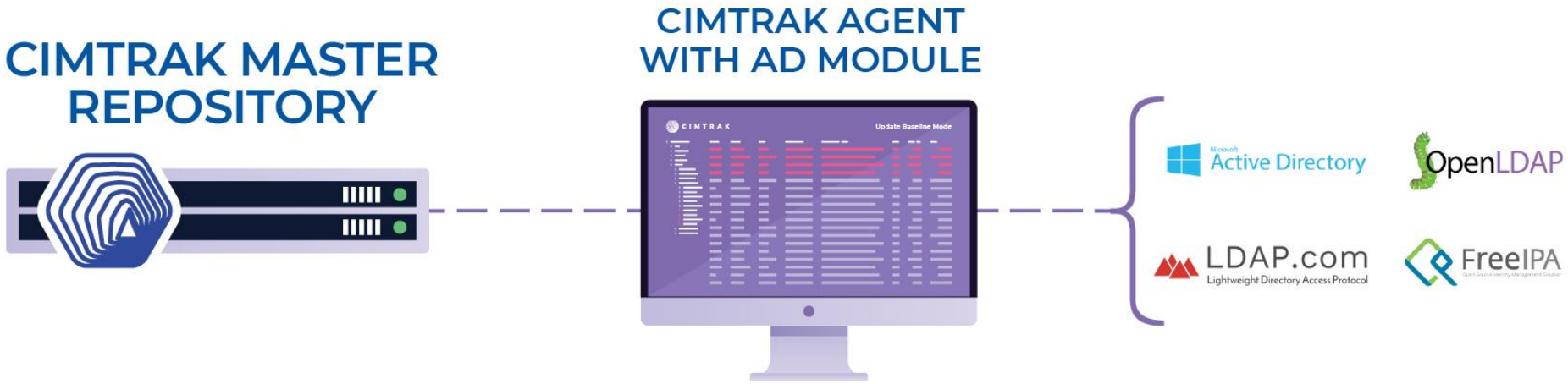
Use Case Demo

Active Directory

CIMTRAK CAN PROTECT, DETECT, & RECOVER CHANGES TO AD/LDAP

Demo Link

https://www.loom.com/share/63549c30c492491ba7089202e199f23b?sid=a04909c1-db5a-4716-a774-b82e87d75222



CIMCOR

CimTrak Management Console | CimTrak Management Console

Search Google or type a URL

CIMTRAK
INTEGRITY, TRUST & RESILIENCY

admin (Logon Type: local) | Settings | Logout

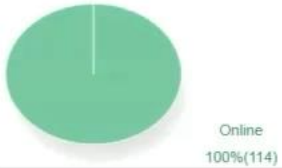
- WIN2019-55
  - Docker Agents
  - EnvironmentA
    - PROD
      - Alma8-78
      - amazon2-79
      - CentOS8-81
      - MacOS-M1-190
      - RHEL7-112
      - SLES12-60
      - Win11-66
      - Win2008-86
      - Win2016-39
      - Win2019-55
        - Compliance Policy
        - Active Directory
        - DenyMode
        - Drivers
        - Installed Software
        - LogMode
        - LogReads
        - Network Share Config
        - NotifyOnly
        - PortMonitor
        - Registry Keys - CimTrak Agent
        - RestoreMode
        - Services
        - UpdateBaseline
        - Users & Groups
        - Windows Operating System
    - STAGING
      - CentOS6-80
      - ESXi-4.3
      - FreeBSD12-35
      - Ubuntu20-85

Object Name or IP

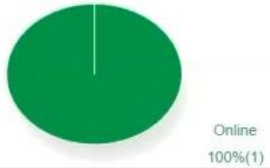
Dashboard | Repository Info | Event Log | Change Log | Logged On Users

