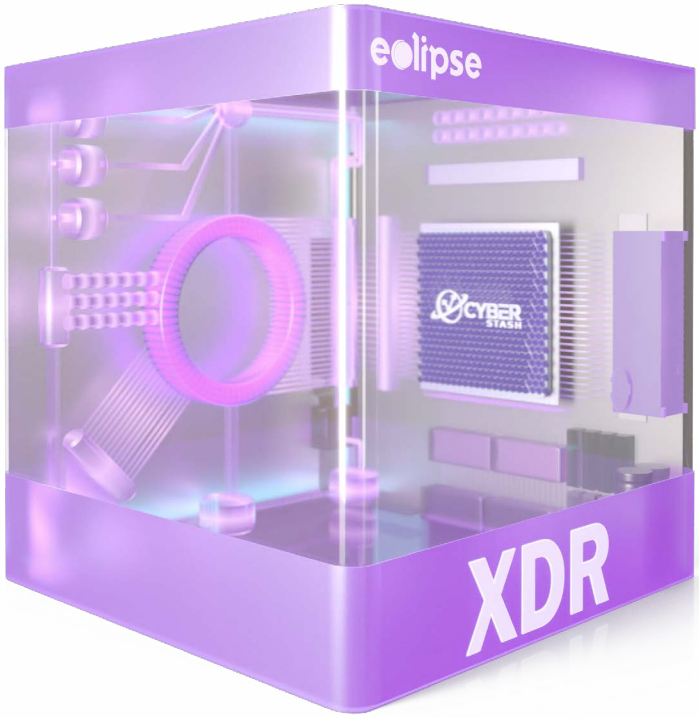
eclipse XDR Datasheet

Discover how eclipse.xdr protects your business and helps to establish trust in your IT environment.

PUSHING THE BOUNDARIES OF SPACE AND TIME

The independent cyber-defense platform **eclipse.xdr** acts as a force multiplier to dramatically reduce an organization's exposure to cyber-attacks and minimize the likelihood of business impact after system compromise. Engrained into the platform is a defense-in-depth threat intelligence architecture that reduces an organization's exposure to a massive number of cyber-threats, and a methodology that minimizes the breach dwell-time through periodic forensic-depth compromise assessments.



Benefits

Strengthens network security defences and evidently reduces risk by proactively blocking threats using real-time defensive controls powered by a vast arsenal of globally collected threat intelligence indicators.

Increases your cybersecurity program ROI by taking proactive blocking action against emerging threats and thereby reducing the workload on your security staff.

Controls the time an attacker lives undetected on your network and reduces the likelihood of a system compromise leading to business impact.

Trust, resilience, and confidence are reinstated and maintained in your IT environment through independent and periodic validation of the compromise state of endpoints.

The Problem

Cyber-criminals continue to outpace and outsmart defenders and cause business impact to organizations by designing attacks that are too sophisticated for them to catch with their current investment in defenses.

Today, many enterprises leverage advanced cybersecurity controls to minimize their vulnerability to cyber-threats. Leveraging NextGen Firewalls, Advanced Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) Platforms do massively reduce an organization's exposure to most threats.

Similarly, NextGen SIEMs, User Behavior and Entity Analytics (UBEA), and Extended Detection and Response (XDR) Platforms do detect threats that defensive controls miss. Nevertheless, as evident from the growing number of cyber-breaches, cyber-criminals are designing an endless number of attacks capable of circumventing such defenses. The result? Financial, regulatory, reputational and operational impact that disrupts an organization's business.

Predictive intelligence must also be automated, real-time, and actionable. It should be integrated with an organization's existing IT infrastructure and, most importantly, be used effectively and efficiently. Knowing about the sources of threats but doing nothing until they target your organization is neither effective nor efficient. To optimize risk and resources, it's better to:

Protect Exposed Services

Proactively block inbound communication from IP addresses used by attackers.

Protect Users

Proactively block outbound communication to IP addresses and domains used by attackers.

Minimize Exposure

Proactively block traffic to and from countries or autonomous systems known to be associated with high levels of cyber-criminal activity.

The Opportunity

Threat Intelligence that's Automated, Real-Time and Actionable

At any given time, the Internet hosts millions of IP addresses and domains with links to malicious cyber activity. All of us are connected to a global network; none of us works in isolation and we all face similar threats from adversarial sources that do not discriminate when deciding who to target.

Every day, an unbelievable 850,000 new malicious IP addresses are launched; 8 billion spam and phishing attacks occur, and 30 to 50 million malicious domains exist at any one time. Too often neutralising cyber threats is reactive and limited to single point-in-time analysis.

These analyses can become irrelevant as the adversary adapts and recalibrates to circumvent protection measures and avoid detection. For most organizations, the big challenge is getting hold of the right-fit technology, skills, and resources to implement a truly effective security program – one that can draw on the immense protective and detective value of collective threat intelligence as part of a defense-in-depth approach to implementing a cybersecurity program that demonstratively reduces business risk.

To stay a step ahead of the adversary, continuous monitoring and coverage of the adversary, their turf and their tools are a necessity. **eclipse.xdr** empowers the collective threat intelligence gathered globally to detect and block known and emerging threats in real-time and reduces an organization's exposure to the staggering number of potential attackers.

Periodic Compromise Assessments using Forensic-Depth Analysis

Unlike other breach-detection strategies, CyberStash doesn't wait for predetermined events to occur before investigating suspected breaches. Instead, we use Forensic Depth Analysis (FDA) to proactively hunt and discover sophisticated and unknown attacks that would otherwise remain invisible in an enterprise environment.

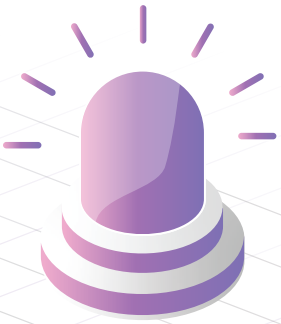
The FDA approach thoroughly validates every aspect of a system independently by going underneath higher-level operating system APIs and working directly with volatile memory structures. We combine FDA with intelligence and the Anomaly Analysis of Operating System Artefacts (STACKING) to generate leads.

