SECURING THE SUPPLY CHAIN WITH CELERIUM

CELERIUM®

It’s always been true that no business or enterprise is an island. Every company has distributors and suppliers they depend on to keep business running as usual. **However, up to 80% of new cyber-attacks begin in the supply chain,** making those crucial partnerships also potential vulnerabilities. Cyber risk in the enterprise supply chain has become such a concern that the United States Department of Defense has launched its new Cybersecurity Maturity Model Certification (CMMC) program, which is designed to help secure the defense industry supply chain by requiring contractors to ensure all downstream suppliers are CMMC certified.

UP TO **80%***

OF NEW

CYBER-ATTACKS

BEGIN IN THE SUPPLY CHAIN

*https://www.nist.gov/blogs/blogrige/lumberjacks-and-supply-chain-cybersecurity-take-time-prepare

THE PROBLEM

A critical partner suffering an attack can cause loss of revenue to the larger enterprise and result in major business disruption. Even worse, an attack on a supplier could be just the beginning of a nightmare; hackers and other bad actors often look for smaller, weaker vendors to work their way up to larger targets.

Ransomware is of particular concern for small organizations; in the second quarter of 2020 alone, 55% of these attacks targeted companies with fewer than 100 employees. Small and medium sized businesses make good targets because they often lack dedicated security teams and resources to maintain a proactive cybersecurity posture. Threat actors also prefer to attack companies in industries where downtime can be disastrous, such as manufacturing networks. This makes securing the manufacturing supply chain more critical than ever.

55%[*] OF RANSOMWARE ATTACKS IN 2ND QUARTER 2020 TARGETED COMPANIES WITH FEWER THAN 100 EMPLOYEES

75%[*] OF RANSOMWARE ATTACKS IN 2ND QUARTER 2020 TARGETED COMPANIES WITH LESS THAN $50 MILLION IN REVENUE

A RANSOMWARE ATTACK WILL TAKE PLACE EVERY ELEVEN SECONDS BY 2021[**]

APPROXIMATELY **$1.4 BILLION**[*] WAS PAID TO RANSOMWARE GROUPS IN 2019

[*] https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report#payment

[**] https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion

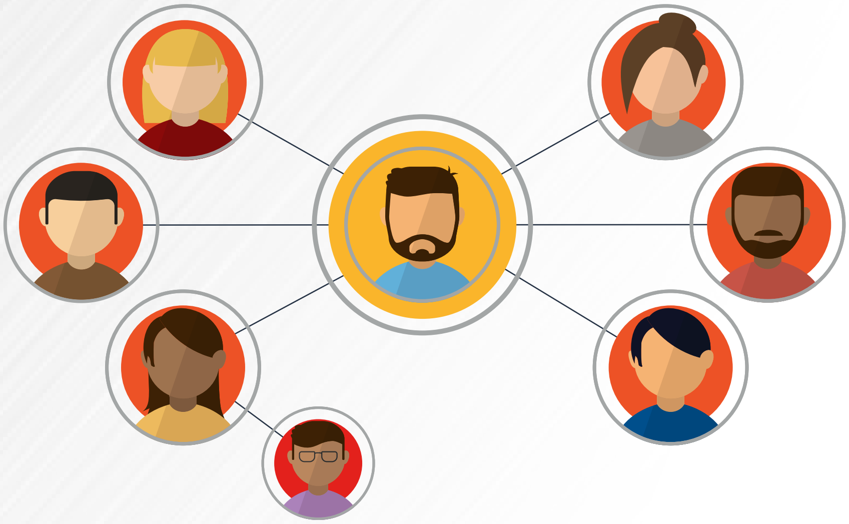
Supply chains are varied and complex; no two are alike, and they all present unique security challenges. The larger enterprise may have information about specific threats or vulnerabilities, but how can it effectively and securely share that information with its partners to help protect the entire chain? How can it see actions that members of the supply chain are taking to help protect the enterprise? Smaller suppliers usually don’t have the budget for dedicated cybersecurity teams; how can security be made accessible for them? How can small teams be empowered to take practical actions that matter?

