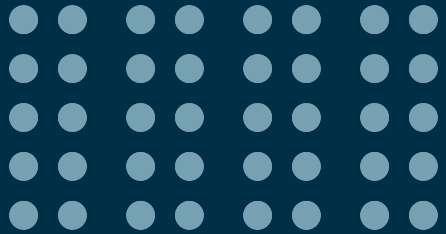
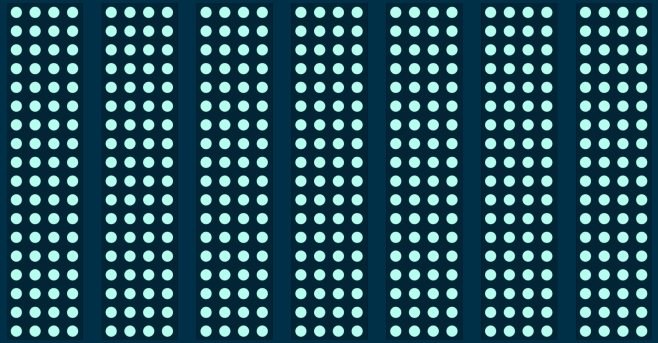

UPLEVEL

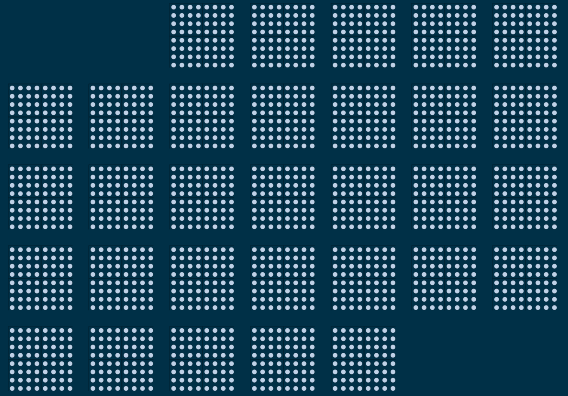
40 Security Vendors

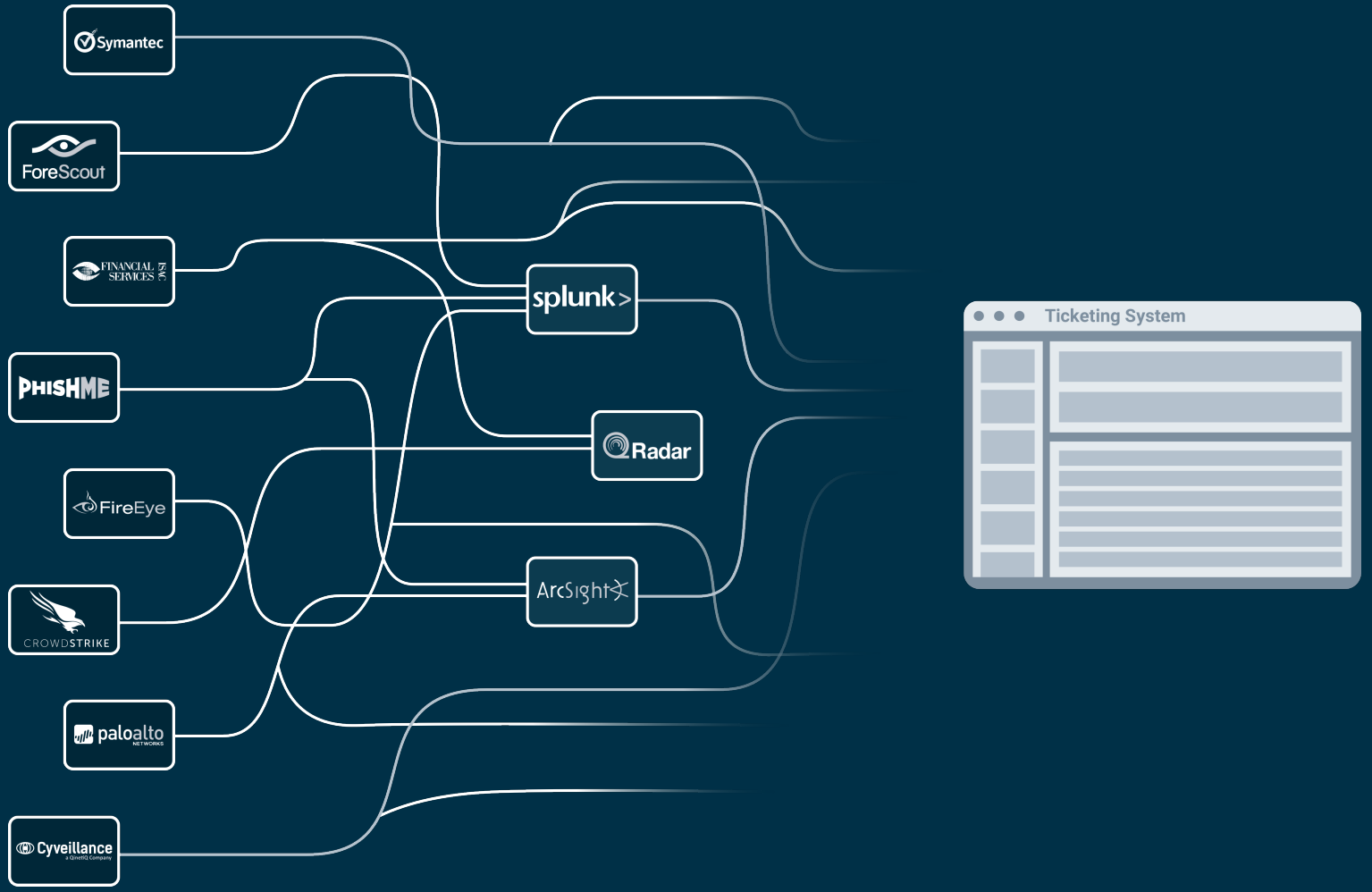


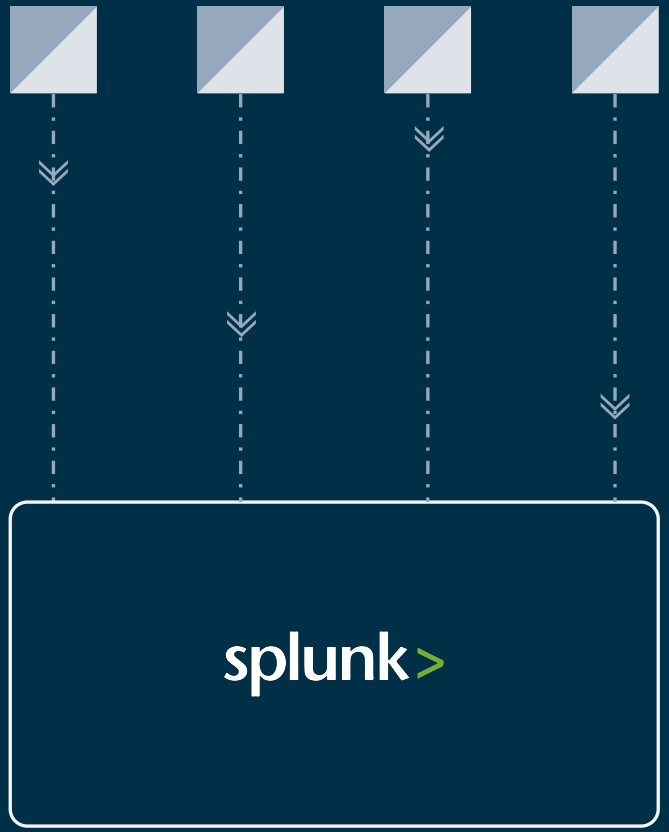