Once we have these forensic leads, we inform and enrich what we have discovered using additional techniques, including Code Comparison, Machine Learning, Sandboxing, Threat Intelligence, and finally Human Analysis.

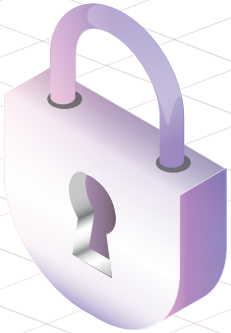
By uncovering compromised hosts within 1 day, eclipse.xdr empowers organizations to reduce the likelihood of actual business impact taking place by 96%.

What You Get

Discovery of all compromised systems in your environment, including servers, workstations, and remote endpoints, whether hosted on-premise or in the cloud.



Detection of systems compromised by advanced cyber-attacks that routinely circumvent existing security controls, whether operating on disk or in memory.



Validated clean-up of all human adversaries, backdoors, and malware following a cyber breach to re-establish trust in the IT environment for the board and executives.

eclipse.xdr Design Principles

As defenders, we must implement groundbreaking controls that help us get ahead of breaches, minimize business impact, and optimize risk and resources. CyberStash has employed 6 critical design principles in developing a revolutionary cyber defense platform that overshadows an organization's existing defensive capabilities.

Methodology	Tactics			Optimization	
Principle 1	**Principle 2**	**Principle 3**	**Principle 4**	**Principle 5**	**Principle 6**
Leverage a defensive methodology that does not depend on prior knowledge of malicious code.	Use a massive number of threat-intelligent indicators, risk-based policies, GEO-fencing, and ASN-fencing, to significantly reduce an organization's exposure to most sources of attacks.	Independently audit every system within an organization as thoroughly as possible at a frequency defined by risk appetite to detect breached systems before they impact business.	Hunt, detect, and respond to unknown and sophisticated attacks that circumvent existing defenses, controlling the breach dwell-time down to 1 day.	Optimize risk and resources through the cost-efficient manner in which threat information is collected, correlated, and disseminated, thus effectively reducing resource overhead for managing threats, thereby providing organizations with a greater return on their investment.	Orchestrate and automate the work a security analyst is required to perform using correlation, enrichment, threat intelligence, dynamic analysis, anomaly detection of operating system artefacts and incident response.

Principle 1 - Methodology

Leverage a defensive methodology that does not depend on prior knowledge of malicious code.

To stay ahead of threats, the methodology used must not depend on detection engines designed to catch the threat itself. The capability used to support such a methodology must be designed to 'catch all leads' and then validate each one and provide a conclusive verdict of either 'compromised' or 'not compromised' without leaving any room for doubt. To achieve this, **eclipse.xdr** uses the following methodology:

Technique and Capability

eclipse.xdr is an integrated, scalable platform underpinned by the following technologies:

Network Threat Intelligence Platform

A vendor-agnostic Threat Intelligence Gateway connected in-line with your network traffic as either a layer-2 bridge device or a virtual cloud instance that inspects network traffic at rates of up to 10Gbps. The threat gateway is empowered by a massive number of threat intelligence indicators updated through the **eclipse.xdr** Cloud which is also used to configure automated policies for blocking malicious traffic.

Endpoint Forensic Collection Agent

A lightweight endpoint agent for Windows, Mac, and Linux operating systems, that collects post-breach forensic artefacts at a frequency configured to meet the organization's risk appetite for controlling dwell-time. Continuous Threat Monitoring and Real-Time Detection are also provided using the same agent that detects the most prevalent adversary behaviors.

Endpoint Incident Response Agent

Leveraging the same agent used for Forensic Collection, the Endpoint Incident Response Agent enables both collection and response action to be performed to limit the damage following a confirmed breach. These incident response actions include but are not limited to:

- Enriching discovery with intelligence
- Enriching discovery with dynamic analysis
- Searching for threat indicators
- Collecting additional forensic evidence
- Isolating an infected host
- Deleting a malicious file or registry key
- Killing a malicious process or service
- Removing a persistence mechanism
- Executing a PowerShell command

Auto Analyst - SOAR Flagging Engine

A configurable Threat Flagging Engine that automates the manual effort performed by a security analyst to quickly enrich and triage threats and rate the level of risk to an organization.

Dynamic Analysis

A Cloud-Native hypervisor-based Sandbox that remains invisible by defeating even the most evasive measures built into advanced threats. Dynamic Analysis transparently monitors every interaction with the target machine to provide end-to-end visibility into malicious behavior.

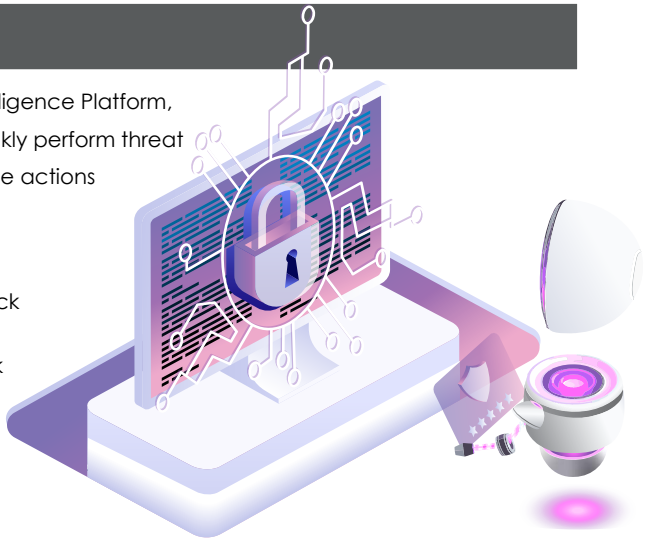
SIEM Threat Detection Platform

A Cloud-Native SIEM that correlates DNS events with logs collected from the eclipse Network Threat Intelligence Gateway to detect advanced threats and to map these to the corporate host targeted by the attack.