HOW CAN SMALL TEAMS BE EMPOWERED TO TAKE PRACTICAL ACTIONS THAT MATTER?

THE SOLUTION

Cyber Defense Network, powered by Celerium®, is a next generation solution that empowers collective defense to better protect the supply chain via secure collaboration, sharing, and security intelligence. It's a pragmatic solution that accelerates cyber defense, making it possible for even the smallest suppliers to be proactive about cybersecurity while allowing larger enterprises to lead the way in effectively managing and mitigating threats and vulnerabilities in their supply chains.

Cyber Defense Network addresses a variety of cybersecurity policy and regulatory requirements across sectors, including the new U.S. Department of Defense Cybersecurity Maturity Model Certification (CMMC) and NIST Special Publication (SP) 800-171.By bringing partners into a Cyber Defense Network, enterprises can easily share specifically relevant threat information with, and receive it from, partners. All members of the supply chain, regardless of size, can engage in dialogue, asking questions or sharing knowledge and information about what they are seeing and doing in their own systems, allowing the entire supply chain to align efforts on emerging and important threats that can impact them all. Cyber Defense Network brings contractors and partners together in building a repository of data for effective research; partners of all sizes can push intelligence into SIEMs or other tools to accelerate defense. Small partners can benefit from the contextualized threat reports provided by CDN, as well as from dashboards that show actions other members of the supply chain are taking on specific threats and indicators of compromise. Powerful reporting allows the enterprise to measure success of the program.



CYBER DEFENSE NETWORK

in action

MALIBU MANUFACTURING

Malibu Manufacturing, a heavy equipment maker, uses Cyber Defense Network to help secure its network of suppliers and distributors. An attack on any of these could result in reputational damage or loss of revenue for Malibu as well as impact its customers; these companies also have connections into Malibu's network, meaning an attack on one could become an attack on Malibu.

Here are three scenarios that show how Cyber Defense Network helps keep Malibu Manufacturing secure:

Matthew

Julia

Rose

SCENARIO 1: **MATTHEW**

Matthew is on the security team at Malibu. Each day he creates discussion threads within Cyber Defense Network to share relevant updates on threats and vulnerabilities such as indicators of compromise and spoofing domains. He also answers questions posted by distributors.

One day, several distributors received a very authentic looking email claiming to be from Malibu, telling them to click a link to view a new payment system. Because of the information Matthew shares in Cyber Defense Network, the distributors knew that spoofed domains were of particular concern to Malibu. When they didn't see this particular domain listed, they were able to quickly ask in a Cyber Defense Network discussion whether this unfamiliar domain was legitimate. Matthew responded immediately that this was also a spoofed domain, and distributors should not click any links. He updated his report in the shared document library and used CDN to implement his own security protocols against the new spoofed domain.

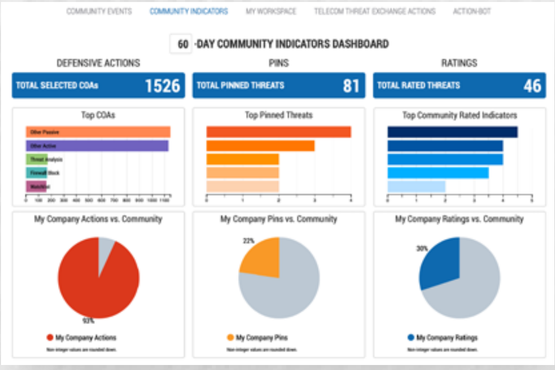
Having one place for contact, discussions, and information about specifically relevant threats streamlined Malibu's communication with its distributor community; there was no phone or email tag, and the entire community of distributors had a place to obtain information and action on a new threat, helping keep Malibu's supply chain secure.

Secure collaboration in real time helps the distributors stay up-to-date.