All children of Repository: WIN2019-55

Agent Operational Status Chart

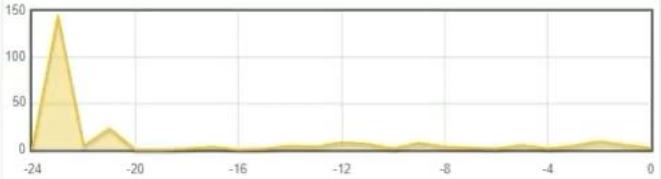


Collector Operational Status Chart

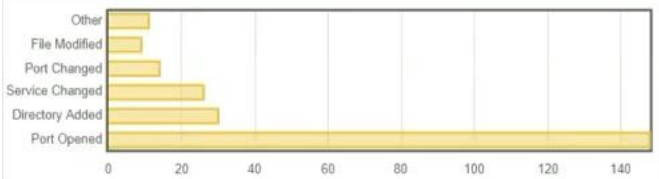


Policy Status

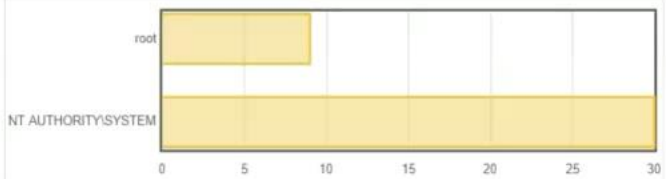
Change Stream (24hrs)



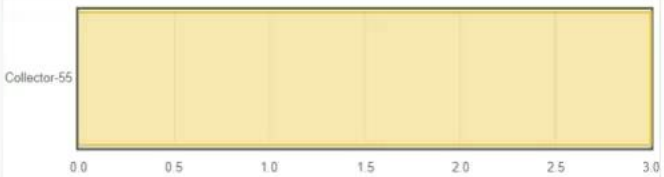
Summary of Changes (24hrs)



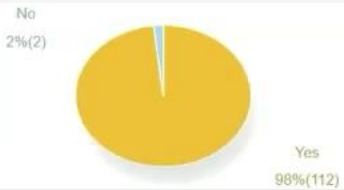
Changes By User (Top 5 in 24hrs)



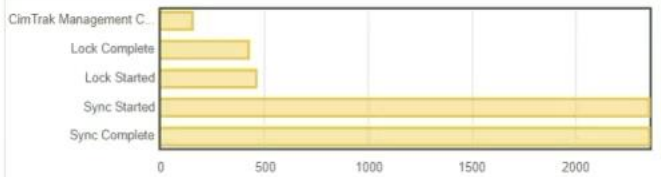
Systems with Alerts (Top 5 in 24hrs)



Agents In Offline Cache Mode



Informational Events (Top 5 in 24hrs)



43°F Sunny | 5:10 PM 11/17/2023

Use Case Demo

Insider Threats

CIMCOR

CIMTRAK CAN HELP BLOCK CHANGES BY INSIDER THREATS

Demo Link https://www.loom.com/share/3b28bfc922c74d9caed0fcfb8f4ed7aa?sid=18b4808f-51d4-421b-8611-580909d06f2d

- **70%** of all DC outages due to human error.
- Nearly **40% of organizations** have suffered a major outage caused by human error over the past three years.
  - Of those incidents, **85% stem from staff failing to follow procedures** or from flaws in the processes and procedures themselves.
- Lots of contractors and personnel are making changes, what visibility do you have?

  Example: FAA

CimTrak Management Console | CimTrak Management Console | CimTrak Management Console | CimTrak Management Console | CimTrak Management Console | CimTrak Management Console | Web Console | LogRhythm

Not secure https://35.208.87.156/cmc/#/

CIMTRAK
INTEGRITY, TRUST & RESILIENCY

admin (Logon Type: local) Settings Logout

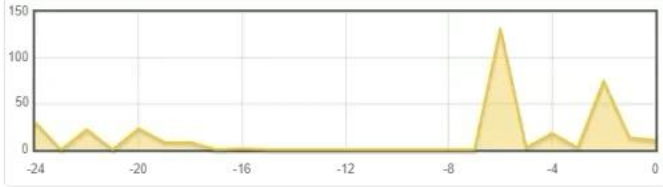
Dashboard | Repository Info | Event Log | Change Log | Logged On Users

- CimTrak Repository
  - Container Orchestrators
  - Hypervisors
  - Network Devices
  - Servers+Workstations
    - FreeBSD
    - Linux
    - MacOS
    - QA
    - Unix
    - Windows
      - Windows-10
      - Windows-2019
      - Windows-2022
        - Compliance Policy
        - Critical Files
        - Demo - Deny Access Mode
        - Demo - Log Mode
        - Demo - Restore Mode
        - Demo - Update Baseline
        - Drivers
        - Installed Software
        - Log Mode TEst Folder
        - Log Reads
        - Network Shares
        - Registry - Env Vars
        - Security Policy
        - Services
        - Users & Groups
        - Website
        - Windows Operating System
      - Windows-8
  - TEST