Network Incident Response Gateway

Leveraging the same gateway used with the Network Threat Intelligence Platform, the Network Incident Gateway allows incident responders to quickly perform threat containment when responding to an attack. The incident response actions include the following:

- Blocking the IP Address associated with the source of the attack
- Blocking the domains associated with the source of the attack
- Blocking the country the attack originates from
- Blocking the ASN the attack originates from



Principle 2 - Tactical

Use a massive number of threat-intelligent indicators, risk-based policies, GEO-fencing, and ASN-fencing, to significantly reduce an organization's exposure to most sources of attacks.

Technique and Capability

eclipse.xdr protects organizations by harvesting and empowering a massive number of threat intelligence indicators and operationalizing these to block attacks in their tracks. Risk-based inbound and outbound policies add weighting to an indicator's base-risk score to compound the level of threat to the organization if the traffic is associated with a high-risk ASN or high-risk country. Your organization's exposure to cyber-threat is immensely reduced through this defensive methodology.

Cyber-Threat Intelligence Framework

The CyberStash Threat Intelligence Gateway solution aligns with the following framework for operationalizing Cyber Threat Intelligence:

Collect

- Collection of millions of accurate threat indicators from multiple sources including commercial and open-source feeds and government advisories
- Multiple types of threat intelligence including IP reputation blocklists, malicious domains and high-risk Autonomous Systems Numbers (ASNs)

Aggregate

- Multiple threat aggregation and consolidation into a single feed
- An open platform that easily integrates threat intelligence with standards like STIX/TAXII
- Analytics to drive advanced intelligence and threat detection

Automate

- Threat feeds dynamically updated in real-time
- Automated emerging threat protection
- Automated risk-based policy application at line-speed

Detect

- Pivot, hunt for and investigate suspicious traffic
- Block previously unknown threats and unwanted traffic
- Advanced network-centric threat detection

For inbound threats that target exposed services, protection is provided by:

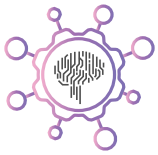
Blocking the traffic if the source IP Address is on a Block List	Blocking the traffic if the source IP Address is on a High-Risk ASN List	Blocking the traffic if the source IP Address is on a High-Risk Country List	Blocking the traffic if the source IP Address is on a Threat List with Risk Adjustment Applied	Detecting allowed source IP Addresses that correlate with a Block List or Threat List to be detected and responded to

For outbound threats that target exposed services, protection is provided by:

Blocking the traffic if the target IP address or domain is on a Block List	Blocking the traffic if the destination IP Address is on a High-Risk ASN List	Blocking the traffic if the destination IP Address is on a High-Risk Country List	Blocking the traffic if the destination IP Address is on a Threat List with Risk Adjustment Applied	Detecting allowed destination IP Addresses or Domains that correlate with a Block List or Threat List

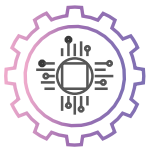
Out-Of-Box Threat Intelligence

The CyberStash Threat Intelligence Gateway solution is integrated with the following commercial threat intelligence feeds. It comes out-of-the-box with millions of indicators and allows organizations to add their own intelligence feeds:



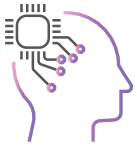
WELL-FED THREAT INTELLIGENCE

Well-Fed threat intelligence is generated by charting attackers to see where they actually live so you have the latest information to protect yourself. Approximately one million malicious domains are monitored every hour and are curated and white-listed to ensure that you have reliable information you need to protect yourself from cyber-criminals. This includes Sinkhole IP Feed, DGA Feeds, and MaldomainML which is a feed based on proprietary machine learning and analytical methods of DNS telemetry developed in Bambenek Labs.



MALWARE PATROL THREAT INTELLIGENCE

Malware Patrol specializes in real-time threat intelligence that protects users and enterprises in over 175 countries against cyber-attacks. The highly refined and continuously updated indicators identify compromised machines, botnets, command and control (C2) servers, malware, ransomware, cryptominers, DGA infrastructure, phishing, DNS over HTTPs (DoH) resolvers, and Tor exit nodes.



INTEL 471 THREAT INTELLIGENCE

Threat Intelligence is derived from across 14 countries to provide near real-time coverage of threat actors and malware activity. Intel 471's Malware Feed consists of Malware IP Indicators possessing high confidence, timely and rich context curated from Intel 471's industry leading access in the cyber-criminal underground. Types of malware covered are banking trojans, infostealers, loaders, spambots, and ransomware.

CYJAX THREAT INTELLIGENCE FEED

The Cyjax Threat Intelligence feed consists of a validated feed of contextualised IP and domain indicators of compromise (IOCs) discovered from Cyjax research and across the threat landscape to allow for additional enrichment and cross-correlation with other threat information and intelligence.

PROOFPOINT ET INTELLIGENCE™

Proofpoint ET Intelligence provides actionable, up-to-the-minute IP and Domain reputation feeds.

WEBROOT BRIGHTCLOUD® IP

Bright Cloud Dynamic domain threat intelligence feed provides us with 5,000 domains per minute, resulting in intelligence on over 230 million domains per month.

DOMAIN TOOLS MALICIOUS DOMAIN BLOCK LISTS

Domain and DNS data covering over 95% of all registered domains, used predictively before any malware has caused damage.

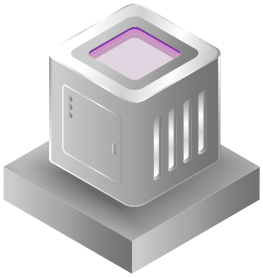
CYBERSTASH EMERGING DOMAINS AND IP BLOCK LISTS

Indicators released by Government advisories and emerging Advanced Persistent Threats (APTs) are added to the CyberStash block list.