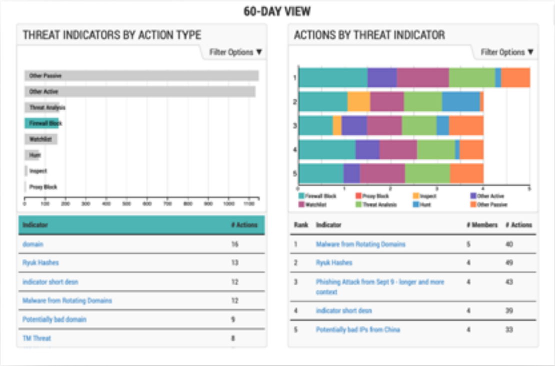
SCENARIO 2: **JULIA**

Julia works for one of Malibu's smallest suppliers. She's been tasked with addressing her organization's cybersecurity as required in Malibu's Supplier Manual. This is new to her IT role; she knows a little about cybersecurity, but she's working to learn more.

By using Cyber Defense Network as part of Malibu's supplier network, she is able to see the immediate threats that Malibu is focused on in the discussion threads shared by Matthew. She's also able to use threat reports and informational spotlights to learn about threats to specific business systems she uses, and about broader cybersecurity campaigns. These reports are designed specifically for small businesses. Cyber Defense Network gives her access to guidance about actions to mitigate risks and helps her put that information to good use. The Cyber Improvement Program within Cyber Defense Network teaches Julia about security best practices and helps her implement them in her organization. Dashboards allow her to see prioritized threats and actions others in the network are taking; she is then able to take those actions herself.



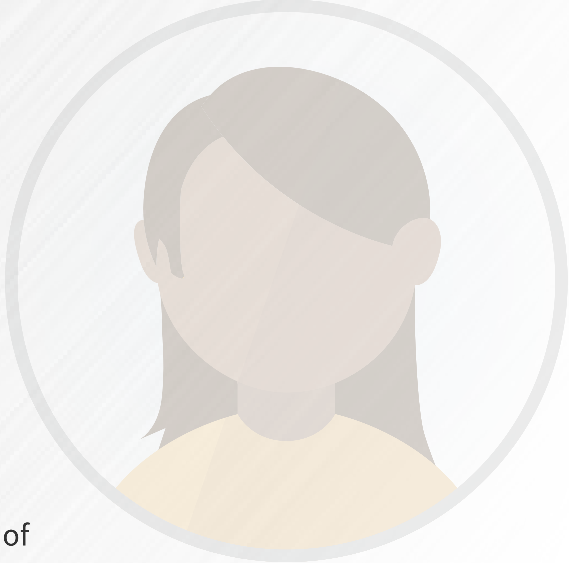
By participating in Malibu's Cyber Defense Network, Julia is helping her organization comply with Malibu's Supplier Manual. She has greatly increased her understanding of cybersecurity and how to secure her organization. And she's done it without having to hire additional staff or substantially adding to her workload. Because Julia is empowered to improve security in this way, Malibu Manufacturing is more secure.



Indicator	# Actions
domain	16
Ryuk Hashes	13
indicator short desn	12
Malware from Rotating Domains	12
Potentially bad domain	9
TM Threat	8

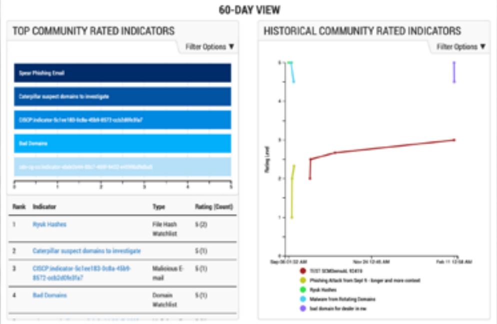
Rank	Indicator	# Members	# Actions
1	Malware from Rotating Domains	5	40
2	Ryuk Hashes	4	49
3	Phishing Attack from Sept 9 - longer and more context	4	43
4	indicator short desn	4	39
5	Potentially bad IPs from China	4	33

SCENARIO 3: **ROSE**



Rose works on the cybersecurity team of one of Malibu's larger suppliers. She's used cyber threat intelligence before and is actively using it to defend her organization.