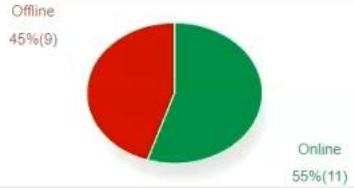
Object Name or IP

All children of Repository: CimTrak Repository

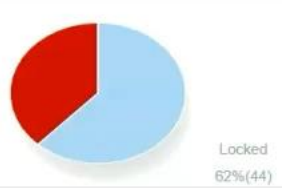
Change Stream (24hrs)



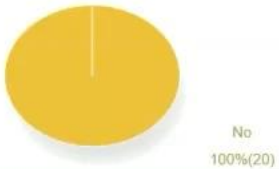
Agent Operational Status Chart



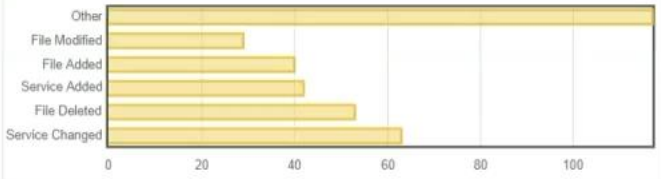
Policy Status



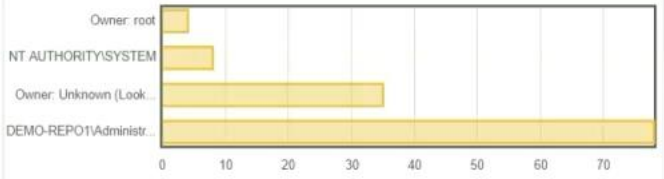
Agents In Offline Cache Mode



Summary of Changes (24hrs)

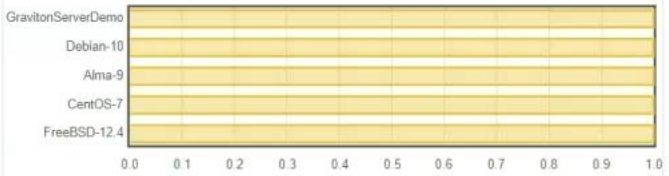


Changes By User (Top 5 in 24hrs)

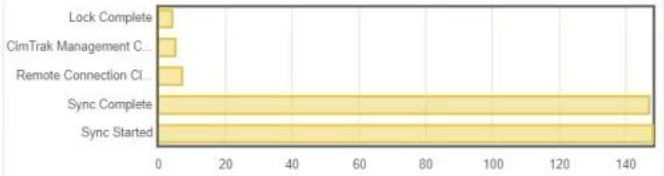


Collector Operational Status Chart

Systems with Alerts (Top 5 in 24hrs)



Informational Events (Top 5 in 24hrs)