BITDEFENDER THREAT INTELLIGENCE FEED

Bitdefender Labs correlates hundreds of thousands of Indicators of Compromise (IoCs) collected through the Global Protective Network (GPN) protecting hundreds of millions of systems globally and turn data into actionable, real-time insights into the latest threats. The Bitdefender Advanced Threat Intelligence solution consists of unique feeds including:

- *Advanced Persistent Threats (APT) Domains - A collection of domains hosting Advanced Persistent Threats Malicious Domains - A collection of domain addresses associated with general malware activities*
- *Phishing Domains - A collection of domain addresses associated with phishing attacks*



Bring Your Own Intel Feeds and Integrations

The Threat Intelligence Gateway also integrates with most other commercial and open-source intelligence providers. This effectively gives our clients the unlimited potential to expand their threat intelligence capability. In fact, we have over 50 point-and-click integrations with Threat Intelligence Platforms, SIEMs, SOARs, and other applications.

Open-Source Threat Feeds

The CyberStash Threat Intelligence Gateway solution is integrated with the following open-source threat intelligence providers:

- **Cisco Talos**
- **Blocklist.de**
- **CINS Army List**
- **Abuse.ch**
- **Check Point Tor List**
- **DHS CISCP**
- **Emerging Threats Block Rules**
- **Ransomware Tracker**
- **State of Missouri SOC**
- **ZeuSTracker**

CyberStash Threat Intelligence Gateway

Deploy as a Cloud, On-Premise or Proxy/VPN Gateway

What You Get

A Threat Intelligence Gateway that provides up-to-the-minute, line-speed protection against known sources of threats, both inbound and outbound, at scales of up to 10 Gbps

Protection against 150 million known threat indicators using continuously updating, risk-based, policy-driven, actionable threat intelligence that blocks and detects known sources of threats

Leverage of a vendor-agnostic open platform with centralised management to enforce risk-driven policies, to inform threat hunting, and to investigate and respond to incidents

Cloud-native management of your policies, intelligence, investigation, and reporting that's self-managed, co-managed or completely managed by CyberStash Security Analysts

RISK-BASED THREAT CLASSIFICATION POLICIES

CyberStash classifies and responds to threats by Threat List Policies, Block List Policies, Country List Policies and ASN List Policies.

Maximise configuration flexibility, risk-based Policies are applied separately to inbound and outbound traffic, to specific asset groups, and to the following threat categories:

- **Command and Control**
- **Endpoint Exploits**
- **Botnet**
- **Drop Site**
- **Web Exploits**
- **Spam**
- **Scanner**
- **Advanced Persistent Threat**
- **Brute Force Password**
- **TOR / Anonymizer**
- **Proxy / VPN**
- **DDOS**
- **Compromised**
- **Fraudulent Activity**
- **Illegal Activity**
- **Undesirable Activity**
- **P2P Node**
- **Online Gaming**
- **Remote Access Server**

Principle 3 - Tactical

Independently audit every system within an organization as thoroughly as possible at a frequency defined by risk appetite to detect breached systems before they impact business.

Technique and Capability

eclipse.xdr detects sophisticated attacks using Forensic-Depth Analysis. Forensic-Depth Analysis is a post-breach threat hunting practice that periodically surveys all endpoints within an organization to discover forensically relevant leads. Leads are also discovered by detecting changes in the forensic state of files. The methodology used does not depend on catching the attack on its way in but takes an adversarial approach to threat hunting whereby endpoints are assumed to be breached and assessed to conclusively confirm their state of compromise.

15 Steps For Conclusive Validation and Response

CyberStash establishes trust in an IT environment by carrying out 15 steps.
The process we follow is akin to that of a highly trained digital forensic analyst, however, we deliver our deep-level analysis at scale through automated host-level surveys before augmenting and enriching what we've discovered. When delivered as a Managed Detection and Response (MDR) service, our security analysts then go over the endpoint meticulously to flag every operating system component as Verified Good, For Review, Potentially Unwanted or Verified Bad. We maintain a memory of these decisions and then work on all the net-new forensic leads we discover on subsequent assessments, thus enabling us to deliver a feasible and scalable service to any size enterprise.

Forensic-Depth of Discovery

Forensic-Depth Of Discovery

The forensic-depth used by **eclipse.xdr** goes beyond other detection methodologies to validate endpoints independently and conclusively as compromised or not compromised.

Forensic Collection, Stacking and Auditing

- CMD
- PowerShell
- NETSH
- SSH
- Privileges
- Shimcache
- VNC
- PSExec
- RDP
- Tunnels
- WMI
- Amcache
- Active Processes
- In-Memory Execution
- Execution Artifacts
- OS Subversion
- Network Connection

Identification and Evaluation

- Process Manipulation such as hooks, inline modifications, patching, etc.
- Operating System Manipulation including list modifications, hidden processes, direct kernel object manipulation, etc.
- Memory Injected Modules – memory un-mapping techniques to export memory objects for offline retention and analysis

Enumeration and Evaluating Persistence Mechanisms

- Cron Jobs
- Registry AutoStart Triggers
- DLL Hijacking
- Boot Process Redirections
- Watchdog Process
- WMI Events

Disabled Security Controls

- Disabled AV
- Reduced authentication requirement configurations
- GPO blocking, etc

Detecting Adversary Techniques

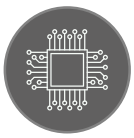
In addition to forensic-depth discovery, our eclipse endpoint agent also provides detection for all prevalent behaviors described within the MITRE ATT&CK Framework. The enables Defense-in-Depth detection whereby we increase the opportunity and the confidence level of detection covering the attack chain.