1,000 Alerts Per Week



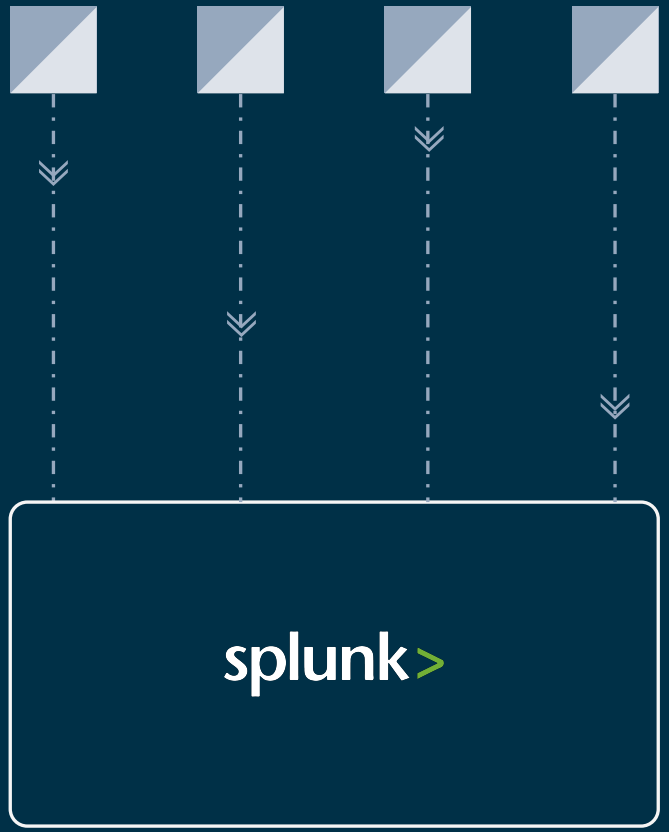
3.5 million Indicators Per Month




Symantec
ForeScout
FINANCIAL SERVICES ISAC
PHISHME
FireEye
CROWDSTRIKE
paloalto NETWORKS
Cyveillance
splunk>
Radar
ArcSight
Ticketing System