Cyber Defense Network gives Rose tools to easily make threat intelligence actionable, and a community of other practitioners force multiply her efforts. It empowers Rose to connect specific indicators of compromise to threat actors or larger campaigns, helping her to better defend her company. She is also able to take immediate defensive action from right within Cyber Defense Network. Because she's able to use the powerful filtering and other threat routing tools, she's able to send only relevant data into her SIEM, saving her company money since their SIEM provider charges based on volume of data. Rose's defensive actions within Cyber Defense Network are also visible anonymously to the entire community of Malibu's suppliers, helping other smaller organizations take the same actions to secure the entire network.



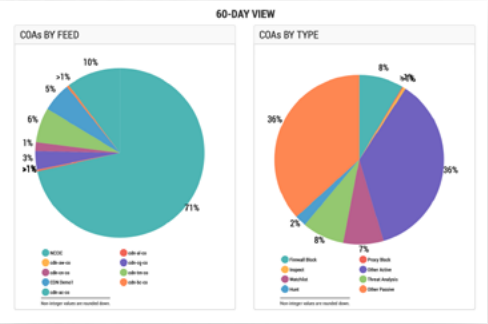
60-DAY VIEW

TOP COMMUNITY RATED INDICATORS

Rank	Indicator	Type	Rating (Count)
1	Ryuk Hashes	File Hash Watchlist	5 (2)
2	Caterpillar suspect domains to investigate		5 (1)
3	CISCP indicator-5c1ee183-0c8a-45b9-8572-ccb2d0fe3fa7	Malicious E-mail	5 (1)
4	Bad Domains	Domain Watchlist	5 (1)

HISTORICAL COMMUNITY RATED INDICATORS

Filter Options ▼
Filter Options ▼
Spear Phishing Email
Caterpillar suspect domains to investigate
CISCP indicator-5c1ee183-0c8a-45b9-8573-ccb2d0fe3fa7
Bad Domains
0
1
2
3
4
5
Rating Level
Sep 08 01:32 AM
Nov 24 12:45 AM
Feb 11 12:58 AM
Phishing Attack from Sept 5 - longer and more context
Ryuk Hashes
Malware from Rotating Domains



60-DAY VIEW

Cyber Defense Network helps Rose work more efficiently while at the same time making it possible for her and other suppliers and distributors to be a security benefit for the entire supply chain community.

REAL STEPS TO IMPROVE SUPPLY CHAIN CYBERSECURITY

Cyber Defense Network gives companies like Malibu Manufacturing a practical way to help secure their supply chains while not overwhelming partners or their own security teams. Informational tools to empower smaller suppliers are built into Cyber Defense Network, while more advanced threat sharing capabilities help larger suppliers be more proactive about security. From simple, secure practitioner discussions to more technical security intelligence, Cyber Defense Network makes it possible for the enterprise to build a culture of cybersecurity across its entire supply chain.

READY TO SEE CYBER DEFENSE NETWORK IN ACTION?

Cyber Defense Network can be customized to meet the needs of any supply chain, distributor network, or other enterprise community. Contact Celerium today to learn more and to schedule a demonstration!

ABOUT CELERIUM

Celerium® is focused on improving supply chain cyber defense within critical infrastructure industries, including the defense, aviation, and automotive industries. Its Cyber Defense Network (CDN) family of solutions empowers organizations to defend and protect against cyber threats via cyber threat intelligence and threat sharing tools.

We do this through the speed and control of the information within the community. Cyber Defense Network(CDN) family of solutions empowers organizations to defend and protect against threats via threat intelligence and collaboration tools.

CONTACT US

(703) 682-6000
info@celerium.com
celerium.com

CELERIUM®