Rank	Tactic	Id	Technique
1	Execution	T1059	Command Line Interface / Powershell
2	Initial Access	T1078	Valid Account Misuse
3	Discovery	T1082	System Information Discovery
4	Persistence	T1060	Registry Run Keys
5	Credential Access	T1003	Credential Dumping
6	Lateral Movement	T1021	Remote Services
7	Execution	T1055	Process Injection
8	Persistence	T1053	Scheduled Tasks
9	Defensive Evasion	T1218	Signed Binary Proxy Execution
10	Persistence	T1547	Boot/Logon Autostart Execution (esp. Shortcut Modification)
11	Execution	T1047	Windows Management Instrumentation (WMI)
12	Defense Evasion	T1036	Masquerading
13	Privilege Escalation	T1574	Hijack Execution Flow
14	Defense Evasion	T1027	Obfuscated Files or Information
15	Defense Evasion	T1497	Virtualization/Sandbox Evasion
16	Lateral Movement	T1544	Remote File Copy
17	Defense Evasion	T1089	Disabling Security Tools
18	Initial Access	T1190	Exploit Public Facing Application
19	C2	T1219	Remote Access Software (e.g. RDP)
20	C2	T1505	Webshells

Finding Code in Memory

Discovering malicious code in memory requires forensic level analysis, and **eclipse.xdr** achieves this through the 5-step process illustrated below:

ENUMERATE LOADED MODULES
Ask the OS for a list of modules in process (WMI, etc.)



PROCESS MEMORY WALK
Brute force a process's private memory regions (heap) using VirtualQuery. Identify and inspect any allocated sections with executable markers (i.e., RWX or RX)

MEMORY/DISK COMPARISON
For disk-mapping modules. Compare the executable section of a module on disk to what it looks like in memory. Fuzzy hash comparison will give variation %.

THREAD WALK
Iterate through each executing thread within a process. Identify and inspect any threads pointing at private memory sections.

INSPECT LOADED TABLES
Inspect the process's import tables to find references to all loaded libraries.

Principle 4 - Tactical

Principle 4 - Tactical

Hunt, detect, and respond to unknown and sophisticated attacks that circumvent existing defenses, controlling the breach dwell-time down to 1 day.

Technique and Capability

In addition to Forensic-Depth Analysis, **eclipse.xdr** employs the following additional threat hunting techniques to discover previously undetected threats within the enterprise:

1.Anomaly Analysis of Operating System Artefacts

- Stacking to look for outliers such as missing or suspiciously signed digital certificates
- Stacking to compare the compile date and size of a file, the location it's running from and its file hash value
- Stacking and comparing other forensic artefacts such as the files entropy or single section entropy, the PE HEADER and API Signatures such as process injection, token impersonation, anti-debugging, keylogging, and hooks

2.Threat Analysis of High-Risk Network Traffic Based on Intelligence, GEO-IP, and ASN.

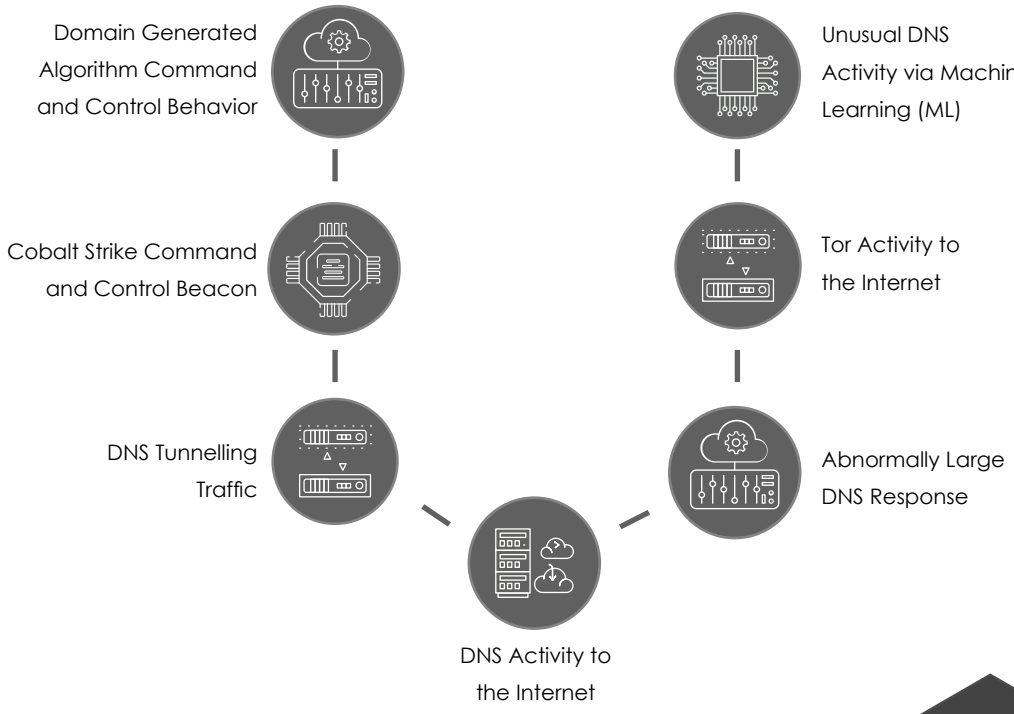
- Detecting traffic that's correlated with a threat intelligence indicator
- Detecting traffic destined to high-risk ASNs and high-risk Countries that can be defined by clients
- Correlating the leads with sources of intelligence and sending them to the eclipse Web Dynamic Analysis Engine, which inspects and validates the actual behavior of a resource (IP Address or URL) and its level of maliciousness to the organization

Principle 5 - Optimization

Optimize risk and resources through the cost-efficient manner in which threat information is collected, correlated, and disseminated, thus effectively reducing resource overhead for managing threats, and thereby providing organizations with a greater return on their investment.

Technique and Capability

eclipse.xdr collects DNS events from the client's environment and correlates these with the logs from its Threat Intelligence Gateways to automatically identify the internal resource associated with an identified threat. The collection and correlation process used by **eclipse.xdr** avoids having to collect logs from the client's firewall or needing to use big data security analytics with full packet inspection. This minimizes the technological footprint required and optimizes resource utilization. Risk detection is also optimized because these same logs are securely forwarded to the eclipse Cloud SIEM for searching, threat hunting, and advanced threat detection. Some of the threat detection capability **eclipse.xdr** SIEM provides include:



Principle 6 - Optimization

Orchestrates and automates the work a security analyst is required to perform using correlation, enrichment, anomaly detection of operating system artefacts, dynamic analysis, and threat intelligence.