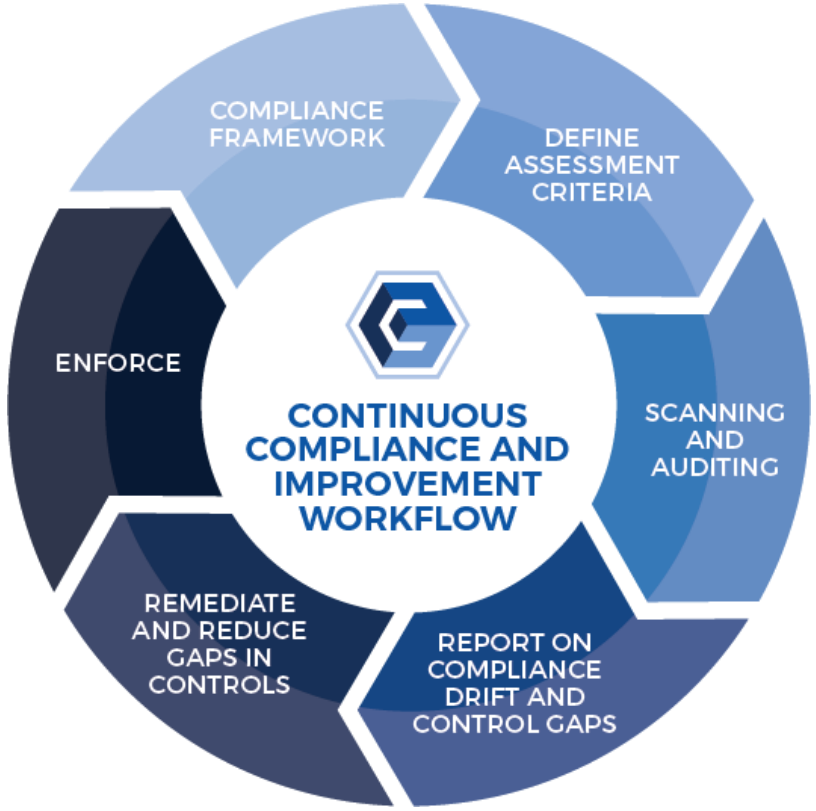
46°F Cloudy 12:59 PM 11/17/2023

Use Case Demo

Continuous Compliance Monitoring

CIMTRAK ENABLES YOU TO MEET CONTINUOUS MONITORING REQUIREMENTS AGAINST DISA STIGS

https://www.loom.com/share/4af455fb39d34f64b3a8c39b862b5535?sid=16ec1077-9f54-4a67-ae67-951278490ded



CIMCOR

CimTrak Management Console | CimTrak Management Console | CimTrak Management Console | CimTrak Management Console | Compliance Benchmark Detail | Compliance Mapping Detail Re | Compliance Mapping Detail Re | Compliance Latest Scan Overvie

Not secure https://192.168.4.55/cmc/#/

CIMTRAK
INTEGRITY, TRUST & RESILIENCY

admin (Logon Type: local) | Settings | Logout

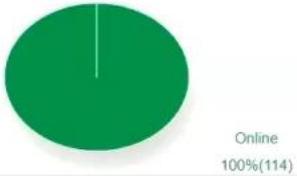
Dashboard | Repository Info | Event Log | Change Log | Logged On Users

- WIN2019-55
  - Docker Agents
  - EnvironmentA
    - PROD
      - Alma8-78
      - amazon2-79
      - CentOS8-81
      - MacOS-M1-190
      - RHEL7-112
      - SLES12-60
      - Win11-66
      - Win2008-86
      - Win2016-39
      - Win2019-55
    - STAGING
      - CentOS6-80
      - FreeBSD12-35
      - Ubuntu20-85
  - ESXi-4.3

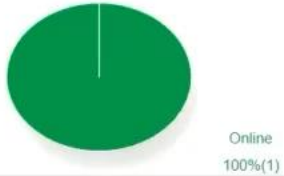
Object Name or IP

All children of Repository: WIN2019-55

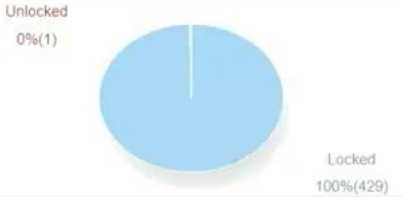
Agent Operational Status Chart



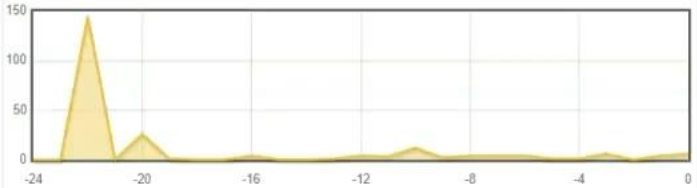
Collector Operational Status Chart



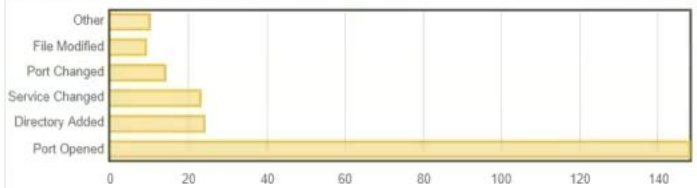
Policy Status



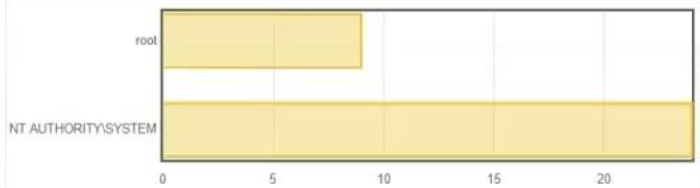
Change Stream (24hrs)



Summary of Changes (24hrs)



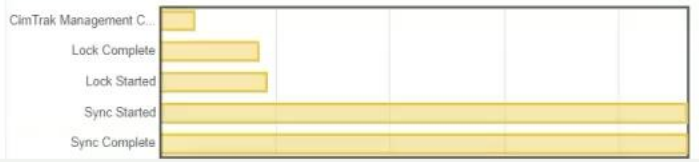
Changes By User (Top 5 in 24hrs)



Systems with Alerts (Top 5 in 24hrs)

Agents In Offline Cache Mode

Informational Events (Top 5 in 24hrs)



Object	Status	Details	Last Update

WIN2019-55 | 4.1.38.0 Build 19002 Enterprise | Copyright © 2023 | Cimcor, Inc.