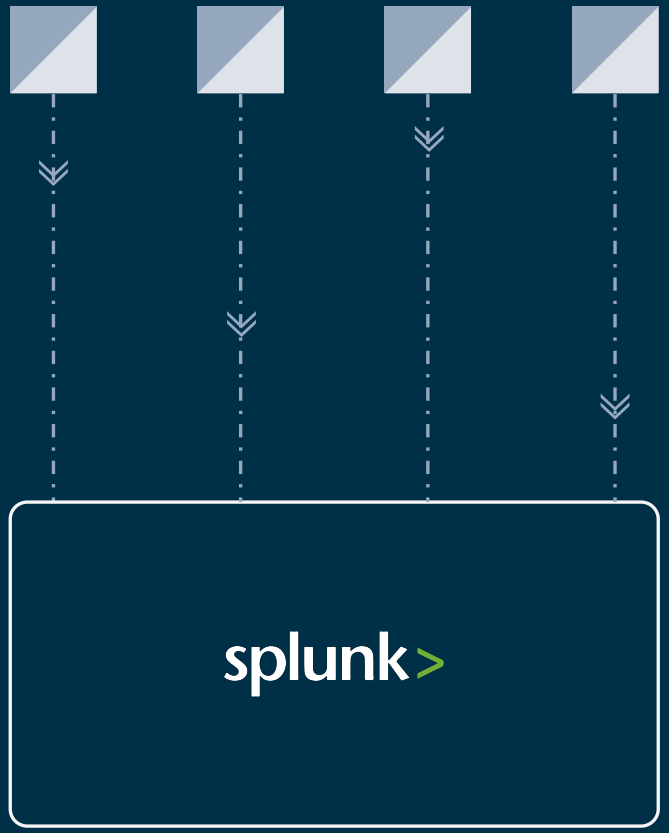
{"preview":false,"offset":0,"result":{"E":"Sophos","_raw":"Feb 27 08:38:07 ptc-opfeyecm901 fenotify-1116646059.alert: CSV:0:FireEye:PTC-OPFEYEEX903:7.9.2.588646:MO:malware-object,osinfo=,sev=majr,malware_type=zip,alertid=1116646057,locations=,header=,cnchost=,protocol=,subject=Fwd: PRICE REQUEST,alertType=malware-object,date=Mon, 27 Feb 2017 11:29:31 +0300,smtp-to=ISR@foo.com,original_name=product list.zip,application=,run_end=2017-02-27T08:35:09Z,last-malware=Backdoor.Androm,sid=,malware-note=,anomaly=,mwurl=product list.zip,profile=,product=eMPS,sname=Malware.archive,fileHash=742ad571587073a355145e027ac0d31c,dvchost=PTC-OPFEYEEX903,occurred=2017-02-27 08:35:09+00,smtp-mail-from=numangedik@pergola.com.tr,smtp-cc=,link=https://PTC-OPFEYECM901.ad.foo.net/emps/eanalysis?e_id=49109921&type=attch,cncport=,url_domain=,smtp-header=Received: from esa3.foocorp.iphmx.com (esa3.foocorp.iphmx.com [68.232.153.43]) \tby PTC-OPFEYEEX903.ad.foo.net (Postfix) with ESMTPS id 3vWvzx6pL1z1fGm5 \tfor <ISR@foo.com>; Mon, 27 Feb 2017 08:30:53 +0000 (UTC) Authentication-Results: esa3.foocorp.iphmx.com; dkim=none (message not signed) header.i=none; spf=Pass smtp.mailfrom=numangedik@pergola.com.tr; spf=None smtp.helo=postmaster@ns1.idsturkiye.com Received-SPF: Pass (esa3.foocorp.iphmx.com: domain of numangedik@pergola.com.tr designates 37.9.202.240 as permitted sender) identity=mailfrom; client-ip=37.9.202.240; receiver=esa3.foocorp.iphmx.com; envelope-from=\"numangedik@pergola.com.tr\"; x-sender=\"numangedik@pergola.com.tr\"; x-conformance=spf_only; x-record-type=\"v=spf1\" Received-SPF: None (esa3.foocorp.iphmx.com: no sender authenticity information available from domain of postmaster@ns1.idsturkiye.com) identity=helo; client-ip=37.9.202.240; receiver=esa3.foocorp.iphmx.com; envelope-from=\"numangedik@pergola.com.tr\"; x-sender=\"postmaster@ns1.idsturkiye.com\"; x-conformance=spf_only X-IronPort-AV: E=Sophos;i=\"5.35,213,1484028000\"; d=\"exe'96?zip'96,48?scan'96,48,48,217,208,96\";a=\"33617025\" X-Original-Recipients: ClientServices@foo.com Received: from ns1.idsturkiye.com ([37.9.202.240]) by esa3.foocorp.iphmx.com with ESMTP/TLS/DHE-RSA-AES256-SHA; 27 Feb 2017 02:24:09 -0600 X-Footer: cGVyZ29sYS5jb20udHI= Received: from [91.228.0.172] ([91.228.0.172]) \tby ns1.idsturkiye.com (Kerio Connect 8.4.1) \tfor marketing@papermachinery.com; \tMon, 27 Feb 2017 11:29:31 +0300 Date: Mon, 27 Feb 2017 11:29:31 +0300 Subject: Fwd: PRICE REQUEST X-Mailer: Kerio Connect 8.4.1/Kerio Connect client X-User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:35.0) Gecko/20100101 \tFirefox/35.0 Message-ID: <3828121062-4476@ns1.idsturkiye.com> X-FireEye: Not Scanned From: numangedik@pergola.com.tr To: marketing@papermachinery.com X-Priority: 3 Importance: Normal MIME-Version: 1.0 Content-Type: multipart/mixed; boundary=\"=-ZViWO4FXlqS3SvF6syAV\",download_end=2017-02-27T08:35:09Z,dvc=10.6.6.41,username=,channel=,release=eMPS (eMPS) 7.9.0.588405,message-id=3828121062-4476@ns1.idsturkiye.com,stype=archive, -....



