Infocyte

Infocyte used for Incident Response during cyber attack, helps Linden Bulk Transportation avoid downtime and get back to business quickly.

CASE STUDY
TRANSPORTATION

Challenge

Linden Bulk Transportation, a subsidiary of Odyssey Logistics, provides safe, reliable bulk and intermodal transport across North America. The organization supports a fleet of over a thousand trucks, power units, trailers, and transportation assets.

In January of 2019, Linden's IT department began receiving a high volume of help desk calls and also noticed an increase in network latency, with communications slowing among their various systems and servers.

When the IT staff investigated some of the servers in question, they noticed a large number of services being enabled and populated. They tried to contain the malware attacks by sectioning off what they believed were the infected systems and servers, but this proved a difficult task for an environment of hundreds of systems across a highly segmented network with multiple locations. The malware was also constantly evolving and replicating itself, further complicating their efforts to manage issues. Even after weeks of intense effort by the Linden IT team, what began as a network slowdown was now a full-fledged attack.

Solution

Linden reached out to Check Point's Incident Response (IR) team for assistance. Check Point deployed Infocyte HUNT from the cloud. Within hours, Check Point's IR team had executed a network-wide scan and Forensic State Analysis with Infocyte HUNT to gain deep visibility of Linden's hosts, systems, and servers. This enabled Check Point to identify exactly which systems were infected and then work with Linden and Sycomp, a Check Point strategic partner, to begin containment and remediation efforts.

CHALLENGE

- Unforeseen spike in incoming help desk calls
- Increase in network latency; slower communications.
- Difficulty identifying infection within large, distributed IT environment.
- Detecting and isolating lateral action by bad actors.
- Lack of in-house technology for identifying and remediating threats.

RESPONSE

- Linden called Check Point's Incident Response team.
- Check Point turned to Infocyte HUNT to gain full visibility into the IT environment.
- Infocyte HUNT deployed within 20 minutes.
- Infocyte HUNT scan and Forensic State Analysis report completed within hours.

RESULTS

- Infocyte HUNT quickly identified all infected systems.
- Threats included Ryuk ransomware, mimikatz trojans, and the Emotet virus.
- Infocyte HUNT report showed that threats had bypassed firewall and antivirus tools.
- Report enabled Linden IT team to focus resources and remediate infected systems.
- Linden continues to use Infocyte HUNT to maintain visibility and identify compromises or suspicious activity.

Results

With Infocyte HUNT, multiple cyber threats were identified within minutes, including Ryuk ransomware, mimikatz trojans, and the Emotet virus, an advanced, modular banking trojan that primarily functions as a downloader or dropper of other banking trojans.

Infocyte HUNT also determined that the malware had breached Linden's IT environment in October and had bypassed installed firewall and antivirus tools.

Linden now leverages Check Point Software to provide protection, and Infocyte HUNT for proactive detection and incident response. Scheduled, ongoing scans of Linden's environment and real-time alerts enable Linden to certify their environment is free of breaches and pinpoint plus investigate any new potential threats quickly, on an ongoing basis.

BENEFITS

- Respond to threats in near real-time.
- Accurate and up-to-date visibility across all IT assets.
- Periodic scans by Linden to certify the security of their entire environment.

TRY INFOCYTE HUNT FOR FREE

Discover why Infocyte HUNT is recognized as a leading solution for proactive detection and IR.

www.infocyte.com/demo

About Infocyte

Infocyte is a recognized leader in proactive threat detection and on-demand incident response. The world's leading security and incident response firms (Check Point, PwC, Grant Thornton and more) use Infocyte's platform to detect and respond to threats hiding within their customers' environments. For partners, Infocyte represents the fastest path for delivering cost-effective and flexible consulting services and ongoing Managed Detection and Response (MDR) services. Infocyte was founded in 2014 and is headquartered in Austin, TX.

About Check Point Software

Infocyte is a recognized leader in proactive threat detection and incident response solutions. Backed by a global network of managed detection and response (MDR) and MSSP providers, Infocyte HUNT and Infocyte HUNT Cloud platforms offer agentless deployment capabilities that allow companies to hunt, detect and respond to sophisticated attacks much faster, thereby stopping security breaches before they inflict damage and reducing dwell time to days rather than months. Learn more at www.infocyte.com.

About Sycomp

Sycomp, a Technology Company, Inc., is a global provider of innovative data center and security solutions that deliver superior business results. For more than 20 years, the company has teamed with 150+ customers in the public and private sectors to design, implement, and support customized, world-class IT solutions that optimize system performance, reliability, and availability. Learn more at www.sycomp.com.

Infocyte

3801 N. Capital of Texas Hwy.
Suite D-120
Austin, TX 78746

(844) 463-6298
sales@infocyte.com
www.infocyte.com