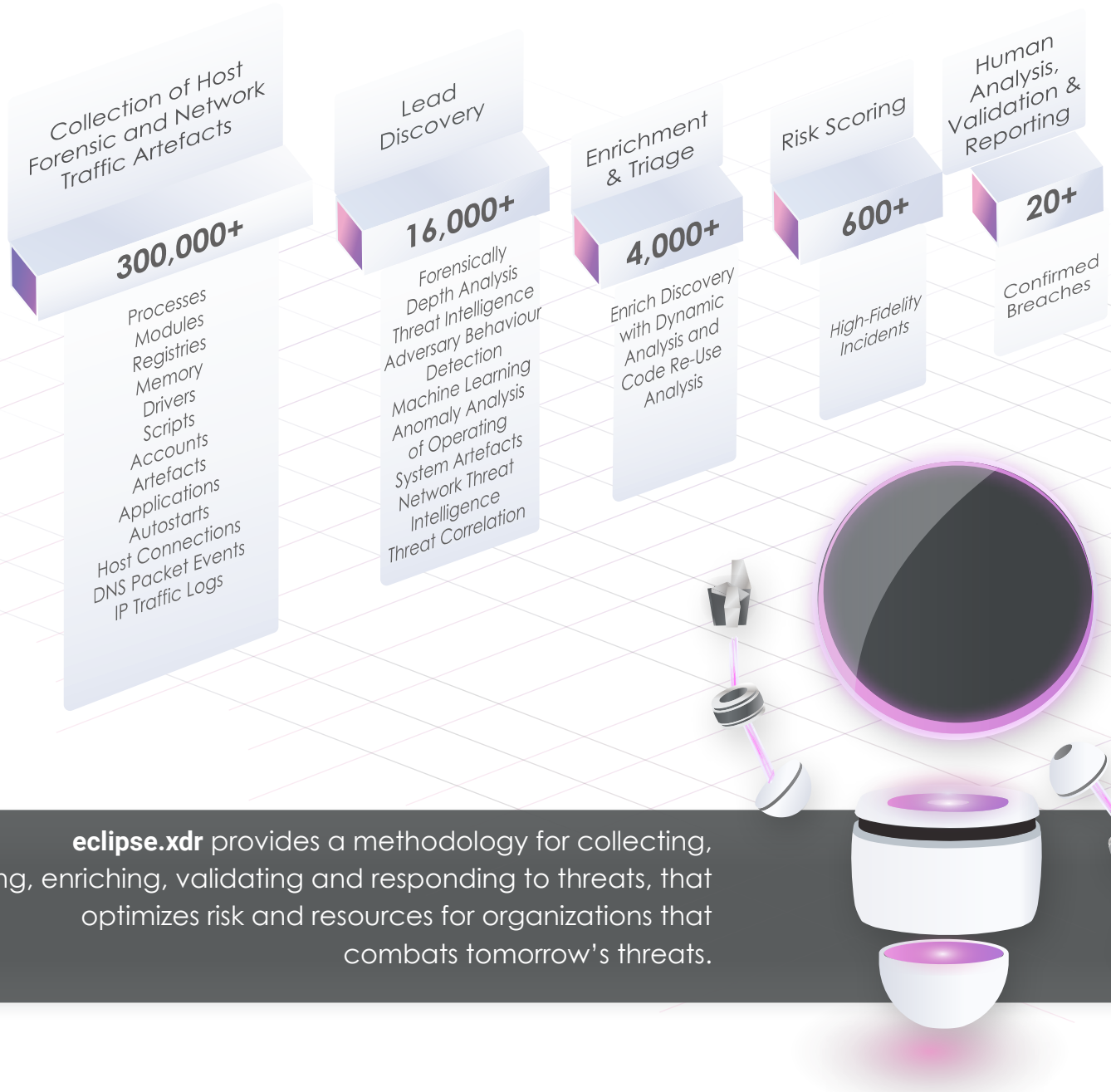
Technique and Capability

With the magnitude of the security alarms generated by today's technologies, security analysts have the impossible tasks of correlation, enrichment, and reverse engineering code to arrive at a final verdict of risk. The orchestration built within **eclipse.xdr** automates the manual heavy lifting a security analyst is required to perform and automatically flags leads as Confirmed Malicious, Probably Malicious, Suspicious, Probably Good, or Verified Good. This enables a security analyst to quickly pin down the areas of risk by filtering on these flags to then perform automated response actions using **eclipse.xdr.**

The **eclipse.xdr** Auto Analyst SOAR Flagging Engine automates the following processes when a forensically suspicious lead is detected:

- Checks the hash of the file within its own database as the same file may have been seen previously in analysis performed against another client's environment
- Checks the hash of the file with existing analysis from intelligence and dynamic analyses platforms
- Downloads the hash of the file and submits it for analysis to intelligence and dynamic analyses platforms
- Automatically creates an alert and/or help-desk ticket for incidents that are rated as high risk and have a high level of fidelity
- Submits URL and IP indicators to web dynamic analyses and threat reputation platforms
- Uses the results to triage and assign a risk rating to the discovered lead
- Takes automatic response actions to block the attack and remove the threat

Principle 6 - Optimization

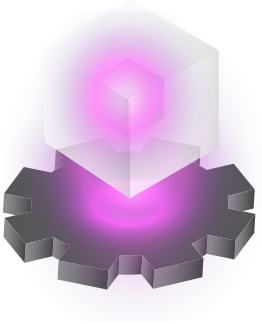


eclipse.xdr provides a methodology for collecting, hunting, enriching, validating and responding to threats, that optimizes risk and resources for organizations that combats tomorrow's threats.

Managed Detection Response

eclipse.mdr | Managed Detection and Response

When delivered as a Managed Detection and Response (MDR) service, CyberStash constantly monitors, detects, hunts, investigates and responds to cyber-threats to keep your business safe.



24/7 Automated Protection | Detection | Threat Hunting | Incident Response

You get a 24/7 cyber-defense capability that's active round the clock. Driven by Security Automation, Orchestration and Response (SOAR), the attack surface of your business is massively reduced. This capability is strengthened by the CyberStash team of security experts who investigate active attacks and take response actions to eliminate them from your environment.