{"preview":false,"offset":0,"result":{"E":"Sophos","_raw":"Feb 27 08:38:07 ptc-opfeyecm901 fenotify-1116646059.alert: CSV:0:FireEye:PTC-OPFEYEEX903:7.9.2.588646:MO:malware-object,osinfo=,sev=majr,malware_type=zip,alertid=1116646057,locations=,header=,cnchost=,protocol=,subject=Fwd: PRICE REQUEST,alertType=malware-object,date=Mon, 27 Feb 2017 11:29:31 +0300,smtp-to=ISR@foo.com,original_name=product list.zip,application=,run_end=2017-02-27T08:35:09Z,last-malware=Backdoor.Androm,sid=,malware-note=,anomaly=,mwurl=product list.zip,profile=,product=eMPS,sname=Malware.archive,fileHash=742ad571587073a355145e027ac0d31c,dvchost=PTC-OPFEYEEX903,occurred=2017-02-27 08:35:09+00,smtp-mail-from=numangedik@pergola.com.tr,smtp-cc=,link=https://PTC-OPFEYECM901.ad.foo.net/emps/eanalysis?e_id=49109921&type=attch,cncport=,url_domain=,smtp-header=Received: from esa3.foocorp.iphmx.com (esa3.foocorp.iphmx.com [68.232.153.43]) \tby PTC-

Name: **fe_fw_search**
Query: **index=fe_fw src=$IP OR dst=$IP$**

identity=mailfrom; client-ip=37.9.202.240; receiver=esa3.foocorp.iphmx.com; envelope-from=\"numangedik@pergola.com.tr\"; x-sender=\"numangedik@pergola.com.tr\"; x-conformance=spf_only; x-record-type=\"v=spf1\" Received-SPF: None (esa3.foocorp.iphmx.com: no sender authenticity information available from domain of postmaster@ns1.idsturkiye.com) identity=helo; client-ip=37.9.202.240; receiver=esa3.foocorp.iphmx.com; envelope-from=\"numangedik@pergola.com.tr\"; x-sender=\"postmaster@ns1.idsturkiye.com\"; x-conformance=spf_only X-IronPort-AV: E=Sophos;i=\"5.35,213,1484028000\"; d=\"exe'96?zip'96,48?scan'96,48,48,217,208,96\";a=\"33617025\" X-Original-Recipients: ClientServices@foo.com Received: from ns1.idsturkiye.com ([37.9.202.240]) by esa3.foocorp.iphmx.com with ESMTP/TLS/DHE-RSA-AES256-SHA; 27 Feb 2017 02:24:09 -0600 X-Footer: cGVyZ29sYS5jb20udHI= Received: from [91.228.0.172] ([91.228.0.172]) \tby ns1.idsturkiye.com (Kerio Connect 8.4.1) \tfor marketing@papermachinery.com; \tMon, 27 Feb 2017 11:29:31 +0300 Date: Mon, 27 Feb 2017 11:29:31 +0300 Subject: Fwd: PRICE REQUEST X-Mailer: Kerio Connect 8.4.1/Kerio Connect client X-User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:35.0) Gecko/20100101 \tFirefox/35.0 Message-ID: <3828121062-4476@ns1.idsturkiye.com> X-FireEye: Not Scanned From: numangedik@pergola.com.tr To: marketing@papermachinery.com X-Priority: 3 Importance: Normal MIME-Version: 1.0 Content-Type: multipart/mixed; boundary=\"=-ZViWO4FXIqS3SvF6syAV\",download_end=2017-02-27T08:35:09Z,dvc=10.6.6.41,username=,channel=,release=eMPS (eMPS) 7.9.0.588405,message-id=3828121062-4476@ns1.idsturkiye.com,stype=archive, -....