45°F Partly sunny | 3:34 PM 11/17/2023

Use Case Demos

- ✓ Ransomware
- ✓ Website Defacement
- ✓ ESXi Monitoring
- ✓ AD/LDAP Monitoring
- ✓ Continuous Compliance Monitoring
- ❑ Integrity of Software Supply Chain
- ❑ Network Device Monitoring
- ❑ Monitor & Alert to Cloud Configuration Changes
- ❑ Changes to Database Schemas, Configurations, Triggers, Stored Procedures, Users, etc.
- ❑ Monitor, Alert, & Log ALL Changes to a Container or Manager
- ❑ Monitor, Alert, & Log Changes to IOT or Odd Devices via SSH

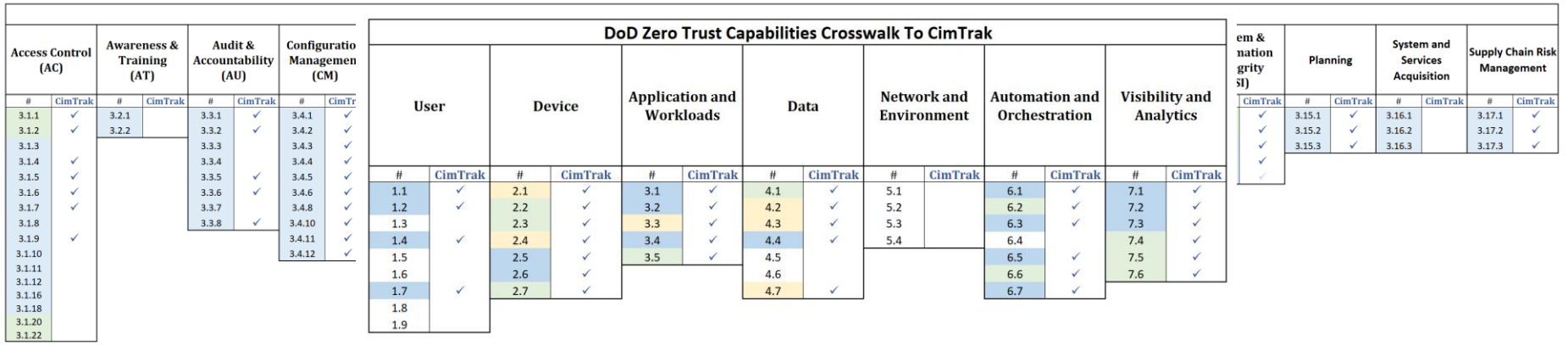
CIMCOR

CimTrak & Control Crosswalks

CimTrak Crosswalk Summary

Compliance/Best Practice Framework(s)	Crosswalk Details		CimTrak/ Control	%	Total Controls	Total Coverage
NIST 800-53 r5	CimTrak Enables or Provides a Solution Within The Domain Sub-Control Category		79/298		+1000	27%
NIST 800-171 r3	CimTrak Meets The Requirement		24/95	25%	95	42%
	CimTrak Enables or Provides Ancillary Capability or Functionality		16/95	17%		
CMMC v2	CimTrak Helps Meet The Requirement or Enables or Provides Ancillary Capability or Functionality	CMMC Level 1	4/13	31%	95	51%
		CMMC Level 2	40/95	51%		
DoD ZT Capability Execution Roadmap (COA 1)	CimTrak Meets The Capability		10/45	22%	45	73%
	CimTrak Enables Capability/Function		17/45	38%		
	CimTrak Provides Ancillary Capability/Function		6/45	13%		

Crosswalks are determined if CimTrak provides a control, automated scan, or enables a process, procedure, or policy to assist with the evidence collection necessary to meet the objective of the defined domain, category, control, standard, component, or assessment factor.



Access Control (AC)		Awareness & Training (AT)		Audit & Accountability (AU)		Configuratio Managemen (CM)	
#	CimTrak	#	CimTrak	#	CimTrak	#	CimTr
3.1.1	✓	3.2.1		3.3.1	✓	3.4.1	✓
3.1.2	✓	3.2.2		3.3.2	✓	3.4.2	✓
3.1.3				3.3.3		3.4.3	✓
3.1.4	✓			3.3.4		3.4.4	✓
3.1.5	✓			3.3.5	✓	3.4.5	✓
3.1.6	✓			3.3.6	✓	3.4.6	✓
3.1.7	✓			3.3.7		3.4.8	✓
3.1.8				3.3.8	✓	3.4.10	✓
3.1.9	✓					3.4.11	✓
3.1.10						3.4.12	✓
3.1.11							
3.1.12							
3.1.16							
3.1.18							
3.1.20							
3.1.22							

DoD Zero Trust Capabilities Crosswalk To CimTrak

User		Device		Application and Workloads		Data		Network and Environment		Automation and Orchestration		Visibility and Analytics	
#	CimTrak	#	CimTrak	#	CimTrak	#	CimTrak	#	CimTrak	#	CimTrak	#	CimTrak
1.1	✓	2.1	✓	3.1	✓	4.1	✓	5.1		6.1	✓	7.1	✓
1.2	✓	2.2	✓	3.2	✓	4.2	✓	5.2		6.2	✓	7.2	✓
1.3		2.3	✓	3.3	✓	4.3	✓	5.3		6.3	✓	7.3	✓
1.4	✓	2.4	✓	3.4	✓	4.4	✓	5.4		6.4		7.4	✓
1.5		2.5	✓	3.5	✓	4.5				6.5	✓	7.5	✓
1.6		2.6	✓			4.6				6.6	✓	7.6	✓
1.7	✓	2.7	✓			4.7	✓			6.7	✓		
1.8													
1.9													

em & nation grity SI)		Planning		System and Services Acquisition		Supply Chain Risk Management	
CimTrak	#	CimTrak	#	CimTrak	#	CimTrak	
✓	3.15.1	✓	3.16.1		3.17.1	✓	
✓	3.15.2	✓	3.16.2		3.17.2	✓	
✓	3.15.3	✓	3.16.3		3.17.3	✓	
✓							
✓							

✓ CimTrak Helps Meet The Requirement or Enables or Provides

4/13	31%	CMMC Level 1
40/95	51%	CMMC Level 2

CMMC L1 r2 was 17
CMMC L2 r2 was 11

The chart above is a crosswalk for all CimTrak products if they provide control, automated scan or enable a process, procedure or policy to assist with the evidence collection to meet the objective of a define domain, category, control, standard, component or assessment facto

✓ CimTrak Helps Meet The Requirement or Enables or Provides Ancillary Capability or Functionality

10/45	22%	CimTrak Meets The Capability
17/45	38%	CimTrak Enables Capability/Function
6/45	13%	CimTrak Provides Ancillary Capability/Function

The chart above is a crosswalk for all CimTrak products if it provides a control, automated scan, or enables a process, procedure, or policy to assist with the evidence collection to meet the criteria of the DoD's defined capabilities definition.

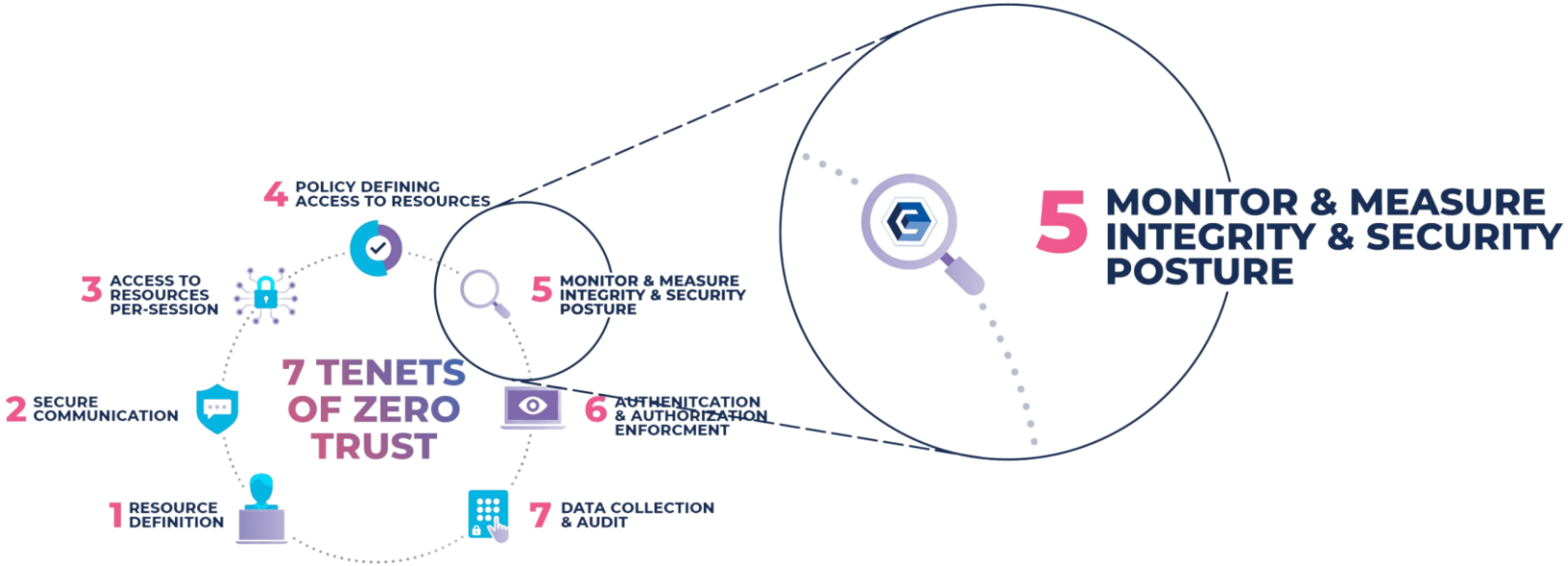
SC-51

CIMCOR

CimTrak & Zero Trust Alignment

CimTrak's core functionality is so CRITICAL that it is called out as TENET #5

> The enterprise MONITORS & MEASURES the INTEGRITY and SECURITY POSTURE of all owned & associated assets"
>
> *ZERO TRUST, NIST 800-207, TENET #5*



CIMCOR

CimTrak + Zscaler

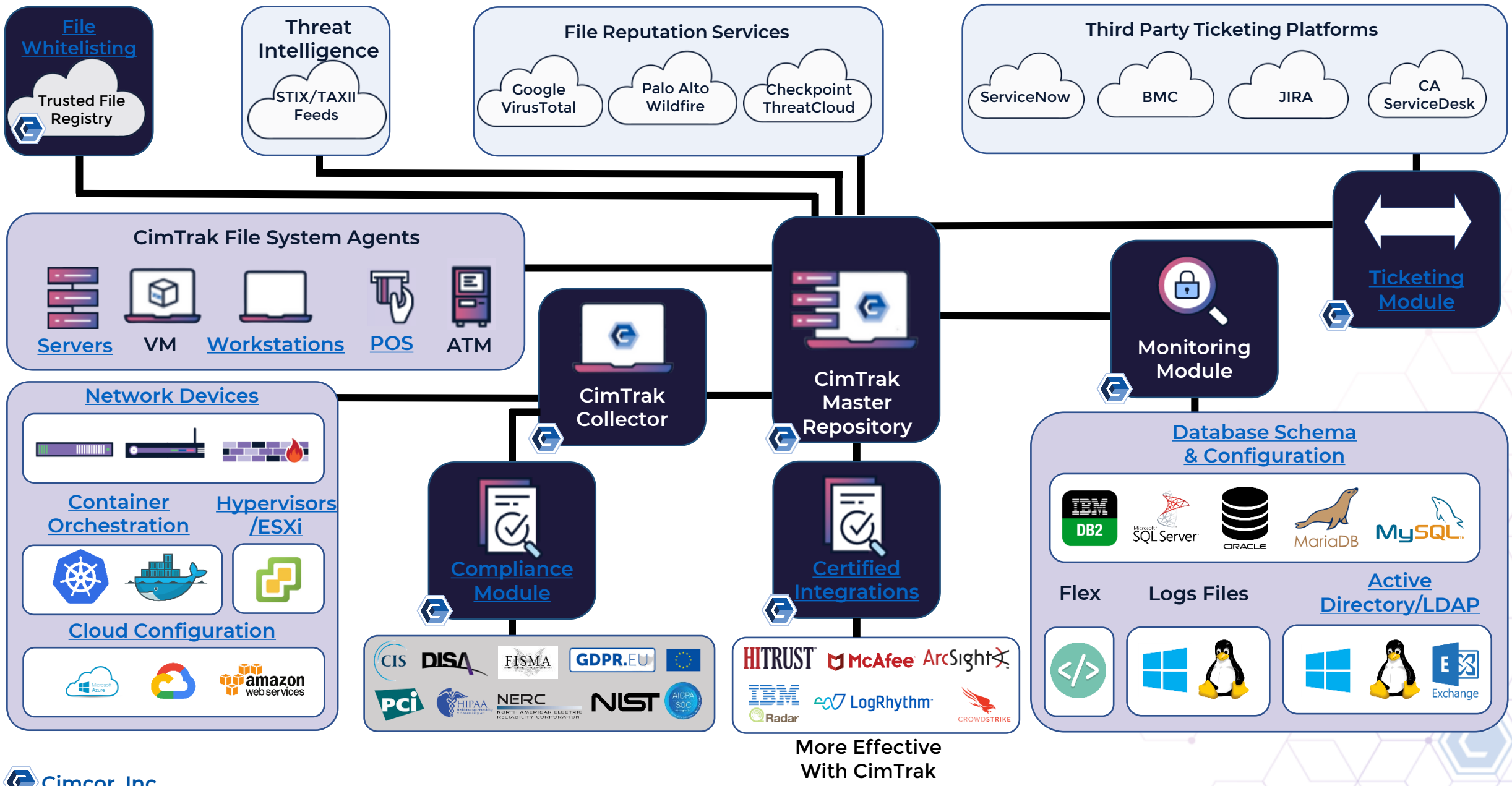
= Zero Trust Platform

“Cimcor has completed initial integration with Zscaler's platform and is working to further enhance additional integrity assurance capabilities for the purpose of further protecting joint warfighter operations in defense of our nation."

Integration Capabilities Include:

- Monitor Zscaler Configuration settings for ZIA, ZPA, ZCC and ZDX to help meet continuous monitoring requirements of NIST 800-172
- Automatically enable Zscaler Browser Isolation if System Integrity compromised
- Automatically enable Zscaler Browser Isolation if System is No Longer STIGed
- Automatically isolate endpoint via Zscaler if Endpoint Integrity is compromised
- Automatically isolate endpoint via Zscaler if Endpoint is no longer STIGed.
- Integration support for several ZPA policy types

CIMCOR


File Whitelisting
Trusted File Registry
Threat Intelligence
STIX/TAXII Feeds
File Reputation Services
Google VirusTotal
Palo Alto Wildfire
Checkpoint ThreatCloud
Third Party Ticketing Platforms
ServiceNow
BMC
JIRA
CA ServiceDesk
CimTrak File System Agents
Servers
VM
Workstations
POS
ATM
CimTrak Collector
CimTrak Master Repository
Monitoring Module
Ticketing Module
Network Devices
Container Orchestration
Hypervisors /ESXi
Cloud Configuration
amazon web services
Compliance Module
CIS
DISA
FISMA
GDPR.EU
PCI
HIPAA
NERC
NIST
AICPA SOC
Certified Integrations
HITRUST
McAfee
ArcSight
IBM Radar
LogRhythm
CROWDSTRIKE
Database Schema & Configuration
IBM DB2
Microsoft SQL Server
ORACLE
MariaDB
MySQL
Flex
Logs Files
Active Directory/LDAP
Exchange
More Effective With CimTrak
Cimcor, Inc.

All Security Issues Start With a Change...

CIMCOR

CimTrak Reduces Dwell Time & Increases Resiliency

Utilizing DISA STIGs:
- CimTrak utilizes STIGs as a best practice to create a foundation of trust
- CimTrak provides prescriptive guidance to fix failed configuration

REDUCES Man-Hours To:
- CimTrak can identify unknown threats, unwanted/unexpected changes
- CimTrak can remediate and recover to trusted baselines in seconds
- CimTrak can provide necessary evidence to meet all major compliance mandates
- CimTrak can deploy secure configurations and ensure they remain trusted

IMPROVES:
- Cyber threat detection and resiliency
- Ability to detect unknown, unexpected, and unplanned changes
- Utilization of current investments (SIEM, ITSM, etc.)

QUESTIONS?

Contact:
Robert Johnson
Johnson.Robert@Cimcor.com
219-670-0104

Mark Allers
Allers.Mark@Cimcor.com
503-705-4779

www.Cimcor.com

CIMCOR

Corporate Headquarters
8488 Georgia St Suite A
Merrillville, IN 46410

Commercial/International Sales:
+1 219-736-4400 ext. 6099
U.S. Federal Government Sales:
219-736-4400 ext. 6097

commercialsales@cimcor.com
governmentsales@cimcor.com