Security Monitoring | Incident Investigation

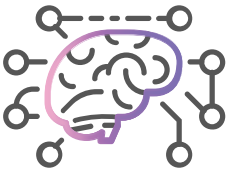
Our team of experts investigates every security alarm and provides an assessment of the level of risk posed to your business.

Incident Response | Threat Containment

Our experts will immediately notify your security or IT team of any threats or compromised hosts. We provide a full comprehensive report that enables you to take informed actions to eliminate the threat. If you have pre-approved incident containment, we will implement it and provide you with a report on what we did, when we did it, and how our actions eliminate the risk to your business. Moreover, your organization has the option to co-manage Incident Response, which would allow authorised personnel in your team to implement response actions that can contain threats as they happen.

Security Consulting | Actionable Advice

Every incident we investigate comes with sound advice and recommendations from our team of security experts. Acting in the best interests of your business, we work to understand the precise nature of the threats you face, the specific challenges you have in managing them, and your organization's appetite for risk.



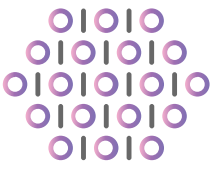
Multiple Layers of Protection, Detection and Response

Powered by the CyberStash **eclipse.xdr** platform, the multiple layers of protection we provide contribute towards a comprehensive defense-in-depth strategy to protect your critical assets:

- Network and Cloud Protection using Threat Intelligence
- Forensic-Depth Breach Detection and Threat Hunting
- Endpoint Adversarial Behavior Detection
- Advanced DNS Threat Detection

Independent and Automated Security Stack

Due to our independent, automated approach to cyber threat detection, we can deliver better detection and greater value to your business. Automated continuous threat hunting followed up by human-driven investigation and reporting that identifies lateral movements, hidden malware and risky connections, and contains them before they can impact your business.



Periodic Tuning and Reinforcement

Acting as an extension of your security or IT team, we periodically improve your security posture by reducing your attack-surface through regular reporting and policy enforcement. We enhance the value of technology with human-led intelligence and consulting, ensuring the level of protection never diminishes but rather returns a greater return on your investment over time.

eclipse.mdr | Service Levels

Service Levels

Capability	XDR		MDR
	Standard	Enterprise	Managed
Throughout	**Up to 10 Gbps per Gateway**		
Forensic Depth Survey Frequency	**Scheduled Daily and On-Demand**		
Service Establishment	✓	✓	✓
Out-of-Box Threat Intelligence	✓	✓	✓
Emerging Threat Protection	✓	✓	✓
Baseline Policy Development	✓	✓	✓
Block List and Allow List Management	✓	✓	✓
Event Logging to Client SIEM	✓	✓	✓
Risk-Based Policy Development	✓	✓	✓
Advanced Threat Detection and Response	✓	✓	✓
CyberStash Cloud SIEM	✓	✓	✓
DNS Logging and Correlation	✓	✓	✓
Real-Time Threat Dashboards	✓	✓	✓
Traffic Event Searching	✓	✓	✓
Auto-Generated Security Reports	✓	✓	✓
Asset Discovery	✓	✓	✓
Anomaly Analysis of Operating System Artefacts	✓	✓	✓
Application Vulnerability Detection and Reporting	✓	✓	✓
Privilege and Non-Privilege Account Discovery	✓	✓	✓

Service Levels

Network Traffic to Process and Accounts Mapping	✓	✓	✓
Automated Hunting for Post Compromise Leads	✓	✓	✓
Breach Clean-up Validation	✓	✓	✓
System Breach Incident Response	✓	✓	✓
Real-Time Process Monitoring	✓	✓	✓
Adversary Behaviour Detection (MITRE ATT&CK)	✓	✓	✓
Virus Total Public API Key	✓	✓	✓
Automated Dynamic Analysis – Sandboxing	—	✓	✓
Auto Analyst - SOAR Flagging Engine	—	✓	✓
CyberStash Threat Intelligence Feeds	—	✓	✓
CyberStash Emerging Threat Management	—	✓	✓
Secure Digital Forensic Data Collection	—	✓	✓
Scheduled Hunting and Post Compromise Investigation	—	—	✓
Human Analysis of Security Alerts	—	—	✓
Asset Inventory Management	—	—	✓
Incident Response Management	—	—	✓
Policy Enhancement and Tuning	—	—	✓
False Positive and Exception Management	—	—	✓
Device Life Cycle Management	—	—	✓
Service Desk Management	—	—	✓
Deep-Dark Web Credential Disclosure Detection	**Optional**	**Optional**	**Optional**
Dynamic Analysis Private License API Key	**Optional**	**Optional**	**Optional**
Virus Total Private License API Key	**Optional**	**Optional**	**Optional**

MSP

Become a Partner

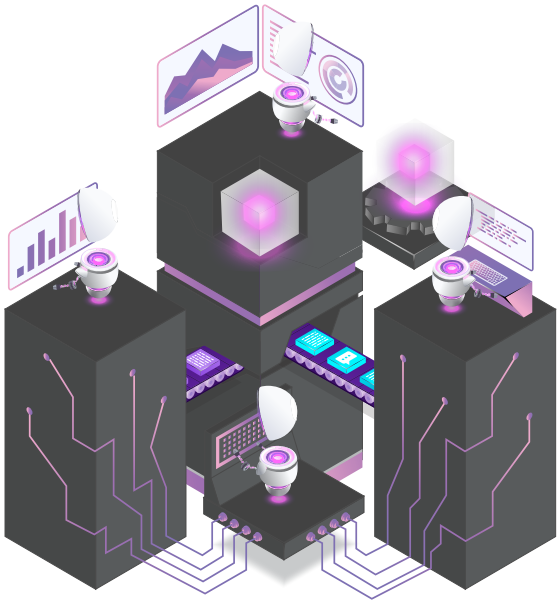
Take your cybersecurity services to a whole new level by becoming a CyberStash MSP Partner.