SECURITY INCIDENT REPORT

OVERVIEW: Behavior of W32/CoinMiner.d virus observed on user's machine.

INCIDENT DETAILS:
Offense id: #68276, #68233, #68210, #68206, #68200, #68194, #68192
Offense: RQ-SM: Malware: Internal Host Communicating with Botnet
Incident id: 300-589660

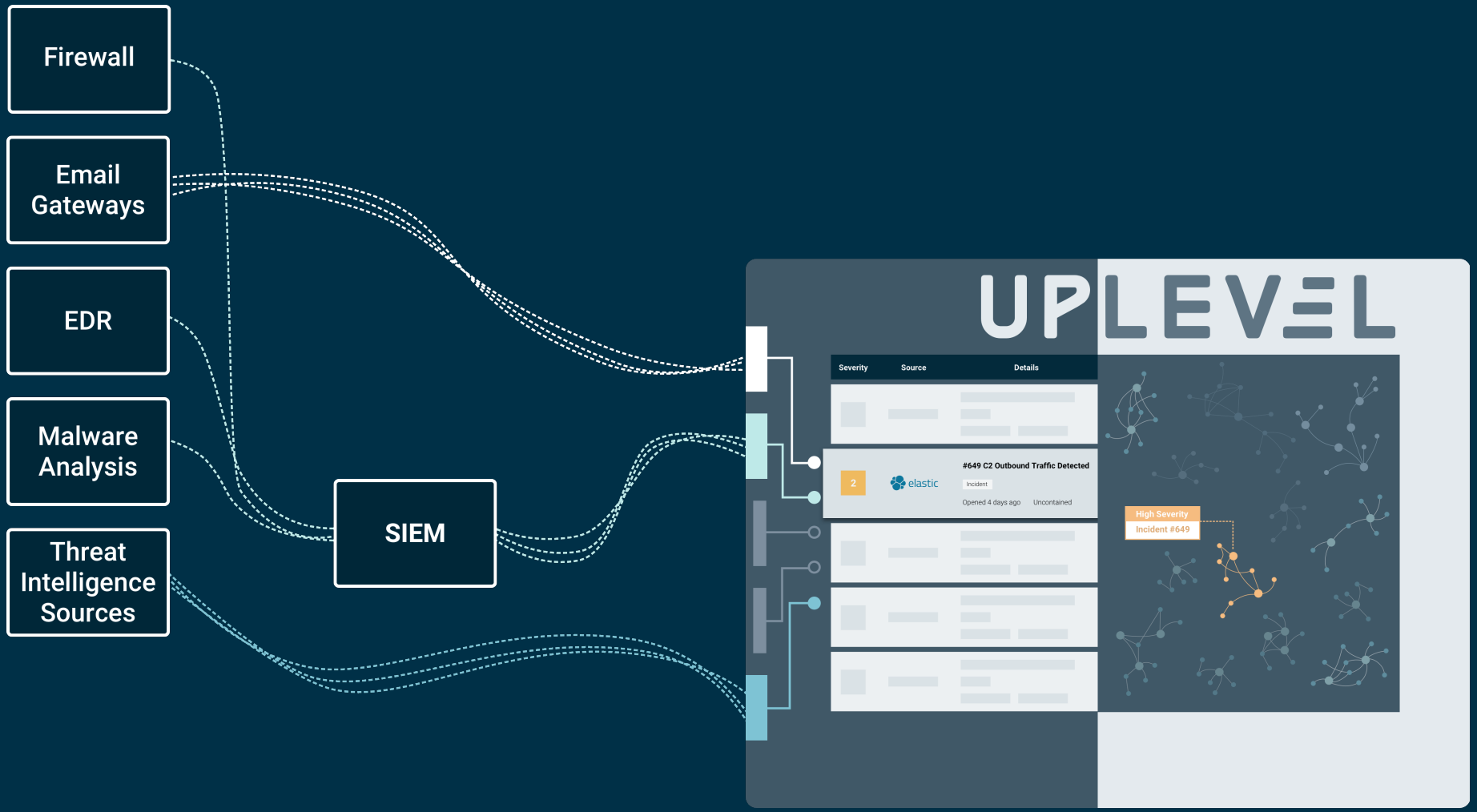
ACQUISITION:
Behavior of W32/CoinMiner.d virus observed on Hyperion servers (USILASP00251 AND USILASP00248) machine.

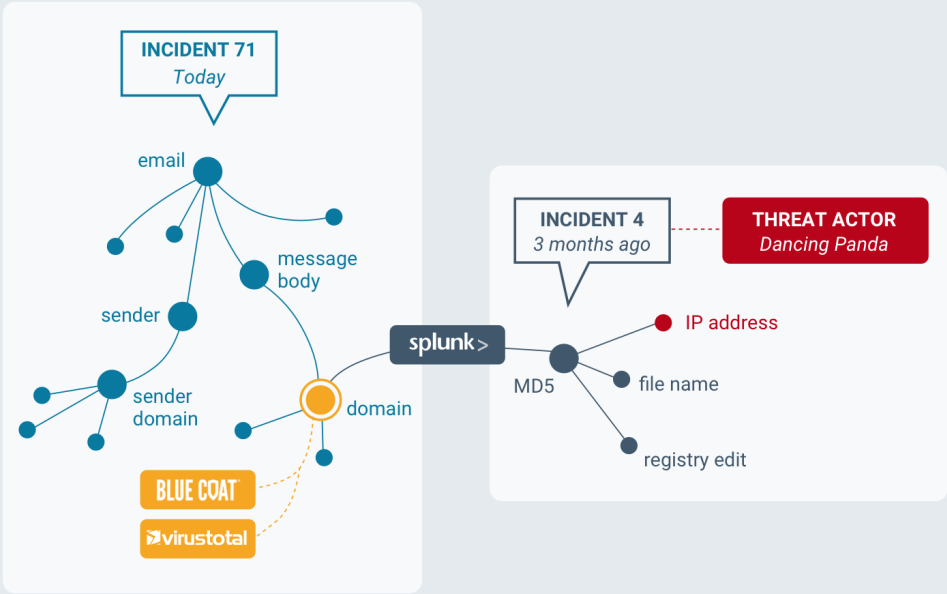
OBSERVATION/FINDINGS:
10/11/16
3:00 PM: George Cyriac contacted Cyber Security team to inform us of a malware file (IMG001.EXE) that was discovered on USILASP00251. Michele Woss (WOSMI01) discovered a suspicious file on USILASP00251, she downloaded and executed the file locally on her system. The file access generated a McAfee alert.

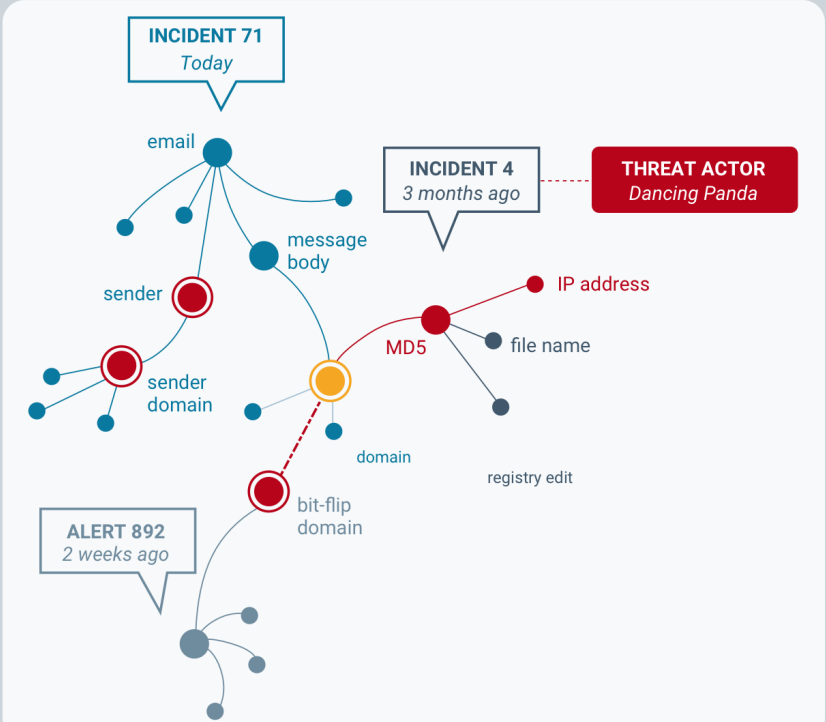
3:30 PM: Meeting with CyberSec
was discovered in the following l
- \\nasilcifs-fs02\SOX-Financial R
- \\cacifs10a\app_MP_hyperion
- \\nasilcifs-finance\CA_Hyperion
- \\USilasp00251\d\FDMData
- \\Usilasp00148\d
- \\usilasp00148\c

It was agreed that McAfe
servers after hour's Eastern Time
scan results to determine if any a

- 6_Months_Coinminer.csv
- 24th Oct - Coin Miner Infec...achines Master Sheet.xlsx
- ATD - IMG001exe Malware Summary.html
- ATD - makensisexe Malware Summary.html
- logs with threatnamecoinminer.d_10days.csv
- Malware analysis checklist.docx
- Malware_Detections_Coin.csv
- Memory_Detections_Coin.csv
- Palo Alto Report - img001.pdf
- PaloAlto - Makensis.html
- SECURITY INCIDENT REPORT - Latest.docx


Firewall
Email Gateways
EDR
Malware Analysis
Threat Intelligence Sources
SIEM
UPLEVEL
Severity
Source
Details
2
elastic
#649 C2 Outbound Traffic Detected
Incident
Opened 4 days ago
Uncontained
High Severity
Incident #649


INCIDENT 71
Today
email
message body
sender
sender domain
domain
BLUE COAT
virustotal
splunk>
INCIDENT 4
3 months ago
THREAT ACTOR
Dancing Panda
IP address
MD5
file name
registry edit


INCIDENT 71
Today
email
INCIDENT 4
3 months ago
THREAT ACTOR
Dancing Panda
message
body
sender
IP address
MD5
file name
sender
domain
domain
registry edit
bit-flip
domain
ALERT 892
2 weeks ago

Associated Events 3

Events	Indicators	Association
#650 Phishing email New Closed Severity: 2	5	
#647 DDoS Attack New Open Severity: 3	0	
#652 Ransomware - CryptoLocker New Open Severity: 1	2	

#650 Phishing Email Severity: 1

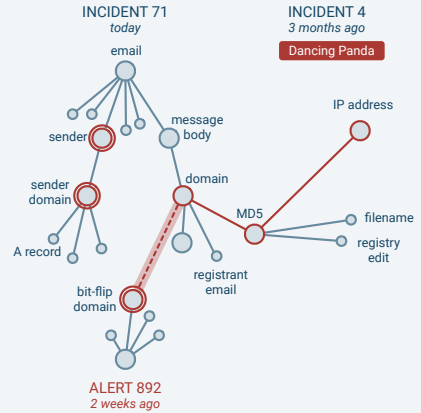
Uplevel Reasoning

SHARED TECHNICAL ATTRIBUTES
www.foo.com 0.8
184.168.221.1 1.0

PREDICTED LINKS
foo.com - f00.com 0.9

NEW INDICATORS
184.168.98.6 0.9
foo.com 0.7

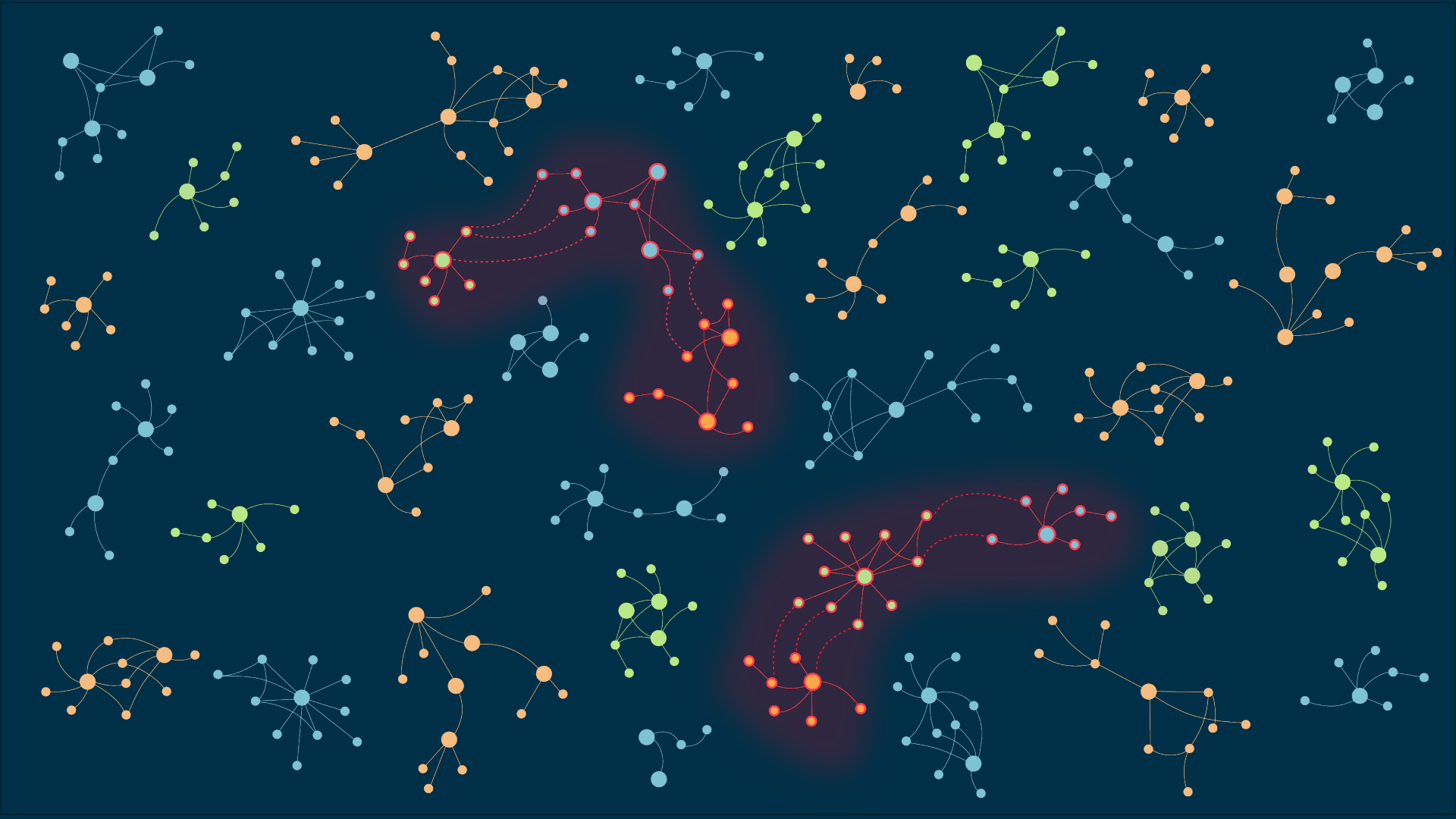
POTENTIAL CONSOLIDATION
Alert 892
Incident 4



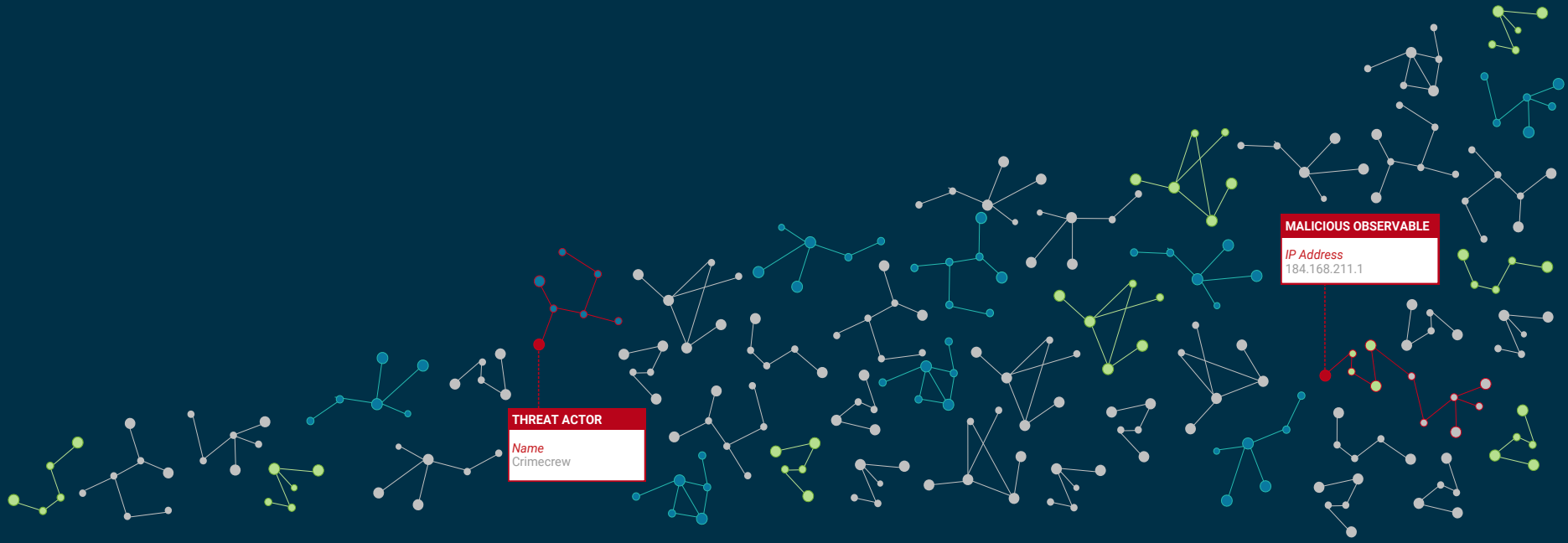
Analyst Motivation

APPROVE

REJECT



UPLEVEL


MALICIOUS OBSERVABLE
IP Address
184.168.211.1
THREAT ACTOR
Name
Crimecrew