



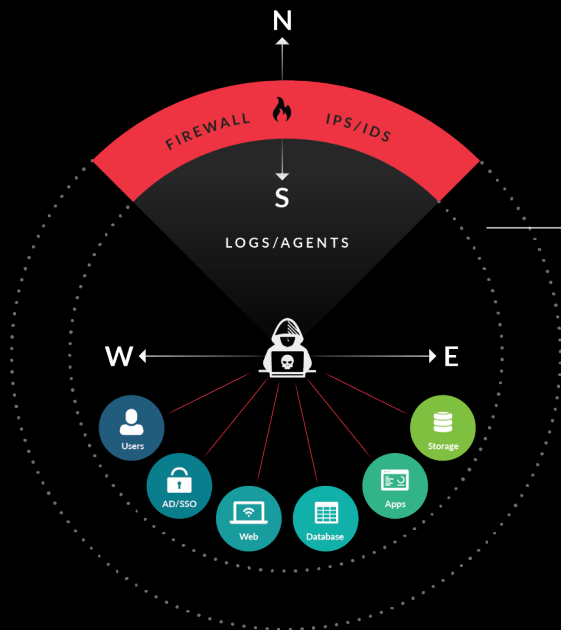
# SECURITY UNCOMPROMISED

Defense Designed for  
Advanced Threats



# Advanced Threats Bypass Traditional Defenses

If you were compromised, how would you know?



## 70% DARKSPACE

Attackers bypass defenses and have free rein



## 67% ENCRYPTED TRAFFIC

Malicious traffic is often encrypted



## 56 DAYS OF DWELL TIME

Median before attackers are found



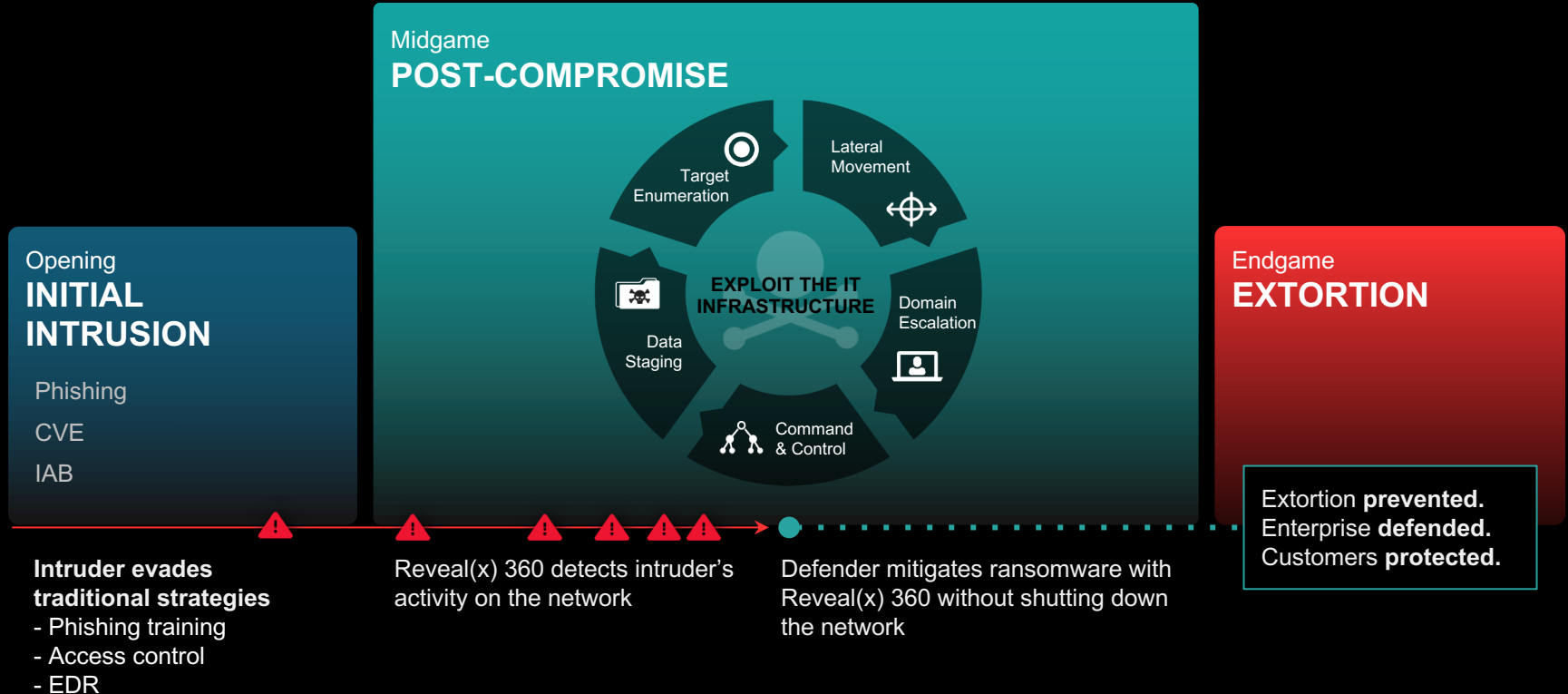
## 72% DESTRUCTION OF LOGS

Attackers easily cover their tracks

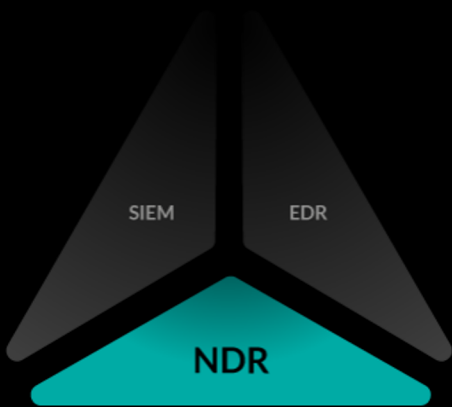
```
meterpreter > run clearlogs
Clearing event logs, this will leave an event 517
[*] Clearing the security Event log
[*] Clearing the system Event log
[*] Clearing the application Event log
[*] Clearing the directory Event log
[*] Clearing the dns server Event log
[*] Clearing the file replication service Event log
All Clear! You are a Ninja!
meterpreter >
```

# Stop Ransomware in the Midgame.

Prevent Real Damage. Reduce the Blast Radius.



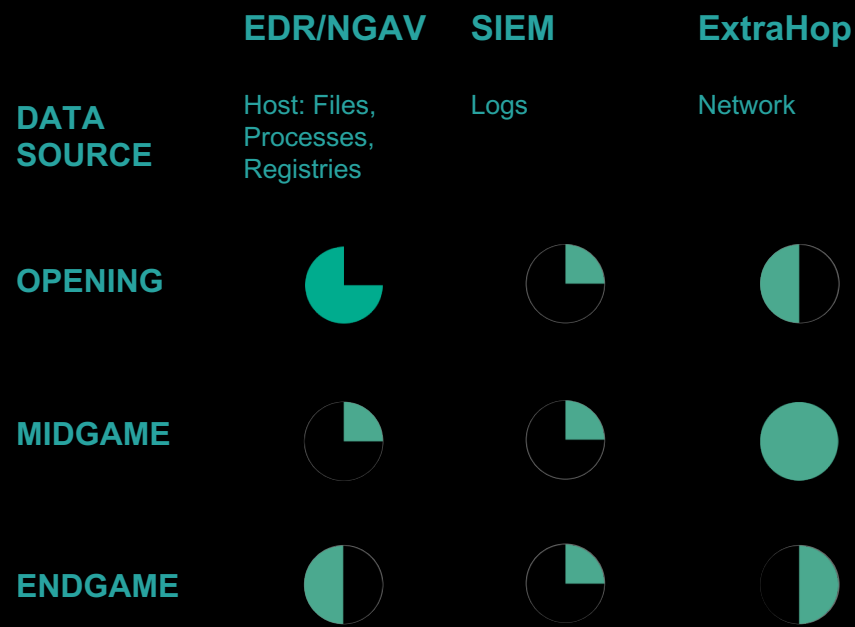
# Gartner's Security Operations Center (SOC) Visibility Triad - Damage Prevention Efficacy




“

"seeks to significantly reduce the chance that the attacker will operate on your network long enough to accomplish their goals."

ANTON CHUVAKIN  
Then: VP ANALYST, GARTNER RESEARCH



# Ransomware as a Service (RaaS): DarkSide, REvil, Dharma, LockBit, etc



WIKIPEDIA  
Die freie Enzyklopädie

Hauptseite  
Themenportale  
Zufälliger Artikel

Mitmachen

Artikel verbessern  
Neuen Artikel anlegen  
Autorenportal  
Hilfe  
Letzte Änderungen  
Kontakt  
Spenden

Werkzeuge

Links auf diese Seite  
Änderungen an verlinkten Seiten  
Spezialseiten  
Permanenter Link  
Seiteninformationen  
Artikel zitieren  
Wikidata-Datenobjekt

Drucken/exportieren  
Buch erstellen  
Als PDF herunterladen  
Druckversion

In anderen Sprachen

Afrikaans  
English  
Español  
日本語  
Русский  
Українська  
中文

Nicht angemeldet Diskussionseite Beiträge Benutzerkonto erstellen Anmelden

Lesen Bearbeiten Quelltext bearbeiten Versionsgeschichte Wikipedia durchsuchen

## DarkSide (Hackergruppe)

**DarkSide** ist eine wahrscheinlich osteuropäische Gruppe von **Crackern**, die sich auf **Ransomware** spezialisiert hat und dies auch „as a Service“ anbietet (sogenanntes RaaS). Die Gruppe hat sich vor allem auf finanzstarke Opfer spezialisiert und fährt ihre Attacken individualisiert, das heißt, der Code ist auf das Opfer zugeschnitten. Nach eigenen Angaben attackiert die Gruppe keine **kritischen Infrastrukturen**, wie beispielsweise **Krankenhäuser**.

### Methoden

Die Gruppe versucht über **TOR**, einen **Windows-Computer** zu infiltrieren. Es wird darauf geachtet, dass keine Nodes mit **Endpoint Detection & Response** verwendet werden. Nach einer Warteperiode versucht man, sich im System zu verschleiern, vor allem werden **Logdateien** gelöscht, um bei einer späteren forensischen Analyse möglichst nicht (oder zumindest erst spät) entdeckt zu werden. Anschließend werden Zugangsinformationen ausgespäht. Über **Filessharing** werden weitere Computer infiziert. **Datelarchive** werden gebildet. Bei den Opfern wird die **Dateiberechtigung** so geändert, dass mehr Benutzer Lese- und Schreibrechte erhalten. Der nächste Schritt ist, **Datensicherungen** (Backups) zu löschen. Auch **Schattenkopien** werden gelöscht. Am Ende folgt die Verschlüsselung ausgewählter Dateien, um ein Lösegeld zu erpressen.<sup>[1]</sup>

Die Gruppe hat auch einen Leaking-Server in Iran aufgestellt, um an Informationen zu gelangen, wie staatliche Stellen oder andere Crackinggruppen versuchen, DarkSide zu schaden.<sup>[2][1]</sup>

### Angriffe

Aktiv wurde die Gruppe etwa im August 2020. Ihr bekanntestes Opfer war bisher **Colonial Pipeline** in den USA. Der Pipelinebetreiber fuhr nach dem Angriff sein IT-System herunter, was dazu führte, dass er im Mai 2021 an der **Ostküste** keine **Ölprodukte** liefern konnte.<sup>[3]</sup> Der Betreiber hat etwa 4,4 Millionen **Dollar** an Lösegeld gezahlt. Bei den Ermittlungen ist es dem **FBI** innerhalb eines Monats gelungen, den **privaten Schlüssel** eines **Wallets** von DarkSide in Besitz zu nehmen. So konnten 63,7 **Bitcoin**s, oder umgerechnet 2,26 Millionen Dollar, zurückerlangt werden. Des Weiteren ist Anfang Juni bekannt geworden, dass ein kompromittierter **VPN**-Zugang genutzt wurde, um bei Colonial Pipeline einzudringen. Ein IT-Sicherheitsspezialist sagte aus, dass dieses VPN-Konto keine **Zwei-Faktor-Authentisierung** hatte und das **Passwort** unsicher gewesen sei. Dieses Passwort tauchte später auch im **Darknet** auf.<sup>[4]</sup>

Nach dem Angriff auf Colonial Pipeline wurden auch noch weitere Attacken auf IT-Systeme mit DarkSide in Verbindung gebracht. So wurde der irische Gesundheitsdienst **Health Service Executive** angegriffen, welcher Ähnlichkeiten zum Angriff auf Colonial Pipeline zeigte.<sup>[5]</sup> Auch teilte die **Toshiba TEC France Imaging Systems SA**, eine französische Tochter der japanischen **Toshiba**, mit, dass DarkSide sie Anfang Mai angegriffen habe, jedoch nur eine geringe Datenmenge abgeflissen sei.<sup>[6]</sup>

### Einzelnachweise

- <sup>1</sup> <sup>a</sup> <sup>b</sup> Snir Ben Shmuel: *Return of the Darkside: Analysis of a Large-Scale Data Theft Campaign*. 10. Mai 2021, abgerufen am 13. Mai 2021 (englisch).
- <sup>2</sup> *DarkSide Ransomware*. Enterprise malware with links to GandCrab and Sodinokibi. Abgerufen am 13. Mai 2021 (englisch).
- <sup>3</sup> *Colonial Pipeline nimmt Betrieb nach Cyberattacke wieder auf*. Es werde noch mehrere Tage dauern, bis die Anlage wieder normal läuft, heißt es vom Betreiber. Unterdessen geht Tausenden Tankstellen im Osten der USA das Benzin aus. In: *Zeit Online*. Zeit Online GmbH, 13. Mai 2021, abgerufen am 13. Mai 2021.
- <sup>4</sup> *Das FBI holt 2 Millionen von Ransomware-Gang Darkside zurück*. In: *Insidre IT*. 8. Juni 2021, abgerufen am 8. Juni 2021.
- <sup>5</sup> *Irlands Gesundheitsdienst schaltet IT-Systeme ab*. Nach der Attacke auf die US-Benzinpipeline hat die Hackergruppe DarkSide offenbar erneut zugeschlagen. Bei Angriffen auf das irische Gesundheitssystem und Toshiba wurden ähnliche Erpressungstrojaner verwendet. 14. Mai 2021, abgerufen am 8. Juni 2021.
- <sup>6</sup> *Toshiba in Europa Ziel eines Hackerangriffs*. Nach Unternehmensangaben ist Toshiba Tec Anfang Mai von der Gruppe gehackt worden, die womöglich auch hinter dem Pipeline-Angriff in den USA steckt. Abgerufen am 8. Juni 2021.

Kategorie: Computer- und Internetkriminalität

# Without Decryption, You are Blind to 60% of the Most Exploited Network Vulnerabilities

CVE Number	Vendor	Type	Exploitable via encrypted channel
CVE-2019-19781	Citrix	Code Execution	Yes
CVE 2018-13379	Fortinet	Path Traversal	Yes
CVE 2020-5902	F5 BIG-IP	RCE	Yes
CVE 2020-15505	MobileIron	RCE	Yes
CVE-2019-11580	Atlassian	RCE	Yes
CVE-2019-0604	Microsoft Sharepoint	RCE	Yes
CVE-2021-26855 - ProxyLogon	Microsoft Exchange	RCE	Yes
CVE-2021-22893	Pulse Secure	Authentication Bypass	Yes
CVE-2021-21985	VMWare vCenter	RCE	Yes
CVE-2020-1472 - ZeroLogon	Microsoft Active Directory	Privilege Escalation	No
CVE-2021-34527 - PrintNightmare	Microsoft Windows	RCE	Yes

# Strategic Decryption Exposes Advanced Threats

## Challenges

Decryption of all traffic is impractical

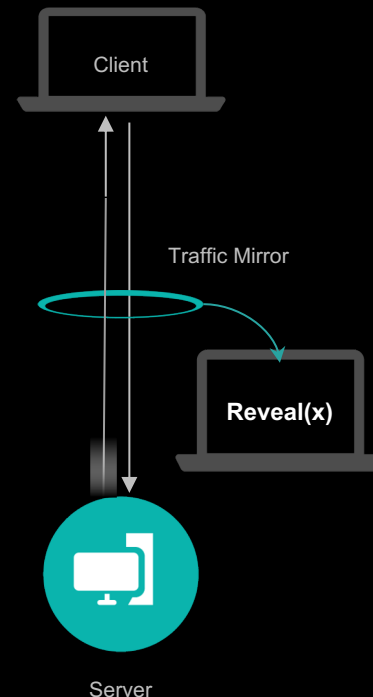
- Browsers do not share PFS keys
- Malware often implements custom keys
- BYOD/IOT devices often have vendor keys
- The most common infection vector remains email

## The Solution

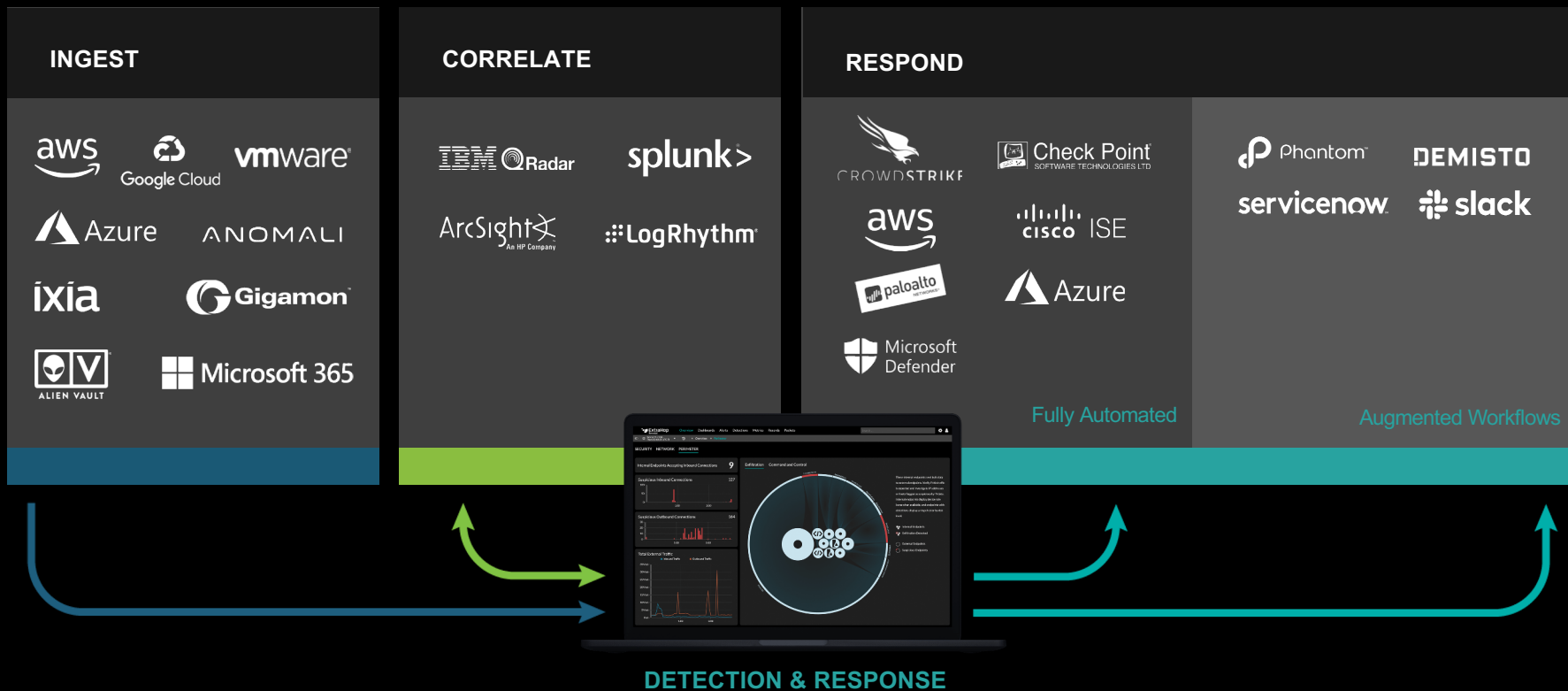
Strategic Out-of-Band Decryption

- Decrypt traffic to and from public facing servers
- Decrypt traffic interacting with internal servers and services
- Decrypt Microsoft authentication and application protocols
  - detect Living-off-the-Land attacks
  - privilege escalation
  - data theft

Out of band decryption + Full Stream Reassembly + Comprehensive protocol parsing = High Fidelity Detections



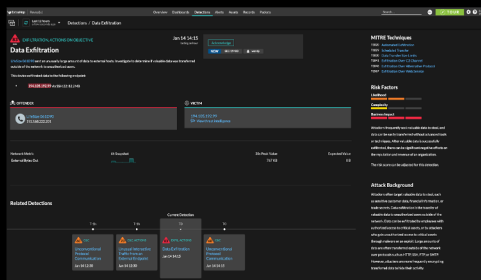
# Enterprise-Level Integrations and Response





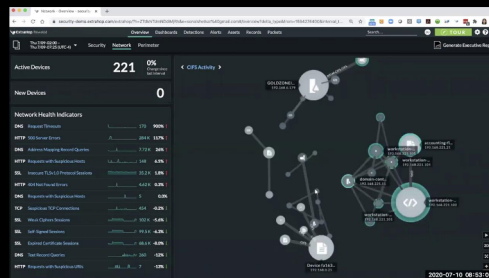
# SOC / NOC Integration

## NDR for SOC Network Detection & Response



incl.

## NTA for NOC Network Traffic Analysis



improve threat response times by **84%**  
and troubleshoot downtime **90%** faster  
up to **90 Day Lookback**



On the Hunt Again?

## Reveal(x)

### FREE TRIAL

Want to unify security across on-premises, hybrid, multicloud, and remote deployments? Test out Reveal(x) 360 with a free trial and see what it reveals in your AWS environment.

FREE TRIAL

## RETURN TO THE LIVE SECURITY DEMO

Try the Performance Demo

### DEFEAT SUNBURST

Stop a notorious supply chain attack  
in its tracks.

STOP THE BREACH

### SECURE THE CLOUD

Use complete cloud visibility to  
detect an intruder.

FIND THE THREAT

### BE THE HUNTER

Investigate a simulated attack  
unfolding in real time.

START THE HUNT

FREE PLAY

Exit the guided walkthroughs altogether, and  
explore the interactive demo alone.

ENTER DEMO

# Thank You

Richard Wieneke

[richardw@extrahop.com](mailto:richardw@extrahop.com)