MSP

Open the gates to new opportunities with **eclipse.xdr** cyber defense platform. An innovative, self-hosted or multi-tenanted platform that's designed to be used by Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs). Help your customers reduce their risk by enhancing their IT security defenses while you benefit from a recurring revenue model and position yourself as a trusted security partner.

Reseller

Resell the CyberStash eclipse platform and let CyberStash deliver the end-to-end service to your clients. CyberStash provides your team members the training, material and support to empower them to position and sell the value proposition of eclipse XDR. We then deliver exceptional services to your clients and guarantee high levels of satisfaction.



Why CyberStash **eclipse.xdr**?

The **eclipse.xdr** platform was purpose-built for MSPs and MSSPs – this capability was not an afterthought. This means that your team will leverage a single platform to manage all its clients, a single pane of glass to manage incidents, and a platform that's optimized for risk and resources.

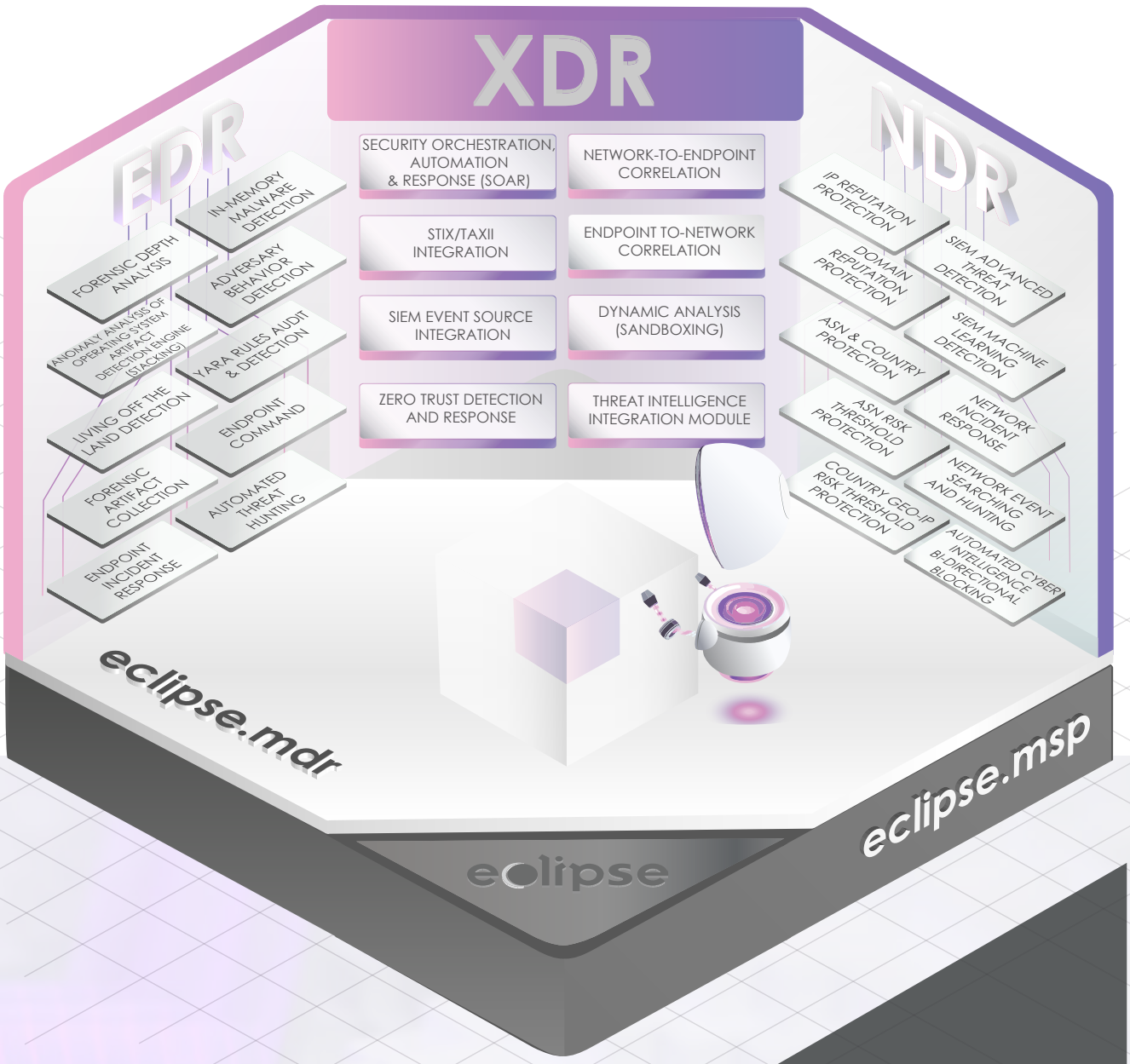
An MSP-Centric Purpose-Built Cyber Defense Platform

Inspired by 20 years and 548,000 hours of SOC and global MSSP experience	A platform that helps MSSPs deliver services proven to increase client retention	Evidently reduces risk with minimum numbers of false positive detections while providing detection certainty
Multi tenant platform that leverages resources across client portfolios to minimize rework	Simple to deploy, manage, licence and operate with role based access controls	Allows client teams to co-manage incident containment and false positives

eclipse.xdr Platform Benefits

By covering the full scope of network and endpoint traffic, **eclipse.xdr** has full visibility and control of advanced threats faced by organizations who use it to uplift their defensive capability.

Easy To Use	Broad Coverage	Effective
High MSP Resource To Client Ratio	Small Tech Footprint	Low Management Overhead



Inquiries
info@cyberstash.com
www.cyberstash.com

Become a Partner
info@cyberstash.com

CYBER STASH

eclipse

www.cyberstash.com

Contact Us

CyberStash **eclipse.xdr** combines automated threat intelligence with technology and architecture to massively reduce an organization's exposure to most known sources of threats on the Internet. It combines human analysis with forensic-depth analysis, malware analysis, and code re-use comparison, to establish a higher level of stakeholder trust in an IT